INTERNATIONAL > Safe Harbour

DROIT > La loi du 3 juin 2016

TECHNIQUE > Collectivités locales et cyber-risques

REVUE de la gendarmerie nationale

REVUE TRIMESTRIELLE / DÉCEMBRE 2016 / N° 256 / PRIX 6 EUROS

Une sécurité intelligente pour les technologies du futur

Smarter security for future technologies

© gendarmerie

LES TECHNOLOGIES DE LA SÉCURITÉ

Les marchés mondialisés obligent à des synergies entre pouvoirs publics, organismes de recherche et firmes industrielles pour produire des nouvelles techniques à forte valeur probatoire et pouvant contribuer à une prévention situationnelle. Elles doivent s'appuyer sur une fiabilité et un paramétrage transparent pour les opérateurs. En effet, la captation de données biométriques et le relevé des activités personnelles doivent être encadrés juridiquement afin de proroger la confiance des personnes dans une gouvernance sociale numérique.

RETROUVEZ EN PAGE 136 LE DÉFI DES COLLECTIVITÉS FACE À L'ACCESSIBILITÉ DES DONNÉES >>

© Fotolia

Ce que pronostiquait bon nombre d'experts en cybersécurité depuis quelques années est finalement arrivé le 21 octobre dernier. La première grande attaque en déni de service préparée via un réseau d'objets connectés a mis à mal, pendant plusieurs heures, le fonctionnement de dizaines de sites américains… et non des moindres : Twitter, Netflix, Reddit ou encore le New York Times... Un adage populaire rappelle que la « *peur n'évite pas le danger* » et il est à craindre que cette attaque, qui sera à n'en pas douter suivie par d'autres du même type, symbolise l'évolution d'une menace réelle. Combien de temps faudra-t-il encore pour que tous les responsables d'organisations passées à l'ère numérique s'interrogent sur la réalité de leurs niveaux de protection.

Industrie 4.0, smart Cities, impression 3D, intelligence artificielle… La digitalisation du monde est en marche et constitue aux yeux de nombreux observateurs une troisième révolution, après l'invention de l'imprimerie et la révolution industrielle. La transformation qui en résultera ne pourra reposer, au-delà du caractère innovant, que sur des bases de sécurité et de confiance. Sécurité parce que « l'on ne bâtit pas sur du sable » et confiance parce que l'usage qui sera fait des technologies et des données qu'elles véhiculent ne doit pas être mis entre toutes les mains.

« *Security by design* », sécurité pensée dès la conception…tel est l'enjeu pour les années à venir… Certes, il faudra faire aussi avec l'existant, l'adapter, le moderniser et c'est bien en cela que le FIC est un rendez-vous essentiel pour tous les acteurs de la cybersécurité. 2007-2017, c'est la 9e édition d'un forum, né de la volonté de quelques gendarmes précurseurs et visionnaires, qui est devenu l'un des plus importants lieux d'échanges européens du monde de la cybersécurité. Le partenariat formé avec cette belle ville de Lille et la région des Hauts de France assure une assise et un cadre de développement très favorables à ce rassemblement annuel avec les territoires, acteurs essentiels de la réussite de cette transformation numérique.

Le ministère de l'Intérieur, ministère de la sécurité et des territoires, s'appuie sur les préfectures, les services de police et de gendarmerie, les services de renseignement intérieur et se mobilise pour relever le défi de la cybersécurité. Il est pleinement engagé dans l'accompagnement de cette transformation avec les collectivités locales et les acteurs économiques de cette filière industrielle.

Thierry DELVILLE

Délégué ministériel aux industries de sécurité et à la lutte contre les cybermenaces

SOMMAIRE

NUMÉRO 256

DOSSIER

Une sécurité intelligente
pour les technologies du futur

L'ORGANISATION INTERNATIONALE DE LA FRANCOPHONIE SOUTIENT LE RENFORCEMENT DE LA CYBERSECURITE DANS L'ESPACE FRANCOPHONE

La conférence de Grand-Bassam a été l'occasion de jeter les bases d'une vision partagée de la cybersécurité et de la cyberdéfense au sein d'un espace francophone. La conscience des limites d'une conception périmétrique de la défense des intérêts d'un pays, de la nécessité d'un partenariat public-privé et de la mise en œuvre d'une coopération internationale ont permis de déboucher sur des actions signifiantes actées dans trois documents fondamentaux.

La définition de stratégies, la protection des OIV, le développement d'un capital humain d'experts au sein d'une communauté francophone seront les leviers de plans de financements activés par un consortium. Les axes d'effort ne négligent pas l'émergence d'une jeunesse francophone susceptible d'intégrer une communauté active et professionnalisée qui pourra collaborer aux stratégies numériques mises en place par les opérateurs régaliens et privés dans le cadre de la déclaration du sommet de la francophonie d'Antananarivo en novembre 2016.

Vers un agenda francophone
de la cybersécurité et de la cyberdéfense

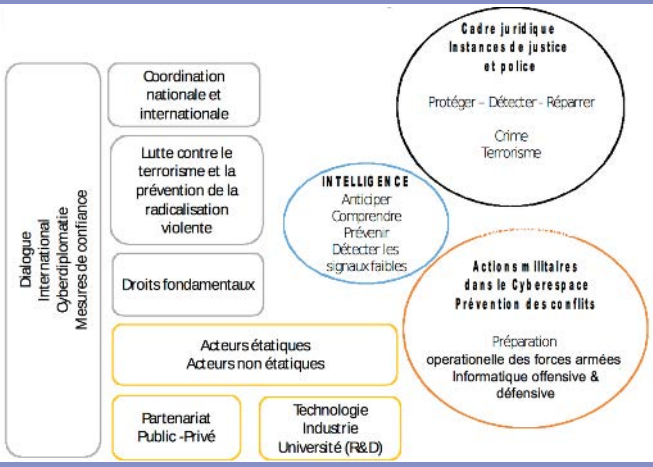
par ERIC ADJA

Du 8 au 10 février 2016, les experts et représentants de pouvoirs publics et d'entreprises provenant des pays francophones d'Afrique, d'Europe et d'Amérique se sont réunis à Grand-Bassam (Côte-d'Ivoire), à l'initiative de l'Organisation internationale de la Francophonie (OIF), autour du thème du renforcement de la cybersécurité et de la cyberdéfense dans l'espace francophone. Depuis lors, un véritable agenda francophone de la cybersécurité se met en place, sur la base des actes et recommandations de la conférence de Grand-Bassam.

ERIC ADJA

Directeur Adjoint de la Francophonie Economique et Numérique.

Animée par des spécialistes internationaux, professeurs, cyber-juristes, officiers de l'armée et de la police, régulateurs, représentants de ministères et de parlements francophones, cette conférence a été structurée autour de plusieurs thèmes dont la lutte contre la cybercriminalité, la sécurité des réseaux et systèmes, la protection des données à caractère personnel, la formation et la recherche, la cyber-défense et la sécurité nationale. Les débats ont permis aux participants de co-construire une vision partagée de la cybersécurité et de la cyberdéfense dans l'espace francophone, au point de proposer l'adoption d'une doctrine francophone en la matière. Cette démarche a été facilitée par l'adoption des trois principaux actes de la Conférence . À l'issue de la rencontre, l'OIF a entrepris un certain nombre d'actions en vue de concrétiser la contribution de la Francophonie au



Cybersécurité et de cyberdéfense sont abordés dans un plan d'action global

renforcement de la cybersécurité et de la cyberdéfense dans les pays membres.

Une doctrine francophone de la cybersécurité et de la cyberdéfense ?

La cybersécurité, une question globale

Les participants à la Conférence de Bassam ont estimé que dans le cyberespace, la sécurité périmétrique est dépassée. Ils ont recommandé une approche à la fois civile et militaire de la sécurité et de la défense, en fonction des cibles et du niveau d'impact recherché. En effet, il existe un continuum cybersécurité/cyber-défense. Les technologies duales à usage civil et militaire confirment cette réalité, ainsi que la relative banalisation et vulgarisation des gadgets du parfait espion par les applications et outils des "TIC grand public".

Les participants à la Conférence de Bassam ont également estimé que le rôle des opérateurs privés dans l'architecture de la cyber-sécurité et de la cyber-défense méritait d'être précisé, étant donné que plusieurs infrastructures d'importance vitale appartenaient à ces acteurs. De ce fait, le renforcement de la coopération public-privé dans la lutte contre la cybercriminalité constitue un impératif catégorique.

En définitive, le caractère transfrontalier des cybermenaces et de certaines

attaques informatiques met en évidence la nécessité d'une coopération à plusieurs dimensions : bilatérale, multilatérale, régionale et internationale.

Une vision partagée de la cybersécurité

Au regard de ces observations et des valeurs que porte le mouvement francophone, les participants à la Conférence de Grand-Bassam ont recommandé que la Francophonie se dote d'une doctrine en matière de cybersécurité et de cyberdéfense. Pour eux, les outils et politiques de sécurité des systèmes et des réseaux d'information doivent viser la protection des données, des informations et des infrastructures critiques contre les attaques et atteintes de toutes sortes qui entravent l'appropriation et l'utilisation des TIC pour le développement et la croissance.

Ces instruments et mécanismes doivent se développer dans le respect de l'État de droit. La protection de la vie privée et des données personnelles des citoyens, la promotion et la sauvegarde de la liberté d'expression en ligne sont des défis majeurs pour les sociétés démocratiques dans leur passage au numérique.

Les actes de la Conférence

Au terme des travaux de la Conférence, les participants ont adopté trois documents fondamentaux constituant les actes :

Un projet de Déclaration de principes sur la cyber-sécurité et la cyber-défense à l'intention des hauts dirigeants de la francophonie ;

Un guide pratique de la cybersécurité qui propose une batterie d'actions et des combinaisons que les Etats mettront en œuvre selon leurs écosystèmes spécifiques ;

Un plan d'action francophone pour permettre à l'OIF de proposer une initiative d'accompagnement des Etats, des entreprises et des citoyens dans le renforcement de la cybersécurité et de la cyberdéfense dans l'espace francophone.

Un projet de déclaration de principes

Il s'agit d'un document politique qui affirme l'engagement des Etats à lutter contre la cybercriminalité et à œuvrer pour la cybersécurité et la cyberdéfense, en renforçant leur coopération, en engageant des actions et en adoptant des mesures, des dispositifs et des règles qui respectent, entre autres, les droits fondamentaux de l'homme (notamment le respect de la vie privée et la liberté d'expression), favorisent l'innovation technologique et le développement économique, et concourent à la protection des infrastructures critiques.

Un guide pratique de cybersécurité et de la cyberdéfense

Réalisé sous la supervision de Madame Solange Ghernaouti, Professeure à

l'université de Lausanne, le guide est conçu comme une boîte à outils. Il propose aux experts et dirigeants des pays francophones :

– d'élaborer des stratégies nationales, sur la base de diagnostics de l'état de la cybersécurité et de la cyberdéfense dans leurs écosystèmes et d'en assurer la mise en œuvre et le suivi ;

– d'identifier leurs infrastructures critiques et de garder un œil vigilant sur tous les opérateurs d'importance vitale, de mettre en œuvre des structures de réponse d'urgence aux incidents de sécurité de l'information, de définir des mécanismes appropriés de protection des données à caractère personnel et de protection des enfants et de la jeunesse dans le cyberespace ;

– de développer le capital humain, le cadre organisationnel et les mesures législatives et d'assurer la coopération régionale et internationale en matière de cybersécurité et de cyberdéfense, en mobilisant des réseaux tels que FRANCOPOL (Réseau francophone des polices).

Un plan d'action francophone

Le troisième acte de la Conférence se décline en une esquisse de plan d'action francophone de renforcement de la cybersécurité et de la cyberdéfense, coordonné par l'OIF. Les cinq lignes d'action suivantes ont été retenues par les participants :

– mettre en place des stratégies nationales de cybersécurité et de cyberdéfense ;

– promouvoir la mutualisation des ressources ;

– développer les métiers de la cybersécurité et de la cyberdéfense ;

– faire de l'éducation numérique la base pour la cybersécurité ;

– encourager l'excellence francophone pour relever les défis de la cybersécurité et la cyberdéfense.

Il a été préconisé également un mécanisme de suivi et de financement du plan d'action qui combine le financement public avec l'apport des acteurs de l'industrie et des services numériques.

Les actions entreprises et les perspectives

Depuis la Conférence de Bassam, des actions ont été entreprises en vue de la mise en œuvre des recommandations. Une opération d'internalisation des conclusions des travaux a été engagée au sein de l'OIF pour partager les résultats et les faire porter par les principaux responsables de notre organisation.

Un consortium pour assurer un réseautage efficace

Un mois après la Conférence de Grand-Bassam, l'OIF a entrepris de mettre en place un consortium francophone sur la cybersécurité, à l'occasion des journées de la Sécurité (Security Days), le 16 mars 2016 à Dakar. Cette plateforme ambitionne de regrouper différentes parties prenantes de l'espace francophone : les représentants des pouvoirs publics, les opérateurs privés, les acteurs de la société civile et les experts du monde académique.

Un pôle de coopération francophone

L'Organisation internationale de la Francophonie (OIF) et l'Agence universitaire de la Francophonie (AUF) conjuguent leurs efforts pour le renforcement de la cybersécurité et de la cyberdéfense, dans le cadre d'une convention de partenariat en discussion. Les deux organisations envisagent de mobiliser leurs réseaux d'expertises et leurs moyens propres pour mener des actions dans quatre directions :

– information, sensibilisation, médiation et formation ;

– recherche, colloques, séminaires et assises francophones ;

– mise à jour des législations nationales ;

– appui à la mise en place de structures de réponse aux incidents de sécurité.

À ce titre, l'AUF et l'OIF ont organisé des assises francophones de la cybersécurité dans l'espace francophone, les 2 et 3 novembre 2016 à Antananarivo. L'OIF envisage également d'autres initiatives avec l'Assemblée parlementaire de la Francophonie (APF), TV5, l'Université Senghor et l'Association internationale des maires francophones (AIMF).

Mobilisation de la jeunesse francophone

L'OIF mobilise un Fond Francophones de l'innovation numérique (FFIN) pour stimuler la créativité des jeunes dans ce domaine. Ainsi en 2016, ont été organisés des « hackathons » ou « innovathons » dans cinq pays francophones: la Côte d'Ivoire, Madagascar, l'Ile Maurice, la Tunisie et le Vietnam. L'objectif est d'amener les jeunes à proposer aux administrations publiques des solutions innovantes pour contribuer à résoudre des problèmes de cybercriminalité dans leurs pays.

Par ailleurs, Madame Michaelle Jean, Secrétaire générale de la Francophonie, s'inscrivant dans la « Francophonie des solutions » a lancé le 10 mars 2016 l'Initiative « Libres ensemble ». Cette campagne, qui connaît un succès retentissant sur les médias et réseaux sociaux (plus de 3 millions de vues sur un internet, une cinquantaine de messages et de projets déposés par des jeunes francophones sur la plate-forme dédiée), se veut une réponse aux stratégies

numériques déployées par les mouvements extrémistes.

La conférence de Grand-Bassam a posé les jalons de plusieurs chantiers en matière de cybersécurité et de cyberdéfense dans l'espace francophone. Le défi est grand. Des financements importants seront nécessaires, au vu l'ampleur de la délinquance cybernétique, mais aussi en raison de la professionnalisation et de la complexification des attaques informatiques, sans compter les usages du cyberespace à des fins de radicalisation des jeunes.

Ayant pris la mesure de ces défis, les Chefs d'État et de Gouvernement, dans la Déclaration du Sommet de la Francophonie à Antananarivo (novembre 2016) précisent fort justement que « *la criminalité en ligne est devenue un défi pour la croissance et le développement économique, la protection des systèmes et réseaux d'information, le respect de l'État de droit et la protection des citoyens* ». Ils saluent à cet effet « *les actions entreprises par la Secrétaire générale de la Francophonie dans le domaine de la cybersécurité et de la cyberdéfense* ». Enfin, ils encouragent « *l'OIF à poursuivre ses efforts pour accompagner les Etats membres dans leur volonté d'instaurer un environnement de confiance numérique, dans le respect des droits fondamentaux des citoyens et l'AUF à développer ses actions de formation et de soutien à la recherche dans le domaine de la cybersécurité, notamment en mobilisant ses réseaux* ».

L'AUTEUR

Eric ADJA est Directeur Adjoint de la Francophonie économique et numérique au siège de l'Organisation internationale de la Francophonie (OIF) à Paris.
Titulaire d'un doctorat en sciences du langage à l'Université Paris 7 et d'un Master en Economie internationale et Globalisation à l'Université Pierre Mendès France de Grenoble, il a occupé les fonctions de Directeur de l'ONG internationale Innovations et Réseaux pour le Développement (IRED) à Genève (2002-2005), Conseiller du Président de la République du Bénin (2006-2011) et de Directeur général de l'Observatoire international des transferts de fonds des migrants (OITFM), auprès du Bureau mondial de coordination des Pays les Moins Avancés aux Nations Unies à New-York (2011-2014).

LA SECURITE DES DONNÉES AU CŒUR DES PRÉOCCUPATIONS DE LA COUR EUROPÉENNE DE JUSTICE

L'accord *Safe Harbour* n'a pas résisté à la question de la protection des données personnelles transférées en dehors de l'Union européenne sans un niveau de protection adéquat, qu'elles soient incluses dans un pack de communications électroniques mal différencié ou que l'on ne dispose pas de voies de droit classiques pour leur protection au regard des programmes de surveillance des États-Unis. Il était reproché notamment une limitation du pouvoir d'enquête des autorités de contrôle.

Le Privacy Shield, nouvelle mouture de cet accord, accorde des garanties réelles mais qui suscitent quelques interrogations. Présenté le 29 février 2016, par la Commission, le dispositif comprend les principes d'un bouclier de protection des données : obligations pour les entreprises, accès encadré par les autorités américaines, protection des droits des citoyens de l'Union et un mécanisme de réexamen annuel conjoint.

Les implications juridiques
et technologiques post "Safe Harbour"

par JACQUES MARTINON

Proclamée par la Courde justice de l'Union européenne[1], la censure de l'accord dit *Safe Harbour* , encadrant le transfert des données personnelles des Européens par 5 000 entreprises américaines[2], a remis les "CNIL" européennes dans un rôle de premier plan et provoqué de nouvelles négociations entre l'UE et les États Unis, dont le *Privacy Shield* est le fruit.

L'invalidation du *Safe Harbour*

L'accord dit *Safe Harbour* a été censuré sur une argumentation solide, engendrant des répercussions à court terme au niveau politique, juridique et technologique.

JACQUES MARTINON

Magistrat, mission de lutte contre la Corruption et la Cybercriminalité de la direction des affaires criminelles et des grâces

Une censure symbolique

Cette censure est le fruit d'une remise en cause du *Safe Harbour* dont l'origine remonte à juin 2013, aboutissant à un fort signal de la Cour de Justice de l'Union européenne.

(1) CJUE, 6 oct. 2015, aff. C-362/14, *Maximilian Schrems c/ Data protection Commissioner.*

(2) Précisément 5561 d'après le décompte officiel au 14 mars 2016 : https://safeharbor.export.gov/list.aspx. En effet, le département du commerce américain continue d'administrer le programme Safe Harbour, dans l'attente du Privacy Shield.

(3) Entre autres : PRISM, Xkeyscore, Boundless Informant, DROPOUT JEEP.

La remise en cause du *Safe Harbour*

Les révélations d'Edward Snowden sur les programmes de surveillances américains et britanniques[3] commencèrent le 6 juin 2013. Quelques jours plus tard, Maximilian Schrems portait plainte contre Facebook devant l'autorité de contrôle irlandaise afin de faire cesser le transfert transatlantique de ses données personnelles. En effet, il est interdit de transférer des données personnelles en dehors de l'Union européenne (directive n°95/46/CE), sauf en présence d'un "niveau de protection

Safe harbour est juridiquement contestable car il ne garantit pas une gestion des données conforme à charte européenne des droits fondamentaux.

adéquat"[4]. Afin de permettre un tel transfert massif des données vers les Etats-Unis, l'accord *Safe Harbour* avait été négocié entre la commission européenne et le département du commerce américain (décision n°2000/530/CE). Cet accord sera annulé deux ans plus tard sous l'analyse de la Cour de Justice.

(4) Article 25-1 de la directive n°95/46/CE.

(5) Arrêt de la CJUE du 8 avril 2014, invalidant la directive 2006/24/CE sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications dans les affaires jointes C-293/12 et C-594/12 Digital Rights Ireland et Seitlinger.

Le signal fort de la Cour de Justice

Il convient d'abord de rappeler l'arrêt du 8 avril 2014 invalidant la directive 2006/24 sur la conservation des données[5]. La Cour estima que « *cette directive comporte une ingérence dans ces droits fondamentaux (articles 7 et 8) d'une vaste ampleur et d'une gravité particulière [...] sans qu'[elle]soit précisément encadrée [...]». En effet, la directive couvrait "de manière généralisée toute personne et tous les moyens de communication électronique ainsi que l'ensemble des données relatives au trafic sans qu'aucune différenciation, limitation ou exception soient opérées en fonction de l'objectif de lutte contre les infractions graves* ».

Autrement dit, même si la directive répondait effectivement à un objectif d'intérêt général, le principe de proportionnalité n'avait pas été respecté, d'autant plus que cette directive n'avait pas imposé que les données soient conservées sur le territoire de l'Union, empêchant que soit pleinement garanti le contrôle par une autorité indépendante.

Les conclusions de l'avocat général Yves BOT dans l'affaire Schrems sont dans le droit fil de ce constat lorsqu'il note que les États-Unis « *n'offrent aucune protection réelle des données conservées sur le territoire [...] contre la surveillance de l'État. [...].*" *et que "l'existence d'une décision adoptée par la Commission européenne [...] n'a pas pour effet d'empêcher une autorité nationale de contrôle d'enquêter sur une plainte alléguant qu'un pays tiers n'assure pas un niveau de protection adéquat [...] et, le cas échéant, de suspendre le transfert de ces données* ».

Le principal reproche que fait l'avocat général à la commission européenne est de ne pas avoir suspendu l'application de la décision *Safe Harbour* alors même qu'elle avait constaté depuis novembre 2013 qu' « *il n'existe [...] aucune possibilité [...] pour les personnes concernées [...], d'obtenir l'accès, la rectification ou la suppression de données ou d'exercer des voies de droit [...] dans le cadre des programmes de surveillance des États-Unis* »[6]. L'avocat général évoque ainsi une « *surveillance massive et non ciblée* », « *disproportionnée par nature* » qui constitue « *une ingérence injustifiée dans les droits garantis* » par la Charte des droits fondamentaux[7].

(6) COMMUNICATION DE LA COMMISSION relative au fonctionnement de la sphère de sécurité du point de vue des citoyens de l'Union et des entreprises établies sur son territoire, 27 novembre 2013, COM(2013) 847 final.

(7) Article 8 de la Charte :
1. Toute personne a droit à la protection des données à caractère personnel la concernant.
2. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification.
3. Le respect de ces règles est soumis au contrôle d'une autorité indépendante.

En conséquence, la Cour de Justice va effectivement trancher en défaveur de l'accord *Safe Harbour*, reprenant les motifs développés par l'avocat général: limitation injustifiée du pouvoir d'enquête des autorités de contrôle, ingérences disproportionnées dans la vie privée du fait de l'absence de différenciation ou de limite de la surveillance de masse, absence de voies de recours pour la personne concernée.

Les conséquences à court terme de l'arrêt de la CJUE

Renforcées par cet arrêt, les « CNIL » européennes regroupées au sein du G29[8] ont posé un ultimatum, laissant des alternatives juridiques au *Safe Harbour*. Un recours accru aux technologies de protection de données est constaté.

(8) En référence au Groupe de travail institué par l'article 29 de la directive 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

(9) http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf

Un calendrier accéléré par le G29

Le 16 octobre 2015, le G29 a publié une déclaration sur les conséquences de cet arrêt[9], avec un ultimatum pour fin janvier 2016, estimant que puisque les transferts de données fondés sur le *Safe Harbour* étaient illégaux, en cas d'absence d'un nouveau cadre juridique satisfaisant à cette date, des actions répressives coordonnées seraient engagées[10].

(10) En France, le transfert de données vers un pays ne présentant pas un niveau de protection adéquat est réprimé par l'article 226-21 du code pénal d'une peine de 5 ans d'emprisonnement et de 300 000 euros d'amende.

(11) Concernent uniquement les transferts de données intragroupes, afin de faire circuler librement ces données entre les diverses entités d'un groupe partout dans le monde.

(12) Communication de la commission concernant le transfert transatlantique de données à caractère personnel faisant suite à l'arrêt de la Cour de justice dans l'affaire C- 362/14 (Schrems), 6 novembre 2015, COM(2015) 566 final.

(13) Certains droits et obligations sont ainsi directement intégrés dans les "CCT", par exemple des mesures de sécurité, de notifications à la personne concernée en cas de transfert de données sensibles, de droit d'accès, de rectification et d'effacement, de règles d'indemnisation en cas de violation de ces clauses.

Il ajoute que des clauses contractuelles types (CCT) ou des règles d'entreprise contraignantes[11] (REC) peuvent être utilisés, sans préjudice pour les autorités nationales de contrôle de mener des investigations, à la lumière des articles 7, 8 et 47 de la Charte.

Les alternatives juridiques actuelles au Safe Harbour : CCT, REC et cas dérogatoires

La Commission a rendu publiques des orientations[12]. En résumé, les entreprises américaines peuvent avoir recours aux mécanismes de "CCT" émises par la Commission[13] ou de "REC" autorisées par les membres du G29. Ces mécanismes contractuels sont censés suppléer l'accord *Safe Harbour* avec des garanties suffisantes. Il existe enfin des dérogations, notamment lorsque la personne concernée a « *indubitablement donné son consentement au transfert* ». Afin d'éviter tout abus, le G29 recommande des bonnes pratiques, notamment pour garantir un véritable consentement « *libre, spécifique et informé* », sans pression particulière, que

(14) Groupe de travail «Article 29», Avis 8/2001 sur le traitement des données à caractère personnel dans le contexte professionnel (WP 48), 13 septembre 2001, p. 31, 32 et 36.

(15) http://www.brmavocats.com/2015/11/invalidation-du-safe-harbor-quelles-consequences-pour-votre-entreprise, article de Me Edouard VERBECQ.

(16) B. Benhamou, secrétaire général de l'institut de la souveraineté numérique. http://www.souverainetenumerique.fr/

l'on peut craindre dans un contexte professionnel du fait d'un lien de subordination[14].

Pour une entreprise française, la pratique encourage de faire signer des clauses contractuelles à ses sous-traitants aux États-Unis, ou d'imposer un hébergement des données en Europe à ces derniers[15].

Un recours accru aux technologies de protection de données

Sur un plan technologique, la protection des données va probablement s'accompagner d'un accroissement des outils cryptographiques, puisque selon certains : « *les données personnelles [...] doivent désormais être protégées [...] par des mesures d'encadrement juridique adéquates et par des mesures de protection technologiques en particulier cryptographiques. En effet, [...] l'évolution des algorithmes de traitement des données en masse (big data), rend plus nécessaire encore la protection de ces données.* »[16] Si une diffusion de ces technologies paraît positive, des effets pervers ont parfois été constatés en termes d'entrave aux investigations judiciaires.

La gestation du Privacy Shield

L'accord *Safe Harbour* étant neutralisé, la sémantique commandait de puiser à

nouveau dans le champ lexical de la sécurité afin de restaurer une confiance perdue, d'où l'avènement du *Privacy Shield*. Au-delà des mots, ce mécanisme désormais finalisé a fait l'objet d'un avis du G29, alors que les enjeux sont considérables pour les acteurs privés et publics.

Un mécanisme finalisé

Les nouvelles garanties du *Privacy Shield* sont réelles mais non exemptes d'interrogations selon certains observateurs et selon l'avis public du G29.

Le dispositif "Privacy Shield"

Présenté le 29 février 2016 par la Commission[17], le dispositif comprend les principes du «bouclier de protection des données», auxquels les entreprises doivent adhérer, ainsi qu'une série d'engagements écrits des États-Unis. La formule *Trust is a must* résume l'esprit affiché de ces textes[18].

Les garanties s'articulent comme suit : entreprises soumises à des obligations fermes[19] ; accès par les autorités américaines étroitement encadré et transparent[20] ; protection effective des droits des citoyens de l'Union et plusieurs possibilités de recours[21] ; mécanisme de réexamen annuel conjoint[22]. Ce mécanisme complète l'adoption en mai 2016 de la nouvelle législation européenne sur la protection des données (un règlement général sur le traitement des données personnelles dans l'UE et une directive sur les données traitées par les autorités policières judiciaires).

(17) http://europa.eu/rapid/press-release_IP-16-433_fr.htm

(18) Déclaration de M. Andrus Ansip, vice-président de la Commission européenne

(19) Mécanismes de surveillance, possibilité de sanction ou d'exclusion, conditions strictes pour les transferts ultérieurs.

(20) En théorie, tout accès des pouvoirs publics américains aux données à des fins de sécurité nationale serait "subordonné à des limitations, des conditions et des mécanismes de supervision [...], empêchant un accès généralisé aux données personnelles" ; de plus possibilité d'un recours pour les citoyens de l'UE dans le domaine du renseignement américain à un mécanisme de médiation indépendant des services de sécurité américains.

(21) éponse des entreprises aux plaintes dans les 45 jours ; mécanisme de règlement extrajudiciaire accessible sans frais ; possibilité pour les citoyens de l'UE de s'adresser à leur autorité nationale chargée de la protection des données, en collaboration avec la Commission fédérale du commerce : mécanisme d'arbitrage disponible en dernier ressort.

(22) Commission européenne et le ministère américain du commerce, associant des experts nationaux du renseignement travaillant au sein des autorités américaines et européennes de protection des données.

Un dispositif finement évalué par le G29

Les réserves de certains observateurs concernant le futur *Privacy Shield*[23], pointant notamment une autorisation de surveillance de masse ("*signals intelligence collected in bulk*") dans la « *Presidential Policy Directive 28* » (PPD28) utilisable dans six domaines (détection et lutte de certaines activités de puissances étrangères, antiterrorisme, lutte contre la prolifération nucléaire,

(23) http://www.lemondeinformatique.fr/actualites/lire-l-accord-privacy-shield-prend-forme-a-bruxelles-64060.html

(24) http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision-annex-6_en.pdf

(25) http://www.nextinpact.com/news/98366-apres-safe-harbor-privacy-shield-un-bouclier-papier.htm

(26) http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf.

cybersécurité, détection et lutte contre les menaces visant les États-Unis et les forces armées alliées et enfin, lutte contre les menaces de crimes transnationaux[24]), ou encore celles de l'eurodéputé Claude Moréas, président de la Commission des libertés civiles, de la justice et des affaires intérieures du Parlement européen, estimant qu'en l'absence de disposition contraignante, cette architecture ne repose que sur une déclaration des autorités américaines difficilement vérifiable[25], ont trouvé un certain écho dans l'avis public du G29 rendu public le 13 avril 2016[26].

Ainsi, concernant le volet "commercial" du *Privacy Shield*, le G29 souhaite des clarifications dans la conservation des données et leur utilisation, ainsi que des garanties explicites dans le cas d'un transfert ultérieur des données à une partie tierce.

Quant au volet « sécurité nationale », le G29 maintient qu'une surveillance de masse et indiscriminée de personnes ne peut être considérée comme proportionné et strictement nécessaire, salue la mise en place d'un médiateur (« Ombudsperson ») tout en se disant préoccupé d'une indépendance potentiellement insuffisante vis-à-vis des autorités américaines.

Les enjeux d'une confiance restaurée ?

Si la finalisation de l'accord *Privacy Shield* était attendue impatiemment par les acteurs économiques, les données personnelles sont également un sujet majeur pour les souverainetés nationales.

Un enjeu de stabilité pour le modèle économique du Big Data

Comme le souligne Myriam Quémener dans son étude de l'arrêt Schrems : « *la justice européenne s'institue en protectrice des données des Européens qui constituent une manne économique* »[27]. Le groupe d'intérêt DigitalEurope (Apple, Google et Microsoft...) paraît se satisfaire du projet de *Privacy Shield*, et les nouveaux textes européens vont certes prendre en compte un renforcement du niveau de protection des données personnelles[28] mais également des précautions pour créer un « *environnement législatif favorable aux futurs champions européens du numérique* »[29].

(27) « *La fin du Safe Harbor au nom de la protection des données personnelles : enjeux et perspectives* », Myriam QUEMENER in Revue Lamy droit de l'immatériel, n°120 (2015)

(28) Renforcement des conditions du consentement (article 7) et en particulier du consentement parental, consécration du droit à l'oubli (article 17), droit à la portabilité des données (article 18)

(29) "Protection des données personnelles : vers de nouvelles règles européennes", Me Jérôme Deroulez, http://www.village-justice.com/articles/protection-des-donnees,21234.htm

(31) L'accord soumet le transfert à l'autorisation préalable de la CNIL. Les apports sont de limiter la durée de conservation des données, avec un droit d'accès et de correction.

Un enjeu de stratégie pour les souverainetés nationales

Au-delà du Privacy Shield, l'accord *Umbrella Agreement* signé le 2 juin 2016 relatif au transfert et au traitement des données personnelles en matière policière

et judiciaire couvre toutes les données (noms, adresses ou condamnations) susceptibles d'être échangées entre l'UE et les États-Unis, garantissant un transfert conforme au droit européen ainsi qu'une égalité de traitement avec les américains[30]. Il constituait un préalable à l'adoption des partages de données tel que le *Passenger Name Record* (PNR) dans le transport aérien, dont la mise en place a été accélérée sous l'impulsion de la lutte antiterroriste.

L'AUTEUR

Jacques Martinon est titulaire d'un DEA en droit privé (Panthéon Assas) et d'un DEA en droit européen (Panthéon-Assas). Magistrat de l'ordre judiciaire depuis 2008 (promotion ENM 2006), ses premiers postes ont été juge d'instruction au Tribunal de Grande Instance de Senlis, puis juge d'instruction au Tribunal de Grande Instance de Bobigny. En janvier 2016, il rejoint la mission de lutte contre la Corruption et la Cybercriminalité de la direction des affaires criminelles et des grâces (DACG), au sein du ministère de la justice. A ce titre, il est amené à suivre l'actualité nationale en lien avec la cybercriminalité ainsi que les négociations internationales (Conseil de l'Europe, Union européenne…). Au-delà de la cybercriminalité au sens strict, ses attributions peuvent s'étendre aux problématiques engendrées par le recueil de la preuve numérique (chiffrement, extraterritorialité...). Enfin, il est le Point de Contact France du nouveau Réseau Judiciaire Européen sur la

La position de la Cour de Justice de l'Union européenne conduit à requérir des gages sérieux visant à strictement limiter et contrôler les surveillances de masse, voire à en bannir l'usage au titre de son caractère potentiellement disproportionné « *par essence* ». L'importance stratégique de la localisation des données stockées et de leur sécurisation, notamment par chiffrement[31], pourrait amener certains acteurs privés à les relocaliser en Europe.

(31) Le 2 décembre 2015, Maximilien Schrems a de nouveau porté plainte auprès des CNIL irlandaise, allemande et belge pour interdire à Facebook de transférer les données de ses utilisateurs européens vers les États-Unis. Il suggère des solutions alternatives comme « *déplacer les données en Europe, chiffrer les données stockées aux États-Unis ou revoir la structure de l'entreprise* », http://www.lemonde.fr/pixels/article/2015/12/03/le-militant-max-schrems-s-attaque-a-nouveau-a-facebook-sur-les-donnees-

Si la puissance publique doit tisser un cadre protecteur pour les données personnelles de ses citoyens, elle doit également pouvoir être en capacité de les exploiter, dans un cadre légal clair et dans le respect du principe de proportionnalité, pour des motifs légitimes (sécurité nationale, investigations judiciaires).

Ces délicats compromis peuvent et doivent se chercher au niveau européen. Les autorités nationales de contrôle et la Cour de Justice de l'Union européenne constituent des garanties supplémentaires déterminantes pour la protection des données personnelles des citoyens européens.

LES ACTEURS RÉGALIENS

LA DACG AU CŒUR DE LA LUTTE CONTRE LA CYBERCRIMINALITÉ

La direction des affaires criminelles et des grâces soutient les initiatives nationales et internationales de lutte contre la cybercriminalité. L'adaptation du code de procédure pénale, une sensibilisation des juridictions et sa participation aux négociations européennes liées au recueil de la preuve dans le cyberespace témoignent de cet engagement. En effet, la définition d'une nouvelle territorialité, l'hyperconnexion des systèmes et les procédés tant cryptographiques que d'anonymisation au sein de réseaux “noirs” sont des freins aux investigations dans le cyberespace.

Enfin, créée en 2014, la « mission de lutte contre la cybercriminalité » permet une analyse transverse de la cyber criminalité, d'en apprécier la substance et d'évaluer la ressource humaine et matérielle à y consacrer. Le soutien aux projets THESEE et PERCEVAL, menés par le ministère de l’Intérieur, afin de respectivement mettre en place un portail de plainte en ligne contre les cyber-escroqueries et un portail de signalements pour les usages frauduleux de cartes bancaires entrent dans cette optique.

La DACG et la lutte contre la cybercriminalité

Entretien avec Robert Gelli

Monsieur le directeur, de quelle manière le ministère de la Justice participe-t-il à la lutte contre cette criminalité croissante et protéiforme ?

Afin de permettre une analyse transversale de ce phénomène en perpétuelle évolution, j'ai créé, en 2014, une mission de lutte contre la cybercriminalité au sein de la direction des affaires criminelles et des grâces du ministère de la Justice. La définition même de la cybercriminalité fait débat, mais deux axes principaux s'en dégagent. Le noyau dur se constitue des attaques informatiques *stricto sensu* (les atteintes aux Systèmes de traitements automatisés de données, STAD), tandis qu'une myriade d'infractions dites traditionnelles sont facilitées, voire démultipliées, par l'emploi de réseaux de communications électroniques. Une tendance récente est par exemple le basculement du trafic d'armes et de drogue vers l'Internet profond. En soutenant des initiatives nationales et internationales de lutte contre la cybercriminalité, en adaptant le code de procédure pénale à cette matière spécifique, en participant aux négociations européennes sur l'amélioration du recueil de la preuve dans le cyberespace et en sensibilisant les collègues en juridiction à ces enjeux nouveaux, ma direction prend activement sa part dans ce combat essentiel pour la confiance de nos concitoyens en l'économie numérique.

ROBERT GELLI

Directeur des affaires criminelles et des grâces Ministère de la Justice

Quels sont les plus grands défis en la matière ?

Ainsi que je l'ai indiqué, il est parfois délicat de définir la cybercriminalité et il n'est malheureusement pas plus simple d'appréhender statistiquement ce phénomène. En effet, outre le problème

classique du « chiffre noir » (ensemble des crimes et délits qui ne sont pas connus du fait de leur non dénonciation), il existe une difficulté actuelle d'ordre statistique. Des pistes de réflexion sont en cours à ce sujet, considérant qu'une sous-évaluation du phénomène criminologique peut avoir pour conséquence une sous-évaluation des moyens nécessaires à son éradication.

Au-delà de la cybercriminalité, c'est en réalité toute la question du recueil de la preuve numérique qui est posée, quel que soit le type d'enquête, qui se heurte aux limites traditionnelles de la territorialité, concept largement dépassé dans notre monde hyperconnecté et sujet à l'explosion de l'informatique dans les nuages (*Cloud*), à un chiffrement des données (certes nécessaire pour sécuriser les échanges informatiques mais parfois difficile à concilier avec les impératifs des investigations judiciaires) et aux nombreuse techniques d'anonymisation prisées par les cybercriminels (Réseau Tor…).

Le contexte actuel de menace terroriste renforce encore l'urgence de trouver des solutions pragmatiques et rapides à ces difficultés nouvelles.

Quelles sont les perspectives d'amélioration à court terme ?

Il est difficile d'être exhaustif en la matière mais je souhaite profiter de cet entretien pour évoquer les projets THESEE et PERCEVAL menés par le ministère de l'Intérieur avec le soutien de ma direction, afin de respectivement mettre en place un portail de plainte en ligne contre les cyber-escroqueries et un portail de signalements pour les usages frauduleux de cartes bancaires. D'autre part, la nouvelle compétence nationale concurrente du parquet de Paris en matière d'atteintes aux systèmes de traitements automatisés de données (STAD) devrait permettre une spécialisation des acteurs particulièrement profitables en la matière.

L'AUTEUR

Robert GELLI est le Directeur des affaires criminelles et des grâces du ministère de la Justice depuis le 11 septembre 2014.
Il exerce ses premières fonctions de substitut du procureur à Gap, puis à Marseille où il devient premier substitut. Nommé procureur de la République adjoint à Aix-en-Provence, il est amené à gérer le détournement de l'Airbus A300 de la compagnie Air France et la prise d'otages, commis par les terroristes du groupe islamique armé les 24, 25 et 26 décembre 1994. De 1997 à 2002, il est le conseiller technique pour la justice de Lionel Jospin, Premier ministre. Robert Gelli est nommé procureur de la République à Nîmes à partir de 2002, puis procureur de la République à Nanterre en 2012. Il dirige alors un ressort qui correspond à la troisième région économique de l'Union Européenne. En 2014, M. Gelli devient le directeur des affaires criminelles et des grâces, exerçant ainsi les attributions du ministère de la Justice en matière pénale.
Il est décoré des titres de Chevalier de l'ordre national du mérite et de chevalier de la légion d'honneur. Il a été président de la conférence nationale des procureurs de la République de 2011 à 2014, et membre en 2013 de la Commission pour la modernisation du ministère public.

ALLER PLUS LOIN

DIRECTION DES AFFAIRES CRIMINELLES ET DES GRÂCES
Ministère de la Justice

La direction de la norme et de la justice pénales

Si elle a longtemps été perçue comme la direction du ministère public, la direction des affaires criminelles et des grâces, qui a célébré son bicentenaire en 2014, apparaît aujourd'hui davantage comme la direction de la norme et de la justice pénales du ministère de la Justice, tant son champ d'action s'étend au-delà de l'établissement de la politique pénale.
La direction des affaires criminelles et des grâces comprend 369 personnes, dont 61 magistrats de l'ordre judiciaire, répartis sur trois sites : à Paris, où se trouvent les trois sous-directions pénales, à Nanterre - au sein de la direction centrale de la police judiciaire - où se trouve une antenne du bureau de l'entraide pénale internationale, et à Nantes, siège de casier judiciaire national de 1982.

Les principales missions de la DACG

Dans le cadre de sa mission d'élaboration, d'animation et de suivi de la politique pénale définie par le garde des Sceaux, la DACG apporte son soutien aux parquets et parquets généraux en mettant à leur disposition son analyse technique, et en leur proposant des ressources, des outils pratiques et des bases de données juridiques et statistiques. La DACG assure, par ailleurs, l'évaluation des politiques pénales, ainsi que la gestion de la base de données juridiques des infractions pénales.
La DACG élabore la législation et la réglementation en matière répressive et examine, en liaison avec les départements ministériels concernés, tous les projets de normes comportant des dispositions pénales.
Ainsi, la DACG développe son expertise au bénéfice du garde des Sceaux et de l'ensemble des magistrats et fonctionnaires de justice dans des domaines aussi variés que la procédure pénale, la lutte contre les atteintes aux biens et aux personnes, les discriminations, le terrorisme, la criminalité organisée, les trafics de stupéfiants, les atteintes à la probité publique, le droit de l'environnement et de la santé publique, la délinquance économique et financière, l'exécution des peines, ou encore la direction de l'enquête judiciaire.
L'Union européenne représentant une source croissante pour le droit interne, la DACG contribue par ailleurs activement aux négociations européennes et internationales dans ses domaines de compétence. Responsable de la mise en œuvre de l'entraide pénale internationale, la DACG œuvre concrètement à la réalisation de l'Europe judiciaire.
Enfin, à travers l'activité du service du casier judiciaire national qui lui est directement rattaché, la DACG est garante de la mémorisation et de la restitution des condamnations prononcées.

Une direction récemment réorganisée

Refondue en août 2015 afin de répondre plus efficacement à l'évolution de ses domaines d'activité, l'organisation de la direction des affaires criminelles et des grâces s'inscrit dans la volonté de fournir une expertise de haut niveau, nourrie de l'expérience en juridiction des magistrats la composant et de la spécialisation de ses divers personnels (assistants spécialisés, personnels détachés, contractuels), pour développer une politique cohérente et ambitieuse. C'est dans ce cadre qu'a été créée la mission de prévention et de lutte contre les atteintes à la probité et contre la cybercriminalité.

LES ACTEURS RÉGALIENS

CREOGN

LES ACTEURS REGALIENS DE LA CYBERSECURITE ET SA GOUVERNANCE

Le 16 juin 2016, co-organisée par la CEIS et le CREOGN, une table ronde réunissait à l'amphithéâtre Foch de l'Ecole militaire, à Paris, les acteurs régaliens majeurs de la cybersécurité.

Ils ont exploré l'approche interministérielle de cette problématique et abordé la notion de continuum défense-sécurité ainsi que la question de la réserve opérationnelle cyberdéfense. Le statut des lanceurs d'alerte, des plateformes de Bug Bounty a été évoqués dans le concept d'un écosystème global de la cybersécurité et des capacités défensives et offensives à développer dans un cadre juridique. La convergence des acteurs publics et privés a été abordée de manière constructive notamment en la replaçant dans le cadre plus large de programmes européens de recherches. Il s'agit pragmatiquement d'une mutualisation des moyens et d'un partage capacitaire qui requiert l'assentiment des grandes puissances européennes.

Cette orientation semble nécessaire puisque le sommet mondial sur la société de l'information (SMSI), en marge de l'assemblée générale des Nations-unies de 2015, n'a pas conclu à l'ouverture d'une négociation relative à un traité international sur l'Internet ou sur la cybersécurité. Les acteurs régaliens ont en conséquence examiné avec acuité le concept d'autonomie stratégique au regard d'ensembles géostratégiques définis par les traités et la question européenne comme en témoigne l'âpreté des négociations internationales (TAFTA, Privacy Shield, réforme de l'ICANN) liées à la construction d'une nouvelle hiérarchie des normes en témoigne.

Les acteurs régaliens de cybersécurité et sa gouvernance

Table ronde animée par le
GÉNÉRAL D'ARMÉE (2S) MARC WATIN-AUGOUARD ET GUILLAUME TISSIER

- **Commissaire divisionnaire Vincent AVOINE, chargé de l'intérim du préfet chargé de la lutte contre les cybermenaces**
- **Vice-amiral Arnaud COUSTILLIERE, officier général cyberdéfense à l'état-major des armées**
- **Isabelle VALENTINI, adjointe à l'officier général cyberdéfense**
- **David MARTINON, ambassadeur pour la cyberdiplomatie et l'économie numérique**
- **Guillaume POUPARD, directeur général de l'ANSSI**

Général d'Armée (2S) Marc WATIN-AUGOUARD
CREOGN, co-organisateur du FIC

Chers amis, nous sommes, Guillaume TISSIER et moi-même, particulièrement heureux de vous voir ici rassemblés dans cet amphi FOCH. C'est un exercice annuel de convergence entre d'une part le centre de recherche de l'EOGN que je dirige et d'autre part, l'observatoire FIC[1] qui assure la poursuite tout au long de l'année de l'activité du FIC avec Guillaume TISSIER, avec toute l'équipe du Forum que je ne remercierai jamais assez pour la qualité de leur engagement.

(1) FIC : Forum International de la Cybersécurité

Chaque année, nous organisons ensemble une manifestation commune. Il y a deux ans, nous réfléchissions sur la gouvernance de l'internet et l'année dernière sur la voiture connectée. Cette année, nous avons choisi le thème des acteurs régaliens dans la cybersécurité, particulièrement peu traité jusqu'à maintenant. Nous avons par conséquent un plateau un peu inédit. En effet, je ne sais pas si jusqu'à présent ont pu être réunis sur la même scène, le directeur général de l'ANSSI (Guillaume POUPARD), l'officier général cyberdéfense (le vice-amiral COUSTILLIERE), le préfet cyber du ministère de l'Intérieur[2] (représenté par le commissaire divisionnaire AVOINE) et notre ambassadeur pour la cyberdiplomatie et l'économie numérique (David MARTINON). Ensemble, nous allons passer quelques dizaines de minutes sur ce thème des acteurs régaliens mais vous verrez que l'on va assez rapidement l'élargir pour voir la relation

(2) Depuis, les fonctions du préfet cyber ont été confiées au Délégué ministériel des industries de sécurité (DMIS)

avec le secteur privé. En ce sens, nous allons procéder à une sorte d'approche concentrique. Nous allons commencer par évoquer le territoire national, puis l'Europe, l'OTAN et enfin le reste du monde.

Merci à Guillaume POUPARD, à Arnaud COUSTILLIERE, au commissaire divisionnaire AVOINE à David MARTINON de votre présence. Merci aussi à Guillaume TISSIER d'être avec moi pour animer cette table ronde.

La première question, si vous le voulez bien portera sur l'interministérialité. Où en est-on aujourd'hui? Il n'y a pas de cybersécurité sans une approche transversale, bien sûr. Chaque ministère à son rôle, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) est un organisme interministériel puisqu'elle relève du Premier ministre. Où en est-on aujourd'hui dans cette interministérialité, comment chacun travaille-t-il avec les autres et comment les autres travaillent-ils pour chacun ? Finalement cette interministérialité est-elle en mouvement ? Est-ce qu'elle se construit progressivement pour effectivement donner à la cybersécurité son caractère transversal ? Guillaume POUPARD veut-il commencer à répondre ?

Guillaume POUPARD - Directeur général de l'ANSSI

C'est là une vaste question. Revenons sur la démarche française dans un sujet qui est la cybersécurité, dont on parle beaucoup depuis quelques années, sujet peut-être même à la mode, puisqu'on est dans une véritable évolution de la société liée au numérique. Quand s'est posée en France la question des menaces, essentiellement en 2008 dans le cadre du travail sur le Livre blanc de la défense et de la sécurité nationale, on a regardé quels étaient les modèles à l'étranger. C'est toujours le premier réflexe. On a vu notamment un modèle anglo-saxon qui intégrait fortement les questions de renseignement, de défense au sens défensif, de protection mais également les questions d'attaque. Suite à de nombreuses réflexions, nous sommes arrivés à la conclusion que ce modèle n'était pas transposable en France. Pour que cela fonctionne chez nous, il faut, au contraire, une séparation claire entre des capacités offensives et des capacités plutôt défensives.

