CYBER CERCLE

collection

PAROLES D'EXPERTS

2022

PAROLES D'EXPERTS

Ce livre est édité sous la direction de
Bénédicte PILLIET, Présidente du CyberCercle

Préface

BENEDICTE PILLIET
Présidente
CyberCercle

Je suis très heureuse de publier aujourd'hui l'opus 2022 de nos Paroles d'Experts inaugurées dans leur format et leur périodicité en avril 2020.

Un troisième opus qui témoigne de notre volonté d'avoir une dynamique de publication de contenus tout au long de l'année, dans la continuité de celle engagée en 2020 à l'occasion de la crise de la COVID-19.

Je remercie très sincèrement tous ceux qui ont ainsi participé à cette rubrique.

En 2022, ce sont 22 Paroles d'Experts écrites par des parlementaires, des représentants d'entreprises - de la start-up au grand groupe, d'administrations de l'Etat, des armées, de collectivités, d'associations, d'écoles et d'organismes de recherche que nous avons publiées le vendredi tout au long de l'année.

Des publications éclairantes sur des sujets de gouvernance, d'enjeux sectoriels, de réglementation, d'innovation, de développement des territoires, de recrutement et de formation, d'éducation, de souveraineté… autant d'enjeux pour l'évolution de notre société vers une véritable « CyberSociété » dont les piliers indispensables sont la sécurité et la confiance numériques.

Ce rythme de publication, cette diversité des contributeurs et des sujets abordés, sont les reflets de la philosophie qui nous anime au CyberCercle.
Permettre un accès ouvert au plus grand nombre à une expertise de confiance pour développer une culture partagée de sécurité et de confiance numériques.
Etre un vecteur de diffusion et de valorisation d'analyses transdisciplinaires de personnalités qualifiées.

Favoriser la réflexion et les échanges constructifs au service de l'intérêt général.

Une nécessité pour mieux appréhender la transformation numérique globale qui touche à la fois l'ensemble des secteurs économiques, la structure même de l'organisation de la société et jusqu'à ce que nous sommes en tant qu'individu-citoyen, avec un impératif : assurer la confiance dans le numérique.

Beaucoup de chemin reste à parcourir pour que le numérique de confiance soit une évidence pour tous : nous continuons au CyberCercle à y travailler.

Je vous souhaite une bonne lecture et vous donne rendez-vous le vendredi sur notre site pour une nouvelle Parole d'Expert.

Le *cloud* au service secret de sa Majesté Enjeux et perspectives des *clouds* pour les services de renseignement

MARINA DE CASTRO
Attachée d'administration
Ministère de l'Intérieur
Advisor du CyberCercle

Au second semestre de l'année 2021, les services de renseignement anglais annonçaient la signature d'un contrat avec *Amazon Web Service* pour l'hébergement de données, en particulier celles classifiées. L'accord est d'une importance majeure puisqu'il concerne trois pôles stratégiques du renseignement britannique. Ainsi, ce sont les données du *Government Communications Headquarters* (GCHQ), du *Security Service* (MI5) et du *Secret Intelligence Service* (MI6) qui seront stockées sur un *cloud* unique hébergé par *Amazon*. Cette solution vise à leur permettre des facilités de stockage, de recherche et de partage de l'information. Ces trois entités, dont les activités englobent la sécurité intérieure comme extérieure (MI5 et MI6) mais aussi la sécurité des systèmes d'information (GCHQ) s'en remettent donc à une entreprise américaine pour garantir la sauvegarde de leurs données confidentielles. Si le montant de la tractation n'a pas été communiqué, il est intéressant de noter qu'*Amazon Cloud Service* compte plus d'un million de clients au cœur de métiers divers tels que le spatial, la téléphonie, l'enseignement universitaire ou encore l'industrie agroalimentaire.

Le Royaume-Uni ne fait pas figure de pionnier en confiant l'hébergement de ses données classifiées à *Amazon*. En effet, en 2014, la CIA américaine avait également recours au service de ce géant du Web. En revanche, ce qui est une première dans le cas britannique c'est l'emploi des services

d'une entreprise étrangère pour traiter des données aussi sensibles que celles des agences de renseignement de sa Majesté.

En dépit de la « relation spéciale » anglo-américaine qui peut exister, le recours aux *clouds* d'industriels étrangers pour l'hébergement de ce type de données pose nécessairement des questions de souveraineté. Quels sont les enjeux que ces *clouds* revêtent pour les services de renseignement ? Les risques encourus sont-ils si compromettants et préjudiciables pour les intérêts vitaux de ces nations ? Quels nouveaux champs ces technologies de stockage ouvrent-elles pour la veille, la collecte, l'analyse et la diffusion du renseignement ?

Des enjeux multiples en termes de réponse opérationnelle

Pour les services de renseignement, le recours aux *clouds* pour l'hébergement de données revêt deux objectifs principaux et complémentaires. Tout d'abord, le regroupement et la centralisation de toutes ces données sensibles faciliteront indéniablement l'usage de technologies de type Big Data pour le traitement et la primo-analyse de ces dernières. Ensuite, cela pavera la voie aux innovations liées à l'intelligence artificielle en matière de production et de gestion du renseignement multi-capteurs[1].

En effet, l'usage des *clouds* devrait permettre aux Agences de développer des lacs de données plus connus sous l'appellation anglo-saxonne *data lakes*. Il s'agit d'un référentiel qui permet de regrouper des données structurées c'est-à-dire provenant de bases de données relationnelles, des données semi-structurées à l'exemple de fichiers CSV ou XML et des données non-structurées comme des e-mails ou des documents PDF. Les *data lakes* peuvent aussi contenir des données binaires correspondant à des images, des vidéos ou des audios. Cette flexibilité est un avantage. Sa finalité est d'intégrer des données brutes dans un ensemble cohérent, de les transformer et de les rendre exploitables à des fins d'analyse. De telles solutions accélèrent l'intégration et offrent un contenu homogène à exploiter même si la nature des données d'entrée est aussi diverse que variée. Alors qu'hier il fallait plusieurs semaines ou plusieurs mois pour

exploiter des données brutes et disparates, aujourd'hui il ne faut plus que quelques minutes. Rendant ainsi l'analyse plus aisée et plus rapide, cet environnement accroît l'opérationnalité de la donnée qui n'est plus uniquement utilisée dans l'objectif de rendre compte. Elle devient ainsi un véritable outil de pilotage, une force motrice qui intervient dès l'orientation du cycle du renseignement. A ce titre, elle favorise le *machine learning*[2] et permet aux analystes et *data scientists* de produire des modèles prédictifs. Ces derniers concourent directement à la planification des opérations et alimentent la fonction stratégique « connaissance et anticipation ».

De plus, l'avènement des réseaux sociaux et de l'Internet des objets[3] (IoT) mettent en exergue le traitement d'importants volumes données et leur collecte massive par des procédés tels que le *scrapping*[4] ou le *crawling*[5], par exemple. Ainsi approvisionnés, les *data lakes* permettraient de systématiser la pratique du *machine learning* à des fins opérationnelles. En février 2020, Jérémy Fleming, le directeur du GCHQ, expliquait que ces moyens devenaient une priorité pour l'espionnage britannique à deux égards : la lutte contre le terrorisme et la lutte contre la manipulation de l'information. En effet, sur de grands volumes de données, le *machine learning* et à terme l'intelligence artificielle permettent d'établir des corrélations invisibles à l'œil nu. Cette méthode est également très utilisée en matière de reconnaissance vocale, de transcription et de traduction des conversations et signaux interceptés. Enfin, la croissance des préoccupations autour des champs immatériels constitue un enjeu déterminant à l'égard de l'usage de *clouds* par certains services de renseignements.

Des risques assumés en matière de souveraineté

De manière générale, si le stockage des données est un enjeu de souveraineté, il l'est encore plus lorsqu'il s'agit de données sensibles et classifiées. Ainsi, ce recours aux services d'hébergement de l'américain *Amazon Web Services* (AWS) soulève de nombreuses interrogations au Royaume-Uni, mais également au sein de viviers d'experts internationaux. Une nouvelle fois, ces pratiques relancent le débat au sujet de la souveraineté de la Grande-Bretagne sur ses institutions et ses industries

stratégiques. Alors que le gouvernement britannique a exclu le chinois Huawei de son réseau télécom 5G, il confie les données de ses services de renseignement à un géant des États-Unis.

En 2013, la CIA signait déjà un accord avec AWS. Toutefois, la question de la souveraineté était moins palpable puisqu'une agence de renseignement américaine contractualisait avec une entreprise dont le siège est dans l'état de Washington. Les notions d'influence ou d'ingérence étrangère n'avaient alors pas lieu d'être. *Amazon* se veut rassurant et précise que l'intégralité des données sera conservée au Royaume-Uni et que la multinationale n'aura aucun accès aux informations contenues dans son *cloud*. Son directeur de la sécurité, Stephen Schmidt, rappelait la philosophie de l'entreprise de « *sécurité par l'obscurité* ». Les employés qui travaillent dans ces segments disposent d'habilitations particulières et ne sont informés que du strict nécessaire à l'exercice de leur travail. Les standards de sécurité d'AWS demeurent très rigoureux.