Déjà à l'époque, on avait le pressentiment que ces questions de cybersécurité appelaient des réponses fondamentalement interministérielles mais pas avec une interministérialité qui conduit à créer des « comités Théodule » à tout propos pour tout coordonner. Chacun a et aura de plus en plus un rôle à jouer dans son métier propre et, en même temps, il reste des fonctions qui sont mutualisées, qui ne rentrent pas dans un ministère particulier.

En 2009 est créée l'ANSSI sur la base d'un existant mais avec justement l'idée

qu'il fallait continuer à pousser les différentes administrations concernées, les différents ministères, vers un développement de la cybersécurité et en même temps avoir une sorte d'entité qui ne soit pas dans un des ministères afin d'être capable d'animer, de coordonner l'ensemble. Coordonner, ça ne veut pas forcément dire donner des ordres, c'est beaucoup plus fin que cela au quotidien. Il s'agit également d'avoir des fonctions en propre comme la prévention, les travaux autour de la politique industrielle, la réglementation, le développement de produits et de services de sécurité, la détection. Ce sont là les métiers internes de l'ANSSI. Tout est mutualisé au sein de l'ANSSI et ce pour éviter de demander à chaque ministère de se protéger lui-même et de réinventer des actions compliquées à mettre en œuvre. C'est d'ailleurs ce qui justifie que les moyens de l'ANSSI soient passés progressivement, mais assez vite, d'une centaine de personnes à 500 aujourd'hui.

Je pense que c'est un modèle adapté à la France, qui fonctionne aussi parce qu'il y a des hommes et des femmes qui s'entendent bien, ce qui reste essentiel. Comment fait-on pour continuer à garder ce modèle extrêmement vivant pour éviter de se faire dépasser ? Comment pose-t-on ce modèle national en interface avec les modèles de nos alliés qui évidemment sont parfois très différents ? J'ai cité l'exemple des Anglo-saxons qui, au contraire, condensent les capacités. Il est possible de parler aussi de nos amis allemands qui ont fait également ce choix de la séparation de l'attaque et de la défense mais notre homologue ne peut pas être interministériel et se retrouve au sein du ministère de l'Intérieur, ce qui comporte certes des avantages mais, on le voit également au quotidien, parfois des inconvénients. Telles sont les questions auxquelles nous devrons aujourd'hui apporter une réponse.

Général d'Armée (2S) Marc WATIN-AUGOUARD - CREOGN, co-organisateur du FIC

Arnaud COUSTILLIERE, quel est le regard du Ministère de la Défense sur cette question ?

Vice-amiral Arnaud COUSTILLIERE - Officier général cyberdéfense à l'État-Major des armées

Depuis 2009, nous avons travaillé avec Guillaume POUPARD, avec Patrick PAILLOUX[3] et Bernard BARBIER[4] sur la construction de ce modèle. On se souvient de tous les modèles que nous avons étudiés et les raisons pour lesquelles on a fait une séparation entre les différents domaines. Je vais reprendre par le bas pour compléter par des signes tangibles. Première interministérialité, premier lien entre le ministère de la Défense, le CALID[5] qui est le centre expert du ministère de la défense. Il est hébergé dans les mêmes locaux que

(3) Ancien directeur de l'ANSSI

(4) Ancien directeur technique de la DGSE

(5) Centre d'Analyse en Lutte Informatique Défensive

l'ANSSI avec deux autorités totalement indépendantes au dessus mais qui travaillent totalement ensemble.

Deuxième sujet, on a bâti ensemble, Guillaume POUPARD, la DGGN[6] et nous, le projet de réserve à vocation opérationnelle porté par le ministère de la Défense mais qui est mis à disposition.

(6) Direction Générale de la Gendarmerie Nationale

Je souligne ensuite tout ce qui gravite autour du pôle d'excellence en Bretagne, en matière de cyberdéfense (PEC) qui opère des rapprochements en matière de R&D et avec des feuilles de route communes avec l'ANSSI sur tout ce qui relève du régalien. Le ministère de la défense investit 25 millions d'euros, l'ANSSI 5 millions d'euros mais la feuille de route est totalement commune. Je parle au nom de mon camarade Frédéric VALETTE, qui n'est pas là ; le rapprochement de l'ANSSI avec le socle technique qu'apporte la DGA du ministère de la Défense – il va d'ailleurs bientôt compter de l'ordre de 500 ingénieurs - est bien une action au profit de l'État, globalement et pas seulement au profit des armées. La continuité est extrêmement forte aujourd'hui si bien que, très souvent, je ne parle plus de continuité sécurité-défense mais d'imbrication totale entre ce qui relève de la cybercriminalité, de la cybersécurité, de la cyberdéfense, parce que se sont les mêmes acteurs, les mêmes outils, les mêmes hommes qui sont impliqués.

Enfin, pour être très clair, tout ce qui relève de l'offensif est hébergé au sein du ministère de la défense, à part quelques petits éléments. Nous avons par ailleurs entre les trois principaux ministères un certain nombre de groupes de travail fermés, classifiés, dans lesquels on échange très naturellement sur des sujets bien réels.

Général d'Armée (2S) Marc WATIN-AUGOUARD - CREOGN, co-organisateur du FIC

Vincent AVOINE, quel regard le ministère de l'Intérieur porte-il justement sur cette interministérialité ? Où en est-on ? Les fonctions « préfet cyber » sont aujourd'hui vacantes ; la délégation va-t-elle se mettre en place ?

Commissaire divisionnaire Vincent AVOINE - Chargé de l'intérim du préfet chargé de la lutte contre les cybermenaces

Effectivement, le préfet LATOURNERIE est parti voici un mois et demi. La « délégation » existe toujours physiquement, nous venons d'ailleurs d'emménager place Beauvau. Je m'en tiens très simplement à la parole du ministre de l'Intérieur. Dans une enceinte qui me paraissait pour le moins sérieuse et face à un public d'initiés, le ministre de l'Intérieur, le 21 janvier, a annoncé qu'un de ses chantiers, à savoir la mise en place d'une délégation en charge de la lutte contre les cyber-menaces, allait être concrétisé par un décret l'instituant. Les événements ont fait que ce n'est pas

encore sorti mais le ministre l'a dit et je ne retiens que cela.

L'autre point sur lequel je voudrais m'exprimer, c'est l'interministérialité. C'est très confortable, en France, d'avoir un pilote de l'interministérialité avec l'ANSSI et le SGDSN qui ont mis en place une stratégie nationale de sécurité du numérique, à charge pour chacun des ministères de la décliner pour ses champs de compétence propres. C'est en cours pour le ministère de l'Intérieur, nous y travaillons avec les services . L'existence de cette agence nationale placée auprès du Premier ministre sous l'autorité du SGDSN est un réel confort qui n'existe pas dans tous les pays. Guillaume POUPARD parlait de l'Allemagne, je suis témoin effectivement de difficultés s'agissant d'appliquer l'interministérialité dans ce pays-là.

Du point de vue du ministère de l'Intérieur, nous inscrivons cette action dans une interministérialité concrète. En me référant à des événements récents, l'intervention de l'ANSSI a été extrêmement précieuse en support du ministère de l'Intérieur, du ministère des Affaires étrangères et du ministère de l'Énergie pour assurer la sécurité de la COP21 mais également de l'euro 2016. L'interministérialité, je la vois aussi dans la projection internationale de la France lorsque notre ambassadeur, David MARTINON, se rend à l'étranger associant l'ANSSI, le ministère de l'Intérieur et le ministère de la Défense ; c'est également le cas avec la direction de la coopération internationale ou, dans les ambassades, les attachés de sécurité intérieure qui agissent avec les autres attachés. L'interministérialité se manifeste aussi dans l'élaboration du diagnostic sur la situation des victimes de cybermalveillances. En effet, il y a tout un travail effectué dans une logique interministérielle associant notamment le ministère de l'Économie et des finances, visant à définir quel était l'état des victimes avec une démarche qui va se mettre en place bientôt. Interministérialité encore avec le ministère de la défense, plus précisément dans le recueil et l'exploitation du renseignement. Il y a des liens forts entre le ministère de la défense, qui dispose de nombreux capteurs comme vous l'imaginez bien et les services du ministère de l'Intérieur qui travaillent sur la lutte antiterroriste.

Voilà pour la manière dont nous pouvons témoigner de l'interministérialité telle qu'elle est pratiquée en France. Évidemment, tout cela est encore perfectible. Il y a des pistes, que ce soit au niveau local, autour des préfectures, dans la sensibilisation, dans l'assistance aux victimes mais aussi, on en parlait avec l'Amiral COUSTILLIERE, dans le développement d'échanges techniques, opérationnels entre les experts du CALID et les enquêteurs qui fondent la police judiciaire tant en gendarmerie que dans la police.

Général d'Armée (2S) Marc WATIN-AUGOUARD - CREOGN, co-organisateur du FIC

On voit bien en vous écoutant qu'il y a un continuum défense-sécurité. Une question pour l'Amiral COUSTILLIERE : la réserve opérationnelle cyberdéfense va-t-elle rester interministérielle dans son action ou rester une réserve militaire, dont l'engagement sera réservé au profit du ministère de la Défense ?

Vice-amiral Arnaud COUSTILLIERE - Officier général cyberdéfense à l'état-major des armées

Non, c'est une réserve dont le projet, comme il a été précisé précédemment, a été bâti en commun avec l'ANSSI, avec un fort soutien de la DGGN et qui a pour vocation de se mettre à la disposition des services de l'État en cas de grandes crises. Elle sera activée par les processus normaux de réquisition des forces armées après avis et/ou sur sollicitation de l'ANSSI. C'est donc l'ANSSI qui, pour ce qui ne relèvera pas du ministère de la Défense, déclenchera l'action de cette réserve.

Pour cette réserve, il y a un objectif de 500 membres d'ici la fin de l'année, tous les textes administratifs ont été signés. Je commence à partir de la semaine prochaine le processus de recrutement que nous avons déjà bien initié avec un certain nombre d'écoles. C'est bien une réserve dont l'un des principaux employeurs, le principal client sera l'ANSSI.

Guillaume TISSIER - Directeur général CEIS, co-organisateur du FIC

Une question à propos de la loi de programmation militaire (LPM) à laquelle Guillaume POUPARD pourra apporter une réponse. La LPM a finalement devancé la directive NIS[7] en introduisant un certain nombre de dispositions visant les opérateurs d'infrastructure vitale. J'ai cru comprendre qu'un certain nombre d'arrêtés étaient en préparation, qu'ils allaient bientôt sortir. Pouvez-vous nous en dire un peu plus sur le contenu de ces arrêtés qui ont donné lieu à de nombreuses concertations ces derniers mois ?

(7) Directive sur la sécurité des réseaux et des systèmes d'information connue sous l'appellation « Network and Information Security (NIS) » du 6 juillet 2016

Guillaume POUPARD - Directeur général de l'ANSSI

Le premier arrêté - c'est un scoop ! - est signé mais pas encore publié. Il va entrer en vigueur au 1er juillet et concernera les produits de santé. Il n'y a pas de message subtil sur la priorité qui serait accordée à ces produits, c'est simplement le premier arrêté qui a été prêt. Il a été écrit en étroite coopération avec le ministère coordonnateur et les OIV[8] eux-mêmes, avec une démarche très positive de co-construction et de co-écriture sur la base de règles génériques que l'on a fournies mais qui ont été bien comprises, bien amendées par ce travail fondamentalement transverse. Les autres

(8) Les opérateurs d'importance vitale

arrêtés prendront effet au 1er octobre. Au-delà de l'aspect calendaire, il faut revenir au fondement même de la LPM et voir finalement pourquoi elle a précédé la directive NIS. Ce n'est pas totalement un hasard. La LPM, c'est notre nom de code à nous mais l'idée c'est bien de modifier le code de la Défense de manière à imposer dorénavant des mesures de cybersécurité aux opérateurs les plus critiques pour la Nation. La démarche qu'ont pu faire nos alliés, consistant à rester dans le domaine du conseil et de l'incitation, est une démarche qui à terme finira par fonctionner mais à mon avis après des drames. En ce qui nous concerne, l'idée est de rendre un peu plus obligatoire la cybersécurité, de réglementer par la loi et par le règlement pour que ces questions de cybersécurité ne soient plus laissées à la seule appréciation des opérateurs les plus critiques. En revanche, pour que cela fonctionne, il faut que ce soit non pas l'occasion de rajouter des règles aux nombreuses règles qui existent déjà mais bien de créer un lien, une coopération avec des gens qu'on n'avait pas l'habitude de voir jusque-là. J'ai coutume de dire qu'au sein de ces opérateurs, le contact avec les RSSI était facile parce qu'on parlait avec des gens qui comprenaient notre langage et qui avaient de surcroît les mêmes préoccupations que nous. Pourtant, pour aller au-delà de ces RSSI, c'était souvent très compliqué parce que la prise de conscience est encore insuffisante. Par conséquent, l'effet conjugué d'une réglementation et d'une actualité qui nous aide aussi à sensibiliser les dirigeants fait que le sujet de la cybersécurité, grâce à l'article 22 de la LPM, devient un sujet de COMEX[9], devient un sujet pour les directeurs juridiques, pour les directeurs financiers et plus généralement pour les PDG. J'étais encore mardi au COMEX d'un gros OIV où la question n'était plus de s'interroger sur la réalité de l'état de la menace ou d'imaginer comment faire pour contourner la nouvelle réglementation. Le débat portait sur la manière de régler finement la coopération entre les différents acteurs étatiques et ces OIV de manière à anticiper les catastrophes qui, autrement, ne manqueront pas de se produire. C'est extrêmement positif et finalement j'attendais essentiellement cela de la part de la LPM : créer ce lien, créer cette prise de conscience. De ce point de vue, l'objectif est pleinement rempli.

(9) Comité exécutif

Dans la rédaction de ces arrêtés, on s'aperçoit qu'il y a beaucoup d'acteurs qui sont impliqués. On en revient au constat fait initialement que le sujet cyber est un sujet fondamentalement transverse. Forcément, quand on veut rassembler autour de la table de nombreux acteurs qui n'ont pas toujours l'habitude de travailler ensemble cela peut prendre un certain temps mais, au final, c'est cependant très positif.

La limite de ce que l'on a fait - mais c'était assumé - est posée par la LPM qui ne s'applique qu'aux OIV *stricto sensu*. Les OIV, il y en un peu plus de 200 en France, à la fois publics et privés. Ils préexistaient à la démarche cyber et il ne fallait pas tomber dans l'écueil consistant à dire : on va faire un dispositif réglementaire pour les opérateurs critiques mais quelle est la liste des opérateurs critiques ? C'est très dur à faire quand on part d'une feuille blanche parce que faire la liste des opérateurs critiques est quelque chose de très binaire. On est ou on n'est pas sur la liste. On a assumé le fait de prendre cette liste des OIV, qui est probablement insuffisante en termes de quantité, mais qui, de fait, regroupe des acteurs qui sont intéressants d'un point de vue du cyber. L'étape d'après va consister à avoir une démarche similaire, mais adaptée, pour élargir le champ. C'est là que la directive NIS arrive. D'une certaine manière, nous avons tout fait pour influencer les travaux européens qui nous semblaient aller dans la bonne direction, de façon à ce que nous avons fait pour les OIV soit tout à fait compatible avec la directive NIS et, en même temps, traiter les acteurs qui aujourd'hui ne sont pas concernés par la LMP. C'est ce qui va maintenant s'enclencher et nous sommes tous impatients de voir la directive publiée officiellement[10]. Concrètement, la directive va concerner un autre ensemble d'opérateurs essentiels. Les OIV seront forcément tous inclus. Pour eux, la directive NIS sera indolore puisque le travail aura déjà été fait. En revanche, cela va évidemment nous permettre d'étendre le champ, d'aller voir d'autres personnes que l'on ne voit pas aujourd'hui et le gros travail va consister à trouver un équilibre entre l'augmentation de la cible et la définition de règles ou de processus qui vont, sans nous saturer et en respectant les spécificités de chacun, permettre de réellement relever le niveau de sécurité, là où c'est nécessaire.

(10) Directive (UE) 2016/1148 du Parlement européen et du Conseil de l'Union européenne du 6 juillet 2016 - JO (UE) du 19 juillet 2016.

Général d'Armée (2S) Marc WATIN-AUGOUARD - CREOGN, co-organisateur du FIC

David MARTINON, un ambassadeur, en principe, travaille « vers l'extérieur ». Comment apporte t-il une plus value à l'action des acteurs régaliens qui, à l'intérieur du territoire, sont en quelque sorte les garants de la cybersécurité ?

David MARTINON - Ambassadeur pour la cyberdiplomatie et l'économie numérique

Pour ce qui est du rôle du diplomate en matière de cybersécurité, je précise tout d'abord que la cybersécurité n'est qu'un aspect de ma mission, puisque je couvre à peu près l'ensemble des sujets liés à Internet et aux nouvelles technologies pour le compte du ministre des Affaires étrangères. S'agissant de la cybersécurité, il y a des fonctions très précises qui sont notamment liées à l'activité de l'organisation des Nations

Unies relatives à la clarification des règles de droit international public applicables au cyber-espace devenu un espace de conflit. Je cite l'ONU, je pourrais également citer l'organisation pour la sécurité et la coopération en Europe (OSCE) qui travaille également sur ces sujets-là. Dans ces deux enceintes, on s'efforce également de bâtir des normes de comportement pour construire une sécurité collective basée sur la confiance.

Pour nourrir les positions et négociations françaises, nous avons besoin d'un travail interministériel. C'est assez classique en réalité. Nous nous parlons, avec l'Amiral COUSTILLIERE, avec Guillaume POUPARD, avec nos collègues du ministère de l'Intérieur et du ministère des Finances. Le but de cette concertation est d'avoir des positions pour la France, comme nous avons des positions « France » au sein des instances communautaires qui sont préparées par le secrétariat général pour les affaires européennes. Dans le domaine qui nous intéresse aujourd'hui, la préparation est plus simple parce que les acteurs sont plus facilement identifiables et repérés.

Général d'Armée (2S) Marc WATIN-AUGOUARD - CREOGN, co-organisateur du FIC

Dans le monde réel, l'offre publique, l'offre régalienne de sécurité est majoritaire. Bien sûr, il y a des sociétés privées de sécurité, des acteurs qui viennent s'agréger mais c'est toujours l'État qui domine. Dans le cyberespace, la puissance publique ne peut être seule, assurément. Elle a donc de plus en plus besoin de bénéficier du concours d'acteurs privés de la sécurité . Finalement, comment voyez-vous cette articulation public-privé dans la cybersécurité ? J'ai une autre question, tout à fait d'actualité : quelle place pour le hacker éthique dans notre dispositif de cybersécurité ?

Vice-amiral Arnaud COUSTILLIERE - Officier général cyberdéfense à l'État-Major des armées

Je vais répondre de façon extrêmement claire et plutôt extrêmement pragmatique. Le hacker éthique c'est l'équipe d'audit «expertise ». Je viens de prendre la direction de l'ensemble des équipes d'audit du ministère de la défense. Notre première tâche va être de les rapprocher des équipes d'audit plus spécialisées et de leur faire faire davantage d'actions de type pentest[11], de type test de pénétration, y compris dans des zones d'exercice bien balisées. Pour ma part, le hacker éthique ne me pose aucun état d'âme de ce point de vue car cela fait partie de l'évolution normale.

(11) Pénétration test : test d'intrusion mené par une équipe informatique et destiné à tester la robustesse des dispositifs de sécurité d'un système d'information.

Prenant l'exemple du Pentagone, on voit bien qu'aux États-Unis quand on prend le Pentagone, qu'ils font appel à des compétences extérieures sous forme de challenge. Nous avons commencé à tester ce genre de pratiques en faisant

appel à des réservistes de la réserve citoyenne, ce qui me paraît en France, en tout cas pour ce qui concerne le ministère de la défense, le bon cadre d'action pour aller vers ce genre d'actions, d'autant plus que je peux habiliter le personnel.

La place de l'industrie est énorme. On voit bien aujourd'hui que les grands opérateurs de la cybersécurité comme SYMANTEC[12] ou KASPERSKY[13] ont une place de choix. Ce que l'on peut regretter, c'est que parmi ces grands acteurs, il y a très peu d'Européens et encore moins de Français. Pour nous, ça pose clairement un vrai problème parce que nous sommes obligés, pour protéger nos réseaux, les réseaux de la DIRISI[14] par exemple, de faire appel à des services émanant de différents pays. Pour nous cela représente quelque 25 pays très divers.

(12) Société américaine spécialisée dans les logiciels informatiques

(13) Société russe spécialisée dans la protection des systèmes d'information

(14) Direction interarmées des réseaux d'infrastructure et des systèmes d'information de la Défense

La stratégie que nous adoptons pour l'instant consiste à panacher des produits venant de l'Est avec des produits venant de l'Ouest pour que nos données passent à travers ces différents filtres. On attend avec impatience l'arrivée de grands acteurs étatiques compétents. Il faut être Français et compétent, du moins je préférerais dire, compétent et Français pour pouvoir refaire partie du cercle des gens que l'on mettra sur nos réseaux et

(15) Pôle d'excellence cyber

(16) Plan France numérique 2012-2020 (http://www.entreprises.gouv.fr/)

c'est bien toute l'action qui est lancée à travers le PEC de Bretagne[15], à travers le P33[16], à travers tout ce qui est lancé actuellement pour faire immerger une vraie offre de sécurité avec des sociétés de taille acceptable en France. Nous avons beaucoup de PME très innovantes, beaucoup de petites sociétés de services mais quand on leur demande la taille de leurs équipes un peu pointues , la réponse est souvent minimaliste. Nous en avons de l'ordre de quelques centaines dans les différents services de l'État, mais on a besoin d'avoir des acteurs de taille moyenne capables de mobiliser des équipes de pentest de l'ordre de 50 à 100 personnes. Si vous considérez les sociétés françaises, ça se compte sur les doigts de la main.

Guillaume POUPARD - Directeur général de l'ANSSI

Aujourd'hui mes capacités d'audit sont de l'ordre de 70 audits par an. C'est beaucoup, certes, mais c'est très peu en pratique face au besoin qui se présente. Les audits sont nécessaires en amont, lors des inspections des ministères ou bien chez certains OIV, pendant le traitement des affaires. Les 70 « tickets » que j'ai à ma disposition sont extrêmement vite consommés et toute la question est de savoir comment faire pour traiter tout le reste ? L'amiral vient de le dire, au sein du ministère de la défense il

y a des capacités d'audit à peu près comparables. Même si on voulait se passer du secteur privé dans ce domaine, cela n'aurait aucun sens. La cybersécurité est une question qui doit être normalisée, traitée comme les autres et les prestataires privés ont un rôle fondamental à jouer. Comment peut-on promouvoir cela ? Tout d'abord, nous avons des liens étroits avec la plupart des personnes qui produisent des équipements de sécurité ou qui proposent des services de sécurité. Ensuite, nous considérons que le rôle de l'État n'est pas de tout faire mais d'indiquer vers qui se tourner pour faire le travail efficacement. C'est exactement la démarche de qualification qui est en place et qui consiste à vérifier qu'un acteur qui propose des produits ou des services est à la fois compétent et de confiance, ainsi que le disait l'amiral. Il y a des personnes très compétentes mais d'une confiance très limitée de notre point de vue national. Il y a également des personnes qui sont de confiance mais pas compétentes : celles-là je vous les déconseille, c'est évident, avec eux vous allez dépenser votre argent pour rien. Nous avons vraiment besoin de ces deux qualités qui sont complètement orthogonales. Cela ne se décrète bien évidemment pas sur la bonne tête des uns et des autres ou sur les bonnes relations que nous pouvons avoir. Ce n'est que le fruit d'un processus sérieux d'évaluation sur la base de règles du jeu claires et ouvertes.

Concrètement, nous produisons des référentiels qui sont publics et qui expliquent ce que nous attendons d'un prestataire de services de sécurité. Ensuite, nous évaluons les prestataires, au vu de ce référentiel, ou, plus exactement, nous les faisons évaluer de manière indirecte par des laboratoires indépendants, comme pour les produits de sécurité. Parfois même, nous sommes obligés d'évaluer les experts, un par un, parce que nous savons très bien, dans le cas type des audits, des pentests qu'il faut avoir confiance dans l'entité mais également dans la personne qui va mener le test lui-même. C'est extrêmement compliqué et lourd, mais in fine, quand on a fait tout ce travail, on peut dire, au nom de l'État français, au nom du Premier ministre que tel prestataire a la compétence et le potentiel pour mener, par exemple, des audits. C'est tout l'intérêt du référentiel PASSI[17] et du dispositif PASSI qui sont en place et déjà opérationnels. Arnaud COUSTILLIERE se plaint un peu du manque d'acteurs. En ce qui me concerne, je suis au contraire agréablement surpris du nombre d'acteurs qualifiés et de la qualité du travail réalisé aujourd'hui .

(17) Référentiel d'exigence applicable aux prestataires d'audit de la sécurité des systèmes d'information

On peut se demander si c'est encore suffisant pour répondre à la demande, mais il s'agit plutôt ici d'un problème positif. La même démarche est amorcée

dans le domaine de la détection d'incidents. Bien évidemment, il est hors de question que les OIV développent leur propre capacité de détection d'incidents. C'est un travail d'expert, même si ça ne veut pas dire qu'ils ne doivent pas s'y impliquer. On appelle de nos vœux la mise en place de prestataires de détection d'incidents de sécurité, des PDIS dans notre jargon. De mémoire, il y en a déjà 8 en cours de qualification à titre expérimental. Même sujet dans le domaine de la réaction des incidents. Par extension, nous nous essayons également. Là, nous sommes en marge de nos métiers. Toutefois, si on veut sortir de la simple agitation de la menace relative au Cloud (attention, le Cloud, c'est dangereux!), il faut au contraire, proposer des solutions et des acteurs compétents et de confiance en termes de sécurité, même si l'objet même du Cloud computing n'est pas de faire de la sécurité. On veut au contraire sélectionner des acteurs qui intègrent la sécurité dans leur métier. C'est en cours et cela marche plutôt bien .

Contrairement à ce qu'à dit l'amiral, ce n'est pas réservé aux acteurs français mais aux acteurs de confiance. Effectivement, la confiance est parfois plus facile à établir avec des acteurs français qu'avec les acteurs étrangers, pour la simple raison qu'ils ont moins d'états d'âme à nous ouvrir les portes, à nous montrer leurs codes sources.

Pourtant, ce serait une erreur stratégique et une erreur en termes de légalité que d'affirmer que nous ne voulons que des acteurs français. Encore faudrait-il avant tout pouvoir définir ce qu'est un acteur français. C'est, en effet, une notion qui a un vrai sens mais quand on cherche à la légaliser, c'est complexe et on se rend compte que certains de nos grands partenaires de confiance, de fait, payent leurs impôts ailleurs ou ont leur siège social ailleurs.

Général d'Armée (2S) Marc WATIN-AUGOUARD - CREOGN, co-organisateur du FIC

Vincent Avoine, voulez-vous ajouter un complément ?

Commissaire divisionnaire Vincent AVOINE - Chargé de l'intérim du préfet chargé de la lutte contre les cybermenaces

Sur le lien avec les entreprises, pour le ministère de l'Intérieur et notamment d'un point de vue de la police et de la gendarmerie, il va de soi que nous sommes parfaitement conscients de l'expertise et de l'aide technique que peuvent nous apporter les industriels de la cybersécurité. Des partenariats opérationnels et des échanges existent, y compris au niveau d'Interpol ou d'Europol. On peut citer des structures tels que le CECyF[18] ou Signal SPAM qui contribuent à la cybersécurité par des actions de prévention au service de la lutte contre la cybercriminalité.

(18) Centre expert de la cybercriminalité français (cecyf.fr)

Le lien avec les entreprises permet au ministère de l'Intérieur d'assurer la salubrité publique sur cet espace qui est le cyberespace. À ce titre, nous sommes bien conscients que les entreprises n'ont pas un rôle facile, d'une part parce qu'elles doivent gérer énormément de données et aussi parce qu'on a l'impression qu'elles sont en capacité de contrôler tout ce qui circule sur les plates-formes, ce qui n'est pas le cas. D'ailleurs, les entreprises n'ont pas une obligation générale de surveillance des contenus. Autre difficulté dont nous sommes conscients, les entreprises doivent appliquer plusieurs droits et la combinaison des différents droits nationaux est un exercice pour le moins difficile, voire parfois impossible. La relation avec les entreprises, évidemment tous les pays du monde l'entretiennent y compris les États-Unis, très concernés par ce lien avec les entreprises, les plates-formes.

Comment assurer cette salubrité publique sur le cyberespace en lien avec les entreprises? Et bien, on exploite ce qui nous est signalé. Les entreprises doivent mettre en place des mécanismes de signalement aux autorités pour qu'il y ait ensuite des retraits de contenus. Nous avons mis en place, avec la loi de novembre 2014, un dispositif de blocage et de déréférencement des contenus qui fonctionne bien. Il monte en puissance. On est bien sur des éléments qui sont communiqués, grâce aux entreprises, à l'autorité publique et qui permettent de nettoyer cet espace voire dans un certain nombre de cas – on a pu l'observer notamment après les attentats de novembre 2015 – d'engager des enquêtes judiciaires, que ce soit sur des faits de menace de nouveaux attentats, des revendications d'attentats ou des cas d'apologie du terrorisme. Ce lien existe et il est important pour nous de continuer à discuter avec les entreprises, notamment pour les besoins de l'enquête. En effet, pour lutter contre la cybercriminalité, il faut que les entreprises nous aident à réagir très vite. Des échanges sont nourris avec les entreprises et c'est l'objet du groupe de contact permanent qui a été mis en place à la demande du ministre de l'Intérieur. Il fonctionne depuis un peu plus d'un an. C'est un lieu d'échange sur les mécanismes d'obtention de données auprès des entreprises pour les services de police et de gendarmerie mais c'est aussi un lieu d'échange sur l'appréciation du droit qui peut être faite par les entreprises. Sur ce point, je pourrais citer un certain nombre d'exemples. Il y a des avancées et ce groupe de contact fait évoluer les entreprises. J'ai même entendu récemment qu'un certain nombre d'opérateurs étaient en train de mettre en place une base de données commune s'agissant des contenus haineux pour que le retrait de ces contenus soit le plus efficient, le plus rapide possible dès lors

qu'ils apparaissent sur les sites internet. Les actions que l'on engage en France sont relayées - je ne sais pas si c'est le fait du hasard ou si c'est due à la puissance de notre pays - au niveau européen. La Commission européenne a d'ailleurs récemment défini avec les opérateurs, un code de conduite relatif à la prise en compte des contenus haineux sur internet.

Général d'Armée (2S) Marc WATIN-AUGOUARD - CREOGN, co-organisateur du FIC

Avant de passer la parole à Guillaume TISSIER, je salue Isabelle VALENTINI, qui remplace l'amiral COUSTILLIERE. Elle témoigne par sa présence de la continuité du service public au sein de la défense. Guillaume, des questions sur les aspects européens de la cybersécurité ?

Guillaume TISSIER - Directeur général CEIS, co-organisateur du FIC

Avant de parler de l'Europe, une question sur les hackers éthiques que nous avons abordée très rapidement tout à l'heure. On parle beaucoup de « cloud security », on voit des plates-formes de *bug bounty*[19] apparaître. Un projet de loi consacre le statut de lanceur d'alerte. Quel rôle donner à ces « white hat » dans l'écosystème sur la cybersécurité ?

(19) Récompense qu'une société offre à tous ceux qui trouvent des failles de sécurité dans un périmètre donné.

Guillaume POUPARD - Directeur général de l'ANSSI

Il y a effectivement un problème de vocabulaire. Tout à l'heure on évoquait le cas des personnes qui font du pentest dans le cadre d'entreprises qualifiées où tout est surveillé. C'est un cas qui ne pose pas débat aujourd'hui, mais on a également la situation que l'on cherche à traiter dans le cadre du projet de loi pour la République numérique qui consiste à prendre en compte les signalements pouvant venir de ce que j'appelle « les citoyens responsables ». On est sur ce terme de « white hat ».

En effet, on a aujourd'hui toute une communauté de gens qui ne sont pas forcément chez les acteurs privés ni chez les acteurs étatiques, qui ont de vraies compétences et qui respectent la loi. Ces gens-là, il faut être capable de les écouter, ce qu'on ne sait pas encore faire suffisamment. Pourtant, ils sont une source d'information très intéressante sur l'état de santé même de notre écosystème numérique.

Dans son état actuel, le projet de loi nous dit que ces personnes peuvent signaler des faits anormaux en termes de sécurité, très souvent autour de sites web ou de systèmes d'information un peu trop ouverts sur internet. Quand ils vont nous signaler cette situation, sans chercher à en tirer parti, ni financièrement, ni en termes de communication, alors nous ne serons pas obligés de les dénoncer systématiquement à la puissance publique et de les traiter comme des malfrats parce que ce ne sont pas des malfrats de fait. C'est un progrès très clairement. On est loin de la question des lanceurs d'alerte, qui est très différente, à

mon avis encore bien plus complexe et j'ai beaucoup milité pour qu'il n'y ait pas de confusion entre les deux notions. Après, nous sommes évidemment prudents avec eux parce qu'aujourd'hui on a un Code pénal qui a quand même été bien écrit. Les articles 323-1 et suivants expliquent clairement que rentrer dans les systèmes d'information c'est mal, modifier les informations qu'il y a à l'intérieur des systèmes d'information c'est encore pire et il n'est absolument pas question de revenir sur ce genre de choses et de ré-ouvrir une boîte de pandore créant une sorte de « far-west numérique » où chacun, au titre de l'éthique ou pas, pourrait commencer à aller faire n'importe quoi. On ne veut surtout pas créer un effet d'aubaine pour des gens qui pourraient utiliser des idées un peu trop bienveillantes et naïves pour masquer une activité qui est fondamentalement malveillante.

Guillaume TISSIER - Directeur général CEIS, co-organisateur du FIC

Après cette première partie de débat consacrée aux questions nationales, je propose de passer au deuxième cercle qui est le cercle européen et celui de l'OTAN, avec une première question assez générale, pour David MARTINON, sur le concept d'autonomie stratégique. J'ai cru comprendre que le terme souveraineté et, notamment souveraineté numérique, froissait parfois un certain nombre de nos alliés et qu'on avait développé un concept qui était celui d'autonomie. Quels sont ces piliers et que signifie exactement l'autonomie stratégique en matière numérique ?

David MARTINON - Ambassadeur pour la cyberdiplomatie et l'économie numérique

Il est vrai que le concept de souveraineté numérique est difficile à saisir. D'abord, je tiens à dire que la souveraineté, elle, ne se discute pas. Les États sont souverains, point ! C'est ce qui les définit et bien sûr cela s'applique au numérique. Les États ont, parce qu'ils sont souverains, la capacité de mettre en œuvre un certain nombre de politiques publiques, de règles, de principes qui peuvent affecter ou régir le cyberespace. Le cyberespace est un autre concept difficile à saisir lui aussi. Lorsque les experts gouvernementaux se retrouvent au sein du groupe des experts gouvernementaux (GGE)[20] de l'ONU pour parler des règles du cyberespace, ils discutent de la souveraineté et de ses limites. En tout cas, ce qui est sûr, lors de sa dernière session, le GGE a conclu que le concept de souveraineté s'appliquait dans le cyberespace avec tout ce que cela emporte de conséquences juridiques en droit international public. Par conséquent, la souveraineté s'applique et, avec elle, la capacité des États à se défendre et à mettre en œuvre le principe de légitime

(20) Se réunit depuis 2004, un groupe d'État dénommé « le groupe des experts gouvernementaux » (15, puis 20 après 2014) , sélectionné par l'ONU en vertu de leur expertise et de leur représentativité géographique et mandaté, à ce titre, pour définir des recommandations visant à renforcer la sécurité internationale du cyberespace.

défense. C'est extrêmement important. En réalité, si tout le monde s'est mis d'accord pour dire que la souveraineté s'applique dans le cyberespace, personne n'est tout à fait au clair sur ce que cela veut dire réellement. C'est la grande difficulté !

Qu'est-ce que la souveraineté dans le cyberespace? Pour nos amis chinois et russes ce sont notamment les infrastructures, les réseaux et tout ce qui passe dedans, toutes les données alors que pour nos amis américains se sont les infrastructures, point ! Dans toutes les discussions internationales - on vient de sortir d'une longue série de négociations dans le cadre du G7 donc au niveau des chefs d'États, des ministres des Affaires étrangères et des ministres en charge du numérique - nos amis Américains n'ont cessé de pousser le concept de « *free flow of data* », de libre circulation des données auquel nous avons mis un holà pour privilégier le concept de « *free flow off information* », c'est-à-dire de transmission sans contrainte de l'information parce qu'évidemment derrière ce concept il y a un certain nombre d'intérêts économiques. Sans aller plus loin dans le débat parce que c'est un débat économique qu'il faut traiter en ayant les idées claires et les yeux ouverts, quelle est notre définition à nous Français de la souveraineté dans le domaine du cyberespace mais également dans le domaine du numérique? Je ne vais pas y répondre aujourd'hui parce qu'on n'est pas au clair. On ne veut certainement pas être assimilé à nos amis Russes et Chinois mais je viens de vous dire qu'un certain nombre de concepts poussés par les Américains étaient pour nous incommodes. La souveraineté dans le numérique c'est un objet qui est difficile à saisir mais en même temps vouloir l'imposer, c'est d'une certaine manière faire preuve de faiblesse. Les États, la France en particulier, n'ont pas à discuter de leur souveraineté dans le numérique. À partir du moment où on commence à le faire, cela veut dire qu'on a peur et que l'on essaye de mettre des tranchées là où il n'y a pas de raison d'en mettre. L'État est souverain. C'est vrai que dans nos réflexions, nous avons plutôt évolué vers le concept d'autonomie stratégique parce que nous le pensons un peu plus opératoire, un peu plus concret et parce qu'il nous ramène à l'idée qui est en réalité sous-jacente dans tout ce qu'à dit Guillaume POUPARD, l'Amiral COUSTILLIERE et le commissaire AVOINE, qui est que nous souhaitons, nous Français, avoir les capacités pour agir de manière autonome dans le cyberespace. Cela veut dire, en effet, développer une industrie, une expertise, des pratiques, des habitudes de travail qui font que nous saurons mieux nous défendre et mieux aider les autres parce que, dans le concept d'autonomie stratégique aussi, il y a la capacité que la France revendique et met en œuvre,

notamment à travers l'ANSSI mais aussi à travers certaines actions du ministère de l'Intérieur, du ministère de la défense et du ministère des Affaires étrangères. C'est ce que l'on appelle le « capacity building ». On peut limiter le concept à ces deux notions, on peut aller plus loin aussi mais à mon sens, ce qui la forge, c'est la nécessité d'être autonome sur les questions cyber et la capacité à aider les autres. C'est désormais une veille antienne mais le réseau est aussi sûr que son maillon le plus faible.

Général d'Armée (2S) Marc WATIN-AUGOUARD - CREOGN, co-organisateur du FIC

Isabelle VALENTINI, peut-être voulez-vous compléter cette réponse ?

Isabelle VALENTINI - Adjoint à l'Officier Général cyberdéfense, État-major des armées

Je rejoins ce que vient de dire David MARTINON. La difficulté du cyberespace dans la définition de la souveraineté, c'est que nous sommes situés dans une zone de brouillard, des zones grises où les États ne se définissent pas toujours en tant que tels. On cite la Chine, la Russie mais nous sommes aussi confrontés à des mercenaires, des corsaires, des groupes criminels qui agissent au nom des États et contre lesquels nous devons intervenir.

La capacité que nous avons au sein de l'union européenne ou de l'OTAN et de nos principaux partenaires européens, c'est bien sûr le partage d'informations sur la formation, le partage de compétences en vue de favoriser l'élaboration de normes, de règles, de lutte informatique défensive. En revanche, ce qui comporte toute la dimension offensive, d'attaque, de « *souveraineté à intervenir* », capacité à réagir quand nous sommes victimes d'attaques - je repense à TV5 MONDE et la coordination très efficace qu'il y a eu lieu entre nos différents services, notamment avec l'ANSSI - l'État, notre pays est totalement souverain mais cela implique également un partage des échanges avec nos principaux partenaires, je pense notamment aux Britanniques en Europe.

La souveraineté, c'est difficile dans une zone de brouillard où nos partenaires, nos adversaires, nos ennemis ne respectent pas les mêmes définitions conceptuelles, la même pratique et le même respect des règles internationales.

Guillaume TISSIER - Directeur général CEIS, co-organisateur du FIC

Peut-être pouvons-nous bénéficier de la vision du ministère de l'Intérieur sur cette question de l'Europe et de la cybersécurité ?

Commissaire divisionnaire Vincent AVOINE - Chargé de l'intérim du préfet chargé de la lutte contre les cybermenaces

Pour nous, sur de nombreux points très concrets, l'Europe de la cybersécurité est en marche. Évidemment, le dispositif de la directive NIS qu'a évoquée tout à l'heure Guillaume POUPARD étend ce qui

est fait en France et va créer autour des OIV tout un écosystème qui va se sécuriser progressivement. On le ressent au travers des interventions de la DGSI[21] ou des autres services de police ou de gendarmerie qui sont au contact des entreprises.

(21)Direction générale de la sécurité intérieure

Plus concrètement concernant l'Europe de la cybersécurité, j'évoquais précédemment les signalements qui permettent d'évacuer, de nettoyer le Net de contenus qui sont illicites. Il existe un dispositif qui est piloté en France par la sous-direction de la lutte contre la cybercriminalité au travers d'un office, c'est le dispositif PHAROS[22] qui reçoit les signalements et les exploite. Il faut savoir qu'au niveau européen, il y a pour des domaines un peu plus limités mais ô combien essentiels, l'équivalent qui a été mis en place à EUROPOL. Ce dispositif s'appelle Europol's Internet Referral Unit (EIRU).C'est une structure qui fait la même chose, qui s'attache avec les opérateurs à effacer les contenus illicites. Un exemple très concret de l'Europe de la cybersécurité: avant-hier matin, suite à ce qui s'est passé en France avec l'assassinat de deux policiers, il y a eu, vous le savez, sur Facebook, une diffusion d'éléments particulièrement odieux. Le travail a été fait en France par Facebook. La structure Europol dont je vous parlais s'est adressée immédiatement à la police judiciaire française pour lui demander s'il fallait relayer cette opération de nettoyage du Net.

(22) Plateforme d'Harmonisation, d'Analyse, de Recoupement et d'Orientation des Signalements

C'est très concret, je l'ai vécu en direct. C'est aussi, toujours dans ce domaine des contenus haineux, le forum de l'internet au niveau de l'union Européenne qui a adopté le 31 mai dernier un code de bonne conduite visant à aller dans le bon sens pour effacer tout ce qui est illicite. Un dernier point très spécifique à la cybercriminalité cette fois-ci et à la lutte qui est entreprise au niveau européen: il faut savoir qu'au niveau de l'union Européenne, il existe une structure d'évaluation des dispositifs en place dans de nombreux domaines, le groupe GENVAL[23] qui s'attache à vérifier que les choses sont plus ou moins bien faites dans les différents pays. Il y a eu une évaluation en France du dispositif de cybercriminalité et cette évaluation depuis qu'elle a été lancée en France s'est portée sur chacun des pays européens.

(23) Groupe "Questions générales, y compris l'évaluation". Il pour missions de prévenir la criminalité organisée et à lutter contre ce phénomène, d'évaluer les pratiques des États membres et déterminer si ceux-ci respectent les obligations internationales qui leur incombent dans le domaine de la répression et de la lutte contre la criminalité organisée.

Tous les pays européens passent par cette évaluation à l'issue de laquelle est produit un rapport qui souligne l'état du dispositif et qui met en exergue les bonnes pratiques. Les autres pays

européens peuvent retenir les observations faites par ce groupe GENVAL. Ce groupe a produit pour la France un rapport qui était, je dois dire, plutôt favorable et qui a fixé la barre assez haut. Depuis lors, les autres pays sont évalués à la lumière du dispositif français. Pour le ministère de l'Intérieur, l'Europe de la cybersécurité a une dimension très concrète.

Général d'Armée (2S) Marc WATIN-AUGOUARD - CREOGN, co-organisateur du FIC

On a parlé tout à l'heure de coopération entre les acteurs publics et les acteurs privés. La commission européenne au travers « DG CONNECT»[24] a lancé un appel à proposition pour un partenariat public-privé (PPP) en matière de cybersécurité. Quel est l'enjeu, quel est l'intérêt de ce PPP? David ou Guillaume peuvent-ils nous en parler ?

(24) Direction Générale des réseaux de communication, du contenu et des technologies (europa.digital-single-market)

(25) Horizon 2020 : portail français du programme européen pour la recherche et l'innovation (horizon2020)

Guillaume POUPARD - Directeur général de l'ANSSI

Ce PPP est une démarche que l'on soutient depuis le départ. Elle montre que les questions de cybersécurité, certaines de ces questions, peuvent être traitées au niveau européen, qu'elles doivent impliquer l'ensemble des acteurs privés notamment, que ce sujet de la cybersécurité, même s'il y a le mot sécurité dedans, se prête bien notamment à une utilisation des fonds de recherche et développement, H2020[25] et autres plans de financement pour ceux qui connaissent. L'idée simple qu'il y a derrière ce PPP, même si la mise en œuvre est bien évidemment beaucoup plus complexe, consiste à dire que pour être capable de « négocier » des crédits de R&D, de bien les orienter et utiliser tout cet argent de manière intelligente, on a besoin d'avoir une structure qui parle avec la DG CONNECT.

La première chose à faire est de créer une sorte d'assemblée, un groupement qui permette de parler avec la DG CONNECT et qui regroupe finalement tous les acteurs qui ont été cités jusque-là, des acteurs privés, des acteurs publics, des États. C'est là que c'est compliqué, probablement toujours un peu inquiétant quand on compare aux autres PPP qui ont pu être montés mais je suis plutôt confiant. A priori tout cela va être signé, de mémoire, le 5 juillet et nous permettra de continuer sous l'impulsion, notamment lancée par le commissaire OETTINGER. Il porte ces questions d'autonomie stratégique avec beaucoup d'énergie. Nous sommes complètement en phase avec lui pour développer tout cela. Le fait que l'Europe prenne la cybersécurité en main, c'est une démarche qui est très positive. Le règlement e-IDAS[26], c'est même encore le cas le plus extrême car c'est l'Europe qui nous aide à avancer. On a des coopérations qui peuvent être

officielles et d'autres qui sont beaucoup plus secrètes entre pays européens de manière à faire face à des menaces communes mais comme il l'a déjà été expliqué, c'est quelque chose qui marche et qui est une réalité aujourd'hui.

(26) Le Parlement européen et le Conseil de l'Union européenne ont adopté, le 23 juillet 2014, le règlement n° 910/2014/UE sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur, dit règlement « eIDAS ».

(27) TTIP (=Transatlantic Trade ans Investment Partnership) et TAFTA (=Transatlantic Free Trade Agreement) désignent le Traité de libre échange entre les Etats-Unis et l'Union Européenne

Aussi, je me dois de dire que l'Europe est également un risque pour la cybersécurité notamment dans le cadre des négociations des traités transatlantiques, des traités économiques qui, non pas dans la hiérarchie des normes mais dans la hiérarchie des règles, sont placés extrêmement hauts. Il faut être particulièrement vigilant à l'égard de tout ce qui peut être négocié dans le cadre des TTIP/TAFTA[27]. Tout cela est très compliqué mais complètement d'actualité, avec les risques de voir arriver par le haut des principes qui vont s'appliquer à nous au-delà même de nos lois nationales. Poser le principe du « free flow of data » comme principe nous pose un vrai problème. Considérer que toute entrave à la libre circulation des données est quelque part quelque chose d'inacceptable nous pose de vrais soucis parce que dans les données que l'on ne veut pas voir librement circuler, il y a bien entendu les données très sensibles concernant la sécurité de l'État. Celles-là, on arrivera toujours à les exclure du champ, mais il y a plein d'autres données sensibles et on serait bien en peine aujourd'hui je pense de faire une liste exhaustive, une liste blanche de toutes les données qui peuvent pâtir d' un tel « free flow of data » poussé à son extrême. Il y a beaucoup de débats autour de ce sujet pour justement refuser ce principe. Il est nécessaire que les États européens conservent une capacité à réglementer en termes de circulation des données, parce que toutes les données ne peuvent pas comme ça, par principe, se balader aux quatre coins de la planète.

L'autre risque qui est associé directement - et autour duquel tournent de vrais enjeux - c'est la question de la localisation des données. On a clairement envie de développer en France des datacenters, des capacités de stockage, de gestion de ces données. Nous considérons que, par définition, ces données ne doivent pas systématiquement traverser l'Atlantique. On a des enjeux qui sont probablement encore plus complexes, qui font le lien avec ce que je disais tout à l'heure, sur les qualifications de produits, notamment des produits de sécurité. Aujourd'hui, si l'on veut avoir confiance dans des produits et si on souhaite réellement jouer le jeu de l'ouverture vis-à-vis des différents partenaires (mais pas uniquement des partenaires Français) on

a besoin d'avoir accès par exemple aux codes sources. Une fois encore, pour savoir si ces produits sont bons ou pas bons, on ne peut pas simplement se contenter de regarder la boîte fermée. Il faut, à un moment, entrer dedans au moins pour les niveaux d'évaluation les plus élevés. Je ne vous cache pas qu'il y a un sujet conflictuel avec nos alliés qui sont contre ce principe. On ne voudrait surtout pas que ces négociations, économiques avant tout, soit l'occasion de cranter des principes qui vont directement contre les intérêts de la cybersécurité, pour l'État mais plus généralement pour les Nations, c'est-à-dire incluant autre chose que la sécurité purement nationale.

David MARTINON - Ambassadeur pour la cyberdiplomatie et l'économie numérique

Je voudrais aller un tout petit peu plus loin que Guillaume sur le sujet des données. En fait, on se rend compte que derrière tous les grands sujets de gouvernance internationale de l'Internet il y a toujours un moment où on en revient à la question des données. Dans ce qu'a dit Guillaume, il y a des choses très importantes et je voudrais rajouter quelques éléments parce qu'on est facilement caricaturé et on caricature facilement les autres.