Si la problématique de la souveraineté peut se poser en termes techniques, elle doit aussi se poser en matière géopolitique. Elle devient d'autant plus capitale dans un contexte international marqué par une course effrénée à la technologie et à l'innovation. En 2020, Richard Moore, le patron de la sécurité extérieure britannique, exprimait son inquiétude d'être distancé par la Chine et la Russie. Il expliquait à l'antenne de la BBC que ces nations « *mettent de l'argent et de l'ambition dans l'intelligence artificielle et l'informatique quantique […] car ils savent que la maîtrise de ces technologies leur donnera un avantage compétitif* ». Il affirmait enfin que « *nous pourrions connaître plus de progrès technologiques les dix prochaines années qu'au cours du siècle dernier, avec un impact en termes de perturbations égal à celui de la révolution industrielle* ». Les craintes qu'il a ainsi exprimées sont partagées par ses homologues d'autres pays européens. La menace chinoise est particulièrement étudiée puisque l'empire du Milieu pourrait dominer d'ici quelques années de nombreuses technologies de pointe parmi lesquelles l'intelligence artificielle. La collecte, le traitement et le stockage de la donnée pourraient devenir des sources de tension, voire de conflits, dans les décennies à venir. Cette méfiance fait écho aux accusations portées par le Royaume-Uni à l'égard de l'équipementier Huawei ou encore aux campagnes de désinformation

en ligne fomentées par le gouvernement chinois, notamment dans le contexte de la pandémie de Covid-19.

Le contrat conclu entre les agences de renseignement britanniques et *Amazon* peut, de prime abord, interroger sur la souveraineté de la donnée. Toutefois, le risque semble être connu et assumé. Il s'agirait davantage d'un choc culturel d'ampleur à absorber. Dans des milieux où le cloisonnement était une règle d'or, la technologie impose de désensiler l'information pour en tirer le meilleur profit. L'impression de décloisonnement que ce recours aux *clouds* peut induire ne contrevient pourtant pas aux traditionnels « besoins d'en connaître ».

Eu égard à la fulgurance de l'information et à l'accélération du cycle d'innovation digitale, les entreprises nationales britanniques n'ont pas été en mesure de fournir des capacités de stockage de données dans le *cloud* satisfaisant au besoin opérationnel. Contrairement à Q dans James Bond, un tel niveau d'expertise technique ne s'obtient pas en un claquement de doigts. Pour Londres, l'étroite coopération avec les acteurs de la Tech' et les GAFAM a été incontournable.

A Paris, le gouvernement préfère soutenir des projets de *clouds* souverains à l'exemple de « Bleu », le *cloud* de confiance porté par Orange et Capgemini. Par ailleurs, en octobre 2021 Google Cloud et Thalès (leader français des hautes technologies sur le marché de l'aérospatial et de la défense) annonçaient le développement conjoint de projets répondant aux exigences du label « *cloud* de confiance ». Avec le recours massif aux *clouds* par les acteurs privés et publics, les institutions et les services de renseignement prennent aujourd'hui la mesure du gain de performance qu'ils procurent, mais également des nouveaux risques opérationnels qui les accompagnent, notamment en termes de confidentialité, de gouvernance et de souveraineté de la donnée.

Parution le 7 janvier 2022

Sources

BABUTA Alexander, JANJEVA Ardi et OSWALD Marion « *Artificial intelligence and UK national security : policy considerations* », Rusi.org, 27 avril 2020

BLANJEAN Romain, « *Pourquoi investir dans le cloud souverain quand on est déjà sur le cloud public ?* », Zdnet.fr, 30 novembre 2021

CORERA Gordon, « *UK spies will need artificial intelligence* », BBC.com, 27 avril 2020

DELUZARCHE Céline, « *Les services secrets britanniques font appel à Amazon pour stocker leurs documents secrets défense* », Korii.slate.fr, 28 octobre 2021.

FILIPONE Dominique, « *Les services secrets britanniques misent sur le cloud AWS* », Le monde informatique, 27 octobre 2021

KONKEL Frank, « *The details about CIA's deal with Amazon* », Theatlantic.com, 17 juillet 2014

LIÈVRE Florence, « *Capgemini et Orange annoncent le projet de créer « Bleu » une société qui fournira un cloud de confiance en France* », Orange.com, 27 mai 2021

TOUSSAINT Léo, « *AWS : une région secrète pour les services de renseignement américains* », Siecledigital.fr, 22 novembre 2017

VONINTSOA, « *Amazon signe un contrat cloud avec les agences d'espionnage britannique* », intelligence-artificielle.com, 15 novembre 2021

« *Data lake : la solution reine du Big Data* », Journaldunet.fr, 15 mai 2018

[1] Le renseignement multi-capteurs désigne une forme de renseignement qui agrège des informations émanant d'origines de collecte différentes : électromagnétique, imagerie, humaine ou encore sources ouvertes.
[2] Le machine learning est une méthode de programmation qui se base sur les statistiques et les probabilités pour permettre aux ordinateurs d'apprendre « par eux-mêmes » en s'entraînant sur de larges jeux de données (datasets).
[3] L'Internet des objets désigne le flux de données émis par tous les objets connectés : de la montre au réfrigérateur en passant par l'assistant vocal.
[4] Le scrapping est une technique de collecte automatisée de données sur des sites web. Généralement des scripts ou des bots extraient le contenu de pages web pour alimenter des bases de données ou des outils de veille et d'analyse.
[5] Le crawling désigne l'exploration de sites webs par des robots à des fins d'indexation de contenus. Les bots scannent les pages webs et récupèrent leur codes sources pour les indexer. Googlebot est l'outil de Google pour cet usage.

La lutte contre le blanchiment de capitaux à l'ère des crypto monnaies

AMAURY GREVESSE-SOVET
Junior Associate
Département Corporate, Banking & Finance
Cabinet Elvinger Hoss Prussen

Le blanchiment d'argent est un délit consistant à masquer l'origine frauduleuse de sommes d'argent. Il est assimilé à un processus réalisé par le biais de plusieurs opérations et est sanctionné en droit luxembourgeois aux termes de l'article 506 du Code pénal. Les criminels, conscients de la dangerosité de l'argent sale, susceptible de constituer une preuve des activités criminelles commises pour son obtention ou encore de faire l'objet d'une enquête et donc d'une saisie, cherchent à donner une apparence honnête à cet argent gagné de façon malhonnête. Ce blanchiment est donc perpétué en dissimulant des actifs d'origine illégale par l'utilisation abusive d'instruments et de circuits financiers, dans l'optique de réduire la probabilité qu'un lien soit établi entre les délits commis et la richesse créée. Il s'agit in fine de réintroduire l'argent illégalement obtenu dans le circuit économique et monétaire légal afin d'en profiter et pourquoi pas le faire prospérer quand celui-ci est par exemple placé sur les marchés financiers.

Les techniques de blanchiment sont variées, tantôt artisanales, tantôt financières et plus récemment digitales. Lorsqu'il s'agit de techniques artisanales, on pense classiquement à l'achat d'or, à la surfacturation, aux faux gains aux jeux ou encore aux fausses ventes aux enchères. Néanmoins, elles peuvent prendre également une dimension financière et plus complexe. Il s'agit là des fausses factures, de l'exemple du prêt adossé des techniques de prêt autofinancé auprès des banques, des opérations immobilières etc. Plus récemment, les nouvelles technologies ont permis

l'essor de nouvelles techniques par le biais des jeux en ligne, des ventes fictives en ligne ou encore par le recours aux crypto monnaies.

Les cryptos monnaies fascinent par le caractère obscur accordé à celles-ci mais aussi en raison de leur nouveauté. Très peu osent les définir et nombreux sont ceux qui, pour les décrire, préfèrent esquisser une définition de ce qu'elles ne sont pas ou offrir une définition trop large et donc imprécise. Tandis que Dominic Wilson estime qu'elles sont « des avoirs financiers à valeur spéculative pouvant servir de moyen d'échange », il conviendrait plutôt de retenir que celles-ci s'apparentent à un moyen de paiement virtuel utilisable essentiellement sur Internet mais dont la portée semble également offrir des perspectives « physiques ». En vertu de l'article 3, paragraphe 18, de la directive 2015/849/UE tel que modifié par la cinquième directive relative à la lutte contre le blanchiment de capitaux (5e directive AML), celles-ci sont : « des représentations numériques d'une valeur qui ne sont émises ou garanties ni par une banque centrale ni par une autorité publique qui ne sont pas nécessairement liées non plus à une monnaie établie légalement et qui ne possèdent pas le statut juridique de monnaie ou d'argent, mais qui sont acceptées comme moyen d'échange par des personnes physiques ou morales et qui peuvent être transférées, stockées et échangées par voie électronique ».

Les crypto monnaies comme nouvel intermédiaire de blanchiment

Les crypto monnaies sont appréciées des criminels qui s'en servent comme nouvel intermédiaire de blanchiment, notamment en raison de transactions très rapides et parfois intraçables selon la transparence inhérente à la blockchain concernée. A titre d'exemple, les opérations en Monero permettent une dissimulation totale en mêlant diverses transactions, rendant ainsi la remontée à l'émetteur impossible. Aussi, il convient d'évoquer le menace relative aux mixeurs. Ils prennent la forme de plates-formes et d'intermédiaires qui transmettent des fonds au nom des utilisateurs en encaissant des crypto monnaies dans une monnaie fiduciaire ayant cours légal, en les convertissant dans une autre crypto monnaie, ou en les transmettant à une autre adresse de crypto monnaie

de telle sorte que le flux de fonds ne puisse être visualisé et retracé directement sur la blockchain. Le fonctionnement repose sur un phénomène de regroupement des crypto monnaies appartenant à de nombreux utilisateurs, sur le fait de mélanger les entrées et les sorties des transactions et finalement redistribuer les pièces parmi les utilisateurs. L'idée est ainsi d'optimiser l'anonymat des pièces en brouillant la piste des transactions pour rendre plus difficile le déchiffrement du flux. Ces mixeurs sont tous particulièrement appréciés lorsqu'il s'agit de blanchir des capitaux par le biais des crypto monnaies.

A cela s'ajoute l'essor de ce qui pourrait être qualifié de crypto-crimes. Ceux-ci sont l'illustration d'une cybercriminalité croissante avec l'obtention frauduleuse de crypto monnaies ainsi que l'usage illicite de celles-ci. A titre d'exemple, de plus en plus d'utilisateurs de crypto-actifs stockent les clés privées pour accéder à leurs fonds de crypto-actifs chez des fournisseurs de stockage en ligne ou des sites de trading qui offrent des services de conservation à leurs clients afin de rendre leur expérience globale dans le monde de la cryptographie plus accessible. Or, en agissant de la sorte, les consommateurs s'exposent à des risques : si les clés privées d'un utilisateur sont volées ou rendues inaccessibles lors d'un piratage du fournisseur de stockage ou de l'échange, il ne pourra plus accéder à ses crypto-actifs, ce qui entraîne une perte des fonds. Une fois subtilisées, ces crypto monnaies seront insérées dans un circuit de blanchiment.

Les crypto monnaies comme moyen de détection et outil stratégique dans la lutte contre le blanchiment de capitaux

Pourtant, les crypto monnaies offrent de réelles perspectives tant technologiques que financières dans un avenir digitalisé. Elles offrent la possibilité de lutter contre le blanchiment d'argent en permettant de retracer les transactions par le biais de la blockchain et ainsi de mettre en lumière les circuits criminels profitant du numérique pour blanchir des capitaux d'origine illégale. En effet, la blockchain offre l'opportunité de pouvoir retracer l'ensemble des transactions correspondantes en partant d'un bloc, d'une adresse, d'un hash de bloc, d'un hash de transaction ou encore d'une adresse IP. Les crypto monnaies deviendront un acteur

majeur en matière de détection et seront garanties de davantage de transparence que les monnaies fiduciaires, qui elles, bien que moins critiquées, sont finalement bien plus propices au blanchiment. On ne peut que sourire face au constat que la décentralisation sera à terme synonyme de plus d'efficacité dans la lutte contre ce phénomène économique.

Face à des avancées technologiques constantes, le législateur se doit lui aussi d'être innovant. A ce titre, évoquons la 5ème et la 6ème directives AML de l'Union européenne fournissant toutes deux de précieux apports en la matière. Le cadre réglementaire est fondé sur la stratégie de suivre l'argent, une stratégie similaire aux prémices de la lutte générale contre le blanchiment d'argent. En effet, en privant les criminels des bénéfices économiques de leurs activités illicites, la réglementation s'attaque à un large éventail d'infractions sous-jacentes. De ce fait, la 5ème directive AML ne vise pas uniquement les transactions suspectes de crypto monnaies susceptibles de faire partie d'un dispositif de blanchiment d'argent. Les tâches de surveillance qui en résultent aident également à détecter d'autres formes d'activités criminelles, qui tirent parti de l'écosystème des crypto monnaies. La 6ème directive AML met quant à elle l'accent sur la prévention relative à la cybercriminalité, sur la nécessité d'accroître la coopération mais aussi par une innovation : celle de la pénalisation des personnes morales pour l'infraction de blanchiment commise par le biais des crypto monnaies.

Des progrès nécessaires pour assurer une lutte efficace

Les 5ème et 6ème directives demeurent néanmoins perfectibles et un rapport en date d'avril 2020, réalisé à la demande de la Commission des affaires économiques et monétaires du Parlement Européen, laisse transparaître les innovations normatives nécessaires pour assurer une lutte adéquate contre le blanchiment de capitaux par le biais des crypto monnaies. Il conviendrait d'élargir le champs de définition des monnaies virtuelles en intégrant les tokens, d'élargir la liste des professionnels assujettis, de prêter une attention accrue aux mineurs de crypto monnaies, d'envisager la mise en place d'un surveillant au niveau européen en matière de lutte contre le blanchiment d'argent, d'accroître les outils de détection et d'enquête ainsi qu'améliorer la clarté et l'accès à l'information légale en matière de crypto

actifs. Il est d'autant plus impérieux de prévoir un cadre règlementaire strict puisque les crypto actifs échappent aux directives MiFID II ou encore EMD2. Enfin, il pourrait être judicieux pour le législateur de prêter une attention accrue à la cybercriminalité avec l'émergence du vol de crypto monnaies ou encore la mise en place de circuits criminels digitalisés. Le même rapport suggère de blacklister les crypto monnaies subtilisées - les bloquant ainsi pour toute transaction future et empêchant une manœuvre probable de blanchiment.

Les criminels ne cessent de faire preuve d'ingéniosité lorsqu'il s'agit de mettre en place des moyens et techniques novateurs de blanchiment. Récemment, l'opportunité de blanchir des capitaux par le biais des crypto monnaies a pu séduire, mais les efforts constants prodigués par le législateur et les organismes compétents, invitent à penser que les crypto monnaies sont promises à un avenir radieux mais surtout à une exposition criminelle amoindrie. La clé réside dans la capacité des innovations juridiques à suivre le rythme effréné des innovations technologiques.

Parution le 14 janvier 2022

Cryptoactifs : une réglementation progressive, une compliance indispensable

MYRIAM QUEMENER
Avocat général, Docteur en droit

Le développement du numérique pose des défis nouveaux au monde de la finance classique, en particulier aux banques qui s'adaptent progressivement à l'inévitable digitalisation des échanges. Ainsi, le secteur des actifs numériques présente un certain nombre de risques en matière de lutte contre le blanchiment de capitaux et de financement du terrorisme (LCB-FT). Ils font l'objet d'une règlementation progressive et doivent avoir aussi toute l'attention de la compliance.

Cryptoactifs : une règlementation récente

La « loi PACTE » propose un encadrement de l'ensemble de ces services et porte modification du Code monétaire et financier. Outre la définition de la notion d'actifs numériques qui comprend les jetons émis dans le cadre d'une ICO et les cryptoactifs (art. L. 54-10-1).

L'article L552-2 du code monétaire et financier définit un actif numérique comme « tout bien incorporel représentant, sous forme numérique, un ou plusieurs droits pouvant être émis, inscrits, conservés ou transférés au moyen d'un dispositif d'enregistrement électronique partagé permettant d'identifier, directement ou indirectement, le propriétaire dudit bien ». Il existe à ce jour plus de 1 500 cryptoactifs dans le monde, à l'instar du Bitcoin et de l'Ethereum.

La loi du 22 mai 2019 relative à la croissance et la transformation des entreprises, dite loi PACTE[1], encadre le secteur des cryptoactifs avec la

création d'un nouveau statut, le « prestataire de services sur actifs numériques » (PSAN).
Dans le cadre de la mise en conformité du droit français suite aux recommandations du GAFI, l'ordonnance du 9 décembre 2020[2] accroît la surveillance des cryptoactifs en permettant un renforcement du cadre de la lutte contre le blanchiment de capitaux et le financement du terrorisme applicable aux actifs numériques. L'ordonnance a été prise en application de l'article 203 de la loi PACTE. Ce texte vise à mettre en conformité le cadre réglementaire relatif aux actifs numériques avec les recommandations du GAFI.

Un des objectifs : renforcer les mesures de lutte contre l'anonymat dans les transactions en actifs numériques. L'ordonnance étend aux services d'échanges dits « crypto-to-crypto » et aux plateformes de négociation d'actifs numériques l'obligation de s'enregistrer auprès de l'AMF, sans contrôle préalable du dispositif LCB-FT. De plus, l'ordonnance soumet les activités précitées aux obligations relatives à la LCBFT. Elle énonce également des mesures importantes telles que l'interdiction pour les prestataires de service sur actifs numériques (PSAN) à tenir des comptes anonymes, l'identification renforcée dès le premier euro ou l'enregistrement obligatoire pour les acteurs étrangers sans établissement fixe. Les dispositions relatives à la vérification d'identité sur les plateformes sont ainsi durcies et les entreprises liées aux cryptoactifs opérant sur le territoire auront un délai de six mois pour se conformer aux nouvelles règles. Ce dispositif constitue un premier pas dans la lutte contre l'anonymat.