Premièrement, quand nos amis américains disent qu'avec « le paquet protection des données » on fabrique du protectionnisme non tarifaire, c'est une blague. Le paquet est beaucoup plus intelligent et permet une circulation beaucoup plus fluide que ce qui était assuré auparavant.

Deuxièmement, ce n'est pas la protection européenne des données qui a empêché les grandes sociétés Américaines de créer le marché de la donnée et de le dominer. Par conséquent, si on faisait du protectionnisme, on le ferait vraiment très mal.

Troisièmement, je n'ai pas envie qu'on laisse caricaturer la France comme étant l'État le plus soucieux de sa souveraineté en Europe sur la question des données. Pour le moment, on n'a pas fait grand-chose en réalité sur ce sujet-là. Arrête-moi Guillaume si je me trompe, mais sur la localisation des données, on a encore rien dit, rien décidé, rien voté alors qu'un certain nombre de nos partenaires à travers le monde et notamment les alliés les plus proches des États-Unis comme l'Australie ou le Canada, ont fait adopter des lois qui exigent, qui imposent la localisation sur leur sol d'un certain nombre de données jugées sensibles et notamment les données de santé.

Quatrièmement, tout ce qu'a dit Guillaume est vrai. Si c'est important alors pourquoi ne l'a-t-on pas fait avant et qu'est-ce qu'on attend pour le faire ?

Cinquièmement, j'aimerais, moi, qu'il y ait une industrie française du Cloud et de l'hébergement de données. Elle existe car

il y a de belles sociétés en France comme OVH. Je veux rappeler qu'on a quand même fait des tentatives très largement subventionnées en France et en Europe pour bâtir des entreprises de Cloud souverains et que, pour le moment, ce n'est pas une grande réussite...

Guillaume TISSIER - Directeur Général de CEIS - co-organisateur du FIC

Pour revenir sur le sujet de la coopération européenne, on voit bien qu'on a aujourd'hui un certain nombre d'échanges d'information, d'exercices et de procédures qui sont mis en place. On est dans le « capacity building » mais au-delà du « capacity building », il y a tout ce qu'on appelle le « pooling and sharing », c'est-à-dire la mutualisation et le partage capacitaire. On voit bien que là c'est beaucoup plus compliqué puisqu'un certain nombre d'États, notamment les plus puissants, sont relativement hostiles. Faut-il par conséquent persévérer dans cette voie-là et si oui, comment ?

Guillaume POUPARD - Directeur général de l'ANSSI

C'est évidemment compliqué parce qu'au niveau national nous sommes en train d'apprendre en marchant. On essaye de marcher vite mais c'est compliqué. Un des éléments, qui est d'ailleurs dans la directive NIS, consiste à pointer du doigt le fait que beaucoup de pays européens n'ont pas pris la mesure et sont bien en peine pour la prendre parce que, pour des raisons de taille, de budget, de masse critique, tous les pays qui n'ont pas d'industries en propre ont du mal à le faire. On voit bien que c'est extrêmement complexe.

La solution, mais David l'a dit, c'est de fonctionner en réseau, faire du capacity building. Il est de notre intérêt, nous France, avec les autres pays européens qui ont commencé un tout petit peu plus tôt, de partager le savoir-faire. Il y a cependant des limites intrinsèques. Pour le partage de renseignement opérationnel notamment, au sens militaire du terme, sur des choses très précises comme « *untel vous attaque sur telle adresse IP* », cela avance mais c'est forcément prudent et forcément fait dans des cercles maîtrisés. Ce n'est pas quelque chose que l'on va faire sur la place publique et que l'on va faire à 28 parce qu'il s'agit de renseignement très sensible issu de sources, que très souvent, on ne voudra pas citer. Ce sont le plus souvent des sources du renseignement venant d'autres partenaires internationaux en dehors de l'Europe, des victimes en France ou à l'étranger chez qui on peut analyser les comportements d'un attaquant et en déduire de nombreuses informations. On n'aura pas envie de dire le nom de ces victimes. C'est notamment un des sujets sur lesquels on s'est battu dans le cadre de la directive NIS pour éviter toute forme d'obligation, de notification d'incidents à un niveau européen. Quand un OIV français se fait

attaquer, avec potentiellement des conséquences graves, on considère que c'est une question de sécurité nationale et pas une question qui doit être partagée au niveau européen. Tout cela pour dire que l'on va vers un fonctionnement en réseau par opposition à un fonctionnement qui serait centralisé ou décentralisé. Ce réseau serait purement européen parce que ça n'aurait pas de sens qu'il en soit autrement, avec un fonctionnement qui doit s'appuyer encore plus qu'aujourd'hui sur l'ENISA[28], l'agence européenne chargée de la sécurité des réseaux et de l'information et qui peut fortement contribuer au développement de tout ce qui est capacity building, mutualisation des moyens, partage de bonnes pratiques. D'ailleurs, le président du board de l'ENISA vient d'être renouvelé, c'est un français, Jean Baptiste DEMAISON, de l'ANSSI en l'occurrence, cela montre quelque part notre engagement dans cette démarche européenne.

(28) enisa.europa.eu

Nous sommes constamment en recherche d'un bon équilibre entre une meilleure prise en compte de ces questions de cybersécurité, en profitant de la taille critique européenne. Le fait que nos voisins sont vraiment nos voisins est pour le coup important : quand ils se font attaquer, on n'est pas loin de se faire attaquer nous-mêmes. Soyons clairs, il s'agit directement de la protection de notre souveraineté nationale.

Isabelle VALENTINI - Adjoint à l'Officier Général cyberdéfense, État-major des armées

En matière de cyberdéfense, nous menons, dans le cadre plus restreint d'un noyau dur de partenaires, des coopérations opérationnelles qui sont évidemment secrètes, en coalition, en cyber-coalition en particulier avec les États-Unis dans la lutte contre Daech. Nous participons également des coopérations dans d'autres domaines que les incidents eux-mêmes tels que les réseaux sociaux, le contre-discours, le contre narratif avec les États-Unis, le Royaume-Uni et d'autres pays encore. Nous recevons à l'instant même, le ministre de la défense suisse au centre opérationnel à Balard, le centre opérationnel de cyberdéfense. Il y a aussi des éléments de coopération très sensibles sur la lutte contre des « foreign fighters[29] ». En matière de discours, nous entretenons une coopération avec la Suisse, la Belgique et la Tunisie. Ce sont des éléments secrets mais qui sont très importants en matière d'échange d'informations et dans la lutte contre le cyberterrorisme ou dans le terrorisme de Daech.

(29) Les foreign fighters (littéralement les combattants étrangers) sont des individus qui s'engagent dans les groupes armés terroristes sur un territoire dont ils ne sont pas issus. Ce sont par exemple des Français ou des Britanniques combattant en Syrie. Susceptibles de revenir ensuite dans leur pays d'origine, ils constituent un sujet d'inquiétude en matière de sécurité intérieure.

Guillaume TISSIER - Directeur Général de CEIS - co-organisateur du FIC

Isabelle, peut-être un mot sur l'OTAN aussi? On a beaucoup parlé de l'Union Européenne mais quel rôle peut-être tenu par l'OTAN en matière de capacity building, en termes de mutualisation capacitaire également ?

Isabelle VALENTINI - Adjoint à l'Officier Général cyberdéfense, État-major des armées

L'OTAN a défini le cyberespace comme un cinquième domaine, un domaine de confrontation permettant, en coordination avec les Américains, les Britanniques, les Néerlandais, la France et un peu l'Estonie, via le centre d'excellence de Tallinn, de définir une posture en matière défensive. Bien sûr, la France est très réservée sur la partie offensive, comme les États-Unis et le Royaume-Uni. D'ailleurs, nous ne souhaitons pas que ces capacity building puissent aller au-delà du partage d'informations sur la formation ou la diffusion de compétences pour les pays qui sont entrain de se construire en matière de cybersécurité.

David MARTINON - Ambassadeur pour la cyberdiplomatie et l'économie numérique

C'est le dilemme habituel des États qui, contrairement aux autres, investissent beaucoup dans un domaine et n'ont pas envie de partager pour rien ces investissements. En matière de cybersécurité, à l'évidence, les Américains sont très loin devant nous. Quant aux Britanniques et aux Français, ils ont beaucoup fait et se sont considérablement améliorés. Nous n'avons pas forcément envie de partager, de mutualiser les capacités. En revanche, dans la logique de l'article 5 du traité de l'Atlantique Nord, il est évident que la France doit jouer son rôle comme les autres dans cette défense mutuelle.

La logique, ça serait plutôt de dire que nous allons mettre nos capacités au service de l'OTAN après avoir défini des objectifs. Ensuite, on se partage ces objectifs, on les atteint, mais on les atteint avec nos capacités nationales.

Général d'Armée (2S) Marc WATIN-AUGOUARD - CREOGN, co-organisateur du FIC

Nous allons passer maintenant, si vous le voulez bien, au reste du monde sous deux aspects. Le premier va concerner la gouvernance. David, tu avais la gentillesse, il y a deux ans, de venir présenter les enjeux relatifs à l'ICANN[30] et à sa réforme. On a vu que le résultat de Marrakech ne satisfait pas forcément le gouvernement français. Première question, peut-on s'accorder sur une gouvernance du cyberespace ? En matière de cybersécurité, c'est la deuxième question, on a beaucoup parlé de souveraineté. La cybersécurité ne nous conduit-elle pas à avoir une approche un peu égoïste dans la mesure où un accord international est assez difficile à mettre en œuvre ?

(30) enisa.europa.eu

David MARTINON - Ambassadeur pour la cyberdiplomatie et l'économie numérique

Sur la deuxième question d'abord, est-on proche d'un accord ou pas ? Ce qui est sûr, c'est que la communauté internationale, réunie au sommet mondial sur la société de l'information (SMSI) en marge de l'Assemblée générale des Nations Unies, en décembre 2015, a décidé qu'il n'y aurait pas d'ouverture d'une négociation globale d'un traité international sur l'Internet ou sur la cybersécurité ou sur la cybercriminalité, parce que c'est une impasse. On sait très bien qu'on n'avancera pas, qu'on va ré-ouvrir des sujets déjà traités sur lesquels nous sommes arrivés à des consensus et ce sera beaucoup de temps perdu pour un résultat à peu près nul. En revanche, cela ne veut pas dire qu'il ne se passe rien, puisque, comme je le disais tout à l'heure, le groupe des experts intergouvernementaux en est déjà à son quatrième rapport et va se réunir fin août à New York. Objectivement, il y a de vrais progrès, de vrais points d'accord, des compromis historiques, enfin historiques, il ne faut pas exagérer...mais il y a eu des points sur lesquels nos amis Chinois et Russes ont fait des concessions pour se mettre sur nos lignes. Il y a des ambiguïtés constructives qui permettent d'avancer, notamment sur la notion de souveraineté dans le domaine du cyberespace. La communauté internationale ou le GGE, qui représente une vingtaine de pays, a dit que la souveraineté internationale devait s'appliquer, que le droit international public s'appliquait totalement dans le cyberespace et qu'il fallait bâtir un certain nombre de normes de confiance qui ressemblent à ce que l'on retrouve dans les négociations internationales sur le désarmement mais avec des spécificités très forte. C'est probablement comme cela que l'on va pouvoir bâtir une sécurité collective dans le cyberespace. Nous espérons qu'il y aura encore des progrès mais ce n'est pas si simple. Il faut essayer de forger de nouveaux concepts parce qu'on se rend compte que certains des concepts habituels ne fonctionnent pas. La notion de dissuasion, qui est tellement opératoire dans le domaine du désarmement, est très difficile à utiliser dans le cyberespace, dans la cybersécurité. La notion de non-prolifération ou de contre-prolifération va être très peu opératoire dans le cyberespace, mais nous avons quand même un certain nombre d'idées sur lesquelles nous travaillons avec nos amis de la défense, de l'ANSSI, du ministère de l'Intérieur pour essayer d'avancer.

Quelles valeurs peuvent avoir ces accords, ces décisions ou ces compromis ? C'est un vrai sujet. Pour le moment, il y a un rapport qui est endossé, dont l'Assemblée générale prend note chaque année. On est dans la nuance de la nuance diplomatique, mais enfin, ce n'est pas rien, parce que d'une

certaine manière c'est endossé par la communauté internationale. Peut-on faire mieux ? On a fait un peu mieux, parce que le dernier communiqué du G20 a également endossé le dernier rapport du GGE. L'étape d'après, ce serait probablement que le Conseil de sécurité annonce pour plus tard, sur le fondement du rapport du GGE, un traité international. Mais je pense que ce n'est pas la bonne manière d'avancer. La bonne manière d'avancer pour le moment, c'est de travailler en un petit groupe d'États, petit groupe qui s'étend puisque l'on va passer de 20 à 25 cette année, avec des États pour la plupart très compétents en matière de cybersécurité, très avancés ou les plus avancés et en même temps manifestant une forme de diversité dans la représentation. C'est probablement comme cela que l'on peut avancer sérieusement et faire des progrès.

Sur la question de la gouvernance internationale de l'Internet, c'est un sujet à part entière. Pour faire court, je dirais que dans quelques semaines, si tu me reposes la question, je te répondrai qu'il est derrière nous. Il est derrière nous parce que la réforme de la ICANN a été forgée et acceptée par la communauté. Nous n'avons pas approuvé cette réforme au final mais nous avons décidé de ne pas bloquer la transmission de cette proposition au Département du commerce américain qui doit maintenant décider s'il accepte ou pas cette réforme[31]. Je dis « dans quelques semaines » parce qu'aujourd'hui le Congrès américain est saisi, il en débat. Ted CRUZ y est opposé depuis le début parce que, pour lui, cela consiste à donner l'Internet aux Russes et aux Chinois, c'est dit comme ça, avec cette finesse extraordinaire qu'on a toujours trouvée chez Ted CRUZ. Il fait une sorte de fillibustering [32], de guérilla législative pour essayer de faire voter une loi qui empêcherait l'exécutif américain de prendre seul la décision de renoncer à la tutelle du département du Commerce sur l'ICANN. Nos amis Américains nous ont toujours dit que ça devait être, c'était et ça resterait une décision de l'exécutif américain et donc qu'au final cette loi ne pourrait pas prospérer. On va voir. Je pense plutôt que c'est ce qui va se passer parce qu'on se rapproche du terme de l'administration OBAMA et que ça fait partie à l'évidence de la legacy de cette administration, de l'héritage politique et symbolique de cette administration. Je pense que la Maison Blanche, l'administration OBAMA et le Département du commerce actuel ne renonceront pas à mettre en œuvre cette transition. Le contrat qui lie le

(31) Le 10 mars 2016, Dr. Stephen D. Crocker, Président de l'ICANN, a remis au gouvernement américain un plan mis au point par la communauté Internet internationale (https://www.icann.org/)

(32) Terme américain employé pour parler d'obstruction parlementaire

(33)

département du commerce à l'ICANN expire au 30 septembre[33]. Je pense que cette date sera tenue. De tout de façon, si elle n'est pas tenue, il sera difficile de renouveler le contrat pour deux ou trois mois, voire de l'étendre jusqu'au 19 janvier 2017, veille du jour de l'investiture du prochain président américain. Je pense que le calendrier est contraint et je ne pense pas que cette administration y renoncera.

Est-ce que c'est une bonne réforme ? C'est une bonne réforme à 80%. Nous avons obtenu beaucoup de choses que nous avions demandées et sur lesquelles nous avons travaillé et fait des propositions pendant deux ans. Au final, je reste frustré parce que la prétention de cette communauté à vouloir donner la parole à toutes les parties prenantes, donc gouvernementales, non gouvernementales, académiques, techniques est en réalité une prétention très largement hypocrite. Au sortir de cette réforme, nous voyons bien que le rôle des États sera limité et que leur capacité à influer les décisions sera encore minorée.

Guillaume TISSIER - Directeur Général de CEIS - co-organisateur du FIC

David MARTINON une question sur le GGE ? Le GGE se réunit cet été. Il y a déjà un certain nombre de comportements responsables qui ont été définis. Va-t-on à un moment parler du contrôle de l'application de ces comportements ? Est-il question, par exemple, de réfléchir à une instance, à un organe qui contrôlerait l'application de ces comportements ?

David MARTINON - Ambassadeur pour la cyberdiplomatie et l'économie numérique

C'est la question centrale à mon sens. Si on veut contrôler et vérifier la pleine application à la fois des normes de droit international public dans le cyberespace et des normes de comportement volontaires que nous avons décidées et si on veut que se soit bien fait, que cela ait du sens, il faut qu'à un moment on soit capable de dire : « c'est untel qui est à l'origine de cette attaque ». C'est extrêmement difficile. On peut probablement aujourd'hui - arrête-moi Guillaume si je suis dans l'erreur - aller déchiffrer jusqu'à la dernière ligne de code d'une attaque en prenant le temps, c'est-à-dire que l'on peut trouver une ligne de code en farsi ou en cyrillique. Est-ce suffisant pour dire que telle attaque est perpétrée par les services Iraniens ou par des mercenaires Russes ? Je pense que l'intoxication reste possible. Les Américains nous disent que c'est extrêmement prometteur de bâtir une sécurité collective dans le cyberespace, dès lors qu'on est sûr de l'attribution et que cette question de l'attribution va être très vite réglée. Moi, je ne suis pas sûr et je serais ravi que Guillaume s'exprime sur ce sujet-là. Autant c'est prometteur, parce que une fois que vous être capable de

dire « *c'est untel qui a fait ça* », vous êtes capables de réengager un certain nombre de règles classiques, traditionnelles, coutumières du droit international public comme la légitime défense, les contre-mesures, le fait de diligenter des commissions d'enquête internationales qui vont être collégiales et qui vont être capables de confirmer l'origine de l'attaque. Il y a par conséquent un certain nombre de conséquences, de responsabilités internationales, qui sont engagées et cela peut déboucher sur des procédures en responsabilité pénale internationale. Tout cela est très prometteur. Mon sentiment est qu'il faut continuer de bâtir sur le principe d'attribution et, en même temps, il faut aussi le contourner parce que je crains que l'on ne soit pas capable d'attribuer avec une totale certitude.

Une réponse possible, c'est effectivement ce que vous avez évoqué dans votre question, serait peut-être de confier à une tierce partie le soin de déterminer l'attribution, de déterminer la culpabilité dans le cadre d'une attaque. Pour que cette autorité soit crédible, légitime et indépendante, il faut cependant mettre sur le papier un certain nombre de paramètres qui ne sont pas simples.

Il faut à l'évidence que ce soit collégial, que ce soient des personnes à la fois politiquement légitimes et d'un très haut niveau technique, venant du public et du privé et il faut que leur verdict soit respecté mais cela ne va pas vraiment de soi.

Guillaume POUPARD - Directeur général de l'ANSSI

Malheureusement, on bute constamment sur cet écueil qui est connu depuis l'origine. Il ne s'agit pas simplement de savoir qui a fait le coup. Très souvent, ne serait-ce qu'en regardant à qui cela profite, en regardant les multiples indices obtenus à droite et à gauche, on finit par avoir une bonne idée mais devant un juge ça ne tient pas 10 secondes. On observe récemment de plus en plus une démarche qui consiste, pour les services offensifs les plus performants, à ne plus attaquer en direct ou par les différents biais qu'on connaissait auparavant mais à attaquer les attaquants eux-mêmes dans d'autres pays, à passer par les infrastructures d'autres attaquants de manière à mener leurs propres attaques. En l'état actuel, c'est le crime de la technologie quasi parfait parce que quand bien même on se rendrait compte de l'attaque, quand bien même on arriverait à la comprendre et à la détricoter, on va tomber sur quelqu'un qui n'a certainement pas la conscience tranquille mais, qui de fait, n'est pas le véritable commanditaire ou celui qui est véritablement à la manœuvre. C'est extrêmement compliqué. Ce que je vous dis là, n'est pas du domaine des élucubrations puisque ça a été révélé par Edward SNOWDEN dans un des très nombreux documents. Cela fait partie de la doctrine et, en même temps, quand on y réfléchit, c'est assez logique de passer par ce type de moyens.

L'attribution restera toujours un problème. Quand bien même, en poussant la

logique jusqu'au bout, on utiliserait l'ensemble de nos capacités offensives, de nos capacités en matière de renseignement et qu'on arriverait par le biais de ces capacités à savoir précisément qui en est à l'origine, pour peu qu'on y arrive, nous n'aurions peut-être pas envie de dire comment on a fait pour avoir l'information. On va au final se retrouver dans la situation, que connaissent peut-être les Américains en ce moment, qui est de dire, « *moi, je sais qui c'est mais comme je ne peux pas vous dire comment je l'ai su, je suis coincé* ». Cela va être très compliqué et, si on continue à se heurter à ce problème d'attribution, cela va durer longtemps. Il faut donc réussir à le contourner pour être efficace.

Général d'Armée (2S) Marc WATIN-AUGOUARD - CREOGN, co-organisateur du FIC

Mes chers amis, l'heure est venue de conclure. Avant de nous séparer, avez-vous une idée, un point particulier que vous n'avez pas évoqué, que vous voudriez absolument transmettre à l'ensemble de nos amis ici présents, un point particulier qui vous tient à cœur ?

Commissaire divisionnaire Vincent AVOINE - Chargé de l'intérim du préfet chargé de la lutte contre les cybermenaces

Sous un angle policier, sous l'angle du ministère de l'Intérieur, je vais donner un signe d'espoir. Les États-Unis sont souvent cités, ils l'ont été par David MARTINON ou par Guillaume POUPARD. Moi je recense dans le traitement des sujets judiciaires, policiers, un réel désarroi américain et c'est là que je vois un réel signe d'espoir. Sur le sujet du chiffrement par exemple, qui n'a pas été évoqué en profondeur aujourd'hui, j'ai entendu dire que le FBI se sentait impuissant. Quand on est impuissant, on essaye de rebondir. J'imagine qu'il va y avoir des démarches collectives internationales sur ce sujet.

Autre point, j'ai eu connaissance d'un colloque organisé le 6 juin dernier par le département de la Justice américain, un peu en urgence, pour envisager les mécanismes internationaux de coopération rendus nécessaires à la fois par les différences de législation en matière de liberté d'expression et de transmission de données aux services de police et aussi en matière de chiffrement. Je me dis que pour que le département de la Justice américain soit perdu au point de recourir à la connaissance de ses partenaires internationaux, pour envisager des solutions, c'est qu'il y a un vrai souci. En même temps j'y vois un espoir puisqu'on va réellement vers une coopération internationale comme le disait David MARTINON. Je crois que cela avance s'agissant du traitement de la cybersécurité vu sous l'angle policier, judiciaire.

David MARTINON - Ambassadeur pour la cyberdiplomatie et l'économie numérique

Encore une fois je n'aime pas la caricature, je ne voudrais pas être caricaturé moi-même. J'ai beaucoup parlé des États-Unis, les États-Unis nous agacent parce qu'ils sont bien meilleurs

que nous en réalité. C'est essentiellement, comme l'a dit Guillaume, un problème transatlantique mais ne nous trompons pas, le danger le plus prégnant ne vient pas d'eux. Nous restons tout de même dans le même camp. En matière de défense, de renseignement nous dépendons énormément d'eux. Au sein du groupe des experts gouvernementaux, encore une fois, nos positions sont très largement les mêmes dans la négociation et ce que nous avons pu obtenir concernant la réglementation du proxy, c'est une idée que nous avons en partage avec les États-Unis. En écoutant Vincent Avoine, il faut dire une chose très simple, je ne voudrais pas être caricaturé en donnant le sentiment que je suis le diplomate français crispé derrière son absence de ligne Maginot par rapport aux États-Unis. Vraiment, ce n'est pas le cas. Par ailleurs, je crois fondamentalement à cette révolution numérique, même s'il faut encore monter en compétence. Pour la vivre pleinement, je suis convaincu qu'elle apporte un surcroît de bien-être, au sens économique du terme, à la collectivité mondiale.

Guillaume POUPARD - Directeur général de l'ANSSI

Je rebondis sur ce mot positif parce que, malheureusement, quand on parle de cybersécurité, on est constamment dans les choses très lourdes. On voit des problèmes partout, des menaces et des attaquants de partout. Je voudrais témoigner, mais je pense que ça a été grandement évoqué, du fait que notre modèle national, mais également quand il se tourne vers l'international, est un bon modèle, au moins en France. Je peux témoigner du fait que, dans des réunions qui peuvent être plus ou moins classifiées, la volonté de travailler ensemble est bien réelle et c'est suffisamment important pour être mentionné, parce que je ne suis pas certain que se soit systématiquement le cas dans tous les travaux interministériels. C'est un élément d'espoir qui d'ailleurs explique pourquoi la France se maintient dans ce cercle assez fermé des pays qui comptent dans le domaine de la cybersécurité, dont la voix est écoutée. Il faut impérativement qu'on reste dans ce premier cercle et qu'on continue à s'en donner les moyens. Je ne nie pas le fait qu'il y des questions compliquées à traiter, de tous ordres et que certaines questions, dont celle du chiffrement par exemple, sont complexes, mais fondamentalement, face à des questions complexes, on peut s'interroger sur l'efficacité d'une réponse triviale. Il faut être capable d'aller jusqu'au bout et de peser ce que l'on gagne et ce que l'on perd. La question autour du chiffrement, pour moi, n'en est pas une aujourd'hui. C'est un outil absolument indispensable pour protéger aussi bien nos infrastructures les plus critiques que les données de nos concitoyens. Comment fait-on pour éviter ou pour limiter le bénéficie que peuvent en retirer nos ennemis ? Mais encore une fois c'est une question qui est extrêmement complexe et qui ne pourra pas avoir de réponse triviale.

Isabelle VALENTINI - Adjoint à l'Officier Général cyberDéfense, État-major des armées

Guillaume tu viens de dire de tenir des propos que j'avais envie de prononcer. Les Français sont souvent pessimistes mais je trouve qu'en matière de cybersécurité, la coordination interministérielle avec notamment les quatre partenaires que nous constituons, se passe très bien. Elle est constructive face aux défis auxquels nous sommes confrontés, tant au plan national qu'international, y compris dans la guerre contre Daech. C'est exemplaire et souvent envié par un certain nombre de pays dont les États-Unis, qui ont beaucoup plus de difficultés intérieures avec les structures qui sont énormes et qui ont d'immenses capacités mais une complication politique que nous n'avons pas. Je trouve que c'est un élément qui mérite d'être valorisé.

Général d'Armée (2S) Marc WATIN-AUGOUARD - CREOGN, co-organisateur du FIC

Merci infiniment pour ces paroles pleines d'optimisme et porteuses d'espérance. Je voudrais avec Guillaume TISSIER, l'équipe FIC et avec toute l'équipe du CREOGN remercier nos cinq intervenants puisque l'amiral nous a quitté et vous dire que notre seul regret, c'est qu'il manque sur cette tribune l'autorité judiciaire. Malheureusement, Myriam QUEMENER, qui est une amicale complice depuis douze ans et pionnière de la lutte contre la cybercriminalité, ne pouvait pas être présente ce matin. Elle m'a demandé de bien vouloir l'excuser, mais nous avons une bonne nouvelle ! Nous avons une bonne nouvelle parce que la loi du 3 juin 2016 relative à la criminalité organisée, à la lutte contre le terrorisme et à son financement a créé une juridiction spécialisée nationale en matière de lutte contre les atteintes aux systèmes de traitement automatisé de données. Cette juridiction, qui sera au sein du Parquet de Paris va avoir un rôle moteur en matière de conduite de l'action judiciaire pour les infractions les plus importantes, les atteintes aux systèmes de traitement automatisé de données. Nous savons bien, maître DOUTRIAUX ici présente et avec qui nous travaillions hier sur des sujets relatifs à l'approche judiciaire de la loi GODFRAIN[34] peut en témoigner, que derrière les atteintes aux systèmes de traitement automatisé de données, on trouve de l'usurpation d'identité, de l'extorsion et bien d'autres infractions. Grâce à cette juridiction spécialisée due à l'initiative de François MOLINS, qui avait créé la section F1 au Parquet de Paris, nous allons avoir un porte-étendard de la justice.

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

Je vous annonce également, qu'en 2017, ici même, nous nous retrouverons pour un observatoire FIC et pour un atelier du CREOGN. Le thème portera sur « le monde judiciaire et le cyber ». Le monde judiciaire, les magistrats mais aussi les avocats ont bien sûr compris l'enjeu à la fois sur le plan civil que sur le plan pénal de la cybersécurité. Merci à vous.

DOSSIER

UNE SÉCURITÉ INTELLIGENTE POUR LES TECHNOLOGIES DU FUTUR

Le dispositif d'assistance aux victimes de cybermalveillance

par JÉROME NOTIN

« Le Gouvernement lancera un dispositif susceptible d'assister sur tout le territoire les victimes d'actes de cybermalveillance (particuliers, collectivités territoriales et entreprises de toute taille). Ce dispositif fournira, par exemple via une plate-forme numérique, un service d'assistance au dépôt de plainte et d'orientation vers des acteurs locaux susceptibles de fournir l'assistance technique la plus adaptée à la situation de la victime.[1] ». L'annonce a été faite lors de la présentation de la stratégie numérique du Gouvernement le 18 juin 2015. Les objectifs de ce dispositif ont par la suite été détaillés dans la Stratégie nationale pour la sécurité du numérique présentée le 16 octobre 2015 par le Premier ministre.

(1) Stratégie numérique du Gouvernement, 18 juin 2015

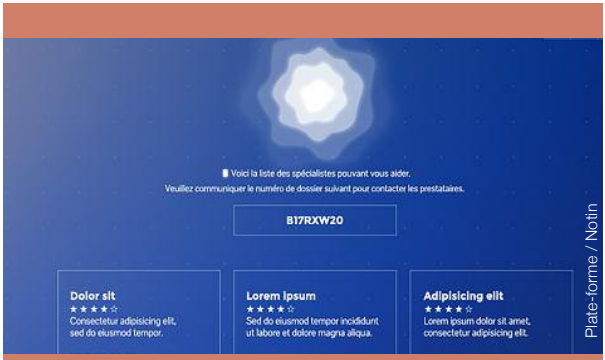
JÉROME NOTIN

Chef de projet
Dispositif d'assistance aux victimes d'actes de cybermalveillance
Agence nationale de la

Nous présentons à travers cet article les différentes missions confiées au dispositif et son organisation. Pour rappel de la stratégie nationale, il s'adressera aux particuliers, aux entreprises et aux collectivités qui ne sont pas supportés par l'Agence nationale de sécurité des systèmes d'information (ANSSI).

Une assistance de proximité

La première mission est de mettre en relation les victimes d'actes de cybermalveillance avec des prestataires référencés qui se seront engagés à travers la signature d'une charte. « *L'instauration d'un environnement de confiance pour les citoyens et pour les entreprises est essentielle au développement des usages du numérique et des échanges électroniques. Le Gouvernement œuvre donc pour la*



La plate-forme permettra un accès direct, intuitif qui donnera rapidement accès à un prestataire qualifié pour assister la victime.

définition d'un écosystème favorable au développement économique sans renoncer à la protection des données personnelles. »

Cet écosystème doit être le moins possible impacté par tout type d'acte de cybermalveillance. Le dispositif permettra donc à tout citoyen, entreprise ou collectivité d'être mis en relation avec des prestataires de proximité susceptibles de les assister dans la remédiation, après avoir été victime de cybermalveillance. Cette jonction sera réalisée à travers une plate-forme numérique qui accompagnera la victime dans la qualification de son incident et lui apportera la réponse adaptée. Elle a donc vocation à devenir le point d'entrée unique pour tous les actes de cybermalveillance. Cette réponse pourra également être un renvoi vers des services existants comme la plate-forme de signalement des contenus illicites de l'Internet (Pharos)[2] pour une déclaration de contenu web illégal ou l'affichage d'une liste de prestataires. Toujours dans l'esprit d'assistance de la victime, la plate-forme accompagnera la victime dans ses démarches du dépôt de plainte et les prestataires seront par ailleurs évalués.

(2) https://www.internet-signalement.gouv.fr/

La sensibilisation du public

La seconde mission du dispositif est la sensibilisation du public aux bonnes pratiques en matière de sécurité informatique et aux enjeux de la protection de la vie privée numérique. « *La sensibilisation de tous est un préalable nécessaire pour que les élus, les dirigeants d'administrations ou d'entreprises puissent prendre en compte le « risque cyber » à son juste niveau et décider des mesures susceptibles de protéger les citoyens qu'ils représentent ou les organismes qu'ils dirigent face à des menaces de vol d'informations ou de propriété intellectuelle, d'atteinte aux données personnelles, voire l'exposition à des ruptures d'activité, d'accidents de production, avec des impacts technologiques ou environnementaux auxquels ils sont potentiellement exposés.* [3]»

(3) Stratégie nationale pour la sécurité du numérique - https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_fr.pdf

Le dispositif développera ainsi des campagnes de prévention nationale sur les sujets liés au numérique, avec comme ambition de réaliser des campagnes sur le modèle de la sécurité routière. Elles permettront ainsi

aux citoyens d'être mieux préparés aux risques numériques. En parallèle des opérations de sensibilisation réalisées directement par le dispositif, ce dernier pourra approuver les campagnes mises en place par des tiers (entreprises, organisations professionnelles …). Cela permettra de fédérer les actions de sensibilisation proposées par les tiers et de s'assurer de la qualité du message délivré.

Observatoire/alerte/prospective

La troisième mission est de mettre en place un observatoire de la menace numérique pour mieux l'anticiper.

« *Les travaux interministériels menés à l'initiative du ministère de l'intérieur depuis 2013 ont conduit au constat qu'il n'existe pas aujourd'hui de statistiques fiables relatives spécifiquement à la délinquance ou à la criminalité informatique, la plupart des infractions concernées étant enregistrées sous une appellation qui ne rend pas compte de cette dimension, aujourd'hui absente des référentiels utilisés. L'absence de telles statistiques est préjudiciable à la conception par les pouvoirs publics de politiques constamment réévaluées et à la mise en place des moyens adaptés.*[4] »

(4) Stratégie nationale pour la sécurité du numérique - https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_fr.pdf

Au-delà des statistiques sur les infractions relevées, cet observatoire offrira une vue réelle et consolidée de la menace numérique afin de mieux l'anticiper. En effet, les seules statistiques disponibles sur le périmètre cible du dispositif (particuliers, entreprises et administrations qui ne sont pas supportées par l'ANSSI) sont fournies par des entreprises qui sont le plus fréquemment des éditeurs de solutions de sécurité et bien souvent d'origine étrangère. La question de la neutralité peut alors se poser au regard des objectifs commerciaux de ces entités. La disponibilité pour le pouvoir politique et la société civile d'une cartographie neutre et d'analyses prospectives permettra une meilleure appréhension de cette menace numérique et donc une meilleure prise de décisions par le pouvoir politique et tous les acteurs impliqués.

En lien avec le premier l'objectif, la plate-forme permettra donc de remonter des éléments d'information sur les incidents informatiques portés à la connaissance des différents prestataires participants. Ces informations seront analysées pour informer et alerter les autorités et le public sur l'état de la menace.

Le véhicule : GIP

Là encore, la Stratégie nationale pour la sécurité du numérique indique clairement : « *Le dispositif adoptera une forme juridique et une organisation lui permettant de bénéficier de l'apport des acteurs économiques du secteur de la cybersécurité — éditeurs de logiciels, plates-formes numériques, fournisseurs de solutions* ». La mission du dispositif est d'assurer l'activité, d'intérêt général, de porter assistance aux victimes d'actes de cybermalveillance. L'ANSSI, qui porte le projet en collaboration avec le ministère de l'Intérieur, a retenu la forme juridique du groupement d'intérêt public (GIP). Il

La fédération des actions de sensibilisation permettra de limiter les atteintes à des victimes qui cernent mal leur intégration dans une écosphère mondialisée et porteuse de vulnérabilités.

dispose d'une autonomie de gestion sur le plan opérationnel tout en restant sous le contrôle de l'État et permet en effet de réunir les talents des acteurs publics et privés.

Afin d'administrer le GIP, le groupe de travail préfigurateur du dispositif a prévu la constitution de 4 collèges. Le premier collège devrait réunir les acteurs publics que sont l'ANSSI , rattachée au Secrétaire général à la défense et à la sécurité nationale, les ministères de la justice, de l'intérieur et des finances. Ce collège disposera de la majorité des voix, conformément à la législation qui demande que l'État soit majoritaire dans les organes de gouvernance. Le deuxième collège réunira des représentants des utilisateurs, comme par exemple des associations de consommateurs. Le troisième collège sera composé d'organisations professionnelles représentant les prestataires qui vont intervenir chez les victimes afin de remédier à l'incident de cybermalveillance. Enfin, le quatrième collège réunira les offreurs de solutions. Il sera donc composé d'éditeurs de solutions de sécurité, d'équipementiers réseaux, d'opérateurs télécom ou encore d'organisations professionnelles représentant des acteurs susceptibles d'intervenir d'une manière assez large dans les domaines de la lutte contre la cybermalveillance.

Conscient du développement de la cybermalveillance pour l'ensemble des acteurs de la société, l'État, et en particulier l'ANSSI et le ministère de l'intérieur, s'est massivement investi dans la mise en place de ce dispositif qui verra le jour en 2017. Une phase expérimentale sera lancée dans la Région Hauts-de France. Son succès reposera sur la mobilisation des prestataires tout comme celle des acteurs étatiques, en particulier en régions. La Gendarmerie Nationale, grâce à son expertise dans l'assistance aux victimes d'une manière générale et sa place au sein de notre Nation, jouera un rôle fondamental dans la réussite de notre dispositif. Chaque personnel sera ainsi le relais du dispositif sur notre territoire.

L'AUTEUR

Jérôme Notin a rejoint l'ANSSI, en mai 2016, en qualité de Chef de projet – préfigurateur du dispositif. Il est impliqué dans la SSI depuis de nombreuses années et dispose d'expériences dans la création et direction d'entreprise. Il est par ailleurs ancien gendarme auxiliaire (94/10 PSIG de Blois) et fait partie de la réserve citoyenne cyberdéfense de la gendarmerie.

PHAROS : agir contre les contenus illicites de l'Internet

par **FRANÇOIS-XAVIER MASSON**

Hébergé au sein de la plateforme de signalement PHAROS[1] depuis 2009, le site www.internet-signalement.gouv.fr mis en place par la DCPJ pour signaler les contenus illicites publics présents sur Internet est l'exemple même du phare qui guide les internautes au cours de leur navigation sur l'océan numérique. Il rappelle que le cyberespace, espace de liberté, n'en est pas pour autant une zone de non-droit. Le dispositif PHAROS incarne une nouvelle vision de la police judiciaire, tournée vers le public et vers le secteur privé, à la fois outil de prévention et d'investigation. Modèle innovant, véritable catalyseur d'énergies, il canalise l'information, en rationalise le traitement et démultiplie le bénéfice de son action par son positionnement au sein de la sous-direction de la lutte contre la cybercriminalité.

(1) Plateforme d'Harmonisation, d'Analyse, de Recoupement et d'Orientation des Signalements

FRANÇOIS-XAVIER MASSON

Chef de l'office central de lutte contre la criminalité liée aux technologies de l'information

La cybercriminalité évolue au rythme de la transformation des réseaux et des équipements. Elle impose aux forces de sécurité intérieure l'adaptation constante de leurs structures et de leurs méthodes. Depuis les années 1990, les pouvoirs publics ont ainsi progressivement pris conscience de la nécessité de répondre de manière innovante aux nouvelles problématiques posées par Internet.

La première d'entre elles est celle de la « territorialité judiciaire ». Quand un délit est commis sur Internet, il l'est en tout lieu du territoire. Même si les contenus illicites, pour la plupart, ne font pas de victime directe, tout service de police ou de gendarmerie, ou toute institution chargée de lutter contre la délinquance du web, est

La plateforme Pharos évite les redondances des enquêtes et concourt à la pertinence des suites judiciaires à donner aux renseignements centralisés.

susceptible de prendre l'initiative d'une enquête. Au début des années 2000, alors qu'il n'existait pas encore de structure de coordination, il était fréquent qu'un hébergeur reçoive jusqu'à 10 réquisitions judiciaires pour le même contenu. Tout autant que ces conflits de compétence « positifs », les conflits négatifs laissaient en friche des pans entiers de la lutte contre la cybercriminalité. C'est la raison pour laquelle, le 13 avril 2005, lors de la présentation des conclusions du « chantier cybercriminalité », le ministre de l'intérieur annonçait « *la mise en place d'un centre national de signalement, afin d'éviter qu'une même information consultée par une multitude d'internautes ne génère une démultiplication des plaintes et des signalements […]* ». Composée à parité de policiers et de gendarmes, cette plateforme était placée auprès de l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC). Elle commençait son activité le 1er septembre 2006 à Nanterre avec deux premiers enquêteurs placés sous le commandement d'un chef de projet. Deux ans, plus tard, le dispositif était pleinement opérationnel et le site www.internet-signalement.gouv.fr était officiellement ouvert au public le 6 janvier 2009. La plateforme prenait une nouvelle dimension dans le cadre de la création de la Sous-direction de la lutte contre la cybercriminalité (SDLC), par arrêté du 29 avril 2014, dans un contexte de mobilisation généralisée des institutions publiques face aux défis de la cybercriminalité. Dans la foulée des attentats des 7 et 8 janvier 2015, PHAROS se retrouvait projeté au cœur du dispositif de réponse étatique à la menace terroriste par la mobilisation totale de ses ressources en matériel et personnel.

Une prise en compte des attentes des internautes

Le site de signalement et la plateforme PHAROS (du nom de l'île qui pendant près de dix-sept siècles porta le phare d'Alexandrie) ont d'abord valeur de symbole. Ils marquent la présence de l'État sur Internet et rappellent que cet espace de liberté n'est pas une zone de non-droit. PHAROS se veut ainsi un repère pour les internautes qui au cours de leur navigation numérique, peuvent se retrouver désemparés face à des contenus ou des comportements illicites. Le caractère massif des signalements reçus dans la continuité des attentats de janvier 2015 l'a bien montré. Dispositif reposant en grande partie sur des actions de communication et de partenariat, PHAROS est rapidement devenu un acteur incontournable et reconnu de l'Internet

français, tant dans son environnement judiciaire que parmi les acteurs privés (hébergeurs, associations, *etc.*). La plateforme répond en effet aux attentes des nombreux professionnels de l'Internet qui ont besoin d'un interlocuteur central lorsqu'ils sont confrontés à des contenus ou à des comportements qui brisent la confiance des internautes dans l'économie numérique. Ces partenaires représentent aujourd'hui la diversité des acteurs du Web : hébergeurs de contenus et fournisseurs d'accès à Internet (Orange, SFR, Free, OVH…), réseaux sociaux (Facebook, Twitter…), fournisseurs de services divers (Vivastreet, Le Bon Coin, Dailymotion...), acteurs américains majeurs (Microsoft, Google, Apple...), associations (LICRA, E-Enfance…) et acteurs institutionnels (Commission Nationale de l'Informatique et des Libertés…). Tous ont aujourd'hui identifié PHAROS comme leur interlocuteur naturel pour la problématique du signalement de contenus illicites de l'Internet.

Rationalisation et transversalité

D'un point de vue plus opérationnel, la raison d'être du dispositif PHAROS est de prévenir la redondance du traitement des contenus illicites de l'Internet. La plateforme est un point de convergence de l'information qui rationalise l'action des services d'enquête dans leur lutte contre la cybercriminalité. L'existence d'un pôle central, clairement identifié et directement accessible en ligne, optimise la transmission des informations dans des délais compatibles avec la courte durée de vie des éléments constitutifs des infractions sur Internet et des éléments permettant l'identification de leurs auteurs.

La compétence matérielle de la plateforme n'est pas limitative. Elle englobe toutes les formes d'activités illicites constatables en ligne : pornographie enfantine, incitation à la haine raciale, proxénétisme, diffusion de procédés permettant la fabrication d'engins explosifs, escroqueries, apologie du terrorisme, *etc.*

Trois grandes catégories se détachent cependant : les escroqueries et extorsions, phénomène de masse qui a toujours constitué près de la moitié des signalements chaque année ; les atteintes sur les mineurs, qui englobent principalement la pédopornographie (véhiculée par des moyens techniques permettant une démultiplication de leur impact sur les internautes), mais également la prédation sexuelle de mineurs en ligne ; les discriminations et autres délits de presse (incitation à la haine, contestation de crimes contre l'humanité, *etc.*).

Cette compétence transversale distingue PHAROS des plateformes mises en place à l'étranger, dont l'action est souvent restreinte à des champs limités de la cybercriminalité : escroqueries, pédopornographie, terrorisme, contrefaçons, *etc.* Le choix français permet de démultiplier l'impact de ses moyens, de son réseau partenarial et de l'expertise de ses enquêteurs, tout en définissant une méthodologie commune à tous les champs de son activité. Le dispositif se veut en outre réactif. Une circulaire interministérielle en date du 19 juillet 2013 prévoit ainsi la transmission directe des procédures judiciaires aux services territorialement compétents pour poursuivre les investigations initiées par PHAROS, à charge pour eux d'en informer

leurs parquets et recevoir les instructions relatives à la conduite de l'enquête. Ce formalisme simplifié permet une transmission rapide des dossiers, adaptée à la courte durée de vie des traces informatiques. Un protocole de compétences associe à chaque infraction susceptible d'être signalée le type de service auquel la plateforme peut adresser ses signalements, au sein de la police nationale, de la gendarmerie nationale, de la direction générale de la sécurité intérieure (DGSI), des douanes et de la direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF).

Une dynamique en mouvement

De 2006 à 2008, la plateforme PHAROS a essentiellement pris en compte les signalements de contenus pédopornographiques qui lui parvenaient par le site www.internet-mineurs.gouv.fr. Le doublement, dans l'intervalle, du nombre de signalements fut la résultante du travail réalisé auprès des acteurs professionnels de l'Internet qui exploitèrent rapidement et relayèrent l'existence du nouveau dispositif très attendu, avant même la campagne de communication publique de 2009. Celle-ci atteignit son objectif : en un an, le nombre de signalements quintupla. L'ouverture du dispositif à toutes les infractions et la focalisation de la campagne de communication sur une délinquance de masse – les escroqueries – entraînèrent une explosion des signalements. De 2009 à 2014, le nombre de signalements fut presque multiplié par trois. La réponse du ministère de l'Intérieur en termes de moyens humains se devait d'être à la hauteur des attentes du public. En 2008, les effectifs de la plateforme étaient portés à 8 enquêteurs (4 policiers et 4 gendarmes). Basées sur une évaluation empirique du flux des signalements, ces ressources se révélaient rapidement insuffisantes. À ce jour, la plateforme compte 16 policiers et 6 gendarmes.

Les enquêteurs de la plateforme PHAROS sont recrutés parmi des personnels motivés et intéressés par la matière informatique. Mais plus que de compétences techniques de pointe, ils doivent percevoir le Web, les réseaux sociaux et les outils de partage de contenus comme leur environnement naturel. L'âge moyen des enquêteurs de PHAROS est de 34 ans. Avec plus de 3 600 signalements par semaine à traiter en 2015, le travail d'évaluation et le volume des flux réclament rigueur, organisation et une bonne aptitude au travail en équipe. Une importante disponibilité est également nécessaire pour répondre aux pics d'activité souvent brutaux survenant lors d'évènements de portée nationale (attentats terroristes, fausses alertes à la bombe dans les lycées, événements sportifs majeurs comme l'Euro de football en juin 2016…).

Les policiers et gendarmes de PHAROS sont par ailleurs soumis à une forte pression psychologique, tenant à la nature des contenus auxquels ils sont exposés au quotidien : pédopornographie, violence extrême, discours extrémistes, etc. La répétition des images, autant que leur caractère choquant, est un facteur de stress potentiel. Les symptômes de l'usure psychologique peuvent apparaître plusieurs mois, voire plusieurs années après la prise de

fonction des personnels, qui sont régulièrement suivis par les psychologues du Service de soutien psychologique opérationnel (SSPO) de la DRCPN.

Autre critère de recrutement, la mixité police-gendarmerie des effectifs de la plateforme constitue une condition importante de son efficacité. La circulaire du 19 juillet 2013 précise que la plateforme « […] *est dirigée en alternance par un fonctionnaire de police nationale ou par un militaire de la gendarmerie nationale. Elle est composée à parité de policiers et de gendarmes, et a vocation à intégrer des fonctionnaires des autres administrations concernées par le dispositif.* »

Centraliser pour prévenir la redondance de l'action et assurer l'efficacité de la réponse

La plus-value apportée par le dispositif PHAROS repose sur sa capacité à centraliser les sources des signalements de contenus illicites de l'Internet pour assurer la pertinence de ses recoupements : internautes, au travers du portail internet public, fournisseurs de services sur internet et services étatiques y participent activement.

Les signalements reçus du public par PHAROS peuvent fortuitement concerner des contenus détectés par ailleurs par des services de sécurité intérieure, au cours d'activités de veille ou d'enquêtes judiciaires. La circulaire interministérielle du 19 juillet 2013 oblige l'ensemble des services à « *signaler les contenus et comportements illicites relevés au cours de leurs investigations* ». Dans une matière où les critères de compétence territoriale ne sont pas immédiatement apparents, les consultations de la base PHAROS permettent de prévenir les enquêtes redondantes et d'effectuer des rapprochements judiciaires. L'application inclut aujourd'hui un moteur de recherche qui permet à tous les services de police ou de gendarmerie de vérifier la présence en base de mots-clés correspondant à des identifiants de l'Internet. En cas de recoupement, l'application précise les suites qui ont été données aux signalements déjà reçus.

Les dernières évolutions : la lutte contre les discriminations, la veille et le blocage administratif des sites à caractère terroriste ou pédopornographique

La lutte contre la xénophobie a pris, depuis les attentats de janvier 2015, une nouvelle dimension, tant la prolifération de la haine et des discriminations sur Internet a semblé se banaliser jusqu'à représenter 30% du nombre total des signalements. Une cellule spécialisée de 4 enquêteurs a donc été installée au sein de la plateforme PHAROS en septembre 2015. Elle dispose d'une expertise juridique spécifique, doublée d'une connaissance approfondie des vecteurs de diffusion des contenus haineux. Le caractère transversal des activités de la plateforme PHAROS et le nombre important de signalements traités au quotidien donnent à ses enquêteurs un point de vue privilégié sur le fonctionnement du « web ». La diversité des signalements reçus par la plateforme et ses contacts privilégiés avec les fournisseurs de services communautaires sur Internet (Facebook, Dailymotion, *etc.*) lui permettent

d'orienter ses recherches sur des sujets précis, en fonction des objectifs du service. Les signalements qui parviennent à PHAROS sont de puissants indicateurs des nouvelles tendances de communication, des sujets, des réflexions ou des humeurs les plus largement répandus sur Internet… autant de phénomènes qui permettent par la suite de mieux cibler les actions de veille. Les enquêteurs de PHAROS sont ainsi en mesure de focaliser leur veille sur des thématiques précises pour compléter le traitement d'un signalement, anticiper un événement ou assister un service d'investigation. C'est par exemple le cas lorsqu'il s'agit de retrouver des contenus diffusés par les médias qui, bien que non encore signalés sur la plateforme, vont impacter le travail des enquêteurs sur une affaire judiciaire donnée ou sur un événement d'ordre public. La création d'un pôle de veille Internet pérenne, directement rattaché à PHAROS, est aujourd'hui à l'étude pour systématiser les actions de ce type, en s'appuyant sur des outils adaptés dont la plateforme se dote progressivement.

Enfin, depuis la loi du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme, l'OCLCTIC a été désigné autorité administrative, sous le contrôle de la CNIL, chargée de mettre en œuvre les mesures de blocage et de déréférencement des sites internet à caractère pédopornographique ou faisant l'apologie du terrorisme voire concourant à sa provocation. Seule entité disposant en temps réel, avec le Centre de lutte contre les criminalités numériques (C3N), d'une vision large des contenus illicites du Web et de l'expertise technique requise, la plateforme PHAROS a naturellement été chargée de la mise en œuvre du dispositif dont les décrets d'application ont été publiés en février et mars 2015. Le but de la procédure de blocage/déréférencement est de protéger la très grande majorité des internautes. Si le blocage peut paraître inefficace pour des pédophiles ou des activistes aguerris aux nouvelles technologies, il joue en revanche pleinement son rôle dans les autres cas en empêchant les internautes d'aboutir à des connexions non souhaitées ou à des contenus choquants ou violents au hasard des navigations et des liens proposés. Ce fut par exemple le cas pour tous les événements terroristes qui touchèrent la France entre novembre 2015 et juillet 2016. L'existence de ce dispositif et la réactivité des enquêteurs de PHAROS dédiés à cette mission ont largement contribué à contrecarrer la politique de terreur de DAECH qui visait à inonder l'Internet français de ses vidéos de propagande et d'exécutions.

L'AUTEUR

Le commissaire divisionnaire François-Xavier MASSON est chef de l'Office Central de Lutte contre la Criminalité liée aux technologies de l'Information et de la Communication (OCLCTIC) de la DCPJ depuis septembre 2015. Diplômé de l'ENSP en 1996 (46ème promotion), il a toujours dirigé des services d'investigation tant au sein de la Direction Centrale de la Police Judiciaire (chef de la section criminelle de la DIPJ Lille de 2000 à 2006) qu'au sein de la Direction Centrale de la Sécurité Publique (chef de la Sûreté Départementale des Yvelines de 2008 à 2012). Avant de rejoindre l'OCLCTIC, il était à la tête du Service d'Information de Renseignement et d'Analyse Stratégique sur la Criminalité Organisée (SIRASCO) de 2012 à 2015.

Les périphériques USB en entreprise : les précautions à prendre

par LUDOVIC HAYE

Les périphériques USB, notamment les clés, ont la cote… c'est indubitable. Qui n'utilise pas ces objets pratiques et simples d'utilisation, aux formes et couleurs variées (ce qui en fait un support publicitaire de choix), pour transporter ses données personnelles et professionnelles ? Ce que l'on sait moins, c'est qu'ils constituent une des causes de contagion virale numérique les plus importantes en entreprises …

Un support de contamination important

Peu onéreux, légers, miniaturisés, d'une capacité et d'une vitesse de transfert toujours plus importantes, les supports amovibles USB (Universal Serial Bus), que l'on appelle plus communément périphériques USB, ont non seulement envahi notre vie privée (photos, musiques, jeux, vidéos, *etc.*), mais également notre vie professionnelle (présentations, compte rendu, softwares *etc.*)

LUDOVIC HAYE

Expert IT en systèmes ERP (SAP)
Chef d'escadron de la réserve citoyenne

Ces supports de données amovibles permettent très aisément de transférer des fichiers d'un ordinateur à un autre en échappant totalement à la surveillance des réseaux. Ce cheminement de PC en PC peut cependant s'avérer problématique en termes de vols de données et d'inoculations de virus. Il permet également l'installation rapide de logiciels illicites ou sans licence, mettant ainsi l'entreprise dans l'illégalité. Si la facilité d'utilisation et la rapidité furtive des clés USB constituent un avantage indéniable, les entreprises doivent cependant prendre conscience du danger qu'elles peuvent représenter et par conséquent prendre certaines dispositions en mettant notamment en place une charte de bonne utilisation des clés USB.

Les chiffres sont éloquents

Ludovic Haye

La miniaturisation, l'augmentation de capacité des clés USB, associées au phénomène de BYOD (Bring Your Own Device), en font un vecteur critique en matière de sécurité des systèmes informatiques d'une entreprise.

Plus du 1/3 des entreprises demandent à leurs employés de ne pas utiliser de clés personnelles sur le lieu de travail mais rien n'est fait pour s'en assurer. Plus de la moitié des entreprises de plus de 200 salariés ne prend aucune mesure pour sécuriser les clés et ne contrôle ni leur usage ni leur accès (Source Clusif). Il apparaît que plus de 70 % des salariés français utilisent des clés provenant de l'extérieur de l'entreprise. Enfin, une étude, réalisée sur 600 millions de systèmes informatiques, révèle que 26 % des infections du système d'exploitation ont été propagées par une clé USB utilisant la fonction AUTORUN (lancement automatique à la connexion de la clé) (Source Windows).

On relèvera aussi que plus simplement les 2/3 des personnes interrogées avouent avoir déjà perdu une ou plusieurs clés contenant des données personnelles, par inattention ou par négligence. À titre anecdotique, rien que dans une ville comme Londres, près de 10 000 clés ont été retrouvées dans des pressings en un an et près de 9 000 dans les taxis, ce qui représente une perte de plus de 10 To de données...

Quels sont exactement les risques auxquels les entreprises s'exposent ?

La propagation des virus

Les risques sont bien réels et sans tomber dans une paranoïa contre-productive nous aurions tort de les sous-estimer. Dès lors que la clé est connectée à un PC hôte, elle peut infecter ce dernier si une vérification n'a pas été faite au préalable. Inversement, la clé peut se voir infectée par son hôte ; elle joue alors sans le savoir le rôle du vecteur de propagation au gré de ses différentes connexions futures, ce qui en fait la cause principale d'infection numérique en entreprise.

Le vol

Le contenu de la clé peut également faire l'objet de convoitise, notamment lorsqu'il s'agit de travaux de recherche, de brevets, de données médicales ou financières, etc. Sa taille la rend très facile à subtiliser et si sa valeur intrinsèque n'est pas très importante, le vol de son contenu peut, lui, être très préjudiciable. C'est la raison pour laquelle bien souvent, seul le contenu de la clé est intégralement copié de manière silencieuse à l'insu de son propriétaire par le PC sur lequel elle est connectée (ce que l'on appelle le PodSlurping), d'où l'utilité de crypter systématiquement son contenu.

L'oubli, la perte

Dans la grande majorité des cas, il n'y a pas de vol caractérisé mais tout simplement une perte ou un oubli de la clé sur le PC hôte par son propriétaire. De même sa taille, toujours

plus petite, facilite grandement sa perte. L'on peut même parfois lire de manière un peu provocante : « *qu'elle est faite pour être perdue* ». En effet, si le contenu est régulièrement sauvegardé mais surtout crypté (c'est-à-dire illisible pour toute autre personne que le propriétaire), les conséquences de la perte s'en trouvent grandement minimisées.

Ces risques étant identifiés et appréhendés, les principales causes de délits liés à des périphériques USB sont bien souvent motivées par de la malveillance interne (salarié mécontent), externe (vol par un concurrent, espionnage etc.) et par la négligence ou la méconnaissance de certains salariés, qui agissent comme un catalyseur de la propagation virale (alors que paradoxalement l'on croit tout savoir sur ces petits objets).

Les solutions existent dans le cadre d'une politique partagée au sein de l'entreprise

Il existe pourtant des solutions peu onéreuses et faciles à mettre en œuvre par les entreprises. La première chose à faire est de bien sensibiliser le personnel aux risques qu'ils font prendre à l'entreprise et ceux auxquels ils s'exposent eux-mêmes. La nomination et la formation d'un RSSI (Responsable Sécurité des Systèmes d'Information) sont indispensables pour bien prendre en compte les problèmes de sécurité actuels et anticiper ceux de demain. Ce responsable peut être amené à faire appliquer et évoluer une charte de bonne utilisation des périphériques USB en entreprise dont les points essentiels seraient les suivants :

• Veiller à ne pas laisser les clés sans surveillance, *a fortiori* celles connectées à un ordinateur,

• Veiller à bien les déconnecter du système d'exploitation avant de les débrancher physiquement (afin d'éviter la corruption des données),

• Fournir aux employés des clés USB agréées et à vocation professionnelle uniquement (également appelées « clés approuvées »),

• S'assurer à l'achat, que ces dernières sont fiables (respect des normes de sécurités),

• S'assurer que le personnel ayant accès à des données confidentielles et sensibles n'utilise exclusivement que des clés sécurisées,

• Crypter systématiquement le contenu de chaque clé (Perdre une clé est possible… ne pas la crypter est une faute …),

• Mettre en place un système d'accès avec mot de passe,

• Prendre l'habitude de s'assurer rapidement avant toute utilisation que la clé est saine et exempte de programme malveillant,

• Savoir qui utilise quelle clé et à quel moment. Cela peut s'avérer contraignant, mais l'efficacité de la procédure est prouvée,

• Mettre en place une procédure de récupération des clés perdues (aujourd'hui seule une minorité avoue la perte d'un tel objet),

• Former le personnel quant aux utilisations qualifiées acceptables ou inacceptables par l'entreprise,

• Ne considérer en aucun cas ce type de support comme fiable dans le temps ; à ce titre, il ne peut nullement se substituer aux

L'AUTEUR

Ludovic HAYE est Expert IT en systèmes ERP (SAP) à l'international, Certifications SAP des systèmes ERP. Il est membre de la SNIPF (Société Nationale des Ingénieurs Professionnels de France) et conseiller auprès des divisions de sûreté niveau groupe.
Chef d'escadron de la Réserve citoyenne de la Gendarmerie Nationale, il intervient en Intelligence économique dans les Brigades Territoriales et les écoles (en lien avec les BPDJ). Il intervient régulièrement lors du Forum du Rhin-supérieur sur les Cybermenaces (FRC) à l'ENA de Strasbourg depuis 2011 (sécurité des périphériques USB, les bonnes pratiques du Cloud, la sécurité des Moyens de paiement, l'authentification et la signature électronique comme moyen de prévention etc.). Il est partie aux Rencontres de la SIM de MULHOUSE (juin 2016) : « La Cybersecurité : Comment protéger efficacement son entreprise ». Contributeur ponctuel au sein du CRIE (Comité Régional pour l'Intelligence Economique), il est délégué Régional (Alsace) de l'ANAJ-IHEDN. Élu local, il est en charge des finances, du développement numérique et des Nouvelles Technologies.

systèmes de sauvegardes en vigueur. Pour rappel, une clé USB n'est autre qu'un morceau de carte électronique qui possède un nombre de cycles de lectures/écritures limité et connu à l'avance. De plus, une mauvaise utilisation réduit leur durée de vie (ex : déconnexion sauvage),

• Plus globalement, créer et mettre en place une politique relative aux usages de la clé USB en entreprise (procédures, affecter une clé par usage etc.)

D'une manière générale il ne s'agit pas d'interdire mais d'utiliser sous condition. Si certains points peuvent être mal vécus par le personnel, ils sont aussi là pour les protéger car les conséquences juridiques et financières peuvent être colossales.

Les conséquences juridiques

La perte de données personnelles ou confidentielles (commerciales, médicales etc.) constitue un manquement grave à la loi Informatique et Liberté (CNIL). Ce dernier peut être, dans certains cas, complété par un second manquement à l'obligation de sécuriser ses données. Dans les 2 cas, une peine d'emprisonnement peut être prononcée, à laquelle peut s'ajouter une sanction pécuniaire pouvant aller jusqu'à 300 000€, sans parler du discrédit en termes d'image et de réputation pour le consultant ou l'entreprise qui a égaré la clé.

En conclusion, dans un contexte d'interconnexion croissante entre les sphères personnelle et professionnelle, couplé au phénomène de BYOD (Bring Your Own Device) ou de bureau mobile, on voit mal comment une entreprise pourrait interdire strictement à ses salariés l'utilisation de leurs périphériques personnels. Tout réside finalement dans l'équilibre entre les droits des salariés sur leur lieu de travail et les pouvoirs des employeurs afin d'œuvrer pour le bon fonctionnement de leur entreprise.

Cela dit, nous avons vu précédemment que les dangers potentiels engendrés par ces appareils (USB le plus souvent) peuvent être qualifiés d'inversement proportionnels à la taille de ces derniers. Les entreprises ont longtemps négligé cette faille de sécurité. Elles n'ont d'autres choix aujourd'hui que de mettre en place une organisation permettant d'encadrer de manière draconienne l'utilisation qui est faite de ces appareils, afin d'éradiquer efficacement les problèmes de sécurité intrinsèques.

Le calculateur quantique,
menace ou solution pour la cryptologie ?

par GÉRARD PELIKS

La catastrophe va-t-elle se produire ? Le chiffrement quantique entraînera-t-il à court terme la fin du chiffrement et donc l'impossibilité d'assurer la confidentialité des données numériques échangées et stockées ? Les cryptanalystes qui cassent les codes vont-ils définitivement l'emporter sur les cryptologues qui conçoivent les codes ? Des fantasmes naissent de cette fin de la cryptologie annoncée comme inéluctable, à laquelle nombre de prédicateurs donnent de la voix.

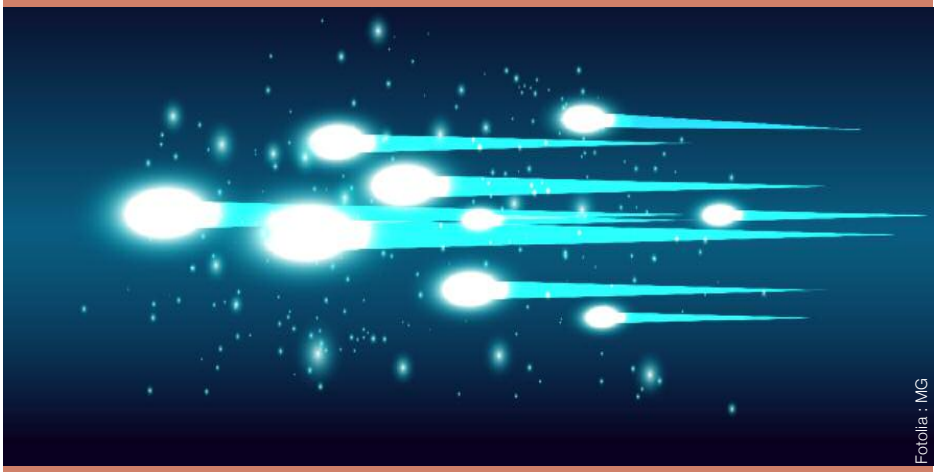
GÉRARD PELIKS

Association des réservistes du Chiffre et de la sécurité de l'information

Essayons d'y voir plus clair dans ces discours alarmants et au-delà du logos, voyons si une réalité plus rassurante peut être envisagée. Voyons même, si plutôt qu'une menace pour la cryptologie, le calculateur quantique ne serait pas au contraire une bonne solution pour assurer la confidentialité de nos informations sensibles. Sortons des mythes et abordons la réalité.

Le chiffrement à clé publique menacé

Le chiffrement à clé publique, dit aussi chiffrement asymétrique, met en jeu deux clés mathématiquement liées. Quand on chiffre avec l'une, on déchiffre avec l'autre. Une des clés est privée, son propriétaire ne la révèle jamais. L'autre clé est publique, son propriétaire la donne à tous ceux qui peuvent en avoir besoin, incluse dans un certificat numérique signé par une autorité de confiance. Donc, bien évidemment, une clé publique n'est pas confidentielle mais à partir d'elle, il n'est pas possible de reconstituer la clé privée correspondante. Si Alice veut utiliser le chiffrement asymétrique pour envoyer un message à Bob, elle chiffre le message avec la clé publique de Bob qui le déchiffre avec sa clé privée.



Fotolia : MG

Selon son état quantique et son orientation, le photon porte une caractéristique discriminatoire quand il frappe un miroir.

Deux éléments demandent des précisions dans le paragraphe précédent. Quand on affirme : « *À partir de la clé publique, il n'est pas possible de reconstituer la clé privée correspondante* », ce n'est pas une vérité mathématique. Il faudrait plutôt affirmer : « *À partir de la clé publique, il est très coûteux en temps de calculs de reconstituer la clé privée correspondante* ». En effet les algorithmes qui lient les deux clés reposent sur un problème très difficile à résoudre par un ordinateur d'aujourd'hui. Soit le problème réside dans la difficulté de factoriser un très grand nombre, produit de deux nombres premiers (chiffrement RSA), soit il réside dans la difficulté posée par le logarithme discret (Diffie Hellman) : à partir de y= ax mod(n), connaissant y, a et n, il est très coûteux en temps de trouver x. Des algorithmes existent, tel l'algorithme de Shor pour factoriser un grand nombre, mais s'il faut plusieurs milliers de milliards d'années pour arriver au résultat, c'est ce que nous appelons « il n'est pas possible de … » en tout cas dans un temps raisonnable. C'est là que survient la menace du calculateur quantique, qui donne toute sa raison d'être à l'algorithme de Shor pour déchiffrer, en retrouvant une clé privée asymétrique, à partir de la clé publique asymétrique correspondante, toutes les clés symétriques secrètes en transit sur le réseau. Nous verrons plus loin ce qu'est le chiffrement symétrique. Retenons ici que l'acheminement sécurisé des clés secrètes symétriques va poser un problème.

Un calculateur quantique manipule non pas des bits à 0 ou à 1, mais une superposition de bits à « 0 et à 1 ». C'est

le principe de superposition d'un état quantique. Cet état peut être encodé dans un photon qui est une entité éminemment quantique. Précisons que la physique quantique s'applique aux nanoparticules comme les électrons ou les photons, pas à vous ni à moi ni au chat de Schrödinger dans le fameux paradoxe, du moins dans la vie réelle. Cet état quantique du photon est assez difficile à obtenir et surtout à conserver par ailleurs car la superposition des bits à 0 et à 1, par un deuxième principe de l'état quantique, le principe de décohérence, peut se réduire simplement à un bit à 0 ou à un bit à 1, alors le calcul est compromis dans ce retour brutal au monde classique. Il ne faut pas grand-chose pour que la décohérence d'un élément quantique s'opère, un obstacle dans la fibre optique, ou une simple observation suffisent. Mais supposons ici qu'il n'y ait pas ce genre de problème.

Le problème de la factorisation d'un grand nombre ou celui du logarithme discret ne poseraient aucun problème à un ordinateur quantique qui calcule beaucoup plus rapidement qu'un ordinateur classique parce qu'il effectue ses calculs en parallèle alors qu'un calculateur classique les effectuerait en série. Un calculateur quantique pourra alors trouver, dans un temps raisonnable, par l'utilisation de l'algorithme de Shor, en factorisant le grand nombre qui intervient dans une clé publique RSA, la clé privée correspondante. Comme bien sûr tout le monde peut obtenir une clé publique, ceux qui disposeraient d'un calculateur quantique pourraient retrouver la clé privée pour déchiffrer les messages chiffrés avec la clé publique correspondante. Le calculateur quantique marque-t-il alors la fin du chiffrement ?

Dans le deuxième élément évoqué, Alice utilise la clé publique de Bob pour chiffrer le message qu'elle lui envoie. Eh bien non ! car ce n'est pas le chiffrement à clé publique qui est utilisé pour chiffrer les données numériques car il est très lent, trop lent pour chiffrer ou déchiffrer les gros fichiers. Donc n'étant pas utilisés pour chiffrer les messages, les problèmes difficiles à résoudre par les ordinateurs classiques, rendus faciles avec les ordinateurs quantiques, ne devraient pas être un motif de crainte. D'autant plus, et nous le verrons dans la suite, que le calculateur quantique apporte aussi une solution élégante à l'échange de clés.

Le chiffrement symétrique renforcé

C'est le chiffrement symétrique qui est utilisé pour chiffrer / déchiffrer car il est très rapide. On chiffre avec une clé symétrique et avec un algorithme (comme l'AES[1]) et on déchiffre avec la même clé et le même algorithme. Suivant le principe

(1) Advanced Encryption Standard : standard de crytage symétrique destiné à remplacer le DES (Data EncryptionStandard) devenu trop faible.

(2) https://www.reseau-canope.fr/savoirscdi/societe-de-linformation/le-monde-du-livre-et-de-la-presse/histoire-du-livre-et-de-la-documentation/biographies/claude-elwood-shannon-1916-2001.html

de Shannon[2], le chiffrement symétrique présente même un cas incassable, prouvé par les mathématiques, connu sous le nom de « chiffre de Vernam » ou masque jetable. Quand la clé symétrique a la même taille que le message à chiffrer et si cette clé n'est utilisée qu'une seule fois et qu'elle a été générée pour être non prédictible, il est prouvé que ce chiffre est incassable. Le nirvana des cryptologues ! Le chiffrement utilisé par le téléphone rouge durant la guerre froide !

Utilisons le fameux couple de la cryptologie, Alice et Bob. Alice chiffre, envoie le message chiffré à Bob qui le déchiffre. Alice génère une clé symétrique… si possible parfaitement aléatoire, et la chiffre avec la clé publique de Bob. Elle chiffre aussi son message avec sa clé symétrique, et elle envoie à Bob d'une part le message chiffré avec la clé symétrique qu'elle a générée, d'autre part la clé symétrique qu'elle a chiffrée avec la clé publique de Bob. Seul Bob peut alors déchiffrer la clé symétrique d'Alice avec sa clé privée correspondant à sa clé publique donnée à Alice, et s'en servir pour déchiffrer le message reçu.

Mais s'il ne sera plus du tout prudent d'utiliser le chiffrement à clé publique, pour faire transiter la clé symétrique, car les ordinateurs quantiques sauraient en un temps raisonnable retrouver la clé privée de Bob, correspondant à sa clé publique qu'il a donnée à Alice et à tout le monde, comment Alice pourrait-elle opérer pour faire parvenir à Bob la clé symétrique qu'elle a générée, avec laquelle elle va chiffrer son message et que Bob devra utiliser pour le déchiffrer ? D'autre part, comment générer une clé symétrique qui soit réellement aléatoire ? Par logiciel, on ne sait générer que des clés pseudo-aléatoires ? En effet si un grand nombre de clés est généré par une fonction logicielle, au bout d'un certain nombre de clés, la séquence de clés peut se répéter.

Rien ne vaut une méthode matérielle pour générer des séquences de clés vraiment aléatoires, et c'est là que la physique quantique apporte, dès aujourd'hui, une solution aux deux problèmes : la génération de clés purement aléatoires et l'acheminement de ces clés de manière sécurisée.

La génération de séquences de clés réellement aléatoires rendue possible

Un photon, particule de lumière ou onde lumineuse suivant qu'on parle de théorie corpusculaire ou ondulatoire de la lumière possède un état quantique : sa polarité. Si un photon dont la polarisation est orientée suivant un axe, rencontre un miroir semi-réfléchissant qui fait un angle α avec l'axe du photon, ce photon polarisé traversera-t-il le miroir ou sera-t-il réfléchi ? La probabilité qu'il traverse le miroir est égale à $\cos 2\alpha$. Il est intuitif que, si le photon polarisé arrive avec un angle nul par rapport à l'axe du miroir : $\alpha = 0$. Le photon traverse. En effet $\cos 2\ 0 = 1$ donc la probabilité que le photon traverse est de 100%. Si le photon arrive avec un angle de 90 degrés ($\pi/2$), donc complètement en travers du miroir semi-

réfléchissant, cos2 $\pi/2 = 0$, donc la probabilité que le photon passe est de 0% et le photon est réfléchi. Si le photon arrive incliné de 45 degrés ($\pi/4$) ou de 135 degrés ($3\pi/4$), la probabilité que le photon passe est, mathématiquement, de cos2 $\pi/4 = (2/2)2 = 0,5$, donc la probabilité pour que le photon passe ou ne passe pas est exactement de … une chance sur deux.

La nature, ou plutôt la technologie nous donne ainsi l'outil pour générer un aléa parfait. Si le photon passe, il est enregistré par un capteur situé derrière le miroir, qui met dans une pile un bit à 0. Si le photon est réfléchi, il est enregistré par un capteur situé devant le miroir, qui met dans la même pile un bit à 1. Et ainsi, photon après photon, on peut constituer un nombre parfaitement aléatoire.

Une application de ce phénomène est librement accessible sur un web de l'université de Genève[3]. Il vous est possible de rentrer comme paramètres la quantité de nombres aléatoires désirés, par exemple 50, et leur limite haute (par exemple inférieurs à 100). Le générateur de nombre aléatoire vous donne alors 50 nombres parfaitement aléatoires inférieurs à 100. Cette application peut être utilisée pour une loterie par exemple.

(3) http://www.randomnumbers.info/

Une distribution des clés symétriques inaltérée, sinon on s'en aperçoit

Nous savons donc, grâce aux propriétés de la physique quantique, générer une clé totalement aléatoire. C'est donc bien parti pour un chiffrement symétrique incassable comme le chiffre de Vernam[4]. Dans cette méthode la longueur de la clé de chiffrement est égale à la longueur du message à chiffrer. Reste le problème de transmettre cette clé de chiffrement au destinataire en toute sécurité, au travers d'un réseau pas nécessairement sécurisé, comme à travers une fibre optique, par exemple.

(4) En 1917, Gilbert Vernam mit au point un algorithme de chiffrement -basé sur une clé secrète qui a longtemps protégé le fameux "téléphone rouge", qui reliait la Maison Blanche au Kremlin. NDLR

Dans le chiffrement classique, pour transmettre la clé symétrique, on utilise le chiffrement à clé publique, mais nous avons vu que de par sa vitesse de calcul qui résout facilement les problèmes jusque-là difficiles à résoudre sur lesquels le chiffrement à clé publique est basé, l'ordinateur quantique rend cette méthode peu sécurisée. Heureusement la physique quantique apporte là encore la solution.

Nous évoquerons ici le protocole BB84, du nom de ses deux inventeurs Bennet et Brassard publié en 1984, mais plusieurs autres protocoles alternatifs existent aussi.

Il est possible par le jeu de l'orientation de la polarité des photons pratiquée par Alice et de l'orientation de filtres pratiquée par Bob d'échanger, en toute sécurité, aujourd'hui à travers une fibre optique, une clé symétrique. Alice choisit la polarité du photon qu'elle envoie mais ne connaît pas l'orientation du filtre choisie par Bob. Celui-ci ne connaît pas la

polarité du photon envoyé par Alice mais constate juste que le photon passe ou ne passe pas par le filtre qu'il a orienté. En fonction de ces renseignements, Alice et Bob pourront constituer une clé de chiffrement symétrique. Comment ? Pour faire simple, Alice convient qu'un bit à 0 de la clé qu'elle a générée (aléatoirement) équivaut à un photon polarisé à 0 ou à 45 degrés. Un bit à 1 se traduit par un photon polarisé à 90 ou à 135 degrés. « Photon par Photon », en faisant correspondre leur polarité au bit à 0 ou à 1 de la clé symétrique, qu'elle a générée, elle envoie les photons qu'elle a polarisés. Bob positionne son filtre de manière aléatoire (0, 45, 90 ou 135 degrés). Si le photon traverse son filtre, il note un bit à 1. S'il n'a pas traversé, il note un bit à 0. Par un autre canal qui n'a pas à être sécurisé, par exemple par téléphone, il indique à Alice si son filtre qu'il a orienté a été rectiligne (0 ou 90 degrés) ou diagonale (45 ou 135 degrés). Alice indique à Bob si la polarisation qu'elle a choisie pour le photon qu'elle a envoyé est rectiligne ou diagonale. Si Alice et Bob ont utilisé la même inclinaison, Bob et Alice valident le bit, sinon ils laissent tomber les bits non validés. Ainsi Bob reconstitue une partie de la clé symétrique générée par Alice. Et ce qui reste des bits retenus est la clé symétrique qu'Alice et Bob se partagent.

Si un espion capte au passage cette clé sur la fibre optique, en utilisant son propre filtre, Bob et Alice sauront que cette clé a été observée. Comment ? D'abord, toute observation du photon entraîne sa décohérence quantique, donc il perd sa polarité et ne peut être rejoué dans l'état où on l'a trouvé. Et comme l'espion n'a aucune idée de la polarisation du photon envoyé par Alice, en renvoyant le photon qu'il aurait à nouveau polarisé à Bob pour ne pas lui mettre la puce à l'oreille … il aura une chance sur deux de se tromper. Alice saura alors que la clé a été compromise et générera d'autres clés tant qu'avec Bob elle n'aura pas l'assurance que la clé sera passée sans avoir été interceptée.

Toutefois, avec les technologies actuelles, l'état quantique d'un photon peut s'altérer avec la distance parcourue (état de décohérence), donc le passage d'une clé à travers une fibre optique est limité aujourd'hui à quelques dizaines de kilomètres, un peu plus avec des répéteurs. Mais la technologie est prometteuse et des expérimentations ont déjà été faites.

Un ordinateur quantique sera-t-il vraiment opérationnel un jour ?

C'est la grande question ! Nous aurions même pu commencer par répondre à cette question, car si l'ordinateur quantique n'existera jamais, le chiffrement à clé publique pour acheminer les clés symétriques a encore de très nombreux jours devant lui. Sur un plan théorique, l'existence d'un ordinateur quantique ne

se pose plus puisque des expériences en laboratoire ont été concluantes avec des portes quantiques, mais il faudra beaucoup de telles portes pour rendre un calculateur réellement opérationnel. Le problème réside dans sa puissance de calcul conditionnée par le nombre de « qubits » (quantum bit, unité quantique de superposition de bit à 0 et à 1). IBM a mis en œuvre un processeur quantique à 5 qubits dans le Watson Research Center à New York, qui est accessible, en mode Cloud, aux chercheurs. De son côté, Google aurait mis en service un processeur quantique à 9 qubits. Un calculateur quantique de l'université d'Innsbruck aurait une puissance de 14 qubits. Précisons que chaque qubit ajouté double la puissance de calcul. Un calculateur quantique de n qubits aurait la puissance de calcul de 2n calculateurs classiques calculant en parallèle. Mais il faudrait beaucoup plus de qubits utilisables que ce qui est disponible aujourd'hui pour parler réellement d'un ordinateur quantique utile.

Mais si un ordinateur quantique existait déjà dans des centres secrets de laboratoires occultes, le saurait-on ?

Le chiffrement post quantique

Dans un chiffrement quantique, l'information est codée dans des photons. Chaque photon contient quelques bits. En altérant leur état par une fonction aléatoire, on chiffre cette information. Par une fonction aléatoire inverse, on la déchiffre. Ces fonctions aléatoires sont contenues dans la clé de chiffrement / déchiffrement. Dans les centres de recherches, on travaille déjà, lit-on dans la littérature spécialisée, sur ce chiffrement.

Maintenant rêvons un peu en évoquant une troisième propriété de la physique quantique : le principe d'intrication. Pour faire simple, si deux objets quantiques sont intriqués, toute modification de l'un entraîne la même modification sur l'autre. Ceci même si l'un des objets quantiques se situe à Paris et l'autre est dans un satellite en orbite autour de la planète mars. Vous voyez le parti qu'on peut en tirer pour le chiffrement symétrique ? Alice conçoit une clé et Bob voit cette clé apparaître chez lui ! Mais qui prouvera à Bob que cette clé qu'il voit apparaître est bien celle conçue par Alice ? Fin du rêve, retour à la réalité et concluons.

Le chiffrement qui combine une clé symétrique (comme l'AES) pour chiffrer / déchiffrer et un couple de clés asymétriques (comme le RSA) pour chiffrer / déchiffrer la clé symétrique afin de l'acheminer de manière sûre, même à travers un réseau public, a encore quelques années devant lui.

Mais la disponibilité probable de calculateurs quantiques opérationnels oblige les cryptologues à concevoir d'autres solutions pour garantir la

confidentialité des données numériques sensibles. L'une d'elles, déjà implémentée aujourd'hui, est d'utiliser le chiffre de Vernam (masque jetable, non prédictible, et de la longueur du message à chiffrer) pour chiffrer / déchiffrer et le protocole BB84 pour transmettre ce masque.

L'AUTEUR

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

« Bug Bounty Program » : l'avènement des plates-formes européennes

par SANDRA ESQUIVA HESSE et TOUFIK AIRANE

Le concept du "Bug Bounty Program" est né Outre-Atlantique en 1996 dans les locaux de Netscape. L'idée est simple et efficace : combiner les besoins en sécurité des systèmes d'information des entreprises et des institutions au talent des hackers. Grâce au développement croissant du secteur de la sécurité informatique et à la ferveur de passionnés de la recherche de vulnérabilités, cette collaboration a remodelé, en quelques années, le paysage de la sécurité informatique et redoré l'image des hackers auprès des acteurs de notre société. Ce modèle est actuellement propulsé par les géants de la toile tel que Google, Twitter, Facebook, Uber ou récemment Apple.

SANDRA ESQUIVA HESSE

Avocat au barreau de Paris et New-York

TOUFIK AIRANE

Consultant en sécurité Société ENKI

Les "Bug Bounty Program" ont ce pouvoir de canaliser l'énergie d'une armée de hackers en effaçant leurs motivations individuelles et hétérogènes par la motivation de gagner des récompenses pécuniaires et une reconnaissance publique. En mettant en place un "Bug Bounty Program", les entreprises coupent l'herbe sous le pied des attaquants malveillants. En effet, les tentations d'exploitations malveillantes sont absorbées par le gain immédiat et légal que représente le fait de soumettre la vulnérabilité sur une plateforme de Bug Bounty. L'esprit de compétition ainsi que le nombre croissant d'auditeurs impliquent qu'une vulnérabilité identifiée sera aussitôt soumise avant qu'un

exploitant malveillant n'en profite. Pour arbitrer les relations et répondre aux challenges, des plateformes de "Bug Bounty Program" ont vu le jour. Ces intermédiaires offrent aux deux parties les interfaces de communication et les règles de conduite pour se comprendre. Du point de vue des entreprises, les bugs sont énumérés unitairement dans un format standardisé. Encore faut-il qu'elles possèdent la main-d'œuvre nécessaire et suffisante pour interpréter les rapports de bugs, une quantité importante de rapports devant être traitée par priorité selon la catégorie et l'impact sur le système.

Cette limpidité offre une grande agilité et une réactivité pour les équipes en charge. Les plates-formes de "Bug Bounty" s'attachent à accompagner les entreprises notamment sur les questions du périmètre et des seuils de rémunération. Quant aux hackers, elles leur offrent un filtre et des ressources pour normaliser et soumettre des rapports de qualité et assurent le bon déroulement des paiements.

La normalisation des vulnérabilités est un défi, accentué par des profils de hackers venus d'horizons divers. Il existe cependant des programmes privés, accessibles uniquement à une élite de chercheurs. Ces programmes garantissent l'appel à des professionnels dans la recherche de vulnérabilités. L'interaction entre toutes ces parties implique un langage commun, par conséquent l'avènement de plates-formes européennes devient une évidence pour l'autonomie et l'efficacité de nos acteurs économiques et institutionnels.

En Europe, les initiatives sont encore timides mais une startup a relevé le défi : YOGOSHA, qui signifie défense en japonais.

Elle innove en proposant l'intégration d'applications auditées sur des environnements virtuels afin de laisser libre champ aux auditeurs en préservant les infrastructures en production. Par ailleurs, la startup accompagne les entreprises avant, pendant et après l'établissement du programme. Les entreprises sont ainsi plus sereines dans la détermination du périmètre et sont encadrées afin d'orienter le travail des auditeurs. Finalement, l'entreprise achète ses propres failles, l'auditeur est rémunéré et la plate-forme veille au bon déroulement des opérations. La sécurité devient un produit. De nouveaux paradigmes sont à inventer et le "Bug Bounty Programs" est au cœur de ces innovations de procédés. Indéniablement, une évolution des rapports de force est en marche et tend vers une relation tripartie gagnant-gagnant basée sur un

élément fondamental : la confiance.

En avril 2016, le programme "Hack the PENTAGON" est lancé, impulsé par le département de la défense numérique Américain en collaboration avec la plate-forme HACKERONE. Plus de 1000 chasseurs de bugs se sont attardés sur les infrastructures gouvernementales, découvrant de nombreuses vulnérabilités. En complément des applications standards de sécurité des systèmes et des audits, les "Bug Bounty Programs" sont une réponse originale et pragmatique à la montée en complexité des attaques et à la créativité des cybercriminels. Apprécié des hackers, le « Bug Bounty Programs » est un système méritocratique et pérenne. Les « Bug Bounty Programs» offrent une récompense à tous ceux qui trouvent des failles de sécurité dans un périmètre donné de leur système informatique. Ils sont soumis à un budget global réparti par l'entreprise sponsor ou son intermédiaire en fonction de critères objectifs et subjectifs d'appréciation.

Plus la faille est critique, complexe, bien documentée avec si possible un « Proof of Concept », des recommandations, voire un patch, plus la récompense sera élevée.

Les entreprises souhaitant recourir à cette pratique fixent le plus souvent les conditions dans lesquelles doit s'exercer la recherche de failles et définissent notamment :

• le périmètre d'action, certains programmes limitant la recherche de faille à un logiciel précis, une application ou à certains sites internet ;

• le type de failles ouvrant droit à rémunération. Il peut s'agir d'identifier une faille affectant la confidentialité ou l'intégrité des données des utilisateurs n'ayant jamais été repérée ou d'un simple bug;

• la durée du Bug Bounty program : le plus souvent la période de test étant enfermée dans un délai précis avec des dates d'ouverture et de fermeture;

• des règles de confidentialité : les Bug Bounty program insistent sur la nécessité de ne pas révéler la faille au public ou à des tiers avant qu'elle ne soit réparée;

• des règles de protection des données personnelles : lorsque les Bug Bounty program concernent des sociétés en possession de données à caractère personnel (ex : Facebook, Google), l'exigence éthique est renforcée vis-à-vis des auditeurs. Ainsi, Facebook ou Google précisent dans leurs conditions l'obligation d'effectuer des tests via des comptes spécialement créés à cet effet ou d'obtenir l'accord explicite du propriétaire du compte sur lequel sont effectués les tests ;

• des règles de conflit de lois : certains programmes précisent la juridiction compétente dans l'éventualité d'un conflit (par exemple, le Bug Bounty program

lancé par Microsoft précise que le programme étant hébergé aux Etats-Unis, il est soumis exclusivement à la loi de l'Etat de Washington);

• les conditions de paiement sont liées notamment à la révélation de la faille à l'entreprise et au respect d'une confidentialité renforcée garante de la bonne foi de l'auditeur à l'opposé de pratiques indésirables telles le spamming, le phishing, la destruction de données ou encore la perturbation du système de données.

La bonne foi trace ainsi la limite de légalité entre des auditeurs ayant une éthique, qui mettent leurs compétences au service de l'identification de faiblesses systémiques et de leur correction, et les hackers qui tentent de pénétrer irrégulièrement et de mener des activités illégales.

L'AUTEUR

Toufik Airane est consultant en sécurité des systèmes d'information au sein de l'entreprise ENKI. Autodidacte passionné par la sécurité des systèmes d'informations depuis l'adolescence, Toufik Airane s'intéresse à divers horizons tels que la retro-ingénierie, la sécurité offensives ou l'analyse de programme malveillants. Actuellement, il travaille sur les cas d'utilisation d'habits connectés « wear-hacking » ou encore la catégorisation de l'information pour prévenir de l'exfiltration de donnée.

L'AUTEUR

Sandra Esquiva-Hesse a rejoint FTPA en Janvier 2016, suite à la fusion absorption de SEH Legal, cabinet d'avocats qu'elle avait créé en Avril 2011. Elle conseille et accompagne des entreprises, entrepreneurs et investisseurs dans leurs opérations corporate, de financement, de structuration ou restructurations (carve-out, recentrage, acquisitions en situations spéciales) et les représente dans les contentieux y afférents. Elle a une extensive expérience en matière de transactions et contentieux multinationaux. Elle a démarré sa carrière à Wall Street, en 1998 en qualité d'US Associate dans le département Bank Finance & Bankruptcy de Shearman & Sterling, elle revient en France en 2002 et devient Counsel au sein du département Financements Structurés de Clifford Chance Paris. En 2006 elle devient Associée du département Finance & Restructuring du bureau de Paris de Paul Hastings, département qu'elle a créé et développé jusqu'en 2011.
Avocate aux barreaux de Paris et New York, elle est titulaire d'un LLM de Columbia Law School (New-York, 1997), d'un dottorato di ricerca in diritto europeo de l'Universita degli Studi di Bologna (1996), d'un DEA de Droit international économique de l'Université Paris-I Panthéon Sorbonne, magna cum laude (1996) et d'un DESS de Droit du commerce extérieur de l'Université Paris-I Panthéon Sorbonne, summa cum laude (major de la promotion du Professeur GAVALDA, 1995).
Sandra est régulièrement classée dans les catégories d'excellence des annuaires professionnels : Chambers Europe and Global, Legal 500, IFLR, Décideurs, Who's Who in France, Who's Who Legal.
Elle a acquis une notoriété pour son approche innovante dans la résolution de situations complexes, seconde du classement du Financial Times pour l'Avocat le plus innovant de l'année 2010, le Magazine de Affaires a décerné son Grand Prix Restructuring Opération Mid-Cap Innovante de l'année 2015 pour ses travaux pour la reprise par ses salariés organisée sous forme de SCIC de Nice Matin.

L'influence de la communauté russophone sur la cybercriminalité

par **ADRIEN PETIT**

Il existe trois principales cybermenaces[1] aux motivations différentes : les groupes sponsorisés par un État (espionnage)[2], les hacktivistes (idéologie) et les cybercriminels (profit). Ces derniers se distinguent par une présence massive sur les plateformes underground. Elles se sont fortement développées au cours des dernières années et permettent aux acteurs malveillants d'étendre leurs activités.

ADRIEN PETIT

Consultant cybercriminalité Compagnie européenne d'intelligence stratégique (CEIS)

Les cybercriminels ne se concentrent pas au sein d'un écosystème unique et global : selon leur origine et leur culture, ils se fragmentent en communautés qui ont chacune leurs particularités en termes de fonctionnement et de nature des activités opérées. Il existe cependant des connexions entre les différentes communautés caractérisées notamment par une certaine influence russophone.

(1) Une cybermenace est un acteur (ou un groupe de personnes) qui se matérialise par la combinaison de trois facteurs, à savoir : une intention de nuire, une capacité d'attaque et enfin une opportunité à exploiter (technique ou humaine).

(2) N.D.A. : Les attaques ciblées (ou APT – Advanced Persistent Threat) ne s'apparentent pas à une typologie de cybermenace mais à un mode opératoire. Elles se diversifient, se multiplient et ne sont plus seulement menées par des groupes sponsorisés par un État, mais également par des communautés cybercriminelles comme Carbanak, Metel ou encore GCMAN.

(3) Pour une présentation des différentes notions, voir Adrien Petit, « Le Dark Web, place de marché des données volées », Revue de la Gendarmerie Nationale, Revue Trimestrielle, n°254, décembre 2015, pp. 53-58

Organisation des cybercriminels sur les plateformes underground

Le Deep Web et son sous-ensemble le Dark Web contiennent des plateformes très variées : réseaux sociaux, blogs, sites de presse, de partage, de diffusion, de stockage, Internet Relay Chat (IRC), forums restrictifs ou encore marchés noirs[3]. Ces deux derniers sont massivement utilisés par les

CEIS

Des communautés jeunes et ouvertes qui diversifient leurs activités

cybercriminels afin de proposer tout un panel d'activités et de produits malveillants : techniques de fraudes, recel de produits volés ou encore malware dédiés aux attaques informatiques. En termes d'organisation, les utilisateurs de ces plateformes se répartissent en plusieurs sphères. Dans son rapport intitulé « Cybercrime and the Deep Web » publié en mars 2016, la société Trend Micro mettait ainsi en avant l'existence de 6 communautés underground réparties selon des régions du monde :

• Russie : pionnière dans le monde cybercriminel, cette communauté professionnelle s'articule autour des thématiques du carding et de l'attaque informatique. Elle fonctionne comme une ligne d'assemblage où chaque acteur joue un rôle précis. De nombreux produits et services de très haute qualité et à forte valeur ajoutée y sont commercialisés. L'accès à cette communauté d'experts élitistes se fait par cooptation ou en montrant sa patte « noire » cybercriminelle.

• Allemagne : plateforme considérée comme étant la petite sœur de celle de la Russie aussi bien pour son organisation que pour les produits et services échangés.

• Amérique du Nord : accessible à tout type d'utilisateur allant du novice au pirate informatique confirmé. Les principaux produits proposés sont ceux issus de la criminalité traditionnelle, à savoir les stupéfiants, les armes (non-létales principalement) ou encore les faux papiers. Quelques malwares sont proposés à la vente.

• Brésil : communauté très ouverte, jeune et axée essentiellement sur la cybercriminalité bancaire. De nombreux chevaux de Troyes bancaires y sont échangés.

• Chine : plaque tournante mettant à disposition de nombreux prototypes aussi bien au niveau hardware que software. Les vendeurs sont très réactifs par rapport aux besoins du marché mais la qualité des produits reste cependant très aléatoire. Cette communauté est composée d'utilisateurs sinophones opérant en dehors de Chine.

• Japon : se distingue largement de ses consœurs de par son organisation (recours à des « bulletin board systems » uniquement accessibles à des utilisateurs natifs japonais) et la nature des contenus. Les utilisateurs échangent surtout sur des sujets qualifiés de tabous.

On constate enfin le développement d'une communauté underground francophone principalement axée sur la fraude (bancaire, faux documents, *etc.)*, la vente de drogues et la fourniture de tutoriels en tous genres. Cette communauté est relativement jeune et ouverte et n'est pas aussi développée que les écosystèmes anglophone et russophone. Elle tente petit à petit de se mettre à niveau en développant des outils offensifs « *Made in France* » et en segmentant certains de ses forums et marchés noirs *via* des espaces privés réservés à une communauté élitiste.

L'impact des malwares d'origine russophone

Les forums restrictifs et marchés noirs présents sur le Deep et Dark Web regorgent de malwares sophistiqués qui sont utilisés ultérieurement lors de vagues de cyberattaques. Ils sont révélés au grand public une fois les campagnes identifiées par les spécialistes en cybersécurité. À titre d'exemple, le ransomware Locky[4] et le malware Android Mazar[5] ont fait la une de l'actualité cybersécurité au début de l'année 2016 mais ils étaient échangés sur les plateformes cybercriminelles russophones depuis le mois d'octobre 2014. Un nombre conséquent de malwares est proposé de manière quotidienne sur les forums restrictifs russophones. Il est possible d'identifier les futures tendances des logiciels malveillants qui seront utilisés au cours des cyberattaques en mettant en place une surveillance optimisée. La combinaison de plusieurs facteurs permet ainsi d'isoler les éléments les plus pertinents :

(4) http://www.forbes.com/sites/thomasbrewster/2016/02/18/ransomware-hollywood-payment-locky-menace/#ad11d

(5) http://www.bbc.com/news/technology-35586446

– Historique et renommée du développeur ;

– Certification de la qualité du malware par les administrateurs des plateformes ;

– Retours d'expérience par les acheteurs et opérateurs ;

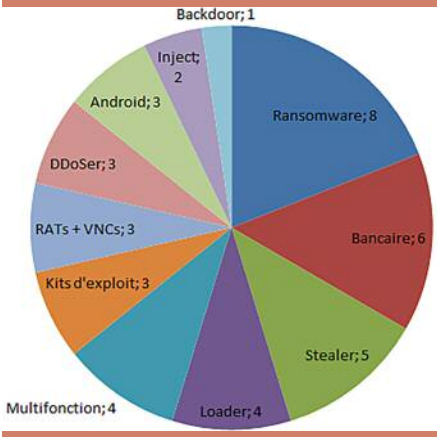
– Modalités d'acquisition ;

– Temps de présence et nombre de vues de l'annonce ;

– Distribution du malware sur d'autres plateformes ; *etc.*

À titre d'exemple, 42 malwares qualifiés de haut niveau et très prisés par les acheteurs/opérateurs ont été retenus depuis le début de l'année 2016 et répartis

suivant une classification évolutive :



CEIS

Une palette de Malware adaptée aux besoins du marché.

Afin de répondre aux besoins du marché, les concepteurs des malwares mettent régulièrement à jour (base hebdomadaire) leurs produits. Ils améliorent la qualité de leur code dans le but de passer outre les systèmes de détection. Ils cherchent également à se démarquer de la concurrence en ajoutant de nouvelles fonctionnalités avancées.

En dépit du cloisonnement des différentes communautés cybercriminelles, des liens se nouent entre elles. De nombreux malwares utilisés par les acteurs anglophones sont ainsi d'origine russophone en raison de la qualité des produits et services offerts par les développeurs de cette région. Cette interaction se fait de deux manières différentes. Certains forums russophones communiquent ouvertement sur leur ouverture à des communautés extérieures. Ils souhaitent avant tout attirer une certaine élite et imposent des conditions comme le paiement d'un droit d'entrée.

Il en résulte que l'utilisateur anglophone dispose de sections où les annonces sont entièrement rédigées en anglais :

L'interaction se passe aussi dans le sens inverse. Des vendeurs russophones ayant pignon sur rue dans leur propre communauté étendent leur marché sur des plateformes étrangères en s'appuyant sur un réseau de revendeurs ou alors de manière directe. Il n'est pas rare de constater que ces pirates commercialisent dans un premier temps leur malware dans la communauté russophone puis étendent leurs activités aux plateformes étrangères.