Cryptoactifs : une compliance indispensable

L'année 2020 a vu naître des schémas novateurs de blanchiment déclenchés par la crise sanitaire mais aussi par l'utilisation désormais habituelle de crypto-actifs. En effet, la technologie à laquelle ils sont adossés permet d'échapper aux institutions financières classiques pour assurer des transactions instantanées, transfrontalières et sans limite de montant, de façon anonyme, ce qui favorise l'opacité d'opérations économiques, et donc la dissimulation du produit du crime ou de l'origine du financement.

Dans ce contexte de numérisation des services de paiement et des relations d'affaires, TRACFIN dans ses derniers rapports met en garde contre la cybercriminalité financière[3], notamment dans les secteurs des cryptoactifs, du financement participatif et de la banque en ligne. Dans son rapport d'activité pour l'année 2019/2020 publié le 10 décembre 2020[4], le service fait état d'une partie entière dédiée aux risques cyber et inhérents aux crypto-actifs. Il est fait mention de nombreuses typologies d'utilisation de ceux-ci : "*support à la commission d'escroqueries aux investissements fictifs, support au blanchiment du produit d'escroqueries réalisées grâce à des identités fictives, moyen de dissimulation de revenus ou intermédiaire dans le commerce de produits illicites*".
L'analyse des déclarations de soupçon relatives aux crypto-actifs révèle majoritairement des cas d'escroquerie - qu'elles soient simples, de type *blockchain* fictive, ou subtiles telles des opérations de manipulation de cours ou des escroqueries de type Ponzi. TRACFIN conclut qu' « en ce sens, les *blockchains* ne créent pas véritablement de nouvelles méthodes d'escroquerie mais offrent un nouveau champ d'application pour les méthodes éprouvées ».

L'émergence des stable-coins[5] (DAI, HAVVEN, TETHER…) suscite aussi des interrogations de la part des autorités. Ces crypto-actifs de nouvelle génération présentent des objectifs de stabilité du fait de leur adossement à un actif sous-jacent, mais les risques BC/FT qui y sont liés demeurent similaires aux crypto-actifs de première génération comme le Bitcoin. Parmi ces risques, on peut notamment retrouver l'anonymat des transactions et la possibilité d'utilisation à des fins de blanchiment ou de financement d'activités illicites directement sur le deepweb ou le darkweb. Conformément aux observations du Financial Stability Board14), TRACFIN évoque la nécessaire création d'un cadre réglementaire international pour les émetteurs de stable coins. La cellule de renseignement TRACFIN s'est d'ailleurs dotée depuis quelques années d'une division d'enquêtes dédiée à la cybercriminalité financière et d'outils pour chercher directement sur les blockchains publiques, « *afin d'améliorer ses capacités d'investigation sur l'analyse de transactions en crypto-actifs* ».
Les obligations relatives à la lutte contre le blanchiment visent à empêcher les cryptoactifs issus d'activités illégales (darkweb, ransomware, etc.) d'être

échangés contre des fonds en monnaie fiat (euro ou dollars par exemple) pour être réinvestis dans l'économie légale.
Avec l'usage croissant de ces supports, les chargés de conformité ont de nouveaux challenges afin de bien appréhender les modalités de contrôles de ces actifs numériques pouvant être utilisés dans des opérations de blanchiment d'argent, mais aussi former les salariés encore peu familiers de ces supports.

En renforçant les obligations de conformité s'appliquant au secteur, les nouvelles recommandations du Groupe d'action financière devraient accélérer les investissements de la « finance traditionnelle » dans les cryptoactifs - en diminuant les incertitudes juridiques. Deux rapports du GAFI, publiés en 2020[6], analysent les risques d'utilisation des stablecoins et des virtual assets (VA)[7]. Ces supports qui facilitent l'anonymat, les transferts rapides de VA par le biais de différentes structures de comptes à travers le monde, favorisent en effet les opérations de blanchiment.

Les inquiétudes liées à la cybersécurité et au blanchiment d'argent sont ainsi de plus en plus d'actualité. L'urgence de la mise en œuvre d'une conformité robuste des actifs numériques s'impose, notamment en raison du glissement de la délinquance vers les innovations numériques[8] comme les cryptoactifs.

Parution le 21 janvier 2022

[1] L. n° 2019-486 du 22 mai 2019 relative à la croissance et la transformation des entreprises, dite « loi PACTE ».
[2] https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000042636234
[3] M. Quéméner, « La cybercriminalité financière, un enjeu majeur », Revue Lamy Droit de l'immatériel (RLDI) n° 167, 1er février 2020
[4] Tendances et analyse des risques de BC/FT en 2019-2020, TRACFIN
[5] Crypto-monnaie dont le cours est stable rassure beaucoup d'acteurs à commencer par les investisseurs institutionnels qui ont en majorité peur du risque de volatilité (surtout les fortes baisses),
[6] GAFI, 12-Month review of the revised FATF standards on virtual assets and virtual asset service providers, June 2020 ; GAFI, Report to the G20 Finance Ministers and Central Bank Governors, June 2020.
[7] V. le glossaire du GAFI, qui s'est vu complété des définitions des termes *virtual asset* (actif virtuel) et *virtual asset service provider (*prestataire de service d'actif virtuel).
[8] M. Quéméner, C. Wiezrre, F. Dalle, « Quels droits face aux innovations numériques » (Lextenso 2020)

Sécurisation du SI : la passion de l'échec

CEDRIC CARTAU
RSSI et DPO
CHU de NANTES et GHT44

Réussir un projet, c'est bien. Réussir un projet en tenant compte de la sécurité du SI, c'est très bien, tout comme réussir un projet strict de sécurité. Mais si l'on nous enseigne à longueur de séminaires (souvent animés par des jeunes et fringants consultants en costume serré et cravate impeccable) comment réussir un projet, jamais ô grand jamais on ne vous dit comment planter un projet. Et c'est une erreur, la méthode gagne à être connue.

Comment donc ? Planter un projet ? Mais qu'est-ce donc que ce sujet qui frise le niveau 7 sur l'échelle de la Richter-stupidité ? Votre serviteur a-t-il fumé ses tests PCR ? Ou prévu d'aller faire pousser des chèvres et du tabac qui fait rire dans le Larzac ? Rien de tout cela en fait.

Les motivations inavouables

La vie professionnelle étant ce qu'elle est, il ne faut jurer de rien, et en particulier ne pas croire que l'on aura toujours intérêt à voir réussir tous les projets. Sur la fin de carrière, poussés que nous serons tous par des jeunes diplômés à l'ambition aussi mordante que les bouts pointus de leurs chaussures (ou quelle que soit la mode vestimentaire à ce moment), il n'est pas inutile de connaître quelques rudiments destinés à planter en beauté le projet de Kevin, le jeune exalté qui vous pourrit vos réunions et votre moral. Il faut en revenir aux fondamentaux, là encore.
Le plus simple est de torpiller le paramètre délai : en suggérant un délai impossible à tenir, vous avez une bonne chance de passer des week-ends sereins (ce qui ne sera pas le cas pour Kevin). Malheureusement, d'une

part les délais ne sont presque jamais tenus, d'autre part il subsiste toujours le risque que Kevin réussisse malgré tout à tenir ses dates.
Il faut alors passer à la vitesse supérieure et lui sabrer ses budgets, le nerf de la guerre sans lequel rien ne se passe. Déjà que tous les projets informatiques ou presque dépassent les montants initiaux, si en plus de cela vous réussissez à lui retirer des ressources humaines (facile à dire, pas trop difficile à faire), vous mettez toutes les chances de votre côté.
En cas de poisse, suggérez que le périmètre initial ne comprend peut-être pas tout ce qu'il aurait fallu prendre en compte. Ce serait bien le drame si Kevin arrive à s'en sortir. Faire constamment varier le périmètre d'un projet est l'assurance presque parfaite qu'il n'aboutira jamais. Un jour on ajoute deux points qui nécessitent de tout reconcevoir, le lendemain on en retire un des deux, et ainsi de suite. Kevin vous haïra (pas grave), mais surtout son projet ne s'en remettra pas (une bonne nouvelle n'arrive jamais seule). Si enfin, comble de malchance, Kevin et son malheureux projet arrivent à survivre à cela, il reste l'arme ultime : torpiller la gouvernance. Changer la MOA, son directeur et son chef de projet, puis y revenir, puis inclure une autre direction dans le projet pour au final la retirer.
La méthode est garantie sans échec connu.

Les motivations carrément immorales

L'ennui est racine du mal et il faut bien occuper ses journées, surtout quand le RSSI croule sous les injonctions contradictoires (tout protéger, tout le temps et partout, sans aucune thune - bon en même temps cela n'arrive jamais, hein ?). Pourquoi ne pas, à votre tour, faire tourner la MOA en bourrique ? Dois-je vous rappeler que le directeur marketing est forcément payé une blinde, tout cela pour produire des flyers en couleur et des goodies qui font *coin coin*[1] : aucune raison de ne pas lui rendre la monnaie. Un bon truc est d'expliquer à vos MOA que « ben non les procédures dégradées ça ne sert à rien, c'est un truc dont les consultants nous bassinent rien que pour nous fourguer des journées homme », voire, s'ils en ont, leur suggérer que « les tester est inutile, on fait confiance ce sont des pro ». A titre personnel j'aime bien le « ne vous inquiétez pas, tous les bugs sont corrigés dans la prochaine version ». Ou encore « la disponibilité de notre informatique est au niveau des 5-9 » : au mieux ils pensent que c'est un code ésotérique uniquement connu des initiés de la

planète Zorglub, au pire ils comprendront que cela veut dire moins de 5 minutes d'arrêt par an et seront admiratifs, pour briller dans les dîners en ville c'est top moumoute.
J'ai remarqué également que l'utilisation du mot « automatique » provoquait un état de quasi transe CBD chez certains métiers : automatique, répétez après moi, au-to-ma-tique, en séparant bien les syllabes : le logiciel bascule sur le serveur de secours de manière au-to-ma-tique (cela ne marche jamais, mais ce n'est pas grave, l'important n'est pas le flacon mais l'ivresse), la clim est redondée de manière au-to-ma-tique, le provisionning des comptes est au-to-ma-tique, on respecte le RGPD de manière au-to-ma-tique. C'est magique, j'adoooore. Evidemment, le jour où le pet se produit, il faut utiliser les excuses classiques des DSI (20 ans d'expérience, j'ai testé) : oui mais ce cas d'usage n'était pas listé dans la matrice des risques pris en charge, oui mais on a un bug d'un sous-traitant qui n'a pas respecté la norme ISO 20 000, oui mais etc. etc. etc.
Je vous garantis que cela serait bien la poisse si, à la prochaine panne, tout ne partait pas en vrille : et vlan, et les salaires des RSSI qui prennent 10 %.

Les motivations tout à fait avouables - les seules valables en fait

Comme dit le célèbre proverbe Shadok et comme le rapportait souvent le Professeur Piéplu : « Ce n'est qu'en essayant continuellement que l'on finit par réussir. Autrement dit : plus ça rate, plus on a de chances que ça marche. »
Etudier les erreurs, c'est le meilleur moyen de ne pas tomber dedans. Pendant la seconde Guerre Mondiale, le commandement des forces aéronavales américaines dans le pacifique voulait savoir comment renforcer la sécurité des Corsair (les avions de chasse que l'on voit dans la série « Les têtes brulées ») en désossant ceux qui rentraient tant bien que mal de mission - les bestioles étaient solides au point de pouvoir continuer de voler avec plusieurs balles dans le moteur. L'idée était de renforcer les parties de la carlingue qui avaient des impacts de balle, mais un mathématicien (Abraham Wald) leur fit remarquer qu'il fallait faire exactement l'inverse. Peut-être que la raison pour laquelle certaines zones des avions n'étaient pas couvertes d'impacts de balle était que les avions qui avaient été abattus dans ces zones ne sont pas revenus. Cette idée a

conduit au renforcement du blindage sur les parties de l'avion où il n'y avait justement pas d'impacts de balle.
Depuis quelques années, cette discipline foisonne : depuis l'excellent « Les décisions absurdes » de Christian Morel (trois tomes en tout, un ultra-classique) on a vu arriver le non-moins excellent « Super Fail », podcast de France Inter animé par Guillaume Herner, « Les stratégies absurdes » de Maya Beauvallet, « Vous allez commettre une terrible erreur » d'Olivier Sibony (qui intervient d'ailleurs régulièrement sur la chaîne Xerfi Canal) et le désopilant « Les lois fondamentales de la stupidité humaine » de Carlo M Cipolla, sans parler bien entendu de l'inénarrable « Les grands Z'héros de l'histoire » de Clémentine Portier-Kaltenbach.
Etudier les erreurs est dans l'ADN de certains secteurs tel l'aéronautique, qui diligente une enquête systématique du BEA après chaque crash, même d'un avion de tourisme, qui oblige à signaler les incidents, qui diffuse les FEI (Fiches d'Evénement Indésirable) sur tout le territoire et où chaque pilote considère que son erreur, bien analysée et communiquée, peut servir à sauver des vies (voir à ce sujet la vidéo sur l'atterrissage raté d'un TB10 à Courchevel, qui est connue absolument de tous les pilotes de France et de Navarre). La SSI a clairement des progrès à faire et des enseignements à retirer des 70 ans de pratiques de l'aéronautique.

Conclusion

Au-delà de l'humour de ce début d'article, il faut bien reconnaître que la culture de l'échec - analyse, étude, REX, etc. - est quasi absente des SI et par transition de la sécurisation des SI, tout du moins si on la compare à celle susnommée du secteur aérien. Cette époque est en train de changer : les CERT, les observatoires sectoriels, les groupes d'experts nationaux ou locaux, les échanges dans les club ou les associations, les Think Tank tels le CyberCercle, tout cet écosystème participe selon sa mission à l'évolution des mentalités.
Il y a quelques jours, je participais à une réunion qui consistait à mettre en place un processus inter établissement pour cadrer l'homologation de projets SI sensibles : pendant 45 minutes il a été question de notes, de fiches de services, de réunions périodiques de bilan, etc. C'est bien, c'est nécessaire, mais ce n'est pas ce qui m'intéresse : moi je ne m'intéresse qu'aux projets qui justement allaient échapper à ce processus, soit par

manque de connaissance institutionnelle, soit par volonté de masquer (plus rare). Comment les identifier, les pister, les ramener dans le troupeau. Faites ce simple test : demandez à votre DSI si le parc de PC est protégé par un antivirus : il va vous montrer la console centralisée de supervision de l'AV. Demandez-lui ensuite s'il a mesuré les PC qui, justement, n'avaient pas d'AV et donc n'étaient pas listés dans la console. Gros blanc. Je ne m'intéresse qu'à l'erreur, l'échec, la liste des trains qui arrivent en retard.
On n'apprend que de l'échec.

Parution le 28 janvier 2021

Bibliographie

« Les décisions absurdes », Christian Morel, trois tomes
« Un brève histoire du futur », Michio Kaku
« La mort de la mort », Dr Laurent Alexandre
« Le Big Data, penser l'homme et le monde autrement », Gilles Babinet
« Culturama », Aiden Erez
« La sécurité du système d'information des établissements de santé », Cédric Cartau

[1] Humour du 18ème degré, on précise tout de même…

Labels de sécurité et confiance numériques : clés de compréhension et perspectives

STEPHANE MEYNET
Président
CERTitude NUMERIQUE

Dans notre société de consommateurs souvent peu avertis mais toujours pressés, les labels occupent une place de premier ordre. Marque, voire garantie ou assurance de qualité, de sérieux et de confiance, les labels représentent pour un fournisseur un différenciant vis-à-vis de ses concurrents et pour le consommateur un critère de choix.
Tout ou presque tout devient aujourd'hui « labellisable », si bien que le but initial recherché par les labels tend à s'effacer devant la complexité produite par la multitude de labels et leur hétérogénéité. Trop de labels tuent les labels. Ce célèbre adage s'applique là encore à merveille !
Pour que les labels leur soient utiles, les consommateurs doivent en comprendre a minima les rouages et ce qu'ils recouvrent. S'assurer que les labels qu'ils retiennent comme critère de sélection, lorsqu'ils ne sont pas imposés réglementairement, répondent bien à leurs attentes. Sans cela, quelle est l'utilité des labels si ce n'est de s'entendre prononcer la très célèbre remarque : « c'est labellisé donc c'est bien ».
Le domaine de la sécurité et de la confiance numériques n'échappe pas à ce constat. Nous voilà rassurés !

Mais que signifie exactement labelliser et qu'est-ce qu'un label ?

Le Larousse propose une définition éclairée du verbe labelliser et du nom label.
Labelliser : attribuer un label.

Label : nom masculin (anglais label, étiquette, de l'ancien français label, ruban, du francique labba). Étiquette ou marque spéciale créée par un syndicat professionnel et apposée sur un produit destiné à la vente, pour en certifier l'origine, en garantir la qualité et la conformité avec les normes de fabrication.

Tout est dit dans cette définition ou presque. Les termes de « syndicat professionnel » pourraient être remplacés par « organisation », « produit » complété par « services ou personnes » et « normes de fabrication » résumé à « normes ».

Quid des labels de sécurité de confiance numérique ?

Ainsi nos labels de sécurité et de confiance numériques entrent parfaitement dans la définition qui recoupe d'ailleurs celle proposée par le COFRAC[1].

En effet, de manière générale, les labels et en particulier les labels de sécurité et de confiance numériques s'appliquent à des organisations, des produits, à des services et prestataires de services et sont délivrés par des associations ou des organismes publics.
En France, l'ANSSI et cybermalveillance.gouv.fr, deux organismes publics, portent des labels de sécurité numérique : les « Visa de sécurité »[2] pour l'ANSSI et plus récemment, le label « ExpertCyber »[3] pour cybermalveillance.gouv.fr.
Le succès des visas de sécurité est indéniable au regard du nombre de visas attribués depuis plus de dix ans maintenant et cela pour une large gamme de produits et de prestataires. Pour s'en convaincre, il suffit de consulter sur le site de l'ANSSI le catalogue des visas de sécurité attribués à des produits couvrant un spectre allant de la carte à puce aux automates programmables industriels et développés par des entreprises aussi diverses que Thales, Atos, Stormshield, Huawei, Schneider Electric, Sogeti, Siemens, Idemia, pour n'en citer que quelques-unes. La liste des visas de sécurité attribués aux prestataires de service impressionne également par son ampleur.
Quant au label « ExpertCyber », créé en 2020, son déploiement est en cours et rencontre un véritable intérêt.