On constate ainsi que les produits de haute qualité et à forte valeur ajoutée proposés sur les plateformes anglophones reflètent l'état du marché russophone des semaines précédentes.

Le carding : une activité lucrative et démocratisée

Le *carding* est une activité de blanchiment des données bancaires volées par les cybercriminels. Il a été originellement développé par la communauté russophone qui continue de baser la

majorité de ses échanges sur cette activité. Cette dernière est depuis largement développée par les autres communautés underground. Le carding se décompose en plusieurs étapes :

Support malware bancaire

1re étape : création du support permettant le vol des données bancaires

Le malware bancaire est un programme informatique malveillant dont le but est de voler des données bancaires par récupération de formulaire, keylogger et attaques man-in-the-browser.

Les premiers malwares bancaire (Zeus ou Carberp) furent développés dans les années 2000 par la communauté russophone. Cette dernière continue de proposer ce type de produits et tend à les rendre de plus en plus simples à utiliser (principe du Malware-As-A-Service).

2e étape : acquisition des données bancaires

Le malware bancaire se transmet par simple visite sur un site infecté. Il peut également être camouflé dans une pièce jointe envoyée lors d'une campagne de spam d'apparence légitime (relance facture, remboursement, etc.). Lorsque la victime ouvre le document le malware se déploie silencieusement sur la machine. Il s'active et vole les informations bancaires lorsque la victime indique ses données bancaires au cours d'un achat en ligne. Il transmet par la suite les données à l'attaquant.

Support kit de phishing

1re étape : création du support permettant le vol des données bancaires

Le kit de phishing est un ensemble de pages web usurpant la charte graphique d'un établissement. Cette technique consiste à faire croire à la victime qu'elle s'adresse à un tiers de confiance — banque, administration, etc. — afin de lui soutirer des renseignements personnels.

La création d'un kit ne requiert pas de compétences particulières. Un débutant en piratage peut aisément développer son propre kit.

2e étape : acquisition des données bancaires

Les pages sont auto-hébergées (l'attaquant crée un site dédié à ce kit de phishing) ou hébergées sur un site qui a été préalablement compromis. L'avantage de cette dernière technique est son temps de présence sur le web, les pages sont moins susceptibles d'être détectées par des outils anti-fraude. Le fraudeur envoie ensuite par spam l'URL redirigeant vers les pages malveillantes. Lorsque la victime renseigne sur ces pages ses données bancaires, ces dernières sont transmises au fraudeur.

Trois autres techniques moins employées permettent à un attaquant de dérober des données bancaires :

Le skimmer est un appareil qui se pose sur un distributeur automatique de billets.

Il capture la piste magnétique de la carte et est associé à un dispositif de surveillance qui enregistre le code à 4 chiffres renseigné par la victime.

Le vol d'une base de données clients à partir d'un site web qui a été compromis. Les pirates cherchent à exploiter des failles présentes au sein de sites e-commerçant afin de voler les bases de données clients qui comprennent notamment les données bancaires.

Le malware PoS (Point of sale) est quant à lui de plus en plus répandu. Il se déploie sur les terminaux de paiement.

Les forums restrictifs et marchés noirs regorgent de produits et services liés à la création ou la mise à disposition des supports permettant le vol des données bancaires. Ils sont en général accompagnés de tutoriels permettant d'optimiser leur utilisation.

Une fois que le fraudeur récupère les données bancaires, deux solutions s'offrent à lui afin de les monétiser :

3e étape : monétisation des données bancaires volées

Revente directe

Le vendeur peut choisir de revendre de manière directe son butin sur les plateformes underground. Il publie des annonces dans lesquelles il donne un ensemble d'indications :

Type de la carte / Origine de la carte /Possibilité d'acheter une ou plusieurs cartes.

Revente indirecte

L'autre solution est d'utiliser au préalable les données bancaires afin de les monétiser par la revente de produits/services achetés en ligne. Le fraudeur poste une annonce dans laquelle il propose son produit.

Si cette approche s'avère plus fastidieuse, elle reste néanmoins très lucrative.

La revente directe tend à se professionnaliser. Le principe d'annonces est peu à peu remplacé par le développement de nouvelles plateformes dites autoshops. L'acheteur va procéder à l'acquisition des données bancaires en quelques clics sur une plateforme

Index	Number	Exp	Holder name	Level	Type	Bank	ZIP Code	Address	City	State	Country	Email	Phone	Valid, %	Price, $	
1	4737027xxxxxxx25:	09/26	Lilia xxxxx	CLASSIC	DEBIT	WELLS FARG	97123	7355 SE Tua	Hillsboro	OR	US	✓	✓	<Low>	13,20	
2	5443687xxxxxxx69!	11/23	Richard xxxx	STANDA	DEBIT	HSBC BANK	12463	3040 Rtxxx	Palenville	NY	US	✓	✓	<Low>	13,20	
3	5129935xxxxxxx77!	09/23	Christopher x	<Empty>	DEBIT	FIRST DATA	07731	31 Wilxxxx	Howell	NI	US	✓	✓	<Low>	17,16	
4	5516380xxxxxxx34(	11/22	Woody xxxxx	STANDA	DEBIT	FISERV SOLL	27360	708 Martin	Thomasvi	NC	US	✓	✓	<Low>	13,20	
5	5403854xxxxxxx79:	03/22	Jose xxxxxx	STANDA	DEBIT	CITIBANK, N	95825	2024 Jexxx	Sacramen	CA	US	✓	✓	<Low>	13,20	

Exemple d'un autoshop

CEIS

automatisée sans qu'il ait besoin de communiquer directement avec le vendeur.

La revente indirecte est quant à elle un phénomène en plein essor notamment auprès de la communauté francophone. Les fraudeurs utilisent eux-mêmes les données bancaires volées pour acheter des produits/services en ligne afin de les revendre par le biais d'annonces sur les plateformes cybercriminelles. Cette approche leur permet de fournir de réels produits/services à un prix inférieur à leur valeur réelle d'acquisition. Les produits/services les plus répandus sont :

Location de véhicules – 25/30% du prix initial ;

Billets de train – 25/30% du prix initial ;

Produits issus de sites e-commerce (High-tech, prêt-à-porter, parfumerie, pièces automobile/moto) – 20/25% du prix initial ;

Services de restauration – 20/40% du prix initial ;

Cartes cadeaux – 25/40% du prix initial ;

Carding du type drive – 20/30% du prix initial ;

Chambres d'hôtel – 25% du prix initial ;

Location de villa/appartement – 15/25% du prix initial ;

Location chez un particulier – 30% du prix initial ;

Location village vacances – 20% du prix initial ;

Billets événements / concerts / parcs d'attractions – 20/25% du prix initial.

Il existe une réelle influence russophone sur les autres communautés cybercriminelles qui s'opère de manière directe et indirecte. D'une part, cela se fait au travers des interactions liées à la distribution de malware. En effet, si les communautés anglophones et francophones tentent petit à petit de développer leurs propres outils, elles ne disposent pas du même niveau d'expérience que leurs confrères. Elles se tournent donc directement vers la communauté russophone afin de déployer ultérieurement les outils acquis au cours de cyberattaques. D'autre part, de par son statut de pionnière dans le monde cybercriminel via le développement de l'attaque informatique et du carding, la communauté russophone tend à être prise pour modèle par les sphères étrangères. En effet, ces dernières ont donc largement adopté et développé une économie liée à l'activité de carding.

L'AUTEUR

Adrien PETIT est consultant senior en Cyber Threat Intelligence et travaille chez CEIS depuis janvier 2015. Il a pour responsabilité la conduite opérationnelle des missions de Cyber Threat Intelligence.
Avant de rejoindre CEIS, Adrien PETIT a travaillé pendant 4 ans au sein du CERT-LEXSI basé à Singapour où il a exercé le métier d'analyste en cybercriminalité auprès de clients internationaux bancaires et industriels. Enseignant vacataire au sein de plusieurs établissements, Adrien a signé de nombreux articles et intervient régulièrement au cours de conférences.

La formation en cybersécurité : un investissement d'avenir

Entretien avec Marie Moin

À l'occasion du 9e Forum International de la Cybersécurité (FIC), nous sommes allés à la rencontre de Marie Moin, directrice de Securesphere by EPITA. Pour nous, elle décrypte les enjeux de formation en matière de cybersécurité. De par son expertise, elle offre un regard éclairé sur la nécessité de développer davantage la formation dans ce domaine et ainsi multiplier le nombre d'experts.

Pouvez-vous nous présenter Securesphere by EPITA ? Comment est venue l'idée de créer ce centre de formation ?

MARIE MOIN

Directrice de Securesphere by EPITA

Commençons par la genèse de SecureSphere et pour cela, rappelons en premier lieu que l'EPITA et la sécurité informatique, devenue aujourd'hui cybersécurité ou sécurité numérique, c'est une histoire de plus de trente ans !

L'EPITA, école d'ingénieurs spécialisée dans l'informatique fondée en 1984, accompagne depuis ses débuts les principaux acteurs de la sécurité des Systèmes d'Information. Une de ses majeures, « Systèmes, Réseaux et Sécurité » (SRS), a formé nombre de RSSI et de DSI des plus grandes entreprises et de l'administration. Son Laboratoire de recherche en sécurité (LSE) est engagé dans plusieurs partenariats avec des institutions spécialisées dans le domaine.

Si nous ajoutons le fait que la proximité avec les entreprises est une des priorités de l'école, l'EPITA apparaît donc comme un observateur privilégié des besoins du marché en termes de compétences en cybersécurité. Notre constat a révélé une pénurie inquiétante d'experts et aussi un certain degré d'inconscience de la part des utilisateurs face aux cybermenaces.

Epita

Une formation adaptée à une diversité de métiers

L'école peut certes accueillir un plus grand nombre d'étudiants mais cela reste insuffisant pour faire face aux demandes que nous recevons et ne couvre pas la totalité des besoins. La numérisation de notre société implique de multiplier le nombre d'experts et impose également qu'au-delà des experts, chacun soit initié à la sécurité.

Nous avons donc décidé de créer SecureSphere, entité dédiée à la formation continue, qui propose :

• Des formations expertes destinées aux équipes sécurité. Ces formations thématiques, courtes, ont vocation à couvrir avec pragmatisme les besoins les plus urgents.

• Des parcours de reconversion pour des collaborateurs souhaitant rejoindre les métiers de la cybersécurité. Ces parcours, dispensés avec l'EPITA permettent de compenser la pénurie d'experts dans cet univers en pleine croissance qui peine à trouver des talents.

• Des formations aux fondamentaux adaptées aux métiers de l'entreprise et destinées à l'ensemble des collaborateurs. Nous sommes en effet convaincus que chacun, quel que soit son poste, doit être impliqué et devenir l'acteur de sa propre sécurité et ainsi participer à celle de sa structure.

Et, parce que la formation professionnelle réclame une expertise différenciée, SecureSphere s'est dotée dès ses débuts d'un Comité de Programme et d'Orientation en Sécurité qui regroupe de nombreuses personnalités issues du monde de l'entreprise, des institutions et académies, ainsi que des experts en sécurité et en cybercriminalité : Bernard Barbier, Alain Bouillé, Michel Cazenave,

Alain Doustalet, Bernard Fesquet, Didier Gras, Adel Jomni, Philippe Leroy, Jean-Yves Poichotte, Myriam Quéméner et Anne Souvira.

Aujourd'hui avez-vous le sentiment que les professionnels, tous domaines confondus, ne sont pas assez formés en matière de sécurité numérique ?

Pour apporter une réponse pertinente, il est essentiel de distinguer au moins trois catégories de professionnels :

• Les professionnels de la sécurité. Ils sont d'une manière générale suffisamment formés mais trop peu nombreux.

• Les professionnels IT. Un grand nombre de ces experts manque encore de compétences en sécurité. Cela peut paraître surprenant mais beaucoup d'ingénieurs (y compris en informatique) n'ont pas été initiés à la sécurité au cours de leurs études.

Considérons les autres métiers. Pour eux, le manque de formation est patent. Depuis quelque temps, des progrès tangibles sont à noter et la prise de conscience de la gravité de la menace est en marche. Mais entre une prise de conscience collective et une adaptation des comportements pour lutter efficacement contre les menaces, il y a encore une étape à franchir et la formation doit les aider ! Si la sensibilisation est le premier objectif à atteindre, elle doit être suivie d'une formation pour parvenir à une montée en compétences qui permettra un réel changement des habitudes.

Pour synthétiser, chaque collaborateur quelles que soient ses fonctions doit avoir des compétences en la matière. La sécurité numérique est un sujet transversal qui ne se limite pas à la seule expertise technique, si essentielle soit-elle.

Comment appréhendez-vous la formation en cybersécurité ? Existe-t-il des fondamentaux à ne pas manquer afin d'optimiser les formations ?

Il est préférable aujourd'hui de parler des formations en cybersécurité et non plus de la formation en cybersécurité. Les professionnels de la sécurité distinguent les non experts desquels ils attendent de plus en plus de maîtrise du sujet et les experts qu'ils souhaitent de plus en plus nombreux.

Et, cette distinction mérite encore d'être affinée. La cybersécurité englobe une grande diversité de métiers. De l'architecte de sécurité au RSSI (responsable de la sécurité des systèmes d'information) en passant par le juriste spécialisé, les enseignements doivent se structurer pour répondre à ces différenciations et la formation doit délivrer des compétences adaptées. La liste de ces métiers est longue et ne manquera pas de s'étoffer dans les années à venir. L'ANSSI (l'Agence Nationale pour la Sécurité des Systèmes d'Information), avec un groupe de travail composé de représentants de l'enseignement supérieur et du monde industriel, a identifié 16 filières actuellement en plein développement.

Quant aux non spécialistes, l'ANSSI a isolé des règles simples qu'elle a qualifiées d'hygiène informatique et qui devraient au minimum être abordées dans toutes les formations. Il est aussi indispensable de différencier la formation initiale et la formation

continue, qui se doit d'être plus souple pour s'adapter aux profils des stagiaires, au temps qu'ils peuvent dégager et au contexte spécifique de l'activité de leur structure. Pour harmoniser les méthodes pédagogiques avec les nouvelles mobilités, nous proposons, en parallèle des formations présentielles, des parcours d'enseignement à distance pouvant être suivis depuis son domicile ou son lieu de travail.

Cela étant, des savoir-faire communs, transversaux et fondamentaux devraient figurer au programme de chaque parcours. Le caractère multidimensionnel de la sécurité numérique impose d'intégrer, en complément des matières scientifiques et techniques des composantes juridiques managériales et comportementales dans tous les enseignements qu'ils soient initiaux ou professionnels et quel que soit leur degré de technicité. La subtilité consiste à trouver le juste équilibre entre ces différentes matières pour une intégration efficace dans chaque cursus.

Il apparaît aujourd'hui nécessaire, si ce n'est indispensable, d'anticiper les attaques, de sécuriser les systèmes et les applications, et de répondre aux incidents de façon appropriée. Que diriez-vous aux personnes qui hésitent encore à se former sur ces problématiques ?

Les évolutions et les innovations qui se profilent ne peuvent se réaliser que dans un climat de confiance. La sécurité doit être consubstantielle au développement des technologies de demain.

Pour assurer une sécurité efficace, nous savons que la montée en compétences de chacun est indispensable. Les solutions techniques seules, si performantes soient-elles, resteront insuffisantes. Faire des collaborateurs la première ligne de défense face à une attaque est le défi que la formation doit relever. Il est grand temps de changer de paradigme. La formation doit être perçue comme un investissement d'avenir et ce n'est pas parce que son retour est difficilement quantifiable, qu'il est inexistant !

Et, pour conclure, c'est la phrase d'Abraham Lincoln que nous retiendrons :

« *Si vous trouvez que l'éducation coûte cher, essayez l'ignorance* »

L'AUTEUR

Juriste, spécialisée en droit des propriétés intellectuelles et en droit des nouvelles technologies, Marie Moin est responsable des enseignements juridiques au sein de l'EPITA, école d'ingénieurs en informatique En 2013, l'école lui confie le développement de SecureSphere by EPITA, son offre de formation en cybersécurité destinée aux entreprises. Depuis deux années, elle poursuit le développement de cette entité et en assure la direction.

ALLER PLUS LOIN

N'hésitez pas à consulter nos sites internet :
www.securesphere.fr & www.epita.fr ou à nous écrire à l'adresse suivante : contact@securesphere.fr

Les crypto monnaies :
une insécurité qui nuit à la confiance

par JEAN-LUC DELANGLE

Il est difficile désormais d'échapper à la vague « bitcoin » et autres crypto-monnaies. Ces dernières se vendent, s'achètent et s'échangent, comme de vraies monnaies. Pourtant elles conservent quelques relents sulfureux. Leur univers, aux règles pas toujours très claires, comporte de très nombreux risques pas seulement « cyber » mais aussi juridiques et économiques. Le manque de confiance qui en découle constitue sans doute une menace majeure pour leur pérennité.

JEAN-LUC DELANGLE

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

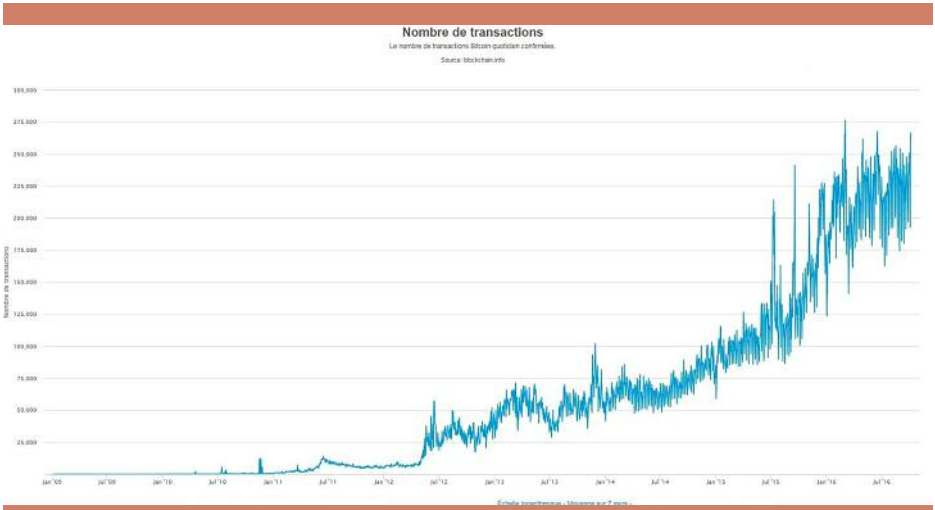
Les termes «monnaie virtuelle» et «crypto monnaie» se sont répandus de façon récente. Les définitions n'en sont pas totalement arrêtées et une clarification reste nécessaire.

Le terme de «monnaie virtuelle» semble avoir été utilisé initialement par la Banque Centrale Européenne pour désigner un instrument numérique utilisé comme une monnaie mais dont les instigateurs - gestionnaires du dispositif voire régulateurs[1]- sont des agents purement privés et dont les utilisateurs constituent de facto une communauté. En sont donc exclues les monnaies locales qui fleurissent ici ou là et sont des avatars de la monnaie nationale[2].

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

(2) Ces monnaies locales sont étroitement liées à la valeur de l'euro et répondent à des obligations règlementaires posées notamment dans les articles L.311-5 et L.311-6 du Code monétaire et financier ; elles n'entrent pas dans le champ du présent article.

À l'origine, les monnaies virtuelles désignent les simulacres de monnaie utilisés au sein des métavers, sites à la fois de jeux de rôles multijoueurs et réseaux sociaux, comme le lindendollar



Un nombre de transactions qui arrive à un palier technique du fait d'une insécurité des transactions.

du site «Second Life». Elles sont cependant très vite sorties de l'univers ludique et le lindendollar s'achète aujourd'hui contre des devises souveraines.

Une seconde vague a été constituée par des dispositifs alliant système de paiement centralisé et monnaie totalement privée. C'est ainsi qu'ont fonctionné E-gold, de 1996 à 2006, et « Liberty reserve » de 2006 jusqu'à son démantèlement par les polices de 17 pays en mai 2013 et la condamnation de ses promoteurs par la justice américaine pour blanchiment d'argent.

La troisième vague a été celle de la décentralisation, avec une « monnaie » dont le parangon est le bitcoin. Reposant sur un algorithme cryptographique, ce type de monnaie est désigné sous le vocable de « crypto-monnaie ». Ses promoteurs se réclament très ouvertement d'une philosophie libertarienne et ne cachent pas leur méfiance envers l'État et envers les banques. Il fonctionne en « peer to peer », c'est-à-dire en échange direct et décentralisé entre internautes permettant les règlements directs. Les transactions financières se dispensent de banques ou de plateformes de compensation, ce qui, selon ses partisans, réduit très fortement les coûts de fonctionnement. Le système est organisé en une sorte de vaste livre de comptes recensant l'ensemble des transactions et dont disposent tous les participants. Autrement dit, le dispositif « bitcoin » est un système de paiement appelé « Bitcoin » disposant de son propre instrument d'échange. Il existe un nombre élevé de crypto-monnaies –

plusieurs centaines dont certaines ont déjà disparu - et le domaine fait preuve d'une recherche constante d'évolution (ce qu'on appelle le bitcoin 2.0). Le bitcoin reste néanmoins le modèle type, celui qui est très majoritairement utilisé dans les transactions impliquant des crypto-monnaies, constituant de ce fait la référence du présent article.

Une « crypto monnaie virtuelle » en plein boom

De création récente - 2009 -, le bitcoin est sorti du cercle des initiés à partir de 2013. Le nombre de transactions quotidiennes a connu une hausse brutale à la mi-2012, atteignant les 25000. Le cap des 100 000 transactions quotidiennes a été durablement franchi en janvier 2015 mais fin 2016 le mouvement semble se stabiliser avec 225 à 275 000 transactions quotidiennes.

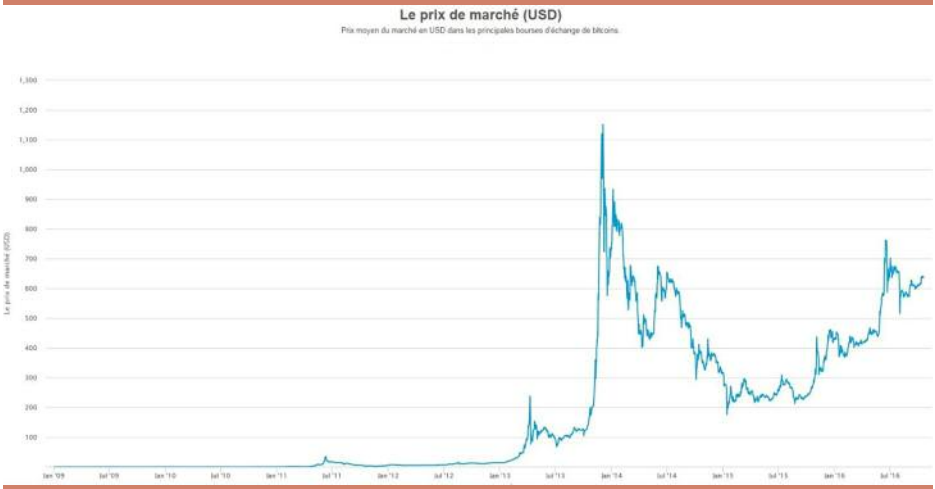
Le nombre de bitcoins en circulation croît selon un algorithme déterminé, atteignant fin 2016 les 16 millions sur les 21 qui pourront être créés. Sans être négligeable, la liste des entreprises qui acceptent ce type de monnaie demeure encore restreinte, voire confidentielle. Quoi qu'en disent ses promoteurs, l'utilisation du bitcoin – et des monnaies virtuelles d'une façon générale – se heurte notamment à une insuffisance majeure de sécurité, contrepartie à payer d'une liberté voulue totale.

Une insécurité juridique des paiements

Le Code monétaire et financier définit différents éléments de protection des utilisateurs de moyens de paiement. Il existe ainsi des possibilités de contestation et de recours juridique en cas d'incident, des règles de fonctionnement légales. Aucune ne s'applique au bitcoin, dont le statut légal est à ce jour parfaitement indéfini. Les promoteurs des monnaies virtuelles utilisent des arguments à géométrie variable au gré de leurs intérêts. Ainsi, se sont-ils réjouis du début de reconnaissance du bitcoin comme monnaie au travers de la décision de la Cour de Justice européenne d'exonérer de TVA « les opérations d'échange de devises traditionnelles contre des unités de la devise virtuelle « bitcoin » (et inversement) » car elles « *constituent des prestations de services fournies à titre onéreux au sens de la directive, dès lors qu'elles consistent en l'échange de différents moyens de paiement* »[3]. Mais tout autant, ils se sont félicités qu'à l'inverse un juge de Floride ait arrêté en juillet 2016 que le bitcoin n'était pas un instrument monétaire, relaxant un prévenu mis en cause pour infraction à la législation sur le blanchiment d'argent.

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

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



Cours du bitcoin contre dollars depuis 2009 (https://blockchain.info)

En France, l'ACPR[4] exige depuis le début de l'année 2014 que les plateformes exerçant des activités de change « bitcoins contre euros » reçoivent un agrément en tant qu'établissement de paiement. Il ne s'agit pas pour autant d'une reconnaissance officielle du bitcoin en tant que devise. Simplement, la réception de fonds en euro pour le compte de la clientèle, nécessaire pour la gestion des opérations de change, « relève de la fourniture de services de paiement » et, à ce titre, est réglementée. L'octroi de cet agrément implique de la part de son bénéficiaire des obligations en matière de contrôle interne, de cyber-protection et de lutte contre le blanchiment.

Une insécurité économique : aucune garantie de valeur

Le bitcoin offre l'avantage d'être convertible en monnaies officielles, à partir notamment de plateformes qui effectuent ces opérations de change. La contre-valeur en monnaies officielles du bitcoin obéit pleinement à la très classique règle de l'offre et de la demande : s'il y a plus de bitcoins à vendre contre une monnaie donnée que de bitcoins demandés dans cette monnaie, le cours du bitcoin baisse ; à l'inverse, s'il y a plus de bitcoins demandés que de bitcoins à vendre, le cours du dans la monnaie donnée augmente.

Les plateformes de change publient les cours en temps réels. Ces cours – sauf accident – ne diffèrent pas trop d'une plateforme à une autre, les opérateurs effectuant des arbitrages[5]. Le cours du bitcoin apparaît comme très instable.

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

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

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

D'aucuns affirment qu'il s'agit là d'un défaut de jeunesse qui passera avec le temps. C'est peu probable, l'instabilité étant inhérente par construction. Le bitcoin fait donc courir un fort risque de change[6] aux détenteurs :

– il ne possède pas de valeur intrinsèque, qui jouerait le rôle d'un garde-fou ; les métaux précieux, par exemple, ont une valeur *a minima* qui est celle fixée par l'offre et la demande industrielles ; son pouvoir d'achat s'établit en fonction de son taux de change ;

– aucune banque centrale n'intervient pour maintenir sa valeur de change ;

– il n'est pas adossé à une économie et de ce fait, la masse monétaire de bitcoins n'est pas garantie par une production de biens et de services[7] ;

– il est en concurrence permanente avec les monnaies officielles et avec les autres crypto-monnaies, ces dernières offrant les mêmes services, voire plus ; un simple effet de mode ou un engouement même passager pour une monnaie virtuelle concurrente se feraient alors sentir sur le cours du bitcoin ; ainsi le « monero » dont les promoteurs affirment qu'il est des plus anonymes a vu son cours doubler au cours de l'été 2016 et se pose en rival ;

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

Il en résulte que le bitcoin est d'une nature très volatile. Il se montre très sensible au contexte politique. Sa première envolée, celle qui l'a fait connaître, date du printemps 2013 avec la crise chypriote et ses conséquences, notamment le blocage des comptes bancaires de l'île. De même, la crise grecque de l'été 2015 et le Brexit au début de l'été 2016 ont provoqué des sursauts. A l'inverse, des prises de bénéfice après de fortes envolées, des interdictions ici ou là, ou le piratage de plateformes ont fait chuter les cours. Pour illustrer ces variations, il suffit de constater une chute de l'équivalent de 110 € (par bitcoin …) en 3 jours fin juillet 2016 à la suite du vol de 119 756 bitcoins sur la plateforme BIFINEX. Dans l'autre sens, le cours du bitcoin a pris 10 % entre le 4 et le 11 septembre 2016 et même 3 % en une heure le 11 octobre 2016 … L'activité économique s'accorde mal avec une monnaie dont, au final, on ne sait trop quel sera son pouvoir d'achat, même à court terme.

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

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

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

Certes, il existe des produits de couverture[8] – qui ne demandent qu'à devenir purement spéculatifs – comme les contrats sur différence (CFD), les contrats à terme ou des swaps entre monnaies virtuelles[9]. Cependant, ces produits sont complexes, parfois risqués car avec de forts effets de levier[10] et évoluant trop souvent dans un univers aux règles floues. Ils sont à déconseiller au commun des mortels!

Enfin, il convient de constater la conception quelque peu schizophrénique du fonctionnement du bitcoin. En effet, la masse monétaire est amenée à se stabiliser alors que ses promoteurs encouragent le développement des échanges, donc de la circulation de la monnaie. De par la demande accrue, chaque bitcoin va être amené à se valoriser, ce qui encourage alors des comportements de thésaurisation pour profiter de l'effet d'aubaine qui ralentissent l'utilisation de la monnaie. Cet antagonisme constitue un facteur d'instabilité latent.

Du pain béni pour le crime

Le système Bitcoin repose sur une technologie innovante, la blockchain, qui est « une technologie de stockage et de transmission d'informations, transparente, sécurisée, et fonctionnant sans organe central de contrôle. Par extension, une blockchain constitue une base de données qui contient l'historique de tous les échanges effectués entre ses utilisateurs depuis sa création. Cette base de données est sécurisée et distribuée : elle est partagée par ses différents utilisateurs, sans intermédiaire, ce qui permet à chacun de vérifier la validité de la chaîne »[11]. La blockchain constitue le grand livre comptable où est recensé l'ensemble des transactions. Pour autant est-elle fiable ? On évoque certes la fraude « 51 » qui permettrait à un individu détenant suffisamment de puissance de calcul d'attaquer l'intégrité du dispositif. Il semble néanmoins que le coût d'une telle fraude soit prohibitif.

(11) Source : https://blockchainfrance.net/decouvrir-la-blockchain/c-est-quoi-la-blockchain

(12) La question s'est posée en son temps de la conservation des différents signes monétaires, c'est d'ailleurs là un des motifs de l'émergence des banques.

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

La vraie question de la sécurité consiste en la protection des bitcoins détenus. Qu'ils soient sur un support informatique personnel ou confiés à une plateforme spécialisée, ils attirent la convoitise des pirates[12]. Les chiffres sont éloquents : MTGOX – qui fut jusqu'à sa disparition

l'une des références du marché des bitcoins – a vu s'envoler[13] l'équivalent de 450 millions de dollars. Au début du mois d'août 2016, c'est BITFINEX qui s'est fait voler 36 % de bitcoins détenus, soit 64 millions de dollars. À côté, le piratage de BITSTAMPS en 2015 fait figure de gagne-petit, avec seulement un vol de 4,3 millions de dollars. Au final, selon des données fournies par REUTER, ce serait 30 % des plateformes qui auraient été piratées depuis 2012, principalement en raison d'un manque de moyens pour assurer une cyber-protection efficace. Les pertes pour l'essentiel ont été répercutées sur les clients. On peut également avancer sans crainte que l'absence d'autorité de surveillance facilite les comportements à risque. Par comparaison, le secteur bancaire a une obligation de protection[14] et rend des comptes à une autorité de contrôle.

(14) Articles 88 et 89 de l'arrêté du 3 novembre 2014.

Le bitcoin n'est pas qu'objet de délit, il en est aussi moyen. Le monde criminel est un univers fort bien structuré, à l'affût de toute innovation permettant d'accroître sa performance et sa rentabilité. Les crypto-monnaies offrent des atouts considérables : discrétion, anonymat, circulation de valeurs sous un volume inexistant, sans frontière et sans le contrôle d'un tiers …

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

En France, la gendarmerie a fermé, en juillet 2014, une plateforme clandestine de change, saisissant au passage 388 bitcoins, l'équivalent de 200 000 €. Elle était notamment utilisée dans le cadre d'activités illicites de jeux en ligne. L'utilisation des bitcoins apparaît aussi avec les rançongiciels qui bloquent les ordinateurs tant qu'un paiement n'a pas été effectué, allant jusqu'à la destruction des données. Selon le GUARDIAN[15], des banques anglaises stockeraient même des bitcoins pour faire face à d'éventuelles attaques de ce type.

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

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

Le bitcoin est parfois comparé à l'argent liquide, ce qui demeure assez inexact. L'usage du numéraire est fortement encadré, la plupart des paiements étant notamment limités à 1 000 €[16] . Le bitcoin, lui, s'il est anonyme, reste

traçable : le « registre » de l'ensemble des opérations est à la disposition des participants au système. Toutefois, il existe des méthodes de blanchiment utilisées entre porte-monnaies de crypto-monnaies, comme le « schtroumfage[17] », altérant cette traçabilité. Mais surtout, le bitcoin permet une circulation transfrontalière et extrêmement rapide de valeurs. Pour le crime, ce peut être un outil formidable … à condition de maîtriser le risque de change.

(17) Multiplication des mouvements entre quelques portemonnaies pour nuire à la traçabilité des flux.

À l'instar d'internet, le bitcoin et les crypto-monnaies constituent une formidable innovation. En revanche, le danger vient principalement de leur environnement. Elles ne pourront trouver leur place que si elles inspirent et méritent confiance. Tant pis pour l'esprit libertarien : elles ont besoin d'un tiers de confiance garant de leur bonne conduite.

L'AUTEUR

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

Le cyberespace et les enjeux environnementaux

par OTMANE BOUSSEBAA

« ***Avec un milliard de capteurs intégrés dans l'environnement tous reliés par des systèmes informatiques, logiciels et services, il sera possible d'écouter les battements du cœur de la Terre, en impactant l'interaction humaine avec le monde.*** » **Peter Hartwell, Chercheur principal, HP Labs.**

Depuis plusieurs siècles, le monde a pu se développer grâce à des révolutions successives ayant comme point commun de générer un changement global du système technique qui influence la société.

OTMANE BOUSSEBAA

Lieutenant de la gendarmerie royale marocaine
Ingénieur, Master 2 « Droit et stratégies de la sécurité

Cela était le cas, dès la renaissance, avec la révolution de la machine dont le symbole reste la presse à imprimer de Johannes Gutenberg en 1450. Ensuite la révolution mécanique de l'ère industrielle a permis la mise en œuvre de trois innovations majeures, en l'occurrence : l'emploi généralisé du métal dans le domaine des matériaux, l'utilisation corollaire de la machine à vapeur dans celui de l'énergie et l'essor du charbon comme combustible. Actuellement, nous sommes en train de vivre l'ère de la 3e révolution industrielle qui est numérique. À l'opposé des précédentes mutations, il a fallu seulement quelques années à l'humanité pour bâtir le cyberespace – un monde parallèle dans lequel nous sommes à la fois des spectateurs et des acteurs – et pour métamorphoser la notion du temps et de l'espace, les habitudes, les relations humaines ainsi que le rendement professionnel… En effet, aujourd'hui, l'être humain est capable de réaliser des tâches extrêmement difficiles en un minimum de temps grâce à l'automatisation. Il est également en mesure de se déplacer virtuellement

n'importe où sur le globe en un simple « clic ».

Ce qui était perçu autrefois comme relevant de l'impossible relève aujourd'hui de la banalité. Ainsi, tout est devenu connecté : un individu peut habiter une maison intelligente permettant de réguler automatiquement ses paramètres d'ambiance. Il peut conduire une voiture intelligente, auto-pilotable, connectée en temps réel au trafic et aux données climatiques. Au travail, plusieurs fonctions s'offrent à lui, facilitant la tâche, comme le contact par mail, la visioconférence, la consultation des données en temps réel,… L'e-commerce est disponible sur le net, offrant l'avantage de comparer les prix d'un large panel de produits. Le soir pour se divertir chez lui sans avoir à se déplacer, plusieurs moyens sont mis à sa disposition, comme le téléchargement de films, les jeux en ligne, les commandes de restauration à domicile…De façon générale, la vie est facilitée grâce au recours à une technologie sophistiquée au service de l'Homme. Cependant, face à tous ces avantages que nous procure le cyberespace, il est judicieux de se poser la question inéluctable de la face cachée de ce développement technologique exponentiel.

Actuellement, la montée en puissance du monde numérique génère une flambée de problématiques. D'une part, tous les ordinateurs, téléphones portables et capteurs, dont nous sommes équipés, ont besoin de l'électricité pour fonctionner et l'augmentation de leur nombre se traduit par une explosion de sa consommation. D'autre part, tous ces équipements, arrivant en fin de vie, deviennent des déchets qui doivent faire l'objet de traitements adaptés. Il faut également appréhender l'enjeu de la sur-extraction des minerais et des matériaux utilisés dans le domaine des NTIC qui entraîne une raréfaction de ces ressources à l'échelle mondiale ainsi que d'autres problèmes liés à l'environnement local comme les nuisances et l'impact sur la santé.

L'appréhension de l'impact environnemental généré par le monde numérique se fait par la maîtrise de la notion d'empreinte carbone, par le diagnostic des différentes problématiques qui en découlent, notamment celle des déchets, de l'énergie, de l'épuisement des matériaux et enfin celles relatives à la santé publique.

À l'instar des autres secteurs, le monde des NTIC a aussi une empreinte écologique, c'est-à-dire un impact environnemental produit par les différents équipements. Aux outils directement perceptibles (téléphones, ordinateurs, capteurs,…) il faut ajouter ceux qui servent au fonctionnement de l'immense toile: des fibres optiques, des câbles en cuivre, des émetteurs Wi-fi, des antennes de téléphonie cellulaire, des routeurs qui relaient les données et établissent les chemins vers les destinations. Il faut y ajouter les fameux data-centers, ces centres où sont traitées et stockées toutes les données générées. Selon le site

(1)http://ecoinfo.cnrs.fr/

« Ecoloinfo[1] » : 5 milliards de personnes sont en ligne dans le monde entier ; les seules infrastructures de télécommunication (les équipements réseaux) seraient responsables de 37 % des émissions de CO2 des TIC ; l'empreinte énergétique du net est en croissance de plus de 10 % chaque année ; Internet pèserait près de 300 millions de tonnes de CO^2 par an, l'équivalent de 2 trajets Paris New-York par an et par Français.

Des déchets dangereux objets de trafics

Les Déchets des équipements électroniques et électriques (DEEE) ont une empreinte écologique très élevée en raison des importantes quantités de ressources en eau, métaux, et énergies mobilisées par la conception, la fabrication, le transport, l'utilisation et le recyclage des composants et objets électriques et électroniques. Les DEEE contiennent des métaux précieux (argent, or, palladium, cuivre et indium en particulier) dont l'exploitation est une source potentielle d'emplois mais d'un usage dangereux s'il n'est pas associé à des législations et des pratiques qui prennent en compte le fait que certains composants sont aussi des déchets toxiques ou dangereux tels que l'aluminium, le cuivre, le plomb, le zinc, des métaux du groupe du platine, l'argent et également des polluants persistants tels que l'arsenic, le mercure, le cadmium et lithium, *etc.*) sans oublier le verre, les plastiques et la céramique. Selon une étude du Programme pour l'environnement des Nations Unies[2], 60 à 90% des déchets électroniques sont revendus et/ou jetés illégalement par des trafiquants. Interpol estime qu'une tonne de déchets électroniques se négocie environ 500 dollars au marché noir. Avec une prévision de 41 à 75 millions de tonnes émises chaque année, dès 2017, le montant du trafic est estimé entre 12 et 19 milliards de dollars, soit 10 à 17 milliards d'euros.

(2) https://www.greenit.fr/2015/05/18/dechets-electroniques-un-trafic-mondial-de-17-milliards-d-euros/

http://www.nextinpact.com/archive/35098-dechets-electroniques-dechets-pollution-nati.htm

(3) http://www.actu-environnement.com/ae/dossiers/efficacite-energetique/data-centers-reduire-facture-energetique-rester-competitifs.php

Une dépense énergétique inégalement répartie

Le monde numérique consomme de l'énergie électrique pour fonctionner. Cette énergie est en grande partie résultante des énergies primaires de type fossiles, qui sont à la fois épuisables et très polluantes. Le caractère énergivore du cyberespace apparaît à travers toutes ses mailles, allant du besoin énergétique des data-centers[3] à celui des simples internautes (ordinateurs, tablettes, téléphones portables,…).

Si aucune statistique n'existe pour quantifier les besoins énergétiques globaux des centres de traitement de données, leur augmentation ne fait

(4) http://www.guide informatique.com/dossiers-actualites-informatiques/consommation-electrique-des-data-centers-29.html

Fotolia : vladimircaribb

Un data center fiable et économique repose sur l'ingénierie des salles, le choix de serveurs et de racks intelligents et des systèmes de contrôle de paramètres évolués.

aucun doute[4]. À l'échelle européenne, la Commission estimait cette consommation à 56 milliards de kilowatts, en 2008, et tablait sur 104 milliards en 2020. Les centres de données, qui consomment 2% de l'énergie mondiale, entraînent de larges émissions de CO2. Cependant, la consommation électrique et les émissions de gaz à effet de serre générées par les data-centers sont plus faibles comparées à celle des ordinateurs qui s'y connectent. Trois facteurs peuvent être pris en compte pour justifier cette idée :

• la consommation électrique propre au matériel,

• le rapport entre le nombre d'utilisateurs et de serveurs et le temps nécessaire pour délivrer la page (temps passé par le serveur à générer la page et par le réseau à l'acheminer jusque chez l'internaute),

• le temps passé par l'utilisateur à interagir avec cette page.

Pour le premier point, les ordinateurs consomment en valeur absolue, de l'ordre de 50 à 100 fois moins d'électricité que les serveurs (30Wh/h pour un ordinateur portable contre 300 Wh/h pour un petit serveur). En valeur relative, les serveurs sont bien plus efficients que les ordinateurs des internautes car ils consomment moins d'énergie pour réaliser le même nombre de traitements informatiques. Concernant le point 2, un seul serveur est généralement capable de répondre aux sollicitations de plusieurs centaines à plusieurs milliers d'internautes. Le rapport est donc très défavorable pour les internautes qui pèsent bien plus lourd dans la dépense énergétique que les serveurs. Google sert

par exemple 3000 utilisateurs de G mail avec un seul serveur d'une puissance de 450 watts.

Enfin pour le troisième point, l'internaute passe plus de temps à lire une page ou à interagir avec elle que le serveur à la générer, d'autant plus si l'on prend en compte des différents caches (navigateur, proxy…). On peut avancer qu'un internaute passe 10 à 100 fois plus de temps sur la page que le serveur à la générer. Les ordinateurs des internautes consomment bien plus d'énergie que les serveurs web, pour une même unité fonctionnelle. À ce titre, une étude a été réalisée chez deux serveurs – Gmail et GrennIT.fr[5] – démontrent que les internautes consomment entre 300 et 900 fois plus d'énergie que les serveurs des data-centers.

(5) https://www.greenit.fr/2015/05/12/quelle-est-l-empreinte-environnementale-du-web/

L'épuisement des matériaux

Depuis plusieurs années, des études présentent les TIC comme l'une des industries ayant le plus fort impact sur l'environnement par unité produite, celle d'Eric Williams[6] en 2002 résume parfaitement ce point de vue. La demande pour les métaux utilisés dans les industries de hautes technologies (dont les TIC) a plus que triplé au cours de 20 à 30 dernières années. Dans la même période, la sollicitation des métaux dans la table de Mendeleïev est passée de 10 dans les années 1980 à 60 métaux dans les années 2010. Un rapport de l'Union européenne précise que certains de ces éléments vont être particulièrement sollicités par ces industries de pointe d'ici à 2030 : le gallium (Ga) va voir sa demande multipliée par plus de 22, l'indium (In) et le germanium (Ge) par 8, le néodyme (Nd) par 7, le titane (Ti) par 4, le cuivre (Cu) et la palladium (Pa) par 3,5 et l'argent (Ag) par 3.

(6) Institut de Technologie de Rochester

La santé publique

Nous n'avons pas actuellement de preuves directes et scientifiques de la responsabilité des radio-fréquences des antennes relais dans la genèse de cancers ou de leucémies, y compris chez les enfants. Le nombre d'antennes relais doit être mis en rapport avec le nombre de personnes exposées. Cinq milliards d'individus sont aujourd'hui exposés aux émissions de radiofréquence. Avec un échantillon de population aussi important, les maladies engendrées devraient être normalement plus nombreuses. L'étude « Interphone[7] » a examiné spécifiquement l'évolution des tumeurs du cerveau et des leucémies. Cette étude a été réalisée dans 13 pays sur 5 000 cas. Cette étude montre qu'il existe une possibilité faible d'augmentation de fréquence des gliomes, tumeurs cérébrales graves, et des neurinomes du nerf acoustique,

(7) La recherche, baptisée Interphone, a réunit des équipes de spécialistes, provenant de treize pays. L'enquête, menée à une échelle très vaste pour éviter tout biais régional, s'est concentrée sur le développement de types spécifiques d'affections tumorales du système crânien : tumeurs du cerveau (gliomes et méningiomes), des glandes salivaires (parotides) et du nerf acoustique (neurinomes), ainsi que les atteintes de tissus lymphatiques (lymphomes). Les personnes ont été sélectionnées dans les zones d'implantation précoce (cinq et dix ans de recul) et sur une classe d'âge active de 30 à 59 ans, ayant une expérience continue de la téléphonie portable.

tumeurs bénignes mais gênantes, chez les personnes qui utilisent très fréquemment le téléphone et notamment à partir de 10 ans d'exposition. Les opérateurs de téléphonie mobile ont, pour pallier ce problème, l'obligation de donner des oreillettes. On préconise d'utiliser un kit main libre pour téléphoner et de privilégier les SMS surtout pour les enfants.

Dans le cadre des scénarios prévisionnels établis par les cabinets d'étude spécialisés, le nombre d'objets connectés atteindrait au minimum 30 milliards d'unités d'ici l'horizon 2020 ce qui conduira à une aggravation des problématiques que nous venons d'exposer. Cela amène la communauté internationale à prendre des mesures sérieuses pour atténuer l'impact environnemental afférent au monde digital. Dans cette optique, la France a mis en place un corpus juridique complet pour réglementer la problématique des DEEE et leur élimination. Le secteur privé tente de mettre en œuvre des solutions pour promouvoir l'efficacité énergétique, en l'occurrence l'énergie libre, les data-centers vertueux et les compagnes de sensibilisation «E-cleaning days».

Actuellement, on ne peut pas nier le fait que plusieurs pays font des efforts considérables pour atténuer les effets négatifs du cyberespace sur l'environnement, cependant cette problématique revêt un caractère mondial car d'une part les GES[8] générés par l'énergie fossile consommée contribuent au réchauffement climatique à l'échelle planétaire, et d'autre part la pollution atmosphérique, causée par les décharges non contrôlées de DEEE, est transfrontalière.

(8) Les gaz à effet de serre (GES) sont des composants gazeux qui absorbent le rayonnement infrarouge émis par la surface terrestre et contribuent à l'effet de serre. L'augmentation de leur concentration dans l'atmosphère concourt au réchauffement climatique.

Une autre problématique résulte du fait de normes et lois en vigueur différentes d'un pays à l'autre. À titre d'exemple, l'exportation des DEEE est interdite en UE alors qu'elle ne l'est pas aux États-Unis. Il serait donc opportun de débattre sur cette problématique et de convaincre les pays producteurs de la nécessité d'allier un bénéfice économique et les contraintes environnementales afin d'aboutir à un développement durable et pérenne.

L'AUTEUR

Otmane Boussebaa, est officier de la gendarmerie royale marocaine. Il est titulaire d'un diplôme d'ingénieur d'Etat, filière génie civil, de l'Ecole Mohammadia d'Ingénieurs (Rabat, 2014) et du diplôme des études universitaires et militaires, branche (sciences et techniques), de l'Académie Royale Militaire. Il est également lauréat du Master « Droit et stratégies de la sécurité » de l'université Paris 2 Panthéon-Assas (Paris, 2016).

Les enjeux relatifs à la technologie Blockchain

par **LUDOVIC PETIT**

« *The blockchain is the most disruptive technology I have ever seen* »

Salim Ismail, Global Ambassador and Founding Executive Director Singularity University[1]

(1) http://www.christian-faure.net/2015/09/13/la-blockchain-et-lemergence-des-distributed-consensus-engines/ http://www.christian-faure.net/wp-content/uploads/ismael2-1024x768.jpg

Avant de disserter sur un tel sujet, il convient d'en expliquer le concept. Une blockchain n'est pas un logiciel, c'est un concept technologique. Une blockchain est un livre de transaction numérique distribué, avec des copies identiques maintenues sur plusieurs systèmes informatiques contrôlés par des entités différentes. La Blockchain est un système de base de données distribuée qui permet de rendre infalsifiable l'historique des transactions effectuées entre des parties.

LUDOVIC PETIT

Directeur Cyber Sécurité
Groupe Altran
Réserve Citoyenne
Cyberdéfense

Un grand livre de transactions

La base de données distribuée des transactions est appelée « *Ledger* » en anglais, littéralement « *grand livre* » ou « *livre de compte* ». Jusqu'à présent, la confiance dans une transaction est, en général, portée par une institution tierce et centralisée. Avec une informatique de confiance permise par le nouveau paradigme technologique proposé par la Blockchain, la confiance est portée par les algorithmes cryptographiques, le chiffrement et l'organisation décentralisée au sein du réseau des données issues de la transaction.

On parle dès lors de consensus décentralisé. Il permet de s'affranchir de l'intermédiation d'une institution centralisée, notamment bancaire dans le

cas des transactions de paiement. De par son concept fonctionnel, c'est ce nouveau paradigme, ce nouveau modèle fonctionnel, qui avère une notion de confiance technologique contextuelle, autrement appelée Sécurité. Nous y reviendrons.

Les ordinateurs équipés de l'interface logicielle nécessaire communiquent ensemble pour réaliser les transactions commandées par les utilisateurs qui, eux, forment le réseau de la blockchain. La valeur d'échange est le token (jeton, que l'on peut assimiler à une empreinte numérique) qui, par exemple dans le cas de transaction financière a valeur de monnaie cryptographique. C'est pourquoi on parle de crypto-monnaie (ou cryptocurrency en anglais, bien que le terme 'currency' soit relatif à la devise).