Une des premières leçons que nous enseignent les labels est qu'il est nécessaire de laisser du temps pour qu'ils deviennent pleinement opérationnels et utiles. Donnons donc rendez-vous à cybermalveillance.gouv.fr dans quelques années pour mesurer le succès de son label. « Rome ne s'est pas faite en un jour »...

Une deuxième leçon porte sur la lisibilité et la compréhension des labels par le marché, et en particulier par les utilisateurs. Cette problématique récurrente préoccupe bon nombre d'acteurs. Non averti ou non familier des labels, un utilisateur peut rapidement se sentir démuni et perdu devant les labels existants. Pire encore, il peut être amené à choisir un produit ou un prestataire simplement parce que celui-ci affiche un label sans s'assurer que le label correspond bien à son besoin et à ses conditions d'usage.
J'ai en tête plusieurs exemples d'utilisateurs - pour des raisons évidentes de confidentialité leurs noms ne seront pas cités - qui indiquaient fièrement avoir fait l'acquisition d'un produit labellisé mais dont les conditions d'emploi ne correspondaient absolument pas à leur environnement. Résultat : un faux sentiment de sécurité et un mauvais investissement… qu'il faudra justifier auprès de la hiérarchie.

L'étude des visas de sécurité par exemple indique que cette appellation, séduisante et simple à comprendre pour le quidam par la similitude avec les visas tamponnés sur des passeports pour voyager, regroupe en fait deux ensembles : certification et qualification.

Peu d'utilisateurs connaissent la distinction, pourtant essentielle, entre ces deux termes. De même, rares sont les utilisateurs qui vérifient le périmètre sur lequel porte le visa de sécurité et quelles sont les conditions ou restrictions d'usages qui y sont associées. Encore plus rares sont ceux qui étudient la cible de sécurité ou le référentiel d'exigences, c'est à dire, pour reprendre la définition du Larousse, la norme que le produit ou le service labellisé doit respecter.

Du point de vue des offreurs de solutions, les labels apportent certes un différenciant commercial, mais nécessitent un investissement en temps et argent non négligeable pour leur obtention, pouvant parfois même en décourager de s'engager dans la voie de la labellisation. En effet, si certains

labels reposent sur une démarche déclarative, peu coûteuse, d'autres en revanche, reposent sur une évaluation de conformité effectuée par un tiers qu'il faudra bien évidemment rémunérer. Cette évaluation, de quelques milliers d'euros à plusieurs dizaines de milliers d'euros, s'étend bien souvent sur une période de plusieurs mois et nécessite un investissement en ressources humaines non négligeable. Ces contraintes doivent donc être mises en balance au regard du marché des produits et services de sécurité et de confiance numériques, fortement concurrentiel et en pleine consolidation. Les coûts et délais « administratifs » nécessaires à l'obtention des labels doivent impérativement être cohérents avec les exigences du marché et le « time to market ».

L'intérêt indiscutable des labels ne doit ainsi pas conduire à des discriminations et distorsion de concurrence, comme cela est malheureusement parfois le cas.

Revenons aux fondamentaux des labels et à leurs caractéristiques.

Pour résumer, certes de manière simplifiée, un label se construit sur 3 piliers :
- un périmètre : un produit, un système, un service, un prestataire
- un référentiel : une norme , un standard, une cible de sécurité, etc.
- un schéma : un organisme (une association, une entité publique ou privée) qui porte le label, en définit les caractéristiques et notamment le mode d'attribution.

Un label peut ainsi être porté par une entité à vocation commerciale ou non, se limiter à une (auto)déclaration de conformité à un référentiel ou recourir à une évaluation rigoureuse par un tiers, être reconnu au niveau national, européen ou international, porter sur un périmètre extrêmement variable et s'appuyer sur une multitude de référentiels.

Les labels, inventés pour apporter une marque de différenciation à la fois pour les fabricants et des critères de choix simplifiés pour les utilisateurs semblent, devant ce champ des possibles, s'être égarés de leur objectif et n'apportent plus aussi efficacement les réponses attendues. Une étude plus approfondie confirmerait certainement ce constat.

S'il faut travailler sur le temps pour qu'un label s'impose, s'il faut des labels lisibles et compréhensibles par l'ensemble des acteurs, s'il faut être vigilant aux coûts et délais administratifs, il semble également fondamental de définir sur le plan stratégique à quoi doivent servir les labels de sécurité et de confiance numériques avant de les construire. Sont-ils un outil au service de l'économie pour soutenir la « filière », pour soutenir les organismes de labellisation ? Sont-ils un outil au service de la souveraineté nationale ? Sont-ils un outil pour la sécurité dans le cyberespace ? Sont-ils un outil pour renforcer la sécurité des installations numériques des institutions et des entreprises ? Sont-ils un outil d'information au service des utilisateurs ? Sont-ils tout cela en même temps ? Etc.

Si pour certains Etats les labels relèvent clairement de la politique industrielle ou de l'influence stratégique, pour la France ils semblent d'avantage relever des intérêts fondamentaux de renforcer la sécurité des systèmes numériques, des institutions, des OIV, des OSE et progressivement de tous. Cette question de l'objectif stratégique des labels pourrait néanmoins se reposer dans le cadre de la stratégie nationale pour la sécurité numérique du prochain quinquennat.

Quid des travaux réglementaires ?

L'Europe, au travers de l'ENISA, travaille sur la questions des certifications de sécurité (des labels) au niveau européen[4]. Un objectif ambitieux et ô combien nécessaire, notamment sur le plan de la politique industrielle afin d'harmoniser les labels des différents Etats membres.

En France, le Sénat porte la proposition de loi n° 629 (2019-2020) pour la mise en place d'une certification de cybersécurité des plateformes numériques destinée au grand public[5] en proposant notamment un cyberscore. Sur le modèle des nutriscores, le cyberscore informerait les utilisateurs sur le niveau de sécurité des produits et de l'usage qui sera fait de leurs données. Un tel label, potentiellement applicable à tous produits numériques, éclairerait le consommateur lors de ses achats et obligerait implicitement les fabricants à traiter la question de la sécurité et de la confiance numériques.

Vers un label de sécurité et de confiance numériques unique ?

L'idée d'un label unique n'est certes pas nouvelle. Un label, potentiellement décliné en trois niveaux (or, argent, bronze par exemple) suivant le mode d'attribution ou le niveau d'exigences à remplir, simplifierait les process et améliorerait la lisibilité pour toutes les parties prenantes.

Mais le label ne représente-t-il pas finalement que le sommet de l'iceberg ? Le travail de fond à mener sur lequel nous devrions concentrer nos efforts ne serait-il pas dans la définition des normes, standards et référentiels utilisés pour les labels et leur déploiement sur le plan international ? La France produit une multitude de normes, standards, référentiels et réglementations mais dont le périmètre n'est le plus souvent que national. Or cette bataille se joue au niveau mondial, a minima au niveau européen : il est clair que la France reste malheureusement bien souvent en retrait des influenceurs en la matière.

L'ISO, organisme international, constitue une référence en matière de normalisation. La série de normes ISO270XX et plus particulièrement l'ISO27001[6], dédiée au management de la sécurité des systèmes d'information, tend à s'imposer. Elle offre en outre la possibilité à des organisations d'être certifiées et de compléter ainsi leur tableau de chasse des labels dont un des plus célèbre et fréquemment rencontré est sans aucun doute l'ISO9001 dans le domaine de la qualité. Si la certification ISO27001 relève le plus souvent d'une démarche volontaire, plusieurs textes réglementaires français la citent comme exemple, voire l'imposent comme un préalable dans le domaine de la santé pour la certification des hébergeurs de données de santé.
Il est fort à parier que les assureurs exigeront demain que les entreprises soient conformes à cette référence internationale qu'est l'ISO 27001 pour les assurer contre les risques cyber.

En conclusion, le sujet des labels de sécurité et de confiance numériques mériterait un rapport d'information voire une thèse, au regard de ses multiples facettes et de l'étendue de son champ d'application.

Les labels représentent aujourd'hui à eux seuls un marché en pleine croissance. Néanmoins, s'il est certain que des travaux de simplification seraient nécessaires pour garantir un minimum de lisibilité et donc d'efficacité des labels, la question que nous devrions nous poser est bien l'objectif recherché.
En attendant une hypothétique réponse à cette question sensible, ne devrions-nous pas retrouver le chemin de la simplicité et de l'efficacité en nous concentrant sur la définition d'un socle « universel » d'exigences de sécurité et de confiance applicable à tous systèmes numériques et leurs données, de même pour les prestataires, ce que l'on retrouve finalement dans la quasi-totalité des standards, référentiels, normes et réglementation ?

Parution le 4 février 2022

[1] https://www.cofrac.fr/quest-ce-que-laccreditation/certification-et-accreditation-quelles-differences/
[2] https://www.ssi.gouv.fr/administration/visa-de-securite/
[3] https://www.cybermalveillance.gouv.fr/tous-nos-contenus/a-propos/label-expertcyber
[4] https://cybercercle.com/matinale-cybercercle-certification-europeenne-cybersecurite/
[5] Rapport de Mme Anne-Catherine LOISIER sur la proposition de loi n° 629 (2019-2020) pour la mise en place d'une certification de cybersécurité des plateformes numériques destinée au grand public présentée par le sénateur Laurent Lafon et enregistrée à la Présidence du Sénat le 15 juillet 2020.
https://www.senat.fr/dossier-legislatif/ppl19-629.html
[6] https://www.iso.org/isoiec-27001-information-security.html

Le chiffrement homomorphe pour un Cloud sécurisé

GERARD PELIKS
Administrateur
ARCSI

Le chiffrement homomorphe permet de travailler sur des données chiffrées sans avoir à les déchiffrer. Comment cette technologie s'applique- t-elle à la sécurité du Cloud ? Quel est son état de l'art ?

Le cloud public est une solution merveilleuse pour stocker les données. Pour un coût de services maitrisé, les entreprises ont la possibilité de disposer de tout l'espace qui leur est nécessaire, sans avoir à investir sur des serveurs et des disques supplémentaires, quand un besoin de plus d'espace de stockage apparait.

Comme la sécurité n'est pas, dans la plupart des cas, le métier des entreprises utilisatrices des services du Cloud, celles-ci peuvent s'assurer, par contrat, que leurs données sont bien en sécurité dans le cloud de leur prestataire. Voilà pour la disponibilité des données et leur protection périmétrique. Quand les entreprises ne maîtrisent pas la sécurité et la sûreté de leurs données numériques, celles-ci font face à de multiples menaces et rares sont les entreprises en mesure de les contrer efficacement. Les prestataires de cloud sont par contre censés bien maîtriser la cybersécurité et censés avoir les compétences dans ce domaine.

Mais qu'en est-il de la confidentialité et de l'intégrité des données confiées dans un cloud extérieur ?

Rappelons que la confidentialité d'une information est l'assurance qu'elle

ne pourra être lue que par des personnes autorisées à en prendre connaissance, alors que l'intégrité est l'assurance qu'elle ne peut être écrite ou modifiée que par les personnes également autorisées à le faire.

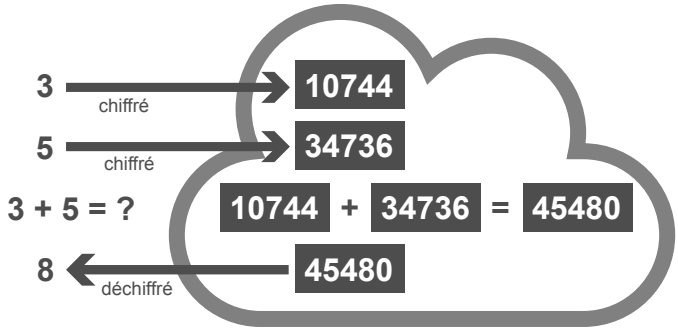
Une solution serait de n'utiliser l'espace d'un cloud public que pour héberger les données non sensibles. Mais alors on se prive de l'avantage de l'espace quasi infini que propose le cloud pour les héberger. Chiffrer les données sensibles et les confier dans un cloud public est aussi une solution, mais qui gère les clés ? L'idéal est bien sûr, pour les entreprises qui confient leurs données dans un Cloud public, de gérer elles-mêmes les clés de chiffrement. Confier la gestion des clés de chiffrement à son prestataire de cloud trouve ses limites dans la confiance que les entreprises clientes accordent à leur prestataire. Gérer les clés de chiffrement en interne dans l'entreprise est une tâche complexe pour qui la sécurité des données numériques n'est pas le métier. Confier la gestion des clés à un autre prestataire différent de celui qui héberge les données chiffrées semble être une meilleure solution. La confidentialité et l'intégrité des données sensibles sont ainsi assurées.

Si les données sont stockées en clair chez le prestataire, alors le client peut en disposer pour effectuer des traitements mais elles sont accessibles à toute personne mal intentionnée disposant d'un accès privilégié chez le prestataire. Si les données sont stockées chiffrées, il est alors difficile d'en disposer pour effectuer des traitements.

Le problème qui se pose est donc : « comment effectuer des traitements sur les données chiffrées ? ». Il est bien évident que, par exemple pour une addition entre deux nombres qui sont chiffrés, la somme des deux nombres chiffrés ne donne pas, lors du déchiffrement, le résultat attendu. Il est bien sûr possible de rapatrier en interne les données à traiter, les déchiffrer pour effectuer les traitements, chiffrer les résultats et les remettre éventuellement dans le Cloud. Cette solution n'est, de toute évidence, pas vraiment jouable.

Alors le Cloud est-il condamné à ne rester qu'un espace de stockage, sans permettre un espace de calcul ? Les données à manipuler ne pourraient-elles pas rester dans le Cloud, chiffrées, et les traitements

s'effectuer sur les données chiffrées en donnant le bon résultat lors du déchiffrement chez l'utilisateur ?
Il existe une solution très élégante déjà opérationnelle pour certains traitements, et qui avance dans les centres de recherche pour prendre en compte tous les traitements possibles, c'est le chiffrement homomorphe.



Avec ce type de chiffrement, le Cloud n'est plus seulement un espace de stockage sécurisé mais devient également un espace de calcul et de consultation sécurisé. Il va vraiment servir, non seulement à héberger l'information sensible, mais aussi à l'utiliser … sans la sortir du Cloud. Seuls les résultats après traitements seront sortis pour être déchiffrés et exploités.

Dans le schéma ci-dessus, on veut obtenir le résultat de l'addition de deux nombres confiés chiffrés au Cloud, « 3 » et « 5 ». Mettons que le résultat homomorphe chiffré de 3 est « 10744 » et que le résultat homomorphe chiffré de 5 est « 34736 ».

Dans le Cloud s'opère l'addition homomorphe 10744 + 34736, qui donne 45480. Le déchiffrement homomorphe de 45480 donne … « 8 », ce qui est le résultat attendu.

Ainsi le Cloud serait devenu non seulement un espace de stockage mais aussi un espace de calculs et de traitements ?

C'est du moins ce qu'on souhaiterait en attendre, mais aujourd'hui le chiffrement homomorphe ne fonctionne que pour certaines opérations. Il ne permet pas, par exemple, de consulter une base de données chiffrée pour obtenir le résultat souhaité en clair. Si un chiffrement dit « pleinement homomorphe » existait dès aujourd'hui, si tout traitement pouvait être réalisé sur les données chiffrées confiées dans un Cloud public, leur confidentialité et leur intégrité seraient garanties. Mais on en est pas encore là, et les opérations qui peuvent déjà fonctionner posent quelques problèmes de performance, mais les recherches vont bon train pour offrir cette faculté inestimable.

Remarquons, sans verser trop dans la technique, et en simplifiant, que l'algorithme de chiffrement utilisé par le RSA, qui est à la base du chiffrement à clé publique, est, par nature, homomorphe pour la multiplication. En effet, le produit de deux nombres chiffrés est égal au chiffré du produit des deux nombres. Ce résultat, une fois déchiffré, est le même que si on fait la multiplication des deux nombres en clair. Un chiffrement homomorphe qui fonctionnerait pour l'addition ET pour la multiplication est appelé « chiffrement doublement homomorphe ». On s'en approche aujourd'hui, mais avec des problèmes de largeur des éléments chiffrés et de bruits numériques engendrés par les traitements. La difficulté du chiffrement homomorphe est de maintenir le « bruit numérique », que les opérations engendrent, au-dessous d'un seuil raisonnable sinon les algorithmes divergent et tout devient indéchiffrable. Nous n'étudierons pas ces problèmes complexes ici, mais nous pouvons espérer que les mathématiciens trouveront une solution élégante aux problèmes posés par le chiffrement doublement homomorphe.

Le chiffrement « cherchable »

Le chiffrement homomorphe ne doit pas être confondu avec le chiffrement cherchable qui permet de spécifier une procédure de déchiffrement à un résultat de calcul dans le domaine chiffré. Ce dernier

type de chiffrement offre une solution pour consulter une base de données chiffrée, obtenir un résultat qui, déchiffré, donne le résultat attendu.

Application pratique : Le vote par Internet

Comme application pratique, voyons comment le chiffrement homomorphe fournit une solution au vote par Internet. Nous ne parlons pas ici des machines de vote électronique, mais de l'électeur qui vote à partir de son navigateur.

Avec l'utilisation des algorithmes de El Gamal, le produit homomorphe des bulletins de votes chiffrés est égal à la somme homomorphe chiffrée des bulletins de votes. Les choix des votants ne sont jamais déchiffrés. A la clôture du scrutin, on effectue une multiplication homomorphique de tous les bulletins de votes. On obtient la somme chiffrée et on la déchiffre. Cette somme est donc le résultat des votes qui est obtenu immédiatement. Oui, le chiffrement homomorphe de El Gamal (entre autres cryptologues qui ont fait avancer cette technologie) permet cela.