Littéralement, une blockchain désigne une chaîne de blocs, des conteneurs numériques sur (en fait, dans) lesquels peuvent être stockées des informations de toute nature : transactions, contrats, titres de propriétés, *etc.* L'ensemble de ces blocs forme une base de données semblable aux pages d'un grand livre de compte. Ce livre de compte est décentralisé, c'est-à-dire qu'il n'est pas hébergé par un serveur unique mais par une partie des utilisateurs. Les informations contenues sur les blocs sont protégées par plusieurs procédés cryptographiques innovants si bien qu'il est (à date) impossible de les modifier *a posteriori*. Enfin, la Blockchain est créatrice d'une crypto-monnaie qui lui permet de rémunérer certains nœuds du réseau qui supportent son infrastructure.[2]

(2) Livre Blanc « Comprendre la Blockchain » publié par la société U change

http://www.uchange.co/download/blockchain-whitepaper/

(3) (3) Satoshi Nakamoto. « Bitcoin: A Peer-to-Peer Electronic Cash System » (24 May 2009)

https://bitcoin.org/bitcoin.pdf

La sémantique est piégeuse. Il s'agit en effet de distinguer LA Blockchain comme technologie, fruit des travaux de Natoshi Sakamoto[3], et UNE blockchain spécifique que chaque organisation pourra potentiellement déployer. Autre difficulté, aujourd'hui l'expression « la blockchain » désigne souvent la blockchain utilisée par la crypto-monnaie Bitcoin, Le problème tient au fait que pour la plupart d'entre nous, le concept de la blockchain est intrinsèquement lié à la monnaie digitale (i.e. numérique) Bitcoin.

La Blockchain a trois propriétés : désintermédiation, sécurité, autonomie. Elles reposent sur trois technologies : architecture décentralisée, protection cryptographique et émission de crypto-monnaie.

Blockchain est la technologie sous-jacente à la gestion décentralisée d'une crypto-monnaie. Plutôt que de consigner toutes les transactions dans un grand livre comptable (à l'instar des organismes financiers, banques centrales), la crypto-monnaie a en effet choisi de décentraliser

(4) The great chain of being sure about things

http://www.economist.com/news/briefing/21677228-technology-behind-bitcoin-lets-people-who-do-not-know-or-trust-each-other-build-dependable

http://cdn.static-economist.com/sites/default/files/imagecache/original-size/images/print-edition/20151031_FBC911.png

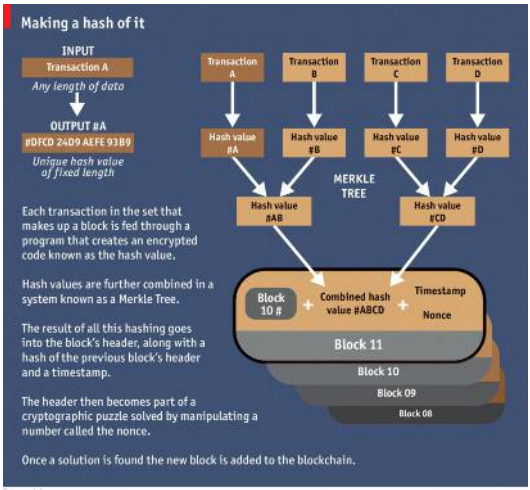
(5) Fonctionnement simplifié de la blockchain

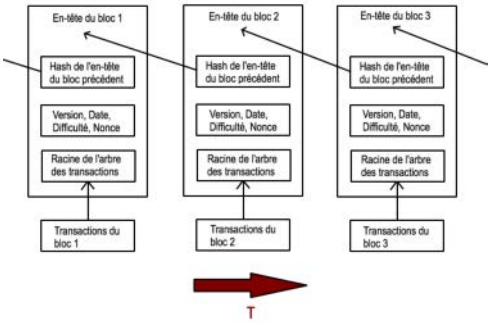
https://i2.wp.com/www.ethereum-france.com/wp-content/uploads/2016/06/blockchainsimplifie.png

https://jurischain.com/bitcoin-2

l'historique des transactions. Ces « blocs » sont détenus par les détenteurs de crypto-monnaie et garantissent à chaque instant l'authenticité et l'unicité des transactions effectuées.

En fait, la validation d'une transaction est assujettie à la résolution par la machine d'un challenge cryptographique qui s'avère coûteux en puissance de calcul. Cette opération mathématique fait appel à des informations contenues dans les blocs précédents de la chaîne. C'est





uniquement lors de sa résolution technique que toutes les transactions de cette dernière sont validées, et un nouveau bloc automatiquement créé est lié aux précédents.[4] [5]

Une approche conceptuelle d'une organisation autonome décentralisée

De nouveaux modèles d'organisation décentralisée et distribuée sont en train de naître, rendus possibles par l'ubiquité d'Internet puis l'émergence de la technologie blockchain, dans le contexte de la mutation de notre civilisation sous l'impact du numérique. Considérées comme une alternative à l'entreprise, aux structures de gouvernance, voire aux Etats, les Decentralized Autonomous Organizations (DAO) – Organisations Autonomes Décentralisées - s'inscrivent dans un nouveau paradigme d'interconnexion collaborative du genre humain.

Les limites de l'organisation verticale de l'entreprise dans le nouveau contexte numérique sont une des raisons de la recherche d'un modèle alternatif pour

l'activité économique et la collaboration. Parallèlement à cela, les limites de nos institutions face à l'accroissement de la population mondiale et à l'épuisement des ressources, expliquent la quête de modèles de gouvernance plus adaptés.

Une brève incise à propos d'un des mythes fondateurs et le contexte d'émergence des DAO : dès la fin des années 1990, à la naissance du World Wide Web, les thèmes qui sous-tendent les débats actuels sur liberté, surveillance et souveraineté du net sont présents. Ceux qui tentent à l'époque de penser le potentiel de ce nouveau réseau ont déjà une intuition forte des tensions à venir. Ainsi, l'économiste Milton Friedman évoque dès 1999 dans une interview le rôle d'une crypto-monnaie, aux caractéristiques proches de celles du Bitcoin que l'on connaît de nos jours, dans l'évolution du rôle central du gouvernement : « *I think that the Internet is going to be one of the major forces for reducing the role of government. The one thing that's missing, but that will soon be developed, is a reliable e-cash, a method whereby on the Internet you can transfer funds from A to B, without A knowing B or B knowing A.* »[6]

(6) http://www.coindesk.com/economist-milton-friedman-predicted-bitcoin/

(7) https://www.eff.org/fr/cyberspace-independence

La Déclaration d'Indépendance du Cyberespace[7] apparaît comme particulièrement prémonitoire dans ce contexte : « *… We are forming our own Social Contract. This governance will arise according to the conditions of our world, not yours. Our world is different. Cyberspace consists of transactions, relationships, and thought itself, arrayed like a standing wave in the web of our communications. (…) Your legal concepts of property, expression, identity, movement, and context do not apply to us. They are all based on matter, and there is no matter here.* » John Perry Barlow, 1996. Barlow a déjà la vision d'un cyberespace constitué de transactions, mais à son époque la liberté et l'autorégulation des transactions, dont il perçoit le potentiel, ne peuvent inclure la matière. La blockchain concrétise aujourd'hui ce lien entre transaction et matière, et va même bien au-delà puisqu'elle le certifie. Elle réintègre directement, et ce dans toute leur puissance, les notions de « *property, expression, identity, movement* » dans le cyberespace. C'est ce lien entre le numérique et la matière qui est nouveau, la blockchain en tant que rupture technologique en ouvre le champ des possibles.

La blockchain sera-t-elle la rupture technologique qui va permettre de concrétiser ces pistes ? La couverture médiatique du sujet est conséquente, une des plus importante de ces dernières années[8]. Décrite comme la « Trust Machine » ou « la machine de confiance »

par The Economist[9], la blockchain est présentée comme la solution de désintermédiation idéale : faible coût, fiable et hautement sécurisée. Le mot est donc lâché : désintermédiation ! La notion de consensus décentralisé ayant pour essence de s'affranchir de l'intermédiation d'une institution centralisée, c'est en cela que l'approche conceptuelle d'une organisation autonome décentralisée telle que la Blockchain, véritable technologie dite de rupture, est dite disruptive, au sens littéral du terme anglais (Perturbateur, adj.).

Dans son rapport intitulé « *Technological Tipping Points and Societal Impact* » de Septembre 2015[10], le World Economic Forum laisse présager que la taxe sera perçue pour la première fois par un gouvernement via une Blockchain en 2025 et que 10% du produit intérieur brut (PIB) mondial sera stocké sur la technologie Blockchain d'ici à 2027. Tel est le champ des possibles.

(8) La Blockchain, « nouvelle star » des médias

http://www.latribune.fr/opinions/tribunes/la-blockchain-nouvelle-star-des-medias-592202.html

http://static.latribune.fr/article_body/592204/02-blockchain.png

(9) The trust machine, The Economist

http://www.economist.com/news/leaders/21677198-technology-behind-bitcoin-could-transform-how-economy-works-trust-machine

(10) Rapport du World Economic Forum « Technological Tipping Points and Societal Impact »

http://www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf

Un concept à intégrer dans un contexte comportant une dimension humaine

Comment pouvons-nous appréhender ce concept tant dans notre quotidien en tant qu'individu, que dans un contexte professionnel, mais aussi relatif aux institutions régaliennes de l'Etat ? Il semble donc évident que l'enjeu majeur de la compréhension, puis de l'adoption de nouveaux modèles organisationnels comme celui d'une organisation autonome décentralisée - Blockchain dans notre cas - est basé sur une constante… l'Humain. Celui-ci, en tant que personne, est le facteur clé de succès de l'intégration de la société numérique d'aujourd'hui, tant dans sa dimension étatique, d'entreprise que sociétale. Notre rapport personnel à d'éventuelles perspectives de changement conditionne donc l'adoption et l'adaptation à ces modèles. C'est notre souhait de vouloir comprendre ce qui va de facto influer notre appétence à ce concept de Blockchain, et par voie de conséquence en assurer le « degré » de prise en compte au sein de notre société. Le champ des possibles est conditionné par cet enjeu majeur. C'est donc en soi une interrogation légitime que de réfléchir au facteur humain et à la maturité de tout un chacun. Le changement dérange, voire perturbe nos habitudes. Je modéliserais mon propos ainsi dans la perspective d'un contexte professionnel d'entreprise :

$$r = f(n^m)$$

r = résistance interne aux nouvelles idées, technologies, aux nouveaux concepts, n = nombres d'employés et m = nombre de niveaux de management.

Il y a donc nécessairement une réflexion à mener.

La technologie Blockchain bouleverse la notion de confiance.

Nous en arrivons maintenant au fondement même de Blockchain, qui par essence conditionne bien des enjeux : Sécurité = Confiance ? Jusqu'à présent, la confiance dans une transaction est, en général, portée par une institution tierce et centralisée. La notion même d'institution implique la reconnaissance officielle tant par le secteur d'activité que par les instances gouvernementales.

Avec une informatique de confiance que pourrait permettre le nouveau paradigme technologique proposé par la Blockchain, la confiance est portée par les algorithmes, le chiffrement et l'organisation décentralisée au sein du réseau des données issues de la transaction. On parle dès lors de consensus décentralisé, qui permet de s'affranchir de l'intermédiation d'une institution centralisée, notamment bancaire dans le cas de transactions de paiement. De par son concept fonctionnel, la technologie Blockchain bouleverse donc de prime abord un point de vue technologique et elle bouscule nos habitudes, bien que l'utilisation de la cryptographie ne soit pas nouvelle. Mais Blockchain est en fait véritablement disruptive dans son concept de consensus décentralisé, qui induit une notion de confiance… technique et technologique. C'est cette confiance technologique inhérente à ce nouveau paradigme, en tant que modèle, qui bouscule notre rapport personnel avec ce que nous concevons être de confiance.

C'est ce nouveau paradigme, ce nouveau modèle fonctionnel, qui avère une notion de confiance technologique contextuelle, autrement appelée Sécurité. Ce qui amène somme toute assez logiquement une réflexion de fond : Devons-nous reconsidérer notre rapport avec le concept de confiance ? Quel est notre rapport psychologique, humain, personnel avec la notion de confiance ? Puis-je concevoir, dois-je concevoir qu'un niveau de sécurité technique, contextuel dans une simple relation bilatérale de pair à pair, implique que je fasse confiance à l'écosystème entier ? Et de laisser notre esprit cartésien tout droit nous mener au sujet de gouvernance et d'autorégulation de la confiance, pour ouvrir le grand livre du Droit (et du devoir), du cadre légal et réglementaire.

Si l'on s'en réfère à la définition du Larousse,

Gouvernance : Action de gouverner, manière de gérer, d'administrer.

Réguler : Fait d'assurer un fonctionnement correct.

Autorégulation : Régulation automatique d'un processus, fonctionnement tel qu'il s'adapte de lui-même aux changements.

Confiance : Sentiment de quelqu'un qui se fie entièrement à quelqu'un d'autre, à quelque chose.

Sécurité : Situation dans laquelle quelqu'un, quelque chose n'est exposé à aucun danger, à aucun risque, absence ou limitation des risques dans un domaine précis.

Il est aussi intéressant de noter la définition suivante :

Dao : Dans l'ancienne philosophie chinoise, principe d'ordre qui fait l'unité de l'univers. La voie.

Au-delà du clin d'œil relatif à l'acronyme DAO (Decentralized Autonomous Organization), le principe d'ordre chinois serait-il la voie vers un système de gouvernance de la confiance ? D'autorégulation ? Gouvernance n'est-il pas in fine question d'ordre et d'unité ? Laissons quelques instants cette perspective pour nous intéresser au cadre légal et réglementaire.

La France dispose certes du cadre légal et réglementaire le plus élaboré au monde mais il convient toutefois de garder à l'esprit que nombre de lois datent, si ce n'est de la période Napoléonienne pour bonne partie de notre Code Civil, au moins d'une époque révolue si l'on se réfère à la dimension temporelle que nous connaissons de nos jours avec l'avènement des nouvelles technologies.

Le monde numérique, dans lequel nous vivons depuis quelques décennies, conditionne de nos jours les enjeux politiques et géostratégiques de l'économie mondiale et de notre économie nationale. C'est donc, notamment, à travers le législateur que cette économie peut trouver croissance, car les lois et les réglementations sectorielles ont certes pour but de réguler un contexte d'activité mais aussi de potentiellement protéger les intérêts des parties. Blockchain s'inscrit dans cette perspective.

Une légitimité à construire

La notion de consensus décentralisé ayant pour essence de s'affranchir de l'intermédiation d'une institution centralisée, comment dès lors le législateur intègrerait-il un concept d'autorégulation de confiance dans la perspective d'une organisation autonome décentralisée ? Rappelons-nous qu'un dirigeant d'entreprise est non seulement civilement mais aussi pénalement responsable au regard de la loi. Cette responsabilité peut-elle être, doit-elle être applicable à un contexte d'organisation autonome décentralisée ?

Juridiques, réglementaires, il est bien des aspects inhérents à la personne, en tant qu'individu. Mais dans le cas d'une organisation décentralisée, que prévoie le législateur ? La notion d'autonomie induit donc par elle-même une perspective de gouvernance, pourquoi pas d'auto-gouvernance, mais qui devra trouver référence dans un cadre légal *ad hoc* pour trouver une légitimité dans un contexte, qu'il soit économique, social ou institutionnel. Ce postulat est fractal, à savoir qu'il est déclinable à l'identique quelle que soit l'échelle – parlons plutôt de contexte - qui *de facto* amène un autre concept, adaptabilité.

Gouvernance et autorégulation de la confiance, une équation multidimensionnelle qui se doit au respect des principes élémentaires de simplicité et de cohérence pour trouver pertinence et écho.

En témoignent les échanges lors du récent Forum Parlementaire de la Blockchain[11] à Paris, je cite Philippe Dewost, chargé de l'économie numérique et du financement des entreprises à la Mission Programme d'Investissements d'Avenir au sein de la Caisse des Dépôts : « *L'économie de l'écosystème d'investissement dans la technologie Blockchain tend à 'migrer' des USA vers la Chine, qui dispose actuellement du plus gros potentiel de calcul dans Blockchain dans le monde (i.e. les Mineurs, Miners). Il faudrait en Europe injecter 500 Millions d'EUR dans la Recherche & Développement sur Blockchain, et 500 Millions d'EUR supplémentaires sur les 3 ans à venir pour accompagner les startups si nous voulons rester dans la course. Entre USA et Chine, il y a l'Europe qui doit saisir sa chance et l'Afrique qui a d'énormes besoins auxquels Blockchain peut apporter réponse.* »

(11) « Code Is Law, On Liberty in Cyberspace », by Lawrence Lessig

Nous vous soumettons quelques témoignages qui permettent de saisir la prise de conscience d'enjeux considérables :

Christian Buchel, directeur général adjoint, chief digital & international officer d'Enedis : « *Un atelier de travail Blockchain est prévu à la prochaine COP22 à Marrakech (Conference Of Parties). Comment la collectivité peut-elle bénéficier de ces modèles de fiabilisation décentralisés ?* »

Corinne Erhel, députée (PS) des Côtes d'Armor : « *L'explication, la pédagogie permet l'anticipation, et les expérimentations doivent mettre en lumière les besoins pour, le cas échéant, légiférer et adapter le cadre légal. La pédagogie par l'exemple.* »

Lionel Tardy, député (LR) de la Haute-Savoie : « *Le rôle du régulateur est d'accompagner et d'identifier la valeur légale de Blockchain, de son usage. Il faut plus de parlementaires spécialistes du numérique au sein de l'écosystème, afin de permettre une meilleure prise de conscience des enjeux.* »

Maître Hubert de Vauplane, avocat : « *il ne faut pas légiférer sur la technologie, mais sur l'usage de ce qui est fait avec Blockchain. « Code is Law »*[12]*, ce sont des chiffres, des mathématiques, a contrario de la Loi qui elle s'exprime en lettres. L'exécution, la faisabilité technique d'un Smart Contract (ou Contrat Intelligent s'appuyant sur Blockchain) implique-t-elle que Code is Law… ou plutôt qu'il faille contrôler la valeur légale d'une action dans le code ? C'est très précisément sur ce point que le législateur doit concentrer la notion de confiance qui s'avère, par des textes et des explications. Le régulateur doit avoir pour but d'accompagner le changement.* »

(12) (13) « Code Is Law, On Liberty in Cyberspace », by Lawrence Lessig

http://harvardmagazine.com/2000/01/code-is-law-html Code is Law - Traduction française de l'article de Lawrence Lessig

Laure de la Raudière, députée (LR) d'Eure-et-Loire : « *La preuve de l'inscription dans la Blockchain doit être avérée, et la notion de 'Tiers de confiance' à caractériser. Blockchain laisse entrevoir des perspectives économiques considérables, il faut annuler le principe de précaution dans notre constitution française, pour y inscrire un principe d'Innovation. Il faut accompagner, il faut de la hardiesse, de l'audace ! Le droit du travail doit être adapté afin de fournir à nos startups les moyens d'évoluer sereinement.* »

Axelle Lemaire, secrétaire d'Etat chargée du numérique et de l'Innovation : « On ne doit pas légiférer tant que l'on n'a pas compris le sujet, les enjeux, les perspectives et les besoins. Il faudra ensuite en revanche adapter notre cadre légal en conséquence. Nous devons nous interroger sur les perspectives. Blockchain devrait intéresser les philosophes, les politiques, parlementaires, les financiers, les organismes de protection de la vie privée, et pas seulement les Responsables de la Sécurité des Systèmes d'Informations et les experts techniques. Il faut avancer ! Nous devons accompagner cette évolution conceptuelle majeure. Un principe d'innovation a été voté par l'Assemblée dans le cadre de la loi Sapin 2. »

Code is law

J'invite à la lecture de « Code Is Law, On Liberty in Cyberspace », par Lawrence Lessig. « … Code is law, and architecture is politics… » ou une brève histoire du Cyberespace : (clin d'œil à 'Une brève histoire du temps' de Stephen Hawking)

Nous sommes à l'ère du cyberespace. Il possède lui aussi son propre régulateur. Ce régulateur, c'est le Code : le logiciel et le matériel qui font du cyberespace ce qu'il est. Ce code, ou cette architecture, définit la manière dont nous vivons le cyberespace. Il détermine s'il est facile ou non de protéger sa vie privée, ou d'agir à dessein. Il détermine si l'accès à l'information est global ou sectorisé. Il a un impact sur qui peut voir quoi, sur qui est qui et qui fait quoi. Lorsque l'on commence à comprendre la nature de ce code, on se rend compte que, d'une

myriade de manières, le code du cyberespace régule. 'Code is Law' est en fait la résultante du concept technologique de la Blockchain.

Rappelons-nous toutefois qu'un Code, quel qu'il soit, ne fait que ce que nous, humains, souhaitons qu'il fasse, car nous l'avons conçu. Avec certes toute notre intelligence… ainsi qu'avec tous nos défauts. Dès lors et par voie de conséquence, quand bien même on s'appuierait sur les normes de qualité et de sécurité les plus évoluées et une implémentation,i.e. le contexte de mise en exécution de tout code, sera potentiellement soumis à défaut. (et de rappeler ici l'importance capitale de la formation des développeurs au 'Secure Coding', i.e. au développement dit 'sécurisé'. La Qualité dans le Code). Qu'il me soit permis de rappeler ici l'excellence française en termes de recherche en mathématiques, de notoriété mondiale. Cryptographie, mathématiques, Blockchain… la France a sa place !

Tel est - certes très brièvement esquissé - le concept de la Blockchain, tels en sont quelques enjeux. Cette législation est en train de changer, elle s'adapte, elle mute. Le 'code du cyberespace' aussi. Et à mesure que ce code change, il en va de même pour la nature du cyberespace.

Les contraires seraient-ils complémentaires ? Assurément, ne serait-ce que dans un concept d'équilibre qui, rappelons-le, est toujours contextuel. L'équilibre est lié au contexte. La sécurité du Code, ou le Code de la sécurité aussi. Le Code est-il force de Loi ? Le Code est-il la Loi ? Le Code deviendra-t-il Loi ? Et à titre de référence légale, devrons-nous concevoir et en appréhender le sens en tant que… Confiance ou 'Code is Law' reste(ra)-t-il un concept abstrait régit par un idiome technologique humainement non concevable en termes de notion de confiance ?

Sommes-nous prêts ? Ou plutôt, sommes-nous suffisamment sages ? Blockchain est plus qu'une technologie. C'est une stratégie. *Connecto, ergo sum.*

L'AUTEUR

Professionnel de la lutte contre la cybercriminalité et de la lutte contre la fraude, Ludovic PETIT est Directeur Cyber Sécurité du Groupe Altran. Il est chercheur associé au Centre de Recherche de l'Ecole des Officiers de la Gendarmerie Nationale (CREOGN), membre de la Réserve Citoyenne Cyberdéfense et Auditeur du Centre des Hautes Etudes du Cyberespace (CHECy).

Former des citoyens
numériquement responsables

par JEAN-PAUL PINTE

Si le cyberespace est devenu un formidable outil d'accès à la connaissance, il est aussi le terrain où se manifestent toutes sortes de déviances, de manipulations et de risques allant jusqu'à mettre à mal les réputations, les identités voire parfois la vie de chacun d'entre nous. Cette société numérique créée par nos interactions et pérégrinations sur la toile répond aujourd'hui au concept de « citoyenneté numérique » pour lequel il convient de former dès le plus jeune âge des citoyens numériquement responsables tout en tentant d'installer ou de rétablir une certaine confiance avec les technologies.

JEAN-PAUL PINTE

Maître de conférences
Faculté des Lettres et Sciences Humaines
Université Catholique de Lille

Citoyenneté numérique : de quoi parle-t-on exactement ?

Le vocable « citoyenneté », emprunté à l'Égypte antique et réservé aux élites de la Macédoine, est l'un des concepts de base de plusieurs disciplines, telles que les sciences politiques, la géopolitique, la sociologie, *etc.* La citoyenneté, pour rappel, évoque les notions de droits civils, politiques et bien évidemment des devoirs civiques qui définissent le rôle, le comportement que le citoyen doit avoir face aux autres membres d'une société donnée. Accouplée à l'adjectif « numérique », qui renvoie aux ressources et aux outils technologiques, elle pose la question de la définition des règles que ledit « citoyen numérique » doit adopter en milieu professionnel, familial et scolaire. C'est, en tout cas, l'une des thèses défendues par Mike Ribble dans son ouvrage « Citoyenneté numérique à l'école »[1]. Ainsi, cette posture

(1) Citoyenneté numérique à l'école, *Technologie de l'éducation*, Mike Ribble – 2014 Editions Reynald Goulet Inc.

épistémologique nous oblige à penser et à accepter que nous sommes dans une « société numérique » existante ou en cours d'exister au regard de nos interactions et pratiques des technologies.

On a longtemps évoqué cette population des Digital Natives de 18 à 35 ans comme des adeptes du numérique. Aujourd'hui il faut reconnaître que pour former des e-citoyens, il conviendra de s'y prendre dès le plus jeune âge. Pour les dépeindre, un néologisme est proposé : les « digiborigènes », un compromis entre « digital natives » et « natifs du numérique ».

Si le Web 2.0, dit social, a marqué et a été le creuset de cette génération avec l'avènement des réseaux sociaux, il ne faudrait pas que les métadonnées générées par ces mêmes réseaux puissent venir industrialiser leurs vies, ce que le Big Data est en train pourtant de faire. Le Web 3.0, dit sémantique, couplé à celui du tout connecté (Web 4.0), si nous n'y prenons garde, pourraient bien aussi dans cette postmodernité faire de nos jeunes citoyens des dépendants du numérique. En effet les réseaux sociaux activent les mêmes parties du cerveau que l'alcool ou la drogue : ils fonctionnent sur le système de récompense et provoquent chez pas mal de jeunes une addiction psychologique.

Se protéger est d'abord une question de bon sens que l'on soit jeune ou adulte et la question se pose souvent de savoir pourquoi on n'adopte pas les mêmes comportements sur Internet que dans le monde réel alors que l'on sait pertinemment, par exemple, que le numérique facilite la tâche des cyberdélinquants. N'allons pas jusqu'à dire qu'il s'agit de tout verrouiller mais apprenons à nos jeunes à évaluer les risques.

Les données transmises par nos enfants de manière volontaire ou involontaire font le terreau de toute une population de personnes mal intentionnées qui, à tout moment s'en serviront pour dénigrer, faire chanter ou encore user de l'identité de ces mêmes enfants. Nous sommes entrés trop vite dans une société dite de l'information, où chacun de nous n'a pu s'adapter aux évolutions de l'Internet, et surtout dans un cyberespace conçu il y a plus de vingt ans sans avoir pensé sa dimension « sécurité ». Nous ne sommes plus sur Internet mais dans Internet et le phénomène de disruption dans lequel nous vivons avec l'avènement des technologies ne peut que nous interpeller.

C'est ainsi que nous nous réveillons aujourd'hui dans une société où les jeunes ont leurs propres prothèses cognitives pour apprendre avec le numérique et où celui qu'on appelle plus communément le sachant a du mal à rentrer dans le flux de ces pratiques. Mais ce n'est pas parce qu'ils disposent d'une technologie que nos jeunes en ont tous la maîtrise. C'est pourquoi il est utile ici

d'évoquer des pistes pour déceler les manques, évaluer et développer des compétences numériques adaptées au contexte.

Une nette méconnaissance des réseaux sociaux

En interrogeant nos jeunes sur les divers réseaux sociaux, on s'aperçoit très vite qu'ils ne connaissent que très peu d'entre eux. À la question « *citez-moi quelques réseaux sociaux ?* », les réponses montrent qu'ils ne connaissent que Facebook, Twitter, Linkedin, Snapchat, Instagram et Whatsapp par exemple.

La réalité est toute autre sur le terrain à la vue de plus de 200 autres réseaux que même les adultes ne connaissent pas. Ces derniers correspondent pourtant à la trame de leur vie et à la capacité pour chacun de surveiller son ADN numérique chaque jour de manière manuelle ou automatisée.

Un outil comme Qwant.com ou encore sa version Qwant Junior développée pour les plus jeunes en est une des meilleures illustrations. La CNIL a d'ailleurs retenu et reconnu ce moteur de recherche comme fiable pour l'intégrer dans les outils numériques des établissements scolaires.

Pas de véritable littératie numérique chez nos jeunes

(2) la littératie est « l'aptitude à comprendre et à utiliser l'information écrite en vue d'atteindre des buts personnels et d'étendre ses connaissances et ses capacités ». Pour tenter une définition numérique : http://habilomedias.ca/sites/mediasmarts/files/publication-report/full/definir-litteratie-numerique.pdf

Il n'existe pas de définition consensuelle de la littératie numérique[2]. Pour se forger une solide culture numérique, on peut retenir l'idée d'une combinaison de capacités

La page d'accueil du moteur de recherche Qwant Junior

technologiques, de compétences intellectuelles et de comportements éthiques autour de l'utilisation du numérique. Habilo Médias, Centre canadien d'éducation aux médias et de littératie numérique, publie en ligne un document de discussion intitulé « *Définir la politique de littératie numérique et la pratique dans le paysage de l'éducation canadienne* ». Michael Hoechsmann et Helen DeWaard, deux auteurs canadiens, indiquent que « *la littératie numérique n'est pas une catégorie technique qui décrit un niveau fonctionnel minimal de compétences technologiques, mais plutôt une vaste capacité de participer à une société qui utilise la technologie des communications numériques dans les milieux de travail, au gouvernement, en éducation, dans les domaines culturels, dans les espaces civiques, dans les foyers et dans les loisirs* ».

Selon une étude récente de l'Université de Stanford[3] ,faisant suite aux rumeurs et questions autour de fausses informations circulant en ligne après l'élection de Donald Trump à la présidence des Etats-Unis, les adolescents se feraient facilement duper et seraient rares à savoir distinguer le vrai du faux.

(3) Most Students Don't Know When News Is Fake, Stanford Study Finds, The W all Street, 21 novembre 2016

Il est donc bien sûr ici principalement question d'éducation aux médias et de culture informationnelle. La mise en place en mai 2015 de la Réserve Citoyenne de l'Éducation nationale après les attentats de janvier avait pris pour mission principale de trouver les volontaires sur le territoire en vue d'intervenir dans les établissements scolaires avec les professionnels en exercice ou en retraite. Cette réserve ne semble pas avoir rempli à ce jour cette mission bien que plus de 4000 personnes se soient portées volontaires pour l'assurer.

En septembre 2016, le groupe MGEN lance un programme d'éducation numérique initiant un vaste programme collaboratif d'éducation numérique à destination des publics scolaires. Placé sous le marrainage d'Axelle Lemaire, secrétaire d'État chargée du numérique, il a pour but de sensibiliser les enfants et les adolescents aux enjeux de la protection de la vie privée sur Internet et de les aider à se prémunir des risques liés à la circulation des informations privées.

Dans la foulée, la décision d'ouvrir un site internet public et gratuit a été prise par le Ministère de l'Éducation Nationale et de l'Enseignement Supérieur. Baptisé PIX, il ouvrira à la rentrée 2017[4] pour permettre aux élèves et étudiants, ainsi qu'à n'importe quel utilisateur, d'évaluer et de développer ses compétences numériques. L'annonce en a été faite par

(4) https://pix.beta.gouv.fr/

(5) Brevets et certificats informatique et Internet mis en place à l'Éducation nationale. Tous les écoliers, collégiens et apprentis, de l'enseignement primaire au lycée et CFA gérés par les EPLE sont concernés par le B2i. Dans le supérieur, les C2i, jalonnent, pour les étudiants, un parcours de formation graduel. À travers la formation des étudiants c'est, à terme, l'ensemble des professions, qui est visée. Il existe aussi un B2i pour les adultes et d'autres attestations informatique et Internet en France et dans d'autre pays. http://eduscol.education.fr/numerique/dossier/archives/b2ic2i

La page beta du site PIX

la ministre de l'éducation nationale, Najat Vallaud-Belkacem, lors du Salon du numérique éducatif Educatec-Educatice, le jeudi 17 novembre à Paris. Ce programme PIX est un service en ligne co-construit et évolutif qui est appelé à remplacer les certificats B2i et C2i[5] actuellement en place du collège jusqu'au supérieur.

Apprendre à coder : pourquoi et comment ?

Il s'agit, par l'apprentissage du code dès le CP, de former des citoyens avertis capables de comprendre comment fonctionnent les programmes en vue de déplacer un robot ou un personnage sur écran, voire à construire une figure simple. Au collège, le code devient même un des thèmes des programmes de mathématiques et de technologie. Tout ceci doit nous rappeler des langages comme LOGO qui servaient il y a plus de trente ans à l'écriture, la mise au point et l'exécution de programmes simples sur les premiers ordinateurs. Au brevet 2017, l'épreuve de mathématiques et sciences comportera obligatoirement au moins un exercice d'algorithmique ou de programmation. « *L'idée n'est pas de former des spécialistes, mais d'apporter aux élèves des clefs de décryptage du monde numérique, de les amener à voir l'informatique autrement que comme une pensée magique à laquelle on n'aurait pas accès* », explique Florence Robine, directrice générale de l'enseignement scolaire au ministère de l'Éducation nationale, dans Le Monde du 6 juin 2016.

Il est aussi question dans un monde d'algorithmes, qui nous construisent

aujourd'hui, de comprendre ce que sont ces calculs qui servent depuis longtemps à décrypter des tendances et à prédire des événements dans presque tous les domaines de notre société. L'école du code initiée par « Bibliothèques sans frontières » et Tralalère[6] est un exemple de programme pour les professeurs et animateurs, sans connaissances de l'informatique, désireux de monter des ateliers d'initiation au code pour les jeunes de 8 à 14 ans. Il propose une formation et un accompagnement sur mesure, ainsi que des ressources numériques et des applications adaptées à l'âge de leurs élèves. Ces ressources ont été développées autour de 3 axes : savoir, savoir-faire, savoir-être.

(6) http://www.tralalere.com/

Davantage orienté « savoir-être », le programme D-Clics numériques[7] a pour objectif de former les acteurs éducatifs pour qu'ils puissent accompagner les jeunes de 8 à 14 ans dans leur apprentissage des usages du numérique. Le but étant de leur donner les compétences nécessaires à l'éducation de futurs citoyens numériques. Pour l'instant, D-Clics numériques s'adresse surtout aux animateurs et citoyens médiateurs du numérique, mais des perspectives pour renforcer les liens avec les enseignants devraient s'ouvrir en 2017.

(7) http://d-clicsnumeriques.org/

Alors que certains jeunes sont plus que des adeptes de la programmation, un projet a été dédié pour les populations les plus défavorisées et ceux qui sont en décrochement scolaire. Ainsi, en partant du constat que seules 38 % des personnes sans diplôme sont internautes (contre 95 % des bacs +5), le projet Capprio[8] a pour vocation de faire du numérique un levier d'insertion pour les jeunes en difficulté de 16 à 24 ans.

(8) http://capprio.fr/qui-sommes-nous/

Aller dans les profondeurs du Web, veiller et connaître les cyber-risques

Les nouvelles pratiques numériques sont parfois risquées et ce n'est pas la tendance au tout connecté qui changera la donne. L'exploration du Web peut distinguer plusieurs niveaux d'accès en fonction des méthodes utilisées pour y accéder : le Web surfacique (ou visible) qui est documenté dans les grands moteurs de recherche, le Web profond (ou invisible) non référencé (parce que les moteurs de recherche n'y sont pas autorisés ou pour lesquels une interaction avec le visiteur est nécessaire), ou encore ce qui est parfois appelé le darknet, en réalité des sites Web - légitimes ou non, en tous cas plus confidentiels - uniquement accessibles via des réseaux d'anonymisation tels que Tor, Freenet ou I2P.

Dans chaque évolution du Web prennent place de nouvelles formes d'ingénierie sociale qu'il convient d'évoquer avec les

Cahiers pédagogiques

Un cahier spécial dédié à la citoyenneté

élèves. Au-delà du *phishing* se trouvent en effet bien des modes opératoires visant à capter des données, à les réutiliser pour nous faire chanter, voire encore pour usurper nos identités. Les méthodes de cyber-harcèlement sont en vogue et fleurissent principalement à partir des réseaux sociaux.

La cartographie avec des outils comme Touchgraph SEO permet ainsi d'apprendre à descendre dans le Web profond dit invisible et pourtant accessible à tous pour qui se donnent la peine de pratiquer les outils gratuits disponibles sur la toile. De même avec Immersion, les jeunes pourraient mieux apprécier les interactions se produisant dans les messageries comme Gmail, Yahoo…

(9) https://www.educnum.fr

Récemment, le projet Educnum[9] a mis en place une plateforme ainsi qu'un concours qui récompense les meilleurs projets chez les jeunes. Sur cette même plateforme la cybersécurité est expliquée par de faux hackers avec la "Hack-Academy", une brillante parodie d'émission de TV réalité pour sensibiliser les jeunes internautes aux quatre principaux cyber-risques qui menacent leurs données personnelles. Les cahiers pédagogiques n° 530 de juin 2016 ont consacré un dossier spécial sur « Former les futurs citoyens[10] ».

(10) http://www.cahiers-pedagogiques.com/Reserve-citoyenne-et-culture-numerique

Vers le retour d'une instruction civique pas seulement axée sur le Djihadisme

La tâche d'une partie des enseignants a été délicate au lendemain des attentats qui ont affecté les intérêts français. La théorie du complot et d'autres discours pervertis par une reproduction d'informations erronées et non contrôlées sont ressortis dans les classes. Peu préparés à ce genre d'événements, ayant un manque de connaissance de la psychologie adolescente d'une partie de leurs élèves, certains enseignants ont fait face à des situations complexes d'autorité car ils n'avaient pas une pratique assurée

quant au traitement de ce type de sujets. La culture du débat à partir d'informations issues du Net devra inclure une rationalité afin que les étudiants puissent considérer qu'un droit ou un fait est le produit d'une histoire continue et interactive entre des pays, des nations, des groupes d'intérêts ou des communautés. Il faudra en assimiler les principes en déconstruisant de graves errements de pensée notamment par des recherches croisées et un réexamen objectif de vidéos en classe. La recherche de la source fiable de l'information et son recoupement avec discernement en compagnie de l'enseignant, voire des parents avec qui on pourrait oser l'éducation dans ce sens, seraient une piste de progrès appréciable. Tout ceci demande de mettre l'objectif de la compréhension des clés de notre monde au centre de l'ensemble des disciplines.

L'AUTEUR

Jean-Paul Pinte, Docteur en Information scientifique et technique est Maître de conférences et chercheur au Laboratoire d'innovation pédagogique de l'Université catholique
Cyber-criminologue.
Il a écrit de nombreux articles dans des revues spécialisées et est le co-auteur, avec Myriam Quéméner, d'un ouvrage intitulé Cybercriminalité des acteurs économiques: risques, réponses stratégiques et juridiques aux Editions Hermés-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 chez Hermés-Lavoisier intitulé "Enseignement, préservation et diffusion des identités numériques".

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 économique et du FIC (Forum International 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'École de Guerre à Paris, à l'École Nationale de Magistrature, dans la formation continue du personnel des tribunaux ainsi qu'à l'Institut National des Hautes Études de Sécurité et de Justice (INHESJ).

La communication « Machine to Machine » (MTM) et ses nouveaux usages, en toute sécurité

par **FRANCK MARESCAL et DARIO ZUGNO**

La relation « Machine to Machine » relève davantage de la réalité que de la science-fiction. C'est l'évolution de la technologie qui a profondément modifié la société et permet aujourd'hui l'interaction d'équipements servant d'interface avec un utilisateur final, comme le conducteur d'une voiture ou un patient suivi à distance. Ceci est dû à la convergence entre les équipements intelligents reliés par des réseaux de communication et un centre informatique en mesure de prendre des décisions.

FRANCK MARESCAL

Colonel de gendarmerie
Chef de l'observatoire central des systèmes de transport intelligents

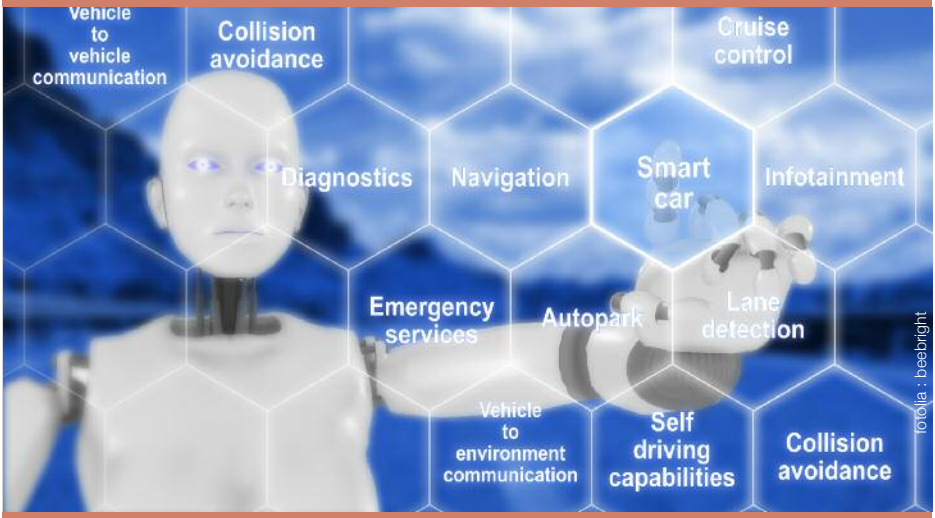
DARIO ZUGNO

Chef d'escadron de gendarmerie
Observatoire central des systèmes de transport intelligents

Qu'est ce que le MTM ?

Le « Machine to Machine » est l'association des technologies de l'information et de la communication avec des objets intelligents et communicants, dans le but de fournir à ces derniers les moyens d'interagir sans intervention humaine avec le système d'information appartenant indifféremment à une organisation ou à une entreprise.

En lisant cette définition, un autre concept très proche et d'actualité nous parvient immédiatement à l'esprit, l'internet des objets (communément appelé IoT en anglais). Toutefois une différence essentielle existe et doit être retenue. L'IoT est considéré comme un système où chaque objet est identifié (avec une adresse IP par exemple) et communique avec une plateforme de type *Cloud* en y envoyant ses données qui peuvent parfaitement intégrer un réseau mondial. À l'instar, le MTM fonctionne dans un espace plus restrictif.



La communication M to M se situe dans un écosystème global intéressant les infrastructures, des calculateurs puissants associés à des serveurs accessibles et la conservation d'une responsabilité juridique en cas d'incidents.

Les données transmises par un capteur sont envoyées à un autre (*via* un serveur si besoin) et sont traitées *via* une application (un logiciel propriétaire). Ce système, plus sécurisé, nécessite de passer par un opérateur de communication. Il s'agit en l'occurrence de philosophies différentes où deux types de technologies existent. Il faut donc bien identifier ses besoins et choisir le processus le plus adapté à son activité.

Le MTM pour quels usages ?

Afin de répondre à des besoins précis, le MTM s'applique tout particulièrement aux secteurs d'activités choisis comme exemples ci-après.

Dans le domaine médical :

La e-Santé a le vent en poupe et apparaît de plus en plus comme une solution adéquate afin de répondre aux défis des systèmes de santé tels que le vieillissement de la population, la prise en charge de la dépendance, les inégalités territoriales d'accès aux soins, …

La e-Santé veut replacer l'usager au cœur du dispositif en répondant à sa volonté d'autonomie. C'est notamment le cas des

patients, maintenus dans leur domicile, atteints de maladies chroniques (diabète, insuffisance cardiaque, …) ou handicapées et nécessitant une assistance spécifique.

Des actes médicaux peuvent être réalisés à distance au moyen de dispositifs utilisant les technologies de l'information et de communication (TIC) comme la télésurveillance médicale avec l'interprétation à distance des données médicales nécessaires au suivi médical d'un patient et le cas échéant une décision relative à sa prise en charge. C'est dans le domaine de la santé que la barrière entre MTM et IoT n'est pas complètement fermée. En effet de nombreux objets connectés permettent de mesurer des données physiologiques ou l'activité physique. Ce phénomène d'auto-mesure est bien connu du grand public. Pourtant il existe également, comme indiqué supra pour les personnes atteintes de maladies chroniques, des outils tel que la pompe à insuline connectée qui permet d'ajuster la dose d'insuline après contrôle du niveau de glucose par le smartphone.

Dans l'automobile (avec un focus particulier sur la gestion de flotte)

C'est probablement dans ce domaine que les innovations attendues sont les plus fortes. La remontée d'informations depuis les véhicules permet à l'entreprise de transport de gérer en temps réel son parc, le suivi de véhicules, sans perdre de vue l'amélioration du comportement du conducteur. La géolocalisation permet d'optimiser le planning des visites (réactivité de l'entreprise face aux demandes des clients). Les données émises par le boiter télématique installé dans le véhicule permettent de connaître la consommation réelle de carburant et de suivre plus précisément l'usure des composants nécessaires au bon entretien des véhicules.

Les constructeurs automobiles s'intéressent aux clients professionnels et proposent des solutions clés en main. C'est le cas du groupe PSA Peugeot Citroën qui commercialise une solution de mobilité connectée « Interparc Connect Management ». Cet outil de gestion permet de remonter des données depuis les véhicules vers le gestionnaire de parc. Toujours sur la gestion de flotte, l'Aéroport de Paris Charles de Gaulle a développé un service permettant d'optimiser le flux des taxis. La solution consiste à mettre en place une zone de stockage des taxis à moins de 2 kilomètres des terminaux, plus une zone tampon non loin du point de prise en charge des clients. Des badges RFID équipent les taxis qui permettent la détection automatique des véhicules dans la zone de stationnement (entrée et sortie) et de prise en charge des clients. Des panneaux électroniques incitent les chauffeurs de taxis à passer d'une zone à

l'autre en fonction de l'arrivée des clients. Les apports du MTM sont indéniables en termes de réduction du temps d 'attente du taxi et des clients. Un autre intérêt non négligeable consiste en la réduction de la fraude car les taxis non équipés de badge sont contraints de repartir.

D'autres exemples voient le jour avec le parking qui communiquera au véhicule la disponibilité de places, l'infrastructure routière (comme le feu de circulation) qui enverra des indications ou les systèmes collaboratifs entre véhicules qui alerteront des dangers (voir le projet SCOOP ci-après).

Il est toujours difficile de parler d'innovations sans parler des nouvelles technologies.

État de l'art technologique

La communication V2X comprend l'échange de données entre véhicules et entre les véhicules et l'infrastructure routière, ceci étant possible dans la bande de fréquence allouée (5,9 Ghz) qui correspond à la norme européenne pour les communications spécifiques de véhicule connue sous le vocable ETSI ITS-G5 (WIFI de dernière génération d'une portée pouvant aller à 1000 mètres).

D'importants travaux de standardisation ont été effectués et, parallèlement à ces travaux, des projets sont en cours pour mettre en application les possibilités offertes par ces nouvelles technologies. Il s'agit d'une volonté forte de l'Union Européenne marquée par la déclaration d'Amsterdam des ministres des Transports d'avril 2016.

Ce système coopératif doit fonctionner dans des circonstances critiques. Il est alors nécessaire de prendre en compte la distance et la vitesse des véhicules qui communiquent, la densité du trafic ainsi que l'environnement qui peut influer sur la propagation du signal, sans oublier la problématique de la congestion où il faudra gérer l'ensemble des transmissions.

D'autres technologies existent pour disposer de la meilleure couverture en fonction de l'environnement. Il est fait ici référence à la technologie cellulaire (4G et dans quelques années 5G), aux technologies de communications à courte distance telles le Li-Fi (transmission de données via les ondes lumineuses) ou à longues portées telles que les solutions IoT (LORA et SIGFOX) qui se caractérisent par de très faibles débits.

Projet Scoop@f

Afin de préparer le déploiement des STI coopératifs à l'échelle nationale, la France s'inscrit dans un projet dénommé Scoop@f qui se caractérise par une grande variété de types de routes empruntées (autoroute, voie rapide, route départementale et de montagne). C'est un projet lancé par le ministère de L'Écologie, du Développement durable et

de l'Énergie en 2014. Il regroupe autour du ministère plusieurs partenaires publics et privés (collectivités locales, gestionnaires routiers, constructeurs automobiles français, instituts ou laboratoires de recherche et PME).

L'échange d'informations entre véhicules et entre le véhicule et la route se fera via la fréquence Wifi ITS-G5 par des unités embarquées dans les véhicules (UEV) et des unités bord de route (UBR) permettant d'établir les communications. Une plateforme assure la collecte des informations et l'envoi des messages aux unités embarquées dans les véhicules dans le cadre d'accident, de présence d'obstacles ou de dangers, de difficultés de circulation, …

Grâce à la collecte des données, l'information routière en temps réel sera relayée aux conducteurs par un traitement en back office assurant la complète sécurité du système.

Scoop@f déploiera 3 000 véhicules sur 2 000 kilomètres début 2017 et vise à améliorer la sécurité routière ainsi que la sécurité des agents d'exploitation qui interviennent sur les routes pour des travaux et autres opérations d'exploitation.

La gendarmerie nationale participera à ce beau projet en ayant des véhicules équipés d'unités (UEV) en Bretagne et sur l'A4, autour de Reims, dans le but de tirer des enseignements de cette expérimentation afin d'améliorer nos modes d'action.

Problématique de la sécurité

Les aspects sécurité et confidentialité sont des problèmes majeurs pour tous les objets de communications. Dans l'exemple du V2X, il faut tout particulièrement veiller à la disponibilité, l'intégrité et à la confidentialité de certaines données qui transitent entre les centres de supervision (constructeurs, opérateurs de service) et le véhicule connecté qui sera un jour autonome, entre le véhicule et les unités de bord de route et entre les véhicules eux-mêmes.

En France, la sécurité des systèmes d'information relève aujourd'hui de l'ANSSI et ce domaine est parfaitement réglementé. Des guides de bonnes pratiques génériques ou spécifiques aident les constructeurs à développer leurs objets connectés. L'ENISA (Agence de l'Union Européenne pour la sécurité des systèmes d'information) propose plusieurs guides en fonction de l'objet (IoT, Transports, Véhicule, …).

Il s'agit là de prévenir des agressions sur les communications, par exemple le déni de service, l'intrusion, l'injection de virus, l'usurpation ...

Des solutions existent pour sécuriser les communications en créant une architecture de sécurité qui exécute une procédure de PKI (Public Key Infrastructure) et qui fait intervenir

différentes autorités de certification afin de protéger la communication V2X contre les attaques externes (société IdNomic est dans ce projet). Ainsi, il est nécessaire d'assurer l'authenticité, l'intégrité et la non-répudiation des messages transmis par une signature, d'éviter le rejet par une datation du message, sans oublier la protection de la vie privée dans le cadre du respect de l'anonymat par une clé de signature à courte vie pour les véhicules (afin d'assurer l'anonymisation).

Le corollaire de ce niveau de sécurité induit par la mise en place de nombreux serveurs (PKI, identifiants, détection d'attaques) est un trafic de communication significatif. C'est une des raisons qui incite à développer l'emploi du cellulaire en appoint du vecteur IEEE 802.11p (Wifi G5). Pour cela, la norme 5G est en cours de définition par les opérateurs de communications mais ne sera pas opérationnelle avant 2025 environ.

Concernant la question de la cybersécurité des véhicules, la *National Highway Traffic Safety Administration* (NHTSA) américaine a publié, le 24 octobre 2016, des recommandations sur la façon dont les constructeurs devaient aborder ce problème. Elles viennent en complément du guide de bonnes pratiques de la SAE (Société des Ingénieurs de l'Automobile US) et de l'AutoISAC (un centre de partage d'informations et d'analyse d'attaques sur les véhicules implanté aux US).

Il est demandé aux constructeurs et aux fournisseurs de faire de la protection des systèmes électroniques et informatiques des véhicules contre les risques de piratage l'une de leur priorité et de s'attaquer à ce problème dès le début du processus de développement des nouveaux modèles (security by design).

La mobilité n'a jamais été autant au cœur des problématiques du bien-être des citoyens avec le véhicule connecté et bientôt autonome et les smart cities, mais ces défis ne pourront être relevés qu'en présentant une technologie sans faille, fiable et suscitant la confiance des utilisateurs.

Comme le prône l'Institut de Recherche Technologique SystemX, située à Saclay, les constructeurs devraient faire de la cybersécurité un avantage commercial. Les projets développés dans cet institut en collaboration avec des industriels permettent d'atteindre cet objectif. Au-delà, les constructeurs devraient faire la preuve du bon niveau de cybersécurité dès la mise sur le marché d'un nouvel objet connecté. Ils sont de plus en plus nombreux à s'inscrire dans cette logique.

Gardons à l'esprit que le nouveau règlement européen sur la protection des données (appelé RGPD), qui entrera en vigueur le 25 mai 2018, définit une obligation de résultat et non pas de moyens. Le défaut de sécurité qui entraînera des problèmes de divulgations de données et donc d'atteinte à la vie privée sera sanctionné par une amende de 4% du chiffre d'affaires mondial du groupe !

La sécurité de l'IoT et du MTM est ainsi devenue une composante incontournable. L'OCSTI, par ses actions de prévention, en montrant les vulnérabilités et les risques encourus, participe à la stratégie nationale pour la sécurité numérique.

chombosan

VARIETE DE NOUVEAUX USAGES ET NOUVELLE POLITIQUE DU RISQUE

Les collectivités territoriales sont confrontées à la complexité et la variété des usages suscitées par les nouvelles technologies. C'est un enjeu primordial, politique sans aucun doute, qui touche à la confiance des usagers en des relations dématérialisées qui se doivent de conserver une dimension humaine au gré d'applications intuitives, accessibles et fiables.

Les réponses existent pour peu que l'on fasse référence aux prescriptions de l'ANSSI, que l'on choisisse des prestataires inscrits dans cette logique dès la conception des produits, que l'on favorise les solutions cryptées et que l'on place la protection des données à caractère personnel au centre des préoccupations.

Cette politique volontariste est la clé de la confiance numérique du citoyen connecté mais elle doit être portée par des directeurs généraux de service qui sachent s'entourer d'organes susceptibles d'identifier les risques encourus, de sérier les dispositifs à installer et de mobiliser les ressources humaines et budgétaires à y consacrer. Dans ce cadre financier, outre les maintenances classiques, on doit obligatoirement inclure le coût des évolutions des systèmes au gré des avancées technologiques et sociétales.

Collectivités locales
et cyber-risques

par GÉRARD COMBES

Les collectivités locales, en introduisant constamment de nouveaux usages des technologies digitales, accroissent inexorablement leur exposition aux cyberattaques. Les enquêtes récentes témoignent globalement d'une insuffisance des mesures préventives. Bien que le risque zéro n'existe pas, les collectivités locales, par une prise de conscience aiguë, peuvent accroître considérablement leur protection et leur résilience.

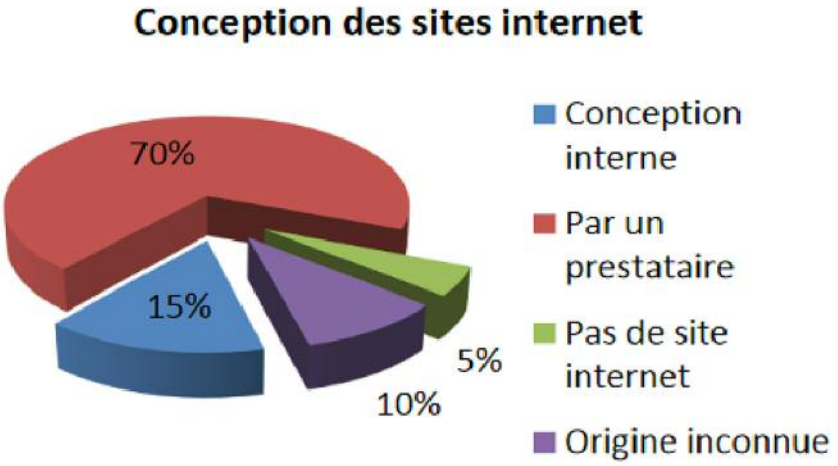
Les collectivités locales, comme les institutions et les entreprises, n'échappent pas à l'introduction massive de nouveaux usages issus des cyber - technologies. La multiplication de ceux-ci accroît la vulnérabilité des systèmes. Le champ des usages du numérique est très vaste pour une collectivité. Il va du simple site informatif jusqu'à l'utilisation d'objets connectés (les feux tricolores par exemple) en passant par des transactions de type commercial.

GÉRARD COMBES
Président de l'association PRIMO FRANCE

En septembre 2015, PRIMO France[1] a publié un rapport[2], fruit d'un travail de plusieurs mois, dressant un état des lieux des cyber-risques des collectivités. Suite à l'envoi d'un questionnaire aux collectivités, les résultats ont été discutés dans un premier groupe de travail réunissant PRIMO, des acteurs privés du monde de l'assurance et des DGS. Cette étude a pu mettre en lumière un réel manque de connaissances et de sensibilisation des collectivités et de

(1) Association dédiée à la gouvernance du risque et à la gestion du risque public. Fondée entre les directeurs généraux des collectivités locales, le groupe Marsh, Dexia, elle fait partie du réseau européen de PRIMO EUROPE, ce qui lui permet de bénéficier des meilleures informations de bonne pratique et de benchmarking. Lieu d'échange et de réflexion, Primo crée un espace collaboratif de dialogue avec tous les acteurs de la gestion du risque.

(2) « Les collectivités locales face aux conséquences du cyber-risque », Septembre 2015



Primo-France et Marsh

Une conception liée à des développements locaux qui n'intègrent pas nécessairement des options de sûreté pourtant impératives.

leurs agents quant à la profondeur des cyber-risques. Bien que bon nombre d'entre elles fassent preuve de conscience et bonne volonté, les collectivités peinent à atteindre un niveau minimal de protection des données ; quand bien même elles auraient mis en place une prévention renforcée (SSI, antivirus, firewall, cryptage…), presque aucune aujourd'hui n'est couverte face aux conséquences du cyber-risque. Les collectivités sont en cela proches des comportements des individus ou des entreprises face à un risque identifié, correctement perçu mais face auquel la prévention et la protection ne sont pas suffisantes.

Quels risques pour les collectivités ?

La défiguration de site (ou défaçage) est l'attaque la moins grave mais elle entachera quoi qu'il arrive l'e-réputation des collectivités et aura de toute évidence un impact sur sa vie politique ; ces attaques sont les plus fréquentes et deviennent de plus en plus virulentes. Les conséquences du vol ou de la perte de données, souvent contre une demande de rançon, sont plus préoccupantes: outre d'éventuelles pertes d'argent pour la collectivité, les données peuvent être détruites ou revendues pour un usage frauduleux. Les possibilités de recours du citoyen sont réelles, puisque la responsabilité civile des élus et du responsable de la sauvegarde des données est engagée. Une attaque en déni de service, consistant à bloquer l'accès aux serveurs et empêcher le bon fonctionnement d'un ou plusieurs services, peut être désastreuse. Enfin, un

hacker qui a tout pouvoir sur le système et qui décide de le libérer ou non, peut avoir la possibilité de détruire toutes les données et les services associés.

Lors d'une rencontre avec des Directeurs généraux des services en 2015, l'un des invités a eu l'occasion de relater son expérience de perte de données survenue récemment dans sa collectivité. L'incident a nécessité un travail de longue haleine et une énergie colossale, mobilisant de nombreux acteurs de la collectivité. Les coûts engagés ont été particulièrement élevés : face à l'urgence de la situation, toutes les solutions proposées ont été tentées, sans pour autant n'avoir aucune certitude sur leur efficacité. Ce type d'incident entraîne d'importants coûts de réparations, d'honoraires pour conseils et d'éventuels frais suite aux réclamations des tiers lésés.

L'attaque idéologique est généralement une réponse à un projet ou un événement récent. Elle nécessite une mise en place rapide par le hackeur et elle est peu organisée et précise. De plus, ces attaques, généralement conçues pour être vues par le plus grand nombre, sont de facto facilement détectables. En revanche, l'attaque crapuleuse, visant à soutirer des informations ou de l'argent à la cible, nécessite d'être extrêmement préparée et très sophistiquée ; en cela, elle est particulièrement difficile à détecter et peut se produire sur un temps particulièrement long.

Les chiffres révélés par l'enquête indiquent une forte exposition des collectivités aux cyberattaques. Dans le panel retenu, aucune des collectivités sondées ne crypte ses données, et 5 % d'entre elles déclarent ne pas connaître cette possibilité, et moins de 15 % ont déclaré avoir pris connaissance du Référentiel général de sécurité. Par ailleurs, alors que 70 % des collectivités interrogées ont déclaré être passées par un prestataire pour la conception de leur site internet, 15 % ont fait concevoir le site par un agent de la collectivité …

Lorsque l'on sait que seulement 10 % des collectivités procèdent à des formations de sensibilisation aux cyber-risques pour leurs agents, et que seulement 13 % utilisent des procédures de révocation des comptes professionnels après le départ des agents, le risque se trouve considérablement accru.

Pourtant, les collectivités sont vouées à se digitaliser, soit par la force des choses et par la volonté des citoyens, soit par les actions du législateur. Ainsi les services publics sont destinés à être de plus en plus accessibles et gérés en ligne. La plupart des collectivités sont d'ores et déjà passées à une gestion informatisée de nombreux services comme la distribution des eaux, l'éclairage public, le traitement des déchets ou la gestion des réseaux électriques. L'évolution rapide des technologies entraîne une augmentation des exigences du citoyen

en matière de participation citoyenne et de gestion administrative.

Les nouvelles pratiques au sein des collectivités : le citoyen connecté

La participation citoyenne aux politiques de la ville est en plein développement : les communes développent de plus en plus des applications pour smartphone ou tablettes pour diffuser de l'information et des messages, faire des signalements voire, comme à Lyon, Aix-en-Provence ou Montreuil, recueillir de la donnée, via la géolocalisation de l'utilisateur. Avec l'essor du concept de « ville intelligente » (ou smart city) on peut s'attendre à ce que de nombreuses applications se développent en lien avec la ville et les services proposés par la collectivité qui devra être la garante de la bonne administration de ses données et bien évidemment de leur protection.

Les plates-formes collaboratives citoyennes semblent recevoir toute l'attention des communes et des habitants. Elles permettent aux citoyens de s'exprimer, d'échanger et de débattre sur leur quartier ou sur leur ville, démontrant que l'échange se passe aussi – et surtout – sur le web, à l'instar de la plate-forme Nantes&Co. Les réseaux sociaux séduisent également de plus en plus les collectivités et les citoyens : 55 % des villes préfectures sont présentes sur Facebook et 50 % ont un compte Twitter. 68 % des conseils généraux sont présents sur Facebook contre 50 % sur Twitter alors que 89 % des conseils régionaux ont un compte Facebook, et 81% ont ouvert un compte Twitter[3].

(3) http://www.ideose.com/barometre-collectivites-territoriales-reseaux-sociaux/

L'administration électronique ou e-administration se veut être un moyen de simplification de l'organisation administrative et des relations avec les citoyens, en favorisant les échanges d'informations et de données. Ces nouveaux enjeux numériques imposés aux collectivités les propulsent dans un monde de données et de menaces auxquelles elles ne sont pas préparées.

De plus en plus, les collectivités proposent des services en lignes pour procéder à des actes administratifs courants, tels que les demandes d'actes d'état civil, le règlement des factures de crèches, des activités gérées par les collectivités (école de musique, d'art, théâtre…), transformant ainsi une simple interface web en site transactionnel. Le Livre blanc - Téléservices et collectivités 2010[4] listait déjà les services les plus demandés par les citoyens. Force est de constater que les demandes sont nombreuses et que la plupart d'entre elles nécessitent la gestion de données personnelles et confidentielles comme les données bancaires. La demande de digitalisation des services est croissante. Elle va demander aux collectivités de s'engager

(4) https://issuu.com/gfiinformatique/docs/gfi_livre_blanc_collectivit__s_d__f

http://www.collectivites-locales.gouv.fr/zoom-sur-ladministration-electronique

dans la sécurisation des réseaux et des process, dans la formation à la collecte, à la gestion et à l'accès aux données, en intégrant cette problématique nouvelle aux politiques publiques. De fait, au vu des nombreux piratages informatiques des années précédentes, il est légitime de s'interroger sur le niveau de protection des collectivités face au cyber-risque, d'autant plus qu'il existe une particularité pour les collectivités qui touche à l'image de l'élu.

Les données des collectivités

Les intervenants externes comme les assureurs spécialisés et les cabinets de conseil en gestion des risques sont tout à fait en mesure d'identifier les risques et les données particulièrement sensibles des collectivités. Un intervenant majeur du domaine et partenaire de Primo France déclarait récemment qu'« *au vu des nombreuses missions que doivent gérer les collectivités, il est évident que chacune d'entre elles est amenée à conserver des données particulièrement sensibles. On pourrait qualifier de donnée sensible toute donnée confidentielle ou à caractère personnel* ». Un article de la loi « informatique et libertés » de 1978 en propose une définition précise : « *Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres* ». Ce dernier point fait référence par exemple, à un numéro de sécurité sociale, l'immatriculation d'un véhicule, un numéro de carte bancaire, une adresse IP, une photo… « *Parmi toutes les données conservées par les collectivités, poursuit-il , on peut distinguer les données personnelles – noms, prénoms, adresse, état civil… – des données purement confidentielles – données bancaires, données sociales des communes, CCAS, départements… – ainsi que toutes les données de gestion des collectivités – service des ressources humaines, service comptable, service paie – qui peuvent détenir des bases de données complètes avec toutes les informations des agents* ».

Les collectivités locales doivent prendre la mesure des risques qu'elles font prendre à leurs administrés. Il est de la responsabilité des élus d'agir, en premier lieu, sur leur capacité à pouvoir réagir vite et contenir les effets d'une perte massive de données. Malgré toutes les mesures qui peuvent être prises en matière de sécurité informatique, les experts sont formels : le risque zéro n'existe pas. Les cibles d'attaques sont parfois des victimes prises au hasard d'un envoi massif d'e-mails infectés, et un simple clic peut plonger la collectivité dans le désastre. Le transfert de ce risque vers l'assurance est l'ultime protection contre les conséquences financières d'une cyberattaque. La plupart des assureurs

spécialisés mettent à disposition des assurés une cellule de gestion de crise externalisée, des experts informatique et en communication, mobilisables en urgence.

Mais auparavant, il convient que la collectivité s'organise pour répondre au mieux aux défis du cyber-risque. La première action , recommandée par l'association PRIMO consiste à connaître parfaitement les risques encourus en les identifiant précisément et en estimant leurs conséquences. La deuxième action consiste à disposer d'un comité spécialisé sur le cyber-risque relevant de l'autorité du Directeur général des services, assurant un état des lieux en continu et en procédant à des simulations d'attaques ou de crash test..

Grâce à ces quelques mesures simples, la collectivité pourra être en mesure non seulement de mieux se protéger mais aussi de se mettre dans une situation plus favorable en termes de résilience.s

L'AUTEUR

Gérard Combes a notamment occupé les fonctions professionnelles suivantes: Directeur général de la Ville de Nancy ; Directeur régional Ile de France de la Caisse des dépôts et Consignations ; Directeur de l'économie mixte et des participations publiques de la CDC , à ces titres a présidé le directoire de la société de financement solidaire Solidec SA, a siégé au Conseil d'Administration de plusieurs sociétés . Il a ensuite été délégué général du CESER Rhône Alpes.
Extra professionnellement il a été : Président du Syndicat National des directeurs généraux des collectivités territoriales et Président fondateur de l'Union des dirigeants territoriaux européens.
Il est actuellement président de l'association PRIMO FRANCE , dédiée aux risques publics.
Il est Chevalier dans l'ordre national du Mérite.

ALLER PLUS LOIN

PRIMO
Public Risk Management Organisation

En collaboration avec
MARSH

COLLECTIVITES TERRITORIALES : COMMENT SE COUVRIR FACE AUX CONSEQUENCES D'UNE CYBER-ATTAQUE ?

Compte-rendu de la rencontre entre PRIMO, Marsh, Beazley et les Directeurs Généraux des Services invités – Octobre 2015.

Fotolia

ADMINISTRATIONS ET ENTREPRISES GARDIENNES D'UN PATRIMOINE INFORMATIONNEL

Une entreprise ou une administration doit être génératrice de services fiables et continus au profit d'un particulier ou d'une collectivité. Ils s'inscrivent globalement dans une économie numérique et un patrimoine informationnel qui doivent être protégés. L'environnement hyper-connecté des systèmes d'information, la croissance du nombre d'utilisateurs et la forte émergence de l'internet des objets augmentent la variété des services et les surfaces d'attaques. L'obligation particulière faite aux administrations de dématérialiser leurs procédures ouvre leurs systèmes d'informations aux services en lignes. Pourtant, malgré la prégnance des incidents par malveillance, près de la moitié des entreprises ne disposent pas d'un instrument permettant leur mise en évidence et leur traitement alors que les cyberattaques sont souvent massives et touchent des cibles indifférenciées.

La sécurisation de cette bulle numérisée doit résulter d'une expertise technique (DSI, prestataires de services, *etc.*) mais également d'une prise de conscience par les décideurs de l'incidence létale pour le système de pratiques inappropriées des techniciens et des utilisateurs. Le fondement d'une politique de sécurité repose sur une prise de conscience, une compréhension des questions de sécurité et le développement d'une culture de la sécurité. C'est une stratégie qui ne peut être conduite qu'à haut niveau pour assurer de son caractère impératif et de sa cohérence.

La cybersécurité efficace,
une affaire de culture

par JEAN-PAUL POGGIOLI

Il n'y a jamais eu autant de matériels et d'intelligence artificielle au service de la cybersécurité, et pourtant elle n'a jamais été aussi malmenée, notamment, par des cyberattaques constitutives de la force de frappe des terroristes et mises au rang d'armement militaire par certains Etats. Toutefois, une cyberattaque réussie est rarement le résultat d'une sophistication technologique et elle est souvent la conséquence des transactions d'un utilisateur insouciant ou berné. Ce qui amène à s'interroger sur le fait qu'une cybersécurité efficace est finalement une affaire de culture.

JEAN-PAUL POGGIOLI
Directeur de projet et consultant
Médiaterra consultants

Dès lors qu'on aborde la question de la cybersécurité auprès de toutes sortes d'organisations, quels que soient leur secteur d'activité et leur taille, celles-ci ont en général toujours le sentiment de disposer d'une sécurité de leur Système d'information (SI) adéquate ou au moins suffisante tout en étant parfaitement conscientes de leur extrême dépendance à leur SI. Pourtant tout porte à croire que malgré des efforts de plus en plus importants en matière de sécurité, notamment du fait de la croissance des investissements technologiques dans ce domaine, le danger est loin d'être écarté.

Des investissements technologiques pour la cybersécurité en croissance et des attaques réussies tout aussi croissantes

Le rapport 2016 du Clusif[1] sur les « Menaces informatiques et pratiques de la sécurité » (MIPS)[2] indique que les incidents logiques par malveillance sont toujours en croissance. Arrivent en tête les infections par virus avec 44% des

maxsim Fotolia

Les opérateurs humains par la variété des connexions liées à leurs métiers sont les maillons faibles d'une sûreté des transactions mise en place par les DSI. Ils sont au cœur d'une culture de cybersécurité réussie

entreprises concernées, soit 14 points de plus que l'année précédente. Pourtant 49 % de ces mêmes entreprises ne disposent toujours pas d'une cellule de collecte et de traitement des incidents de sécurité de l'information… Près du tiers ne prennent pas en compte la continuité d'activité alors que toutes se savent dépendantes de leur SI !

Nous avons tous en tête les attaques spectaculaires qui ont frappé de grands groupes internationaux avec un impact économique particulièrement conséquent. Fin novembre 2014, l'affaire Sony Pictures fait la une de l'actualité de la cybercriminalité. Une attaque aurait démarré à son encontre en février 2014 avec l'extraction de plus de 110 To de données. Le 21 novembre,

(1) Clusif : Club de la Sécurité de l'Information Français - https://www.clusif.fr/ - club professionnel, constitué en association indépendante, ouvert à toute entreprise ou collectivité. Sa finalité est d'agir pour la sécurité de l'information, facteur de pérennité des entreprises et des collectivités publiques.

(2) https://www.clusif.fr/fr/production/ouvrages/pdf/CLUSIF_2016_Rapport-MIPS_vF.pdf

l'établissement reçoit un courrier électronique de demande de rançon. Le groupe pirate « GOP » menace de publier sur la toile l'ensemble des informations piratées (films, mails confidentiels, contrats et secrets commerciaux, données personnelles…). Tandis que Sony Pictures refuse de payer, 3 jours plus tard un malware se propage sur l'ensemble des postes de travail Windows et 75 % des serveurs du groupe. Sony Pictures est paralysé, les personnels sont privés de leurs outils logiciels de travail. La France n'est pas épargnée avec, en avril 2015, le piratage de tout le système informatique de production et de diffusion des sites web, twitter, Facebook… de la société TV5 Monde. Il aura pour conséquence l'arrêt de la diffusion dans plus de 200 pays !

Des attaques de masse non ciblées qui visent tout type de système informatique

Mais ces histoires, bien qu'ayant fait la une de l'actualité grand public, ont eu assez peu de conséquences dans la plupart des organisations sauf certainement dans les grands groupes qui ont actionné leurs plans de prévention, leurs revues de sécurité et autres missions d'audits. Finalement cette actualité aurait même tendance à faire penser que seuls les grands groupes, les opérateurs industriels stratégiques ou les entreprises détenant des informations de forte valeur marchande comme des numéros de cartes bancaires sont potentiellement la cible d'une cyberattaque. Or, il n'en est rien, car il y a de plus en plus d'attaques de masse, avec par exemple les malwares de type « cryptolocker » plus communément baptisés « ransomwares ». Ces derniers une fois exécutés s'attaquent aux unités de stockage, locales ou sur serveurs, et cryptent les fichiers. Il est demandé une rançon pour permettre leur décryptage. Une fois les fichiers contaminés, la seule solution est de repartir de sauvegardes saines à condition d'en disposer. Payer la rançon n'offre que rarement une issue favorable ! Selon une étude menée par Trend Micro auprès des directeurs des systèmes d'information des entreprises françaises, 40 % avouent avoir été touchés par des ransomwares dans les deux dernières années. Si 50 % de ces victimes ont accepté de payer la rançon, seulement 32 % d'entre-elles ont pu effectivement récupérer leurs données.

Il nous faut rajouter de nouvelles menaces qui visent directement l'économie de nos pays, voire nos modèles sociaux et politiques. Les terribles événements de janvier 2015, qui ont visé Charlie Hebdo et la supérette kasher de la porte de Vincennes, ont été suivis de nombreuses attaques de sites web, particulièrement des sites institutionnels de petites organisations (environ 20 000 sites web ont été défacés affichant des images de Daesh en lieu et place de leur page

d'accueil). Depuis il n'est plus rare d'entendre parler de piratage de comptes de réseaux sociaux à des fins de propagande, comme ce fut le cas pour le compte twitter du journal Le Monde piraté par l'Armée électronique syrienne fin janvier 2015.

Une surface d'attaque en forte croissance qui n'épargne pas les administrations

L'environnement hyper-connecté dans lequel se trouvent les systèmes d'information, la croissance du nombre d'utilisateurs ou encore l'explosion en cours de l'internet des objets ne peuvent que contribuer à l'aggravation des risques, on parle alors d'augmentation de la surface de cyberattaque.

Dans son rapport sur les prévisions à cinq ans sur la cybersécurité, McAfee Labs[3] spécifie l'augmentation de la surface de cyberattaque avec la croissance de 5 facteurs d'ici 2019 :

(3) McAfee Labs est la division de recherche sur les menaces d'Intel Security. C'est l'une des principales références à l'échelle mondiale en matière d'études et de cyberveille sur les menaces. Rapport sur les prévisions en matière de cybermenaces en 2016 et au-delà : http://www.mcafee.com/fr/resources/reports/rp-threats-predictions-2016.pdf

– les utilisateurs, au nombre de 3 milliards en 2015, passeront à 4 milliards en 2019 ;

– les connexions de smartphones qui passeront de 3,3 milliards à 5,9 milliards ;

– les équipements IP qui verront leur nombre passer de 16,3 milliards à 24,4 milliards ;

– le trafic réseau qui passera de 72,4 exaoctets à 168 exaoctets de trafic IP par mois ;

– les données dont les volumes passeront de 8,8 zettaoctets à 44 zettaoctets.

n sixième facteur impacte plus spécifiquement les administrations : l'obligation de dématérialiser leurs procédures administratives a pour conséquence une large ouverture de leurs systèmes d'information aux services en lignes.

Un dénominateur commun pour 85 % des compromissions en secteur public

Ce qui est le plus frappant lorsqu'on analyse la plupart des cyberattaques, c'est la facilité et la rapidité avec laquelle elles ont pu se dérouler. Le rapport d'enquête 2015 sur les compromissions de données, élaboré par Verizon[4], précise que dans 60 % des cas, les attaquants ont pu compromettre une organisation en quelques minutes. Il faudra des jours pour contenir l'incident dans près de 40 % des cas, et des semaines, voire des mois, pour 26 % des

(4) Verizon : Groupe US de télécommunications et de réseaux implanté dans 150 pays. Le Rapport d'enquête Verizon 2015 sur les compromissions de données (DBIR) fournit une analyse détaillée de près de 80 000 incidents, dont 2 122 compromissions de données confirmées : http://www.verizonenterprise.com/r3s0u4c3s/es_dbir-executive-summary_fr.pdf

cas. Dans ce même rapport, on apprend que pour le secteur public 85 % des compromissions portent sur 3 modèles d'attaques et que le dénominateur commun de ces modèles est l'humain :

– logiciels criminels (50 % des compromissions) : Il s'agit d'une catégorie large, couvrant toute utilisation d'un logiciel malveillant pour compromettre des systèmes. Cette action est habituellement opportuniste et motivée par l'appât du gain ou la volonté de nuire aux institutions. L'activation de l'attaque par ces logiciels criminels est toujours le fait des utilisateurs, la plupart du temps sans qu'ils en aient l'intention, par exemple en ouvrant une pièce jointe compromise ou en cliquant sur un lien malicieux…

– erreurs diverses (23 % des compromissions) : On peut citer l'envoi d'informations sensibles à des destinataires incorrects, la publication de données non publiques sur des serveurs Web publics et la destruction non sécurisée de données personnelles et/ou médicales.

– menace interne (12 %) par délit d'initié et abus de privilèges : Il s'agit principalement d'une utilisation abusive de données ou de fonctionnalités par les employés de l'administration mais le plus souvent par des personnes extérieures (du fait d'une collusion) et par des partenaires (parce que des privilèges leur ont été accordés).

– attaques des applications Web : L'utilisation d'identifiants volés ou l'exploitation de vulnérabilités dans des applications Web — comme les systèmes de gestion de contenu (CMS) ou les plateformes de commerce électronique.

– vol ou perte physique : La perte ou le vol d'ordinateurs portables, de clés USB, de documents imprimés et d'autres actifs d'information, principalement dans les bureaux et les véhicules. Dans ce cas également la responsabilité des utilisateurs est évidente.

Développer une culture de la sécurité

Il ne faut donc pas limiter son regard aux seuls environnements techniques mais s'intéresser aussi à la composante humaine des systèmes d'information. L'OCDE (l'organisation de coopération et de développement économique) l'avait identifié dès 2002. Dans les "Lignes directrices régissant la sécurité des systèmes et réseaux d'information », sous-titrée « Vers une culture de la sécurité », la préface indiquait : « Du fait de leur connectivité croissante, les systèmes et réseaux d'information sont désormais exposés à un nombre croissant et à un éventail plus large de menaces et vulnérabilités, ce qui pose de nouveaux problèmes de sécurité. Les présentes lignes directrices s'adressent

donc à l'ensemble des parties prenantes à la nouvelle société de l'information, et suggèrent le besoin d'une prise de conscience et d'une compréhension des questions de sécurité accrues, ainsi que la nécessité de développer une culture de la sécurité ».

En effet, les erreurs de manipulation des techniciens de l'informatique ou même des simples utilisateurs, le manque de précaution à l'égard des identifiants trop simples, trop accessibles, ou beaucoup trop facilement communiqués, l'ouverture de pièces jointes compromises ou encore la saisie de données confidentielles sur des formulaires usurpant des sites licites, sont en réalité les principales causes de pertes, de compromissions ou de fuites de données, d'altération parfois totale d'un patrimoine informationnel. Dans son livre « *Secrets & Lies. Digital Security in a Networked World* » (Secrets et Mensonges. Sécurité numérique dans un monde en réseau), Bruce Schneier[5] résume très bien cette problématique par cette considération : « *Si vous pensez que la technologie peut résoudre vos problèmes de sécurité, alors vous n'avez rien compris à vos problèmes ni à la technologie* ».

(5) Cryptologue, spécialiste en sécurité informatique et un écrivain américain auteur d'une littérature reconnue traduite en de nombreuses langues notamment sur les sujets de la cryptographie, il est également auteur d'algorithmes de chiffrement populaires et inviolés à ce jour.

Ainsi, la cybersécurité intéresse autant les technologies que les process ou encore une culture nécessaire de tous les utilisateurs. Dans une infrastructure informatique, aussi sophistiquée soit-elles, du point de vue technologique et de sa cyberdéfense, l'utilisateur non averti constituera toujours un point de vulnérabilité majeur. La culture de la cybersécurité doit alors être partagée par tous les utilisateurs des systèmes d'informations de nos organisations, c'est à cette condition que nos cybersociétés deviendront plus sûres.

L'AUTEUR

Jean-Paul Poggioli est ingénieur diplômé du département Informatique de l'INSA de Lyon. Il a fait une première carrière d'une quinzaine d'années en sociétés de services et d'ingénierie informatique dans un large éventail de responsabilités, du génie logiciel à l'intégration d'infrastructures notamment pour des administrations et collectivités locales. Depuis une vingtaine d'années, il intervient en mission d'assistance à maîtrise d'ouvrage ou en maîtrise d'œuvre auprès des DSI ou des directions générales des collectivités locales pour tout ce qui touche aux systèmes d'informations. Actuellement , il assure la direction de mission d'un marché de conception et d'accompagnement à la mise en œuvre d'un schéma directeur des systèmes d'information au Conseil Départemental des Hauts de Seine.

- échanger sur les usages et les services des réseaux de l'Internet,
- mettre en place une veille technologique adaptée et efficace,
- conseiller sur les choix de technologies d'information et de communication,
- peser sur les décisions politiques et administratives dans le domaine des télécoms et réseaux,
- diffuser les informations les plus fiables dans un secteur innovant.

MISSION ECOTER
DÉVELOPPEMENT DES SYSTÈMES DE COMMUNICATION ET D'INFORMATION DANS LES COLLECTIVITÉS TERRITORIALES

mission ECOTER

LA MISSION ECOTER EST UN ATOUT POUR LA GOUVERNANCE TERRITORIALE NUMERIQUE

La Mission Ecoter est un outil accompagnant le secteur public local dans un mouvement de modernisation sans précédent et continu. Aux premiers premiers portails web des collectivités, à la numérisation des procédures, au lancement des réseaux s'ajoutent de nouvelles technologies, comme le RFID / NFC (expérimentations de cartes sans contact) qui obligent les DSI et les directions « métiers » à travailler ensemble à la conduite de projets plus complexes. La dématérialisation impulsée par l'ADAE et son plan Adèle (ADministration ELEctronique 2004/2007) implique l'élaboration et la publication de référentiels d'accessibilité, d'interopérabilité et de sécurité. Elle concourt à instaurer une confiance numérique, une résilience des SI et la sécurisation du patrimoine informationnel des collectivités territoriales.

L'instauration d'un référentiel général de sécurité, intégrant la compétence d'ingénieurs territoriaux et des experts sécurité comme les syndicats mixtes numériques, permettrait de réguler un empilage de SI métiers difficilement interopérables, une « smart city » qui suscite par sa complexité une vulnérabilité et une inflation des données produites. Gageons que le Data Protection Officer obligatoire pour le 1er janvier 2018 aura un effet déclencheur sur une partie de la sécurité des données.

La mission Ecoter
et les collectivités locales

par PATRICK BELLIN et ELODIE BOUIGUES

Les structures territoriales connaissent toutes les évolutions technologiques et organisationnelles imposées par les adaptations indispensables aux attentes de l'État et du citoyen. Elles subissent les contraintes d'optimisation budgétaires et se doivent de servir le plus efficacement et le plus rapidement leur territoire et leurs habitants. Aujourd'hui, l'usage du numérique étant totalement intégré dans les organisations et les process territoriaux, la sécurisation des données en possession des collectivités est un nouveau défi à placer en face d'obligations qui peuvent être vues comme contradictoires comme l'open data.

PATRICK BELLIN
Conseiller technique
Mission ECOTER

ELODIE BOUIGUES
Responsable des programmes
Mission ECOTER

Un accompagnement des collectivités dans leur modernisation numérique

La mission Ecoter est une association de loi 1901 qui réunit des collectivités et des entreprises. Créée en 1997, elle est un espace de veille, de conseil, d'information et de formation sur le numérique sous l'angle des infrastructures, des usages, des services et de leurs impacts dans les organisations et la gouvernance des Collectivités Territoriales.

Par ses activités de veille et d'observation, son club « collectivités », ses colloques, ses guides, sa veille hebdomadaire, la mission Ecoter se positionne depuis toujours comme un outil accompagnant le secteur public local sur les sujets de modernisation. Il

Ecoter

Une sensibilisation sur des thématiques associées aux nouveaux développements numériques qui induisent des relations dématérialisées avec l'usager et la protection des données sensibles.

se veut pédagogique, pragmatique et aussi stratégique, avec un regard accru sur la question de la sécurité et de la protection des données.

Les grandes étapes du numérique dans les Collectivités ?

Il faut comprendre que ces vingt dernières années ont propulsé les collectivités territoriales et leurs administrations dans un mouvement de modernisation sans précédent... et continu.

Une première phase 1997-2000 qui correspond au développement de l'internet, souligné par le vice-président Al Gore avec les autoroutes de l'information (1994), au passage à l'an 2000 et à l'informatisation des services, à la libéralisation des télécoms et aux réseaux boucle local radio…

Une seconde phase 1997-2004 où l'agenda de l'association se construit, avec le concours de collectivités pionnières, sur la question de l'aménagement numérique du territoire et du déploiement des réseaux fixes haut débit, sur l'administration électronique avec les premiers portails web des collectivités, la numérisation des procédures, l'intranet… et sur une sensibilisation à la sécurité des SI et des réseaux avec le lancement du Wifi, de l'UMTS, et du Wimax.

Une troisième phase 2004-2008 où nous augmentons le nombre de nos rencontres, dans un contexte volontariste de faire entrer les collectivités territoriales dans la dématérialisation impulsée par l'ADAE et son plan Adèle (ADministration ELEctronique 2004/2007). Il s'agit de mettre en œuvre la dématérialisation des marchés publics, du contrôle de légalité, des titres de recettes et mandats, de l'archivage, des moyens de paiements, des tiers de confiance, de la signature électronique. En externe l'effort porte sur la relation avec les usagers et de nouveaux services dématérialisés : carte

de vie quotidienne (bouquet de services municipaux comprenant les entrées aux piscines, aux bibliothèques) et le paiement par internet de la cantine scolaire, *etc.*

Les DSI et les directions « métiers » travaillent ensemble à la conduite de projets plus complexes, et la première gère la relation avec les nouveaux acteurs que sont les fournisseurs de solutions.

Ainsi, si la sécurité des SI conserve toujours sa place dans les réunions, l'attention est principalement portée sur l'organisation des services et la gouvernance au regard du caractère transversal du numérique qui s'oppose à une administration organisée en silo.

Une quatrième phase 2006-2010 est marquée par l'arrivée de nouvelles technologies, de référentiels, de services et la mobilité avec :

– le RFID / NFC (expérimentations de cartes sans contact) pour développer le commerce électronique, dématérialiser les titres de transport et les moyens de paiements… et les premiers smartphones avec les applications téléchargeables sur les plates-formes,

– la vidéoprotection, dont les collectivités commencent à s'équiper et qui pose la question des données, du stockage, de l'hébergement, de l'interopérabilité,

– une adoption du logiciel libre par de nombreuses collectivités,

– l'élaboration et la publication des référentiels d'accessibilité, d'interopérabilité et de sécurité.

Pour la première fois, nous associons dans nos réunions les termes de confiance numérique à ceux d'intégrité, de sécurité des données, de pérennité, de résilience des SI et de sécurisation du patrimoine informationnel, dans un contexte où les systèmes d'information sont de plus en plus complexes et où de nouvelles offres technologiques se dessinent.

Depuis 2011 à aujourd'hui, une cinquième phase, qui continue de s'écrire, est à la fois caractérisée par une avalanche de technologies et de solutions : cloud computing, virtualisation des SI, IoT, capteurs, smart grid et smart metering, plates-formes guichet unique et GRC, d'open data, d'archivage électronique, etc.. Elle se caractérise également par l'explosion de données sensibles, critiques, à caractère personnel, en cours d'être ouvertes et réutilisables. Elle comporte enfin une chaîne numérique complexifiée, aux multiples acteurs où la DSI semble réduite dans ses fonctions alors que les directions métiers achètent « sur étagères ».

On notera que les PC, les tablettes, les smartphones, les clés usb et messageries sont les principaux moyens de travail des agents territoriaux ; les fichiers s'échangent souvent sans cryptage ; les postes restent allumés… Des habitudes

de travail qui peuvent peser lourd pour l'intégrité du SI et des données.

Une évolution des DSI dans le cadre d'une appréhension du risque « sécurité »

Les DSI semblent isolées face aux directions métiers, qui construisent les bouquets de services publics dématérialisés, aux habitudes de travail des agents et enfin au support incertain que les DGS et les élus leur accordent pour sécuriser les SI[1] et sensibiliser aux bonnes démarches les acteurs des collectivités.

(1) Etude PRIMO La gestion du cyber risque au sein des collectivités françaises. Etat des lieux, septembre 2015

Nous donnons la parole aux DSI (communes, intercommunalités, département, région), depuis cinq ans sur la transformation informatique : cloud computing, hébergement et stockage, virtualisation des postes et plateformes, impact de la convergence fixe mobile, gestion des données. Nous pouvons effectuer le constat suivant.

Des performances en déclin avec la montée en charge et la sécurité insuffisamment prise en compte ; un empilage de SI métiers difficilement interopérables et une « smart city » qui apporte son lot de vulnérabilités ; une inflation de data produites à gérer, caractériser et protéger ; et en définitive, une cartographie des SI (logiciels métiers, sig, outils de travail) et une réingénierie nécessaire à conduire.

Néanmoins, suite à une enquête que nous avons conduite sur l'évolution des SI des collectivités vers des centres de services (février 2015), tout ne semble pas si noir.

Sur 106 réponses (8 régions, 14 départements, 10 communes de plus de 100 000 habitants, 16 de 50 à 99 000, 19 EPCI) :

- 60 % avaient mis un centre d'appel et d'un point d'entrée pour l'ensemble de leurs prestations et pour les utilisateurs des directions métiers.

- 46 % avaient un projet en cours pour renforcer la sécurité du SI par des prestations et/ou des infrastructures complémentaires (PRA, audit RGI RGS, *etc.*), 26 % pensaient à renforcer la sécurité du fait d'une évolution prévue des infrastructures mais pas avant deux ans, 23 % avaient un projet à l'étude pour renforcer la sécurité des SI, 10 % n'avaient pas l'intention de renforcer la sécurité de leurs infrastructures.

Des stratégies à conduire pour réduire les risques

Les nouvelles technologies et la complexification croissante des SI posent la question des compétences, de la sensibilisation des agents (et des élus), des RH et finances et de l'organisation. Il existe des réponses pour chaque domaine.

Plus de ressources humaines

On déplore souvent le manque de fortes compétences en interne pour administrer la sécurité des SI, ou mettre en place le Référentiel général de sécurité, pourtant le « métier » existe comme en témoigne le guide des métiers territoriaux du CNFPT : RSSI, Expert sécurité SI ou chargé de la sécurité SI. Par ailleurs, le CNFPT, en mettant à son catalogue de formation des stages pour « *définir et piloter la stratégie de sécurité des systèmes d'information et garantir l'intégrité, la confidentialité et la pérennité des informations de la collectivité territoriale* », se préoccupe désormais de la montée en

compétence des ingénieurs territoriaux. Ces experts sécurité apparaissent principalement dans les organigrammes de grandes collectivités au détriment des petites et moyennes collectivités. Pour pallier à ce qui peut être lié à des difficultés RH ou budgétaires, une mesure de progrès serait de mutualiser les RSSI, comme dans le secteur hospitalier, sur plusieurs sites ou s'appuyer sur les structures satellites que sont les syndicats mixtes numériques.

Une optimisation de l'emploi des Correspondants informatique et libertés

Rappelons que les collectivités ont la gestion de l'état civil, des listes électorales, de l'inscription scolaire, des activités sportives et périscolaires, de l'action sociale, de la gestion foncière et de l'urbanisme, de la facturation de taxes et redevances.

La CNIL ne compte que 1 250 correspondants informatique et libertés. Ce chiffre est insuffisant pour sensibiliser agents et élus (responsables des traitements) aux risques liés à l'absence de sécurité et de protection des données à caractère personnel, alors qu'ils sont dans l'obligation d'y veiller sous peine de sanctions. Si les régions de France métropolitaine, les départements et les communautés urbaines sont bien équipées, restent toutes les autres collectivités. Gageons que le Data Protection Officer[2] obligatoire pour le 1er janvier 2018 aura un effet déclencheur sur une partie de la sécurité des données.

(2) Nouveau métier du numérique, Le data protection officer est responsable de la protection et de la conformité des données de l'entreprise.

Convaincre les élus

Si un maire peut estimer que sa commune n'est pas une cible particulière et digne d'intérêt, ce n'est pas la logique des hackers, que des motivations diverses (sur commande, par défi, par idéologie, *etc.*) conduisent à inonder massivement les systèmes informatiques de leurs programmes invasifs. Statistiquement, il y aura toujours un nombre d'agents qui cliqueront sur un message douteux. Sécuriser et sensibiliser pour prévenir a un coût et nécessite de mettre en place des processus transverses qui sont trop

Ecoter

ECOTER accompagne les élus et des décideurs (DGS et cadre de maîtrise) pour qu'ils puissent coordonner et financer les actions utiles à la protection de leurs systèmes d'informations.

souvent négligés voire ignorés par les élus et par les directeurs généraux des services. Il faut aussi veiller à faire une place pour la sécurité dans la commande publique et consacrer une part du budget aux actions de sensibilisation.

Vers un changement d'organisation

La fin du travail en silo et des achats sur étagères dans les directions, assis sur la réorganisation des processus avec une DSI, à la fois maîtrise d'ouvrage et maîtrise d'œuvre, permettrait la mise en place d'une véritable politique de sécurité informatique des collectivités, plus efficace face aux risques.

Quels sont les chantiers ouverts ou à ouvrir pour les Collectivités Locales et comment la mission Ecoter peut-elle les accompagner ?

La mission Ecoter va poursuivre ses actions de sensibilisation et d'information dans ses futures actions :

– par des piqûres de rappel sur la protection des données à caractère personnel, car l'évolution de la réglementation avec l'obligation d'avoir un Data Protection Officer va faire passer les collectivités dans une autre dimension à compter de 2018. Les collectivités encourront jusqu'à 20 millions d'euros de pénalité à partir du 25 mai 2018[3],

(3) Titre II le volet de la « protection des citoyens dans la société numérique » de la Loi Pour une République numérique, adoptée en seconde lecture par le Sénat (28 septembre 2016)

(4) Loi pour une République numérique

Par la mise en perspective de l'ouverture des données publiques[4] avec l'organisation de la collectivité et la fin des silos,

Par l'assistance à la sensibilisation des personnels territoriaux à l'importance des gestes basiques de protection de l'information,

– par le repositionnement des SI comme outil transverse de pilotage de l'organisation, de la conception et de la mise en œuvre des politiques publiques,

– par la mise en évidence, pour les élus, des nouveaux droits des citoyens et de leur recours, en ce qui concerne l'obligation, pour les collectivités locales, de l'ouverture « par défaut » des données publiques.

MISSION ECOTER

UNE NOUVELLE LEGISLATION POUR LA LUTTE CONTRE LA CYBERCRIMINALITE

Les nouvelles dispositions de la loi du 3 juin 2016 ouvrent la voie à une législation globale dédiée à la lutte contre la cybercriminalité. Elles mettent en œuvre un large spectre de nouvelles infractions numériques en référence à tout lien avec le terrorisme et étendues à la législation sur les explosifs. Sous contrôle des magistrats, elles permettent de mettre en œuvre de nouvelles procédures adaptées au numérique. Outre le règlement de la concurrence des compétences, la capacité d'investigation est renforcée par un nouveau régime de l'interception des informations numériques, de la gestion des scellés de données numériques. Il est utilement disposé de la mise au clair de données cryptées et du développement de mesures intrusives tant par le recours à l'Imsi-Catcher, qu'à la captations des données et à la procédure de l'achat.

Les évolutions en matière de numérique issues de la loi du 3 juin

par MYRIAM QUÉMÉNER

L'arsenal pénal en matière de lutte contre la cybercriminalité, sous la pression de la menace terroriste et du crime organisé, vient à nouveau d'être renforcé par des dispositions créant d'une part de nouvelles infractions dites de prévention en matière terroriste et en développant d'autre part des procédures intrusives tout en améliorant les règles de compétence territoriale pour améliorer la lutte contre la cybercriminalité.

La loi n°2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement et améliorant l'efficacité et les garanties de la procédure pénale, composée de 120 articles, intègre comme désormais la plupart des textes la dimension numérique des activités en lien avec le terrorisme et logiquement la cybercriminalité. Cette loi apporte des évolutions notables tant au niveau du droit matériel que du droit processuel.

MYRIAM QUÉMÉNER

Magistrate, conseillère juridique
Ministère de l'Intérieur
Docteresse en droit

Les nouvelles infractions numériques

En lien avec le terrorisme

Le nouvel article 421-2-5-2 du code pénal incrimine la consultation habituelle d'un service de communication au public en ligne mettant à disposition des messages, images ou représentations soit provoquant directement à la commission d'actes de terrorisme, soit faisant l'apologie de ces actes lorsque, à cette fin, ce service comporte des images ou représentations montrant la commission de tels actes consistant en des atteintes volontaires à la vie : les peines prévues sont de deux ans d'emprisonnement et de 30 000 € d'amende. L'infraction[1] n'est par

(1) L'infraction a été retenue, le 8 août dernier par le tribunal correctionnel de Chartres, pour condamner un internaute à 2 ans d'emprisonnement

contre pas établie lorsque la consultation est faite de bonne foi, qu'elle résulte d'un travail journalistique, intervient dans le cadre de recherches scientifiques ou est réalisée pour servir de preuve en justice.

L'art. 421-2-5-1 du code pénal crée une nouvelle infraction. Ainsi, désormais, est puni de cinq ans d'emprisonnement et de 75 000 € d'amende le fait d'extraire, de reproduire et de transmettre intentionnellement des données faisant l'apologie publique d'actes de terrorisme ou provoquant directement à ces actes en vue d'entraver les mesures d'arrêt d'un service de communication en ligne par voie judiciaire ou les retraits ou blocages demandés par l'autorité administrative.

En lien avec le financement du terrorisme

Il faut relever également les modifications du code monétaire et financier. Bien qu'elles ne soient pas pénales à proprement parler, des sanctions peuvent être prévues sous forme de dispositions relatives au plafonnement des cartes prépayées ainsi que celles permettant à la cellule de renseignement financier TRACFIN de signaler des situations présentant un risque élevé de blanchiment ou de financement du terrorisme: une sanction pénale est prévue si les personnes informées communiquent à leurs clients ou à des tiers les informations transmises par TRACFIN.

En lien avec les explosifs

L'article 322-6-1 du Code pénal, qui incrimine le fait de diffuser par tout moyen, sauf à destination des professionnels, des procédés permettant la fabrication d'engins de destruction élaborés à partir de poudre ou de substances explosives, de matières nucléaires, biologiques ou chimiques, ou à partir de tout autre produit destiné à l'usage domestique, industriel ou agricole, aggrave les peines de un an d'emprisonnement et 15 000 euros d'amende, à trois ans d'emprisonnement et 45 000 euros d'amende. Si cette infraction est commise par le biais d'un réseau de communication électronique à destination d'un public déterminé, les peines sont portées à cinq ans d'emprisonnement et 75 000 euros d'amende.

Les nouvelles procédures adaptées au numérique

L'adaptation de la compétence territoriale à la cybercriminalité

La cybercriminalité présente des particularités nécessitant une adaptation des règles de compétence afin de disposer d'un critère certain qui soit de nature à sécuriser les procédures d'un point de vue juridique notamment en matière de lutte contre la criminalité organisée et contre le terrorisme. La compétence des juridictions françaises aux infractions commises par le biais d'un

réseau de communication électronique, même hors du territoire de la République, à l'encontre d'une victime résidant en France et sans exiger la condition d'une plainte préalable de cette dernière posée par l'article 113-8 du Code pénal. Cet objectif est atteint par la création d'un nouvel article 113-2-1 du Code pénal prévoyant que toute infraction commise par le biais d'un réseau de communication électronique est réputée commise en France. En second lieu, concernant les infractions commises sur le territoire national, le présent projet de loi propose la création d'un nouveau critère de compétence du procureur de la République, du juge d'instruction et du tribunal correctionnel lié au domicile de la victime en complément 43 des critères de compétence habituels existants. Ce second volet implique la modification de la rédaction des articles 43, 52 et 382 du code de procédure pénale.

L'article 706-72 nouveau du Code de procédure pénale dispose que les actes incriminés par les articles 323-1 à 323-4-1 et 411-9 du Code pénal, lorsqu'ils sont commis sur un système de traitement automatisé d'informations, sont poursuivis, instruits et jugés selon des règles particulières fixées par les articles 706-72-1 à 706-72-6 du Code de procédure pénale. Il est ainsi créé une compétence concurrente pour les infractions informatiques, c'est-à-dire la cybercriminalité au sens strict. Cela ne signifie pas le dessaisissement automatique des juridictions compétentes en vertu des articles 43, 52 et 382 du Code de procédure pénale. Des modalités de dessaisissement sont prévues à l'article 706-72-2 du code de procédure pénale. Par contre les infractions commises voire facilitées par Internet et les réseaux numériques ne sont pas visées par cette compétence concurrente. Cependant, il convient de rappeler que le procureur de la République de Paris a déjà créé un pôle numérique composé de quelques magistrats et assistants spécialisés qui traitent la cybercriminalité y compris les infractions non visées par ce nouveau texte comme les « escroqueries au président ».

La copie des données provenant des scellés

L'article 60-3 du Code de procédure pénale consacre, clarifie et simplifie les opérations réalisées par des personnes qualifiées portant sur les scellés d'objets, les supports de données informatiques, notamment les téléphones portables ou des ordinateurs. Les articles 77-1-3 (enquête préliminaire) et 99-5 (commission rogatoire) se réfèrent au même article. Ainsi, lorsqu'ont été placés sous scellés des objets qui sont le support de données informatiques, le procureur de la République ou l'officier de police judiciaire peut, par tout moyen, requérir toute personne qualifiée, inscrite

sur une des listes prévues à l'article 157 ou ayant prêté par écrit le serment prévu à l'article 60, pour procéder à l'ouverture des scellés afin de réaliser une ou plusieurs copies de ces données en vue de permettre leur exploitation sans risquer de porter atteinte à leur intégrité.

Mise au clair des données chiffrées

L'article 230-2 du code de procédure pénale prévoit les modalités de mise au clair de données cryptées. Un nouvel alinéa 2 autorise l'organisme chargé d'y procéder à ouvrir les scellés.

Le développement des procédures intrusives

Pour la poursuite des infractions relevant de la criminalité organisée (articles 706-73 et 706-73-1 du Code de procédure pénale), la loi élargit aux enquêtes menées sous la direction du parquet (enquête préliminaire et enquête de flagrant délit) le recours aux techniques spéciales d'enquête prévues dans le cadre d'une information.

Le recours à l'Imsi-catcher

L'IMSI catcher est une sorte de fausse antenne relais mobile agissant dans un rayon de quelques kilomètres, qui se substitue aux antennes des opérateurs en permettant de disposer de données émises ou reçues par les terminaux ainsi leurrés qui y sont connectés. L'emploi de ce dispositif pour recueillir les données techniques de connexion permet l'identification d'un équipement terminal ou du numéro d'abonnement de son utilisateur, ainsi que l'acquisition des données relatives à la localisation d'un équipement terminal utilisé. L'autorisation est délivrée pour une durée maximale d'un mois, renouvelable une fois dans les mêmes conditions. Ce même équipement peut être utilisé afin d'intercepter des correspondances émises ou reçues par un équipement terminal selon les modalités prévues aux articles 100-4 à 100-7 du Code de procédure pénale (art. 706-95-4 du Code de procédure pénale). Le décret n° 2016-1159 du 26 août 2016 pris pour l'application de l'article 706-95-8 du code de procédure pénale fixe la liste des services dont les agents peuvent être requis par le procureur de la République, le juge d'instruction ou l'officier de police judiciaire pour utiliser un Imsi-catcher.

La captation de données

Les nouvelles mesures prévoient la mise en place d'un dispositif technique ayant pour objet, sans le consentement des intéressés, la captation, la fixation, la transmission et l'enregistrement de paroles prononcées par une ou plusieurs personnes à titre privé ou confidentiel, dans des lieux ou véhicules privés ou publics, ou de l'image d'une ou de plusieurs personnes se trouvant dans un lieu privé (art. 706-96 du Code de procédure pénale).

Il est aussi prévu le recours à un dispositif technique ayant pour objet, sans le consentement des intéressés, d'accéder, en tous lieux, à des données informatiques, de les enregistrer, de les conserver et de les transmettre, telles qu'elles sont stockées dans un système informatique, telles qu'elles s'affichent sur un écran pour l'utilisateur d'un système de traitement automatisé de données, telles qu'il les y introduit par saisie de caractères ou telles qu'elles sont reçues et émises par des périphériques audiovisuels (art. 706- 102-1. du Code de procédure pénale). Le procureur de la République ou le juge d'instruction peut désigner toute personne physique ou morale habilitée et inscrite sur l'une des listes prévues à l'article 157, en vue d'effectuer les opérations techniques permettant la réalisation du dispositif technique mentionné au premier alinéa du présent article. Ils peuvent également prescrire le recours aux moyens de l'État soumis au secret de la défense nationale (Centre Technique d'Assistance – CTA).

L'extension de la procédure dite du «coup d'achat

Le nouvel article 706-106 du code de procédure pénale crée une nouvelle technique d'enquête, dite du coup d'achat. Déjà prévue en matière de stupéfiants à l'article 706- 32 du code de procédure pénale, elle est étendue aux infractions mentionnées au 12° de l'article 706-73, c'est-à-dire les infractions relatives au trafic d'armes et aux explosifs. Sur autorisation du procureur de la République ou du juge d'instruction, les officiers et agents de police judiciaire peuvent sans être pénalement responsables acquérir des armes ou leurs éléments, des munitions ou des explosifs, et mettre à la disposition des personnes se livrant à ces infractions des moyens juridiques, financiers ou matériels. Les actes ne doivent pas constituer une incitation à commettre une infraction. Cette technique du coup d'achat est également prévue en matière douanière par l'article 67 bis-1 du code des douanes.

La loi du 3 juin 2016 procède à un rééquilibrage du cadre judiciaire[2] face à une certaine dérive vers le cadre administratif en accordant à la justice des moyens identiques à ceux accordés aux services de renseignement s'agissant de l'accès à distance aux correspondances stockées par la voie des communications électroniques. La voie est peut-être enfin ouverte vers une législation globale dédiée à la lutte contre la cybercriminalité.

(2) L'infraction a été retenue, le 8 août dernier par le tribunal correctionnel de Chartres, pour condamner un internaute à 2 ans d'emprisonnement

Fotolia

LA LOI DU 3 JUIN 2016 FACILITE LES POURSUITES

La loi n°2016-73 du 3 juin 2016 apporte des réponses pertinentes à la question de la détermination de la compétence territoriale des juridictions pénales en matière de cybercriminalité. La volatilité de la preuve numérique, l'origine planétaire des actes incriminés rendent difficile l'exercice des voies de droit classiques. L'extension des compétences inscrites à l'article 113-2 du Code pénal lève le problème de l'accessibilité à l'auteur opérant depuis l'étranger dès lors que la victime réside sur le territoire français. De même, l'extension des critères des articles 43, 52 et 382 pérennise la compétence du premier parquet saisi et de nouvelles dispositions (C. pr. pén., nouv. art. 706-72-1 à 706-72-6) donnent à la seule juridiction parisienne une compétence concurrente. Il reste que la chancellerie devra éviter des conflits de compétence en matière d'atteintes aux systèmes de traitement automatisé de données. En effet, des infractions commises au moyen des nouvelles technologies de l'information pour véhiculer des contenus illicites ou pour faciliter la commission d'une autre infraction, ne sont pas concernées par cette compétence concurrente. On peut également envisager la création d'un réseau de magistrats référents « Cybercrime» au plan national et la reconnaissance de la cybercriminalité comme un contentieux à part entière.

Cybercriminalité et compétence territoriale : dernières évolutions législatives

par MYRIAM QUÉMÉNER

La détermination de la compétence territoriale des juridictions pénales en matière de cybercriminalité est essentielle pour lutter contre cette délinquance en pleine extension. À cet égard, les apports de la loi n°2016-73 du 3 juin 2016 en la matière sont des plus pertinents mais devront s'accompagner de formation et de moyens adaptés.

La cybercriminalité présente des spécificités nécessitant une adaptation des règles de compétence afin de disposer d'un critère certain permettant de sécuriser les procédures pouvant être contestées sur ce point.

MYRIAM QUÉMÉNER
Magistrate, conseillère juridique
Ministère de l'Intérieur
Docteresse en droit

La question de la compétence territoriale en matière de lutte contre la cybercriminalité est l'une des difficultés majeures car les infractions étant commises dans le cyberespace, il est par voie de conséquence très difficile de localiser leur origine et souvent encore davantage le lieu où se trouvent leurs auteurs[1]. On constate ainsi qu'Internet heurte le droit classique et le met en difficulté en raison de son caractère volatil et ubiquitaire. Le développement de la cybercriminalité impose des évolutions de la procédure pénale concernant l'application de la loi pénale dans l'espace.

(1) M.Robert, Cybercriminalité : les nouvelles réponses législatives – Marc Robert – AJ pénal 2016. 412

En effet, identifier les auteurs de cyber-infractions est complexe puisque ces infractions, souvent instantanées, sont fréquemment commises à distance, en partie de l'étranger, par des auteurs anonymes. En outre, la volatilité de la preuve numérique met souvent en échec les moyens juridiques classiques.

Les dispositions nouvelles prévoient la résidence de la victime sur le territoire français sans obligation de sa nationalité française.

En cela, la loi n°2016-73 du 3 juin 2016, renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale vient apporter des réponses pertinentes tant sur le plan de la compétence des tribunaux français que sur les critères de compétences territoriales.

L'évolution de la compétence des tribunaux français en matière de cybercriminalité

Jusqu'alors, les critères classiques des articles 113-2 et suivants du code pénal[2] privilégiaient l'élément matériel, alors même que le lieu de commission d'une cyber-infraction est, le plus souvent, méconnu en début d'enquête et que seule la victime est identifiée.

(2) https://www.legifrance.gouv.fr/affichCode.do;jsessionid=18C815016B8059EE9269B948C964A91F.tpdila08v_1?idSectionTA=LEGISCTA000006165262&cidTexte=LEGITEXT000006070719&dateTexte=20161106

La compétence du juge pénal français est établie par les articles 113-1 à 113-13 du Code pénal et 689 à 689-13 du Code de procédure pénale[3]. L'article 113-2 du Code pénal dispose que le juge peut se saisir de toute infraction, dès lors que l'un de ses éléments constitutifs a lieu sur le territoire national. Il suffit, par exemple, qu'un site Internet soit accessible depuis la France pour que l'infraction, dont il est le vecteur, soit considérée comme constituée. Ainsi, le juge français s'est déclaré compétent à

(3) https://www.legifrance.gouv.fr/affichCode.do;jsessionid=18C815016B8059EE9269B948C964A91F.tpdila08v_1?idSectionTA=LEGISCTA000006151920&cidTexte=LEGITEXT000006071154&dateTexte=20161106

propos de la vente aux enchères sur Yahoo.com d'objets nazis, en violation de l'article R.645-1 du Code pénal[4] et de l'Art. 113-2 du Code pénal, du seul fait de l'accessibilité du site en France, même si ce dernier était entièrement en anglais et destiné à un public américain. En 2008, la Cour de cassation[5] a admis la compétence du juge français pour une infraction de contrefaçon dont était victime le journal Le Monde, bien que l'œuvre ait été reproduite à l'étranger, parce qu'elle était accessible depuis le territoire français.

(4) https://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000006419560&cidTexte=LEGITEXT000006070719
Est puni de l'amende prévue pour les contraventions de la 5e classe le fait, sauf pour les besoins d'un film, d'un spectacle ou d'une exposition comportant une évocation historique, de porter ou d'exhiber en public un uniforme, un insigne ou un emblème rappelant les uniformes, les insignes ou les emblèmes qui ont été portés ou exhibés soit par les membres d'une organisation déclarée criminelle en application de l'article 9 du statut du tribunal militaire international annexé à l'accord de Londres du 8 août 1945, soit par une personne reconnue coupable par une juridiction française ou internationale d'un ou plusieurs crimes contre l'humanité prévus par les articles 211-1 à 212-3 ou mentionnés par la loi n° 64-1326 du 26 décembre 1964.

(5) Cass.crim., n°07-87281, Giuliano F., 9 septembre 2008, Legifrance.

La loi du 3 juin 2016 crée, un nouvel article 113-2-1 dans le Code pénal qui dispose : « T*out crime ou tout délit réalisé au moyen d'un réseau de communication électronique, lorsqu'il est tenté ou commis au préjudice d'une personne physique résidant sur le territoire de la République ou d'une personne morale dont le siège se situe sur le territoire de la République, est réputé commis sur le territoire de la République* ».

Ainsi, le nouvel article 113-2-1 assimile à une infraction commise sur le territoire français tout crime ou délit réalisé au moyen d'un réseau de communication électronique lorsqu'il est tenté ou commis au préjudice d'une personne, physique ou morale, résidant sur ce territoire ou dont le siège y est situé. Le législateur privilégie ainsi le domicile de la victime, soit une personne physique ou morale en retenant alors le siège social de l'entreprise pour retenir leur compétence. Un critère complémentaire, à savoir celui du domicile des victimes, est donc créé.

Dans la loi, ce texte s'inscrit dans un chapitre sur les « *dispositions améliorant la lutte contre les infractions en matière d'armes et contre la cybercriminalité* ». Présent dès le projet de loi initial, il s'inspire partiellement de la 30e des 55 recommandations du rapport « Protéger les internautes. Rapport sur la cybercriminalité [6]», qui préconisait[7] que « *toute infraction commise par le biais d'un réseau de communication électronique, de nature criminelle ou de nature correctionnelle mais punissable d'un emprisonnement, lorsqu'elle est tentée ou commise au préjudice d'une personne, physique ou morale, de nationalité française au moment de sa commission, est réputée avoir été commise en France* ».

(6) M.Quéméner Protéger les internautes : rapport sur la cybercriminalité,RIdI, N° 107, 1er août 2014

On peut cependant noter que le critère de la nationalité française de la victime

n'est pas retenu et qu'il suffit que cette dernière réside sur le territoire français. Cette modification s'explique compte tenu de la difficulté à lutter contre la cybercriminalité, délinquance souvent complexe et par essence internationale. De plus, cette criminalité flirte souvent avec le terrorisme et peut être à son service comme le remarque d'ailleurs un auteur[8] , ce qui explique aussi cette modification et aussi par voie de conséquence l'introduction de nouvelles infractions dans la loi du 3 juin 2016 comme la simple consultation de sites à caractère terroriste et l'obstacle au blocage administratif ou judiciaire de ces mêmes sites[9].

(8) R.ParisotLoi du 3 juin 2016 : aspects obscurs de droit pénal général – RSC 2016. 376

(9) C. pén., art. 113-7 et 113-8.

(10) Cour de cassation. Cass. Crim, n°15-86645, 12 juillet 2016, Agness X. Compétence du juge pénal français

Cependant, le législateur ne consacre pas pour autant une compétence universelle de la loi française et un arrêt récent de la cour de cassation en date du 12 juillet 2016[10] vient d'ailleurs de le rappeler. S'agissant d'infractions de presse, réputées commises en tout lieu où les propos incriminés ont été reçus, lorsque ces derniers ont été diffusés sur le réseau Internet, la compétence territoriale du tribunal français saisi ne saurait être universelle. En l'espèce les plaignantes sont étrangères et résident à l'étranger. L'auteur présumé est étranger. Les propos, en langue anglaise, sur un site américain, concernent des faits s'étant déroulés hors du territoire national. L'accessibilité depuis le territoire français n'est pas un critère suffisant de compétence, la Cour de cassation exigeant que les propos soient orientés vers un public français[11]

(11) Voir M.Watin Augouard, Veille juridique N°50, septembre 2016, http://www.gendarmerie.interieur.gouv.fr/crgn/Publications/Veille-juridique/Septembre-2016

Les critères de compétence territoriale en matière de cybercriminalité

L'article 43 du code de procédure pénale privilégie, en droit commun, le lieu de commission ou celui de résidence, d'arrestation, voire de détention du suspect ; en pratique, dans la grande majorité des cas, c'est en fonction d'une plainte qu'un parquet se saisit et ordonne une enquête en matière de cybercriminalité ; et si cette dernière aboutit à l'identification d'un auteur supposé mais que ce dernier réside dans un autre ressort, le parquet est dans l'obligation de se dessaisir au profit d'un autre parquet qui confie l'enquête à un nouveau service, d'où une perte de temps et de motivation.

En étendant les critères des articles 43, 52 et 382 au lieu de résidence ou du siège des personnes physiques ou morales victimes de l'infraction, la loi autorise la poursuite de l'enquête par le premier parquet saisi. Le projet de la Chancellerie prévoyait de donner compétence concurrente, pour connaître

de ces infractions à la loi, dite Godfrain, à l'ensemble des juridictions interrégionales spécialisées. Le Sénat, suivi par l'Assemblée nationale, en a décidé autrement en reconnaissant au seul parquet et à la seule juridiction parisienne une compétence concurrente (C. pr. pén., nouv. art. 706-72-1 à 706-72-6). L'article 706-72 nouveau du Code de procédure pénale dispose que les actes incriminés par les articles 323-1 à 323-4-1 et 411-9 du Code pénal, lorsqu'ils sont commis sur un système de traitement automatisé d'informations, sont poursuivis, instruits et jugés selon des règles particulières fixées par les articles 706-72-1 à 706-72-6 du Code de procédure pénale.

Perspectives

La nouvelle loi prévoit des règles de compétence particulières adaptées au domaine de la cybercriminalité et ces évolutions devraient permettre de faciliter le travail des services d'enquête et des parquets. Il conviendra cependant que la chancellerie donne des orientations de politique pénale précises afin d'éviter des conflits de compétence s'agissant d'une compétence concurrente en matière d'atteintes aux systèmes de traitement automatisés de données. Par ailleurs, ces évolutions ne règlent pas tous les problèmes liés à la cybercriminalité puisque les infractions commises au moyen des nouvelles technologies de l'information, soit pour véhiculer des contenus illicites, soit pour faciliter la commission d'une autre infraction, ne sont pas concernées par cette compétence concurrente. Or, ces infractions sont nombreuses et souvent complexes. À l'heure actuelle, le parquet de Paris dispose d'un pôle numérique en charge de ces infractions mais il devra s'étoffer à l'avenir. D'autres calages auront certainement lieu en matière organisationnelle avec par exemple un réseau de magistrats référents « Cybercrime» au plan national[12].Il faut en effet que la cybercriminalité soit véritablement reconnue comme un contentieux à part entière nécessitant des moyens humains et une spécialisation obligatoire comme c'est le cas au niveau des officiers de police judiciaire.

(12) En ce sens M. Watin Augouard, veille juridique N°48, mai 2016, http://www.gendarmerie.interieur.gouv.fr/crgn/Publications/Veille-juridique/Mai-2016

tashatuvango

REVOLUTION NUMERIQUE ET SECURITE DES PERSONNES

La révolution numérique bouleverse l'approche et l'exercice des droits attachés à notre personnalité juridique. Sa publicité sur les réseaux et au sein des systèmes d'information confère à l'information qui est rattachée à une personne une permanence et une inaltérabilité.

Différentes affaires judiciaires en Italie et en Espagne montrent que le déférencement des moteurs de recherche est possible en Europe si le détenteur étranger de la donnée en tire un usage commercial non consenti mais il est quasiment impossible dans le monde anglo-saxon où la donnée a valeur de marchandise. La publicisation de la personne en fait un objet de mercantilisme.

On doit également s'interroger sur la question de la maîtrise des algorithmes qui traitent nos données au sein d'un Big Data, qu'ils soient dédiés à la reconnaissance de comportements ou à une sélection préventive voire curative d'individus présentant des profils particuliers. Ces algorithmes, d'autant plus lorsqu'ils seront intégrés au sein d'une intelligence artificielle, seront sujets de décisions qui entraîneront la responsabilité ou la lésion de particuliers. C'est la porte d'un eugénisme social basé sur le traitement opaque d'une bulle informationnelle.

Un autre aspect de
la sécurité des personnes

par **FABRICE LORVO**

La révolution numérique est un fait inexorable. Ambivalente, elle nous a apporté du très bon et du moins bon (qui peut même être très dangereux). La difficulté, aujourd'hui, est que l'intervention pour lutter contre les aspects négatifs du numérique risque d'entraver les effets positifs.

Cette révolution numérique est si profonde qu'elle a bouleversé notre relation avec le temps, en faisant disparaître le passé et en imposant un présent permanent. Elle s'attaque dorénavant au futur, avec les Big Data, en tentant de supprimer l'aléa.

FABRICE LORVO
Avocat au Barreau de Paris
Associé du cabinet FTPA

Dans ce contexte de mutation, la sécurité est un enjeu essentiel du cyberespace. On perçoit assez facilement la dimension pénale du risque. Le cyberespace est d'abord un outil qui peut être utilisé pour commettre des infractions. C'est ensuite un espace dans lequel des délinquants tentent de s'introduire. Il existe un autre volet de la sécurité, qu'on pourrait qualifier de civil (pour le distinguer de son aspect pénal) qui concerne tant la sécurité de l'individu que celle de l'Homme.

La sécurité de l'individu

Avec Internet et les réseaux sociaux, l'individu peut se retrouver exposé à la vue du monde entier. Le paradoxe est que les réseaux sociaux comme internet ont eu besoin de contenu (un tuyau sans contenu n'a pas d'utilité). L'astuce extraordinaire a consisté à convaincre les gens (surtout les jeunes) qu'ils n'auraient d'existence qu'en s'affichant sur le net, entraînant ainsi la publicisation de soi (c'est-à-dire renoncer à sa vie privée).

Cependant, ce qui n'a pas été dit, ou compris, est que tout ce que vous mettez

L'abolition du droit à l'oubli, un déterminisme consacré par des algorithmes de prédiction du comportement humain forment un danger pour les libertés fondamentales des personnes.

sur internet pourra être retenu contre vous. En effet, la révolution numérique a notamment aboli le passé.

La fin de l'oubli

Le passé est étroitement lié à l'oubli qui est consubstantiel à l'Homme, c'était jusqu'à très récemment un régulateur social. Or, le numérique nous a apporté d'une part l'impérissabilité des données et d'autre part l'accès immédiat à ces données par les moteurs de recherche. En conséquence, toute donnée publiée sur le net est immédiatement et de manière permanente accessible. Le numérique ne permet donc plus l'oubli qui se faisait jusqu'à très récemment d'abord par la disparition du support. L'oubli résultait du fait de la disparition des témoins (un vieillard qui meurt est une bibliothèque qui brûle) ou de la destruction du support, qu'elle soit volontaire (l'incendie de la bibliothèque d'Alexandrie) ou involontaire (désagrégation naturelle du papier, catastrophe naturelle, *etc.*). L'oubli résultait ensuite indirectement de l'enfouissement du support (un journal succède à un autre journal) ou de son inaccessibilité (éloignement géographique). L'oubli résultait enfin de l'effet de mécanismes légaux (par exemple, la prescription civile ou pénale, l'amnistie, la réhabilitation, *etc.*).

Techniquement, le numérique a mis fin à cet oubli. On tente donc d'imposer un droit à l'oubli numérique mais c'est un

droit difficile à établir et difficile à appliquer.

Le difficile droit à l'oubli

Un droit difficile à établir car tout ne doit pas être oublié et il ne s'agit pas de réécrire l'histoire. Il faut aussi distinguer entre les données relevant du droit à l'information du public et celles publiées volontairement par l'individu. Il est probable que l'on doive donner une nouvelle définition du « *consentement à la publication* ».

Prenons le cas de Tiziana Cantone, en Italie. En 2015, cette jeune femme se fait filmer en pleine pratique sexuelle et diffuse la vidéo dans un cercle restreint d'amis. A son insu, l'un d'eux a posté, sur les réseaux sociaux, cette vidéo qui est devenue virale en Italie. Devant les juridictions italiennes, la jeune femme a tenté de faire valoir son droit à l'oubli auprès des moteurs de recherche. Elle a été déboutée de sa demande et condamnée à payer 20 000 euros de frais d'avocats au motif qu'elle était consentante lors de la captation de son image. Elle l'était certes, mais pour une diffusion restreinte et probablement pas pour devenir une star. Le côté grivois de cette histoire s'efface pour laisser place à la tragédie car le 13 septembre 2016, Tiziana, par désespoir, s'est pendue, à son domicile. Elle avait 31 ans.

Un droit difficile aussi à appliquer car le numérique a mis fin aux frontières. Notre vision de la vie privée ou de la donnée personnelle est en concurrence avec la vision anglo-saxonne qui est différente (la vie privée n'a pas la même portée aux USA et la donnée est une marchandise aux USA, pas en Europe). Ces deux visions s'affrontent aujourd'hui, d'où les difficultés de la CNIL avec notamment Google qui veut bien appliquer le déréférencement sur google.fr mais pas sur google.com.

Ce déréférencement n'est pas toujours facile à obtenir. Prenons le cas de Monsieur X, chef d'entreprise qui a fait l'objet d'une condamnation pénale pour un délit il y a plus de 20 ans. La peine a été exécutée et elle a fait l'objet d'une réhabilitation légale automatique, dans son cas, en janvier 2014 (soit au bout de 10 ans à compter de l'expiration de la peine). Or, à ce jour, en tapant son nom sur un moteur de recherche, on trouve toujours des articles de presse d'il y a plus de 20 ans indiquant soit qu'il a été condamné, soit qu'il sortait de prison. Cette information est en contradiction avec l'objectif de la réhabilitation légale. Une demande de déréférencement a été faite, Google a refusé au motif que le public a le droit de savoir…. Il faut donc saisir la CNIL.

La sécurité des individus est donc un enjeu fondamental du cyberespace. Dans l'intervalle, l'École doit permettre de sensibiliser les jeunes aux dangers de la publicisation de soi. En effet, la divulgation sur le web de données me concernant, spontanément ou pas, est de nature à figer mon identité numérique et à me porter préjudice à l'avenir.

La sécurité de l'Homme

Il faut aussi veiller à ce que la révolution numérique ne modifie pas implicitement notre conception de l'Homme et de la société.

Les algorithmes prédictifs du comportement humain

Le numérique tente de supprimer le futur et donc l'aléa avec les algorithmes prédictifs du comportement humain. Tenter de prédire le futur n'est pas fautif en soi. On prédit, et c'est louable, l'évolution de la météo, des catastrophes naturelles (tremblements de terre, ouragans, typhons, tsunamis, avalanches, *etc.*) ou des risques épidémiques (Sida, SRAS, grippe aviaire, *etc.*). Il faut cependant être prudent lorsqu'on a recours à des algorithmes pour prédire le comportement humain.

Aux USA, on évalue déjà la prédiction de la récidive. Aujourd'hui, certains se lancent dans la prédiction de la commission d'infractions (PREDPOL aux USA et HORIZON en France). Jusqu'où irons-nous ? Probablement vers la prédiction de l'identité du délinquant pour l'arrêter au stade de la tentative ou du flagrant délit.

Des ingénieurs travaillent déjà sur de tels algorithmes. De manière sous-jacente et implicite, de tels programmes partent du postulat que le comportement humain est prévisible, ce qui consacre la théorie du déterminisme : tout obéit à des lois donc les faits humains sont causés par leurs antécédents et par conséquent tout est modélisable. Sommes-nous tous d'accord avec un tel postulat ? D'autres ne pensent-ils pas qu'il existe un aléa incompressible, c'est-à-dire autant d'hypothèses que d'hommes, ce qui rend vains de tels algorithmes ?

Cette question ne concerne pas que la délinquance. Elle se pose aussi pour la voiture autonome (sans chauffeur). Si deux voitures vont se percuter de plein front, laquelle doit se jeter dans le fossé ? Doit-on prendre en compte l'âge des passagers ? Leur nombre ? Leur rang social ? Autant d'informations qui seront probablement à la disposition de l'algorithme. Qui va prendre l'initiative et la responsabilité de les paramétrer ?

Admettons que l'on doive fixer et donc hiérarchiser ces choix. Ne devrions-nous pas imposer que tout ce qui touche à la norme humaine, et notamment celle du comportement humain idéal ou du comportement social moyen, devrait faire l'objet d'une discussion ou d'une validation préalable obligatoire, sous un angle éthique. C'est à la Société (soit politique, soit civile) de décider et en connaissance de cause, pas aux ingénieurs, de manière implicite et uniquement sous un angle économique.

D'autre part, comment s'assurer de la fiabilité et de l'intégrité des algorithmes ? Le scandale des moteurs diesel de Volkswagen démontre qu'il ne s'agit pas d'une question théorique. La grande

question de l'antiquité était de savoir qui gardera les gardes ? Celle de l'ère numérique sera de savoir qui gardera les algorithmes. Il appartient au législateur d'intervenir sur ces questions et de trouver un équilibre entre le secret des affaires et la protection de l'ordre public. Notre société n'aura rien de bon à gagner en remettant son destin entre les mains de formules mathématiques secrètes.

Allons-nous vers la tyrannie des Big Data personnelles ?

L'internet des objets permet la collecte permanente des données d'un individu et permet d'avoir une visibilité sur la durée. En matière de santé, cette connaissance est un progrès et permettra un traitement médical réellement adapté à chaque personne. Le suivi continu des données du patient sera le standard de demain. La prudence s'impose dès lors que nous ne mesurons pas toutes les conséquences de la publicisation de nos données personnelles dans ce domaine.

Outre les questions d'atteinte à la vie privée, gardons-nous de créer une fracture numérique entre les individus. Plus on aura d'ancienneté et donc de traçabilité dans les Big Data personnelles, plus la vie sera facile (si les dites données sont «bonnes» !). A l'inverse, la vie sera beaucoup plus difficile pour ceux qui n'auront pas de Big Data personnelles ou qui en auront de mauvaises, c'est-à-dire différentes de la norme attendue.

Gardons-nous aussi d'utiliser ces données pour procéder à une sélection entre les individus. Dès lors que la connaissance sera accessible, n'allons-nous pas trier entre les individus à soigner ou à assurer ? Une telle démarche est de nature à remettre en cause notre principe de mutualisation. Promouvoir un modèle économique permettant de ne sélectionner que les bons clients (qu'ils soient assurés ou patients) sera peut être profitable mais uniquement à court terme. Que se passera-t-il pour les mauvais clients ? A terme, c'est la cohésion sociale qui sera remise en cause avec des conséquences que l'on ne peut pas mesurer.

Le numérique nous donne accès à une nouvelle connaissance et nous devons fixer de nouvelles règles qui intègrent absolument une dimension éthique dans l'utilisation desdites données.

L'AUTEUR

Fabrice LORVO est avocat au Barreau de Paris, et associé du cabinet FTPA. Il intervient notamment en droit des médias, de la communication et des nouvelles technologies. Il est l'auteur de « Numérique : de la révolution au naufrage ? » chez www.fauves-editions.fr (Avril 2016). Il est également chroniqueur sur France Culture pour l'émission « le Secret des sources ».

Fotolia

LE *RANSOMWARE* DEMONTRE LA VALEUR INTRINSEQUE D'UN PATRIMOINE INFORMATIONNEL

Le *ransomware* est une nouvelle forme massive de prédation qui touche tant les particuliers que les entreprises au travers du caractère substantiel de leur capital informationnel pour leurs activités. Le cryptage frauduleux des données numériques d'un tiers et le rétablissement de leur accès moyennant une rançon est un acte répréhensible mais dont la qualification pénale est délicate. Est-il un vol, un chantage, une contrainte ou une infraction particulière ? La réponse pénale, normalement dissuasive, peut paraître encore inadaptée et il existe encore des marges de progrès quant au temps de traitement et à l'exemplarité des condamnations. La question de la preuve numérique appliquée à des auteurs situés hors du territoire et intervenant à partir de plusieurs nœuds du réseau trouve toute sa pertinence du fait de la difficulté à réunir les éléments de l'infraction.

Le *ransomware* entre toutefois dans une économie juridique particulière car le règlement européen (RGPD) n°2016/679 du 27 avril 2016, applicable à compter de mai 2018, oblige les entreprises à notifier la violation de données personnelles dans les 72 heures à compter de sa connaissance auprès de l'autorité de contrôle et lorsque la violation est susceptible d'engendrer un risque élevé pour les droits et libertés de la personne. Cette disposition peut concourir à une évaluation réelle du chiffre noir de ce phénomène.

Régime juridique du ransomware ou prise d'otage numérique

par ERIC A. CAPPRIOLI

Avec la généralisation du numérique, la cybercriminalité se développe sans cesse que ce soit en quantité, diversité ou en qualité. Ses contours évoluent et s'adaptent aux mesures de sécurité mises en place pour parer les menaces. La société Symantec, dans son rapport annuel 2015 sur l'évolution des menaces informatiques dans le monde, a souligné l'augmentation de plus de 36 % des logiciels malveillants par rapport à 2014 (en 10 ans, on serait passé d'environ 22 000 à 430 millions logiciels malicieux).

Cela peut aussi se traduire par du piratage de données plus ou moins sensibles, comme dans l'affaire Ashley Madison (site de rencontres extraconjugales avec 37 millions d'utilisateurs concernés) ou dans celle du fabricant de jouets connectés VTech (soit 6,3 millions de profils d'enfants dont 1,2 million français). OS Microsoft, Mac, Linux, Androïd, Apps, tous les terminaux (ordinateurs fixes et mobiles, téléphones portables et smartphones, tablettes, IOT) et tous les systèmes sont visés par des malwares. Après la vogue des fraudes aux dirigeants qui ont défrayé la chronique, on observera cependant une recrudescence de ce que l'on nomme désormais le *ransomware*. En effet, pourquoi se fatiguer à siphonner des données et les revendre, alors qu'il est plus facile de les rendre inintelligibles et de vendre les clés de déchiffrement à celui qui pâtit du blocage, d'autant que la qualification juridique de l'infraction est encore incertaine. Pour la France, le baromètre de la cyber-sécurité des entreprises, de janvier 2016, du Club des experts de la sécurité de l'information et du numérique (http://www.cesin.fr/publications/docume

ERIC A. CAPPRIOLI
Avocat à la cour de Paris

Le paiement de la rançon ne garantit pas la fin du chantage numérique. Il vaut mieux amorcer une réponse en collaboration avec les autorités compétentes.

nt/display/121) constate que 61% des entreprises interrogées ont été victimes de demandes de rançons. On a recensé 391 000 attaques de ce type en France !

Les contours du Ransomware

Éléments de définition

Le ransomware est un logiciel malveillant qui a la particularité de prendre en otage des données d'une entité en les chiffrant ou de bloquer l'accès d'une machine à tout utilisateur. Il existe aussi un ransomware appelé « virus gendarmerie » qui consiste à bloquer un ordinateur et à faire croire que la gendarmerie a découvert des activités illicites et demande le paiement d'une amende. Pour déchiffrer les données avec une clé cryptographique ou disposer de l'équipement ou de la clé permettant de déverrouiller la machine, la victime doit verser une somme d'argent, le plus souvent par Bitcoins, crypto-monnaie sulfureuse qui doit son développement aux divers trafics réalisés dans le web profond (Dark Web)[1]. En mars 2016, l'Agence France Presse a été victime de deux tentatives successives de demande de rançon, avec le ransomware Locky. Ces tentatives ont été déjouées sans paiement de la rançon. Mais comme l'a expliqué le RSSI, l'AFP refuse le chantage et : « *Nous portons plainte auprès de la police judiciaire. Nous isolons les ordinateurs infectés, nous les reformatons, nous*

(1) Sur le Dark Web , v. Adrien Petit, *Le Dark Web, place de marché des données volées*, Rev. de la Gendarmerie nationale, 4e trimestre 2015, n° 574, p.53 et s.

restaurons les données dans la journée et nous conservons les fichiers cryptés comme nous le conseillent les enquêteurs »[2]. Il convient de préciser que les sauvegardes des données avaient été faites hors ligne ; heureuse précaution !

(2) http://www.silicon.fr/ransomware-locky-lafp-touchee-son-rssi-temoigne-142797.html

À côté de ces méthodes reposant sur du chiffrement, il existe d'autres procédés apparentés, sans utilisation de produits cryptographiques qui, par exemple, orientent la victime vers des numéros gratuits mais qui sont en réalité surtaxés ou de faux techniciens soi-disant support de Microsoft qui imitent des pages d'erreurs et bloquent l'ordinateur avec une prise de contrôle à distance avec team Viewer. Parmi les ransomwares les plus connus, on peut citer Cryptowall (actuellement la V.4.0) ou teslaCrypt, ou plus récemment Samsam qui s'attaque aux serveurs utilisant Jboss. Selon l'Agence nationale de la sécurité des systèmes d'information (ANSSI), on entend par les termes « Chantage/Ransomware » : « *Forme d'extorsion imposée par un code malveillant sur un utilisateur du système. Si ce dernier refuse de payer ou d'effectuer une tâche imposée, le service auquel il veut accéder lui est refusé par le code malveillant. Remarques : Un tel code peut par exemple chiffrer des fichiers pour les rendre inexploitables. L'utilisateur se voit présenter des instructions, telles que le paiement d'une somme d'argent, pour récupérer ses fichiers. Céder au chantage ne garantit pas que les fichiers seront restaurés et crée un risque de prélèvements frauduleux ultérieurs sur les moyens de payement utilisés* »[3].

(3) ANSSI, Glossaire, v. http://www.ssi.gouv.fr/administration/glossaire/c/.

Risques juridiques

Ces risques sont de natures diverses. Parmi eux, on citera non seulement les pertes de données à caractère personnel, mais également la préservation de la sécurité des données afin notamment qu'elles ne soient pas déformées, endommagées ou que des tiers non autorisés n'y aient pas accès (art. 34 de la loi du 6 janvier 1978) sous peine de sanctions de la CNIL ou de sanctions pénales (art. 226-17 du code pénal : 300 000 euros d'amende et 5 ans de prison). Cependant, avec le nouveau Règlement européen (RGPD) n°2016/679 du 27 avril 2016 sur la protection des données[4], applicable à compter de mai 2018, toutes les entreprises auront l'obligation de notifier les violations de données personnelles contrairement à la loi de 1978 actuellement en vigueur qui vise les fournisseurs de services de communications électroniques en vertu de l'article 34 Bis. Selon l'art. 33 du

(4) JOUE du 4 mai 2016, L. 119/1.

RGPD, cette notification doit intervenir dans les 72 heures à compter de sa connaissance auprès de l'autorité de contrôle et lorsque la violation est susceptible d'engendrer un risque élevé pour les droits et libertés de la personne, la notification à la personne concernée doit s'opérer dans les meilleurs délais (art. 34 du RGDP). D'un autre côté, il ne faut pas oublier qu'il existe aussi l'impossibilité d'accéder aux autres données, qui portent sur les produits, les services ou les marchés, de nature technique, économique et ne concernent pas les traitements de données à caractère personnel. Cela fait référence, par exemple, à celles qui auraient été marquées comme relevant du secret des affaires[5] et ne sont pas protégées par les droits de propriété intellectuelle.

(5) Directive (UE) 2016/943 du Parlement Européen et du Conseil du 8 juin 2016 sur la protection des savoir-faire et des informations commerciales non divulgués (secrets d'affaires) contre l'obtention, l'utilisation et la divulgation illicites ; Sabine Marcellin et Thibaut Manoir de Juay, *Le secret des affaires*, Lexisnexis, 2016.

(6) Jean-Laurent Santoni, *Cybercriminalité, Le ransomware est-il assurable ?*, Expertises, Juin 2016, v. p. 219.

Le ransomware est-il assurable ?

Le fait que le ransomware soit assurable suscite une objection majeure : cela « *pourrait favoriser la collusion frauduleuse entre l'assuré et l'auteur de l'extorsion*[6] ». Si l'on raisonne par analogie, on peut également s'interroger sur la licéité de l'assurance portant sur les rançons versées à l'occasion d'enlèvement de personnes physiques. Mais pourquoi interdire en droit français des assurances ce qui serait autorisé aux concurrents étrangers ? Cela risquerait de créer une forte distorsion de concurrence au préjudice des assureurs français.

II/. Quelles qualifications juridiques ?

Les infractions juridiques

Face à ces nouvelles formes de menaces numériques, le Code pénal dispose d'un arsenal de dispositions aptes à apporter des réponses à ces pratiques délictuelles. À ce titre, on observera tout d'abord que les textes légaux classiques depuis la loi Godfrain de 1988 (modifiés à plusieurs reprises) permettent de réprimer les atteintes aux systèmes d'information avec les articles 323-1 et 323-3 du Code pénal : introduction, maintien frauduleux dans un système d'information, altération du fonctionnement du SI, introduction frauduleuse des données dans un STAD (extraction, détention, reproduction, transmission, suppression modification). Les sanctions varient entre 2 et 5 ans d'emprisonnement et de 60 à 150.000 euros d'amende, sauf dans l'hypothèse où l'on est en présence d'un système de traitement de données à caractère personnel mis en œuvre par l'État, pour lequel le Code pénal prévoit des sanctions plus lourdes (articles 323-1, al.3[7], 323-2, al. 2[8] et 323-3, al.2 du Code pénal).

Dans le cadre du ramsonware, on aura plutôt recours à une qualification se fondant sur l'article 323-3 du Code pénal:

(7) « *Lorsque les infractions prévues aux deux premiers alinéas ont été commises à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à cinq ans d'emprisonnement et à 150 000 € d'amende.* »

(8) « *Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à sept ans d'emprisonnement et à 300 000 € d'amende* ».

(9) CA Paris, pôle 4, ch. 10, 5 févr. 2014, n° 13/04833 : Comm. com. électr. 2014, comm. 40, Éric A. Caprioli. ; Cass. Crim. 20 mai 2015, n° de pourvoi : 14-81.336, JurisData n° 2015-011834 ; Comm. com. électr. septembre 2015, comm. 74, Éric A. Caprioli.

« *le fait d'introduire frauduleusement des données* » dans un SI, « *d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données qu'il contient* », puisqu'il y a modification lorsque les données sont chiffrées par un tiers de sorte qu'elles soient inutilisables. L'introduction frauduleuse de données est réalisée (les données de chiffrement). En revanche, la qualification de vol, telle que l'a consacrée la Cour de cassation le 20 mai 2015[9] n'est pas possible car en l'espèce, il n'y a ni soustraction, ni reproduction des données contenues dans le système.

D'un autre côté, il semble également envisageable de s'appuyer sur l'article 323-3-1 du Code pénal qui permet de sanctionner l'offre, l'importation, la détention, la mise à disposition ou la cession de programme malveillant si tant est que l'on puisse saisir « *un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3* ».

De plus, ces infractions sont encore plus sévèrement réprimées dès lors que la préparation s'effectue en groupe ou qu'elles sont commises en bandes organisées, ce qui est souvent le cas des attaques de type ramsonware (ex : près de 325 millions de dollars au même groupe de cybercriminels avec cryptoWall 3.0).

Deux autres délits non spécifiques au numérique pourraient trouver à s'appliquer : l'extorsion de fonds et le chantage. S'agissant du premier, l'article 312-1 du Code pénal dispose : « *L'extorsion est le fait d'obtenir par violence, menace de violences ou contrainte soit une signature, un engagement ou une renonciation, soit la révélation d'un secret, soit la remise de fonds, de valeurs ou d'un bien quelconque. L'extorsion est punie de sept ans d'emprisonnement et de 100 000 euros d'amende.* » La qualification semble délicate à établir dans la mesure où il sera difficile de considérer que le fait de chiffrer des données appartenant à autrui soit de la violence ou une menace de violence ou encore une contrainte. L'action réalisée avec le ransomware est d'un autre type non prévu par le texte. En ce qui concerne le chantage, là encore, la formulation du délit n'est pas adaptée au cas de prise d'otage de données numériques. Ce délit est réprimé à l'article

312-10 : « *Le chantage est le fait d'obtenir, en menaçant de révéler ou d'imputer des faits de nature à porter atteinte à l'honneur ou à la considération, soit une signature, un engagement ou une renonciation, soit la révélation d'un secret, soit la remise de fonds, de valeurs ou d'un bien quelconque. Le chantage est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende.* »

Les limites à la répression

Les plaintes pénales, lorsqu'elles aboutissent à des poursuites judiciaires, durent plusieurs années avant qu'une éventuelle condamnation n'intervienne. Or, pour y parvenir, encore faut-il d'une part, identifier le ou les délinquant(s) qui se trouvent souvent hors du territoire français et européen et agissent à partir de plusieurs points d'un réseau et, d'autre part, réunir les éléments de faits de la ou des infraction(s) afin de les constituer. Mais finalement, on peut constater que les tribunaux français, contrairement à ceux d'autres systèmes judiciaires (ex : USA, Royaume Uni) sanctionnent assez faiblement la cybercriminalité alors que les textes autorisent des peines beaucoup plus sévères. Or, avec le ransomware, le mal étant fait, les victimes paient souvent sans porter plainte sans qu'elles n'aient pas pour autant des garanties d'accès à leurs données comme on a pu le voir, en mai 2016, avec le Kansas Heart Hospital où au lieu de débloquer le système, les délinquants ont demandé un nouveau paiement. Le fait de ne pas porter plainte ne facilite pas la tâche des services de police et de gendarmerie.

Après les ransomwares comme Locky on a vu arriver de nouvelles versions de ce dernier, ainsi que des nouveaux produits tels que Crysis ou Ke.Ranger. À peine détectés, il en apparaît de nouveaux. Plus récemment est apparu le concept de RaaS (« Ransomware as a Service ») qui permet à l'auteur de partager la rançon avec le diffuseur qui personnalise le ransomware. Les paiements s'effectuent sous couvert d'anonymat de l'auteur et du diffuseur, car ils utilisent le réseau TOR et la crypto-monnaie « bitcoins » fondée sur la technologie blockchain.

Si des parades existent notamment logicielles (tels que Malwarebytes et les solutions développées par des sociétés de sécurité informatique) ou l'analyse forensics, le nettoyage et la restauration des données, la meilleure façon de lutter contre le ransomware reste l'anticipation. Dans ce cadre, il est conseillé de:

- procéder à la sauvegarde régulière des fichiers et données hors réseau ;
- sensibiliser régulièrement les personnels sur les bonnes pratiques et avec plusieurs supports (e-learning, formation, jeux, vidéos) ;
- contrôler les utilisateurs sous réserve de disposer de chartes informatiques et de

procéder aux formalités Informatiques et libertés et de protéger le patrimoine informationnel de l'organisation en cause ;

• préparer une procédure d'alerte pénale pour collecter les éléments de preuve en vue d'une plainte auprès des services judiciaires.

De façon plus générale, la sécurité de l'information suppose une remise en question permanente et une grande capacité d'adaptation de l'organisation aux nouvelles menaces. Seule l'application d'une méthodologie fondée sur la roue de Deming (Plan-Do-Check-Plan) est à même de résoudre les problèmes de sécurité et de l'améliorer en permanence. Une histoire sans fin …

L'AUTEUR

Après une période de dix ans passée dans des entreprises technologiques (juriste d'entreprise et directeur général), un master en gestion des entreprises suivi d'un doctorat en droit (thèse sur le crédit documentaire, publiée aux éditions Litec en 1992), Eric A. Caprioli est devenu avocat en fondant le cabinet d'avocats Caprioli & Associés. Parallèlement, il a enseigné le droit de l'informatique et du numérique, le droit des affaires en Ecole de Commerce (EDHEC Business School) pendant une quinzaine d'années, ainsi qu'à l'Université de Nice Sophia-Antipolis, puis aux Universités de Paris II (Panthéon-Assas) et Paris I (Panthéon-Sorbonne) jusqu'à ce jour.
Il est titulaire des spécialisations délivrées par le Conseil National des Barreaux en droit des nouvelles technologies, de l'informatique et de la communication et en droit de la propriété intellectuelle.
Il est Membre de la délégation française aux Nations Unies en matière de droit du commerce électronique depuis 1993.
Vice-Président de la Fédération des Tiers de Confiance Numérique (FNTC) et du Club des Experts de la Sécurité de l'Information et du Numérique (CESIN).
Depuis plus de 10 ans, il tient la chronique mensuelle « Sécurité de l'information » dans la revue Communication, Commerce Electronique (LexisNexis).
e.caprioli@caprioli-avocats.com

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**

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, à la prévention (site CECyF Prévention) et à la recherche & développement contre la cybercriminalité. Le CECyF compte 34 membres dont les douze premiers étaient issus du projet européen 2CENTRE et de leurs 15 partenaires. Il rassemble des services de l'État, des établissements d'enseignement supérieur et de recherche, des entreprises et des associations. La gendarmerie en assure la présidence et le secrétariat général.

Le CECyF est partenaire du Festival du film de sécurité d'Enghien.

Partenaire de Cyberlex, association qui regroupe des spécialistes du droit du cyberespace et des technologies numériques, il organise avec elle une masterclass sur le droit pénal de l'espace numérique à l'occasion du FIC 2017. En synergie avec cet événement, il co-organise la 3e Conférence sur la réponse aux incidents et l'investigation numérique, CoRI&IN.