Les bulletins sont chiffrés par la clé publique de l'urne, le déchiffrement de la somme des bulletins se fait par la clé privée de l'urne. Cette clé privée peut être répartie en plusieurs morceaux détenus par le président du bureau de vote et ses assesseurs. A l'ouverture du scrutin, le président et ses assesseurs reconstituent la clé de déchiffrement et obtiennent quasi immédiatement le résultat attendu.

Que le produit homomorphe des bulletins de votes chiffrés soit égal à la somme homomorphe chiffrée des bulletins de votes est une belle application de ce type de chiffrement.

Pour ceux qui aiment les formules mathématiques, si Ek(mn) est le bulletin de vote mn chiffré avec la clé publique k de l'urne :
Ek(m1) x Ek(m2) x … x Ek(mn) = Ek(m1 + m2 + … + mn)

Cette méthode est élégante dans sa simplicité d'utilisation. Les bulletins dans l'urne ne sont jamais déchiffrés pourtant on connaît le résultat de la somme des votes qui est d'ailleurs le seul renseignement qui est intéressant

et non confidentiel après la fermeture du scrutin.

Cette méthode a déjà été utilisée pour les élections des représentants des Français résidant à l'étranger. Elle peut être utilisée aussi pour les élections des représentants du personnel ou dans les conseils d'administration des entreprises. Mais pour les élections présidentielles, sénatoriales ou législatives, elle n'est pas autorisée en France. Nous ne parlons ici que du fondement cryptologique d'une application pratique d'un chiffrement homomorphe qui fonctionne. Le vote par Internet qui ne donne pas l'obligation de passer par un isoloir, et qui ne nécessite pas la cérémonie républicaine du dépouillement des votes, est-il à recommander ? C'est un débat intéressant, mais dans lequel nous ne prendrons pas parti ici.

Parution le 11 février 2022

Sensibilisation à la sécurité numérique : l'enfant, le smartphone et l'exemple

LAURANE RAIMONDO
Fondatrice LR Conseils & Stratégies
Chercheure associée au CLESID

Avez-vous déjà posé la question à un enfant - qui n'est pas le vôtre - sur ce que signifie pour lui la « sécurité numérique » ? Certains vous diront que c'est de faire attention à ne pas se faire voler son smartphone ; d'autres que c'est d'éviter que les parents puissent lire leurs conversations. Parfois certains parleront de cyberharcèlement, le sujet est d'ailleurs au cœur des « préoccupations numériques » des établissements scolaires. Dans 80% des cas, lorsque le responsable d'une école sollicite une intervention c'est que des événements malheureux se sont déroulés en son sein. Aussi grave soit-il, le cyberharcèlement n'est que l'arbre cachant la forêt. Il focalise l'attention, écartant la question fondamentale de l'exemple que nous donnons aux jeunes dans notre rapport aux outils numériques.

Les dangers et conséquences

Nés avec une puce de silicium dans la main mais sans le manuel de sécurité, ils ont entre onze et quinze ans et représentent en 2022 la part de la population la plus exposée aux risques et menaces issus du cyberespace ou induits par son utilisation. Qu'il s'agisse du cyberharcèlement, de la cyberprédation, du revenge porn, des arnaques en tout genre mais aussi des troubles du sommeil, de l'attention, de la fertilité jusqu'aux collectes de données abusives aux répercussions mesurées en décennies, qui se charge de le leur dire ? Ils ont entre onze et quinze ans et sont en danger. Ignorant tout des conséquences de leur usage des outils numériques, parents et enseignants n'en savent guère davantage. Il

y a effectivement une différence entre « être habile » sur ces supports et « être habile » en sachant se protéger, soi et les autres.

L'exposition involontaire est là, l'apprentissage via les outils numériques aussi : films d'animation en anglais, jeux de logique, etc. L'autonomie peut être encouragée tant que l'outil n'est pas connecté à un réseau. Ecrire des histoires sur un traitement de texte n'a pas les mêmes effets que les donner en pâture aux trolls du Web sur un blog. A bidouiller l'outil, l'enfant en découvre seul les fonctionnalités et devient un petit hacker qui cherchera à contourner les restrictions parentales ou à modifier et améliorer certaines d'entre elles. Les vraies problématiques se posent lorsque l'outil est connecté, car la sécurité numérique n'est pas qu'une affaire personnelle que l'on peut rapporter à « je n'ai rien à cacher ». C'est l'affaire de tous. Que l'on décide de s'exposer volontairement pourrait passer pour un choix personnel, si l'opacité des algorithmes des réseaux sociaux et les multiples « autorisations d'accès » données sur un terminal n'en faisaient un choix qui est tout sauf personnel. Accorder à une application l'accès aux contacts n'est pas anodin. Monsieur ou Madame « je n'ai rien à cacher » ont-ils demandé l'autorisation desdits contacts pour donner leur numéro et les informations qui y sont associées, à l'entreprise propriétaire de l'appli ? La décision est donc finalement collective. Décision ou soumission, puisque, même avec toute la volonté du monde, il n'est pas possible d'y échapper - une seule personne parlant de vous en ligne suffit à vous créer une e-réputation.

Aussi opaque qu'il est transparent, le cyberespace semble complexe à appréhender. Une règle est pourtant limpide : rien ne disparaît jamais d'Internet. Cette « loi de l'Internet » ramène ainsi à une question binaire : acceptez-vous ou non que ce que vous enregistrez, commentez et diffusez depuis vos outils numériques puisse être collecté et analysé, avec en outre une probabilité plus ou moins importante que ce soit utilisé non dans votre intérêt mais dans celui des entreprises auxquelles vous avez autorisé l'accès. Si des adultes rencontrent déjà des difficultés avec cette approche, nous n'avons pas le droit de priver les enfants de cette réflexion et de sous-estimer leur capacité à y apporter une réponse.

Un âge pour chaque usage

« Tous concernés » pourrait être le slogan d'un groupe manifestant contre la fermeture de la dernière épicerie du village. Il convient tout aussi bien à la question de la sensibilisation à la sécurité numérique des enfants dès le plus jeune âge. Avant trois ans, la question des écrans n'est pas à poser : elle est proscrite. Leur développement est en jeu : un bébé joue aussi bien avec un cube coloré qu'avec un smartphone, les conséquences, elles, ne sont pas les mêmes. A Taïwan les parents exposant leurs enfants de plus de deux ans au-delà de 30 minutes par jour aux outils numériques se voient redevables d'une amende de 1400€. Une loi qui fait rêver lorsque l'on entraperçoit la moitié des répercussions d'un usage abusif sur les plus jeunes.

Au-delà, difficile de les tenir éloignés. Après tout, le numérique est magique, lorsqu'il est utilisé à bon escient et surtout qu'il ne nous prive pas de nos capacités initiales. Or une situation terrifiante qui devrait susciter un scandale national se déroule sous nos yeux : une large majorité des bacheliers n'est pas capable d'écrire une phrase sans de multiples fautes d'orthographe. Entre la stigmatisation des élèves atteints de troubles de type dyslexie et le corps professoral presque sommé de ne plus pénaliser les jeunes bourreaux de la langue française il y a un pont aussi grand que la distance entre Lyon et Washington. Les raisons sont nombreuses. L'une d'elles n'est pas étrangère au goût de la facilité et de l'immédiateté induites par les outils numériques. Quelle levée de boucliers lorsque, enseignant l'histoire du numérique à des jeunes en première année dans le Supérieur, j'ai interdit en cours l'usage de l'ordinateur et la présence du smartphone sur la table ! Le résultat a été une incapacité quasi-totale pour les étudiants à noter les concepts-clefs du cours ; une absence d'autonomie dans la recherche personnelle devant le compléter ; une confiance aveugle aux éléments « trouvés sur Internet » sans la moindre preuve de la fiabilité de la source et un choc réel lorsque j'ai suggéré de mettre un pied dans une bibliothèque. Dès le départ, le numérique ne doit pas se substituer aux supports physiques mais venir en complément. Apprendre à chercher une information fiable commence entre les pages de différents ouvrages : ce n'est pas parce que l'on peut le « palper » que c'est « passé ». Aux premières interrogations de l'enfant c'est un livre qui doit lui être mis entre les mains.

Plus tard, l'apprentissage complémentaire des outils numériques peut venir compléter les capacités acquises. Un texte en anglais à traduire doit nécessiter l'usage d'un dictionnaire soutenu ponctuellement par un site, tel que wordreference.com par exemple.

Il est ainsi essentiel de garder à l'esprit et de transmettre l'idée que les outils numériques doivent rester… des outils. Adultes, nous constatons parfois notre affaiblissement intellectuel en nous surprenant à utiliser la calculatrice du smartphone au lieu de faire un calcul mental ou à utiliser l'assistant vocal pour rédiger un message et l'envoyer à une personne située de l'autre côté du couloir. Lorsque les plus jeunes utilisent ces outils sans avoir eu le temps d'apprendre comment faire autrement, ce n'est plus du progrès mais un abrutissement civilisationnel. De fait, les réflexes primaires comme se protéger finissent par nous échapper. Prenons l'exemple des hérissons. Nos routes sont un mouroir pour eux. Une espèce si ancienne qu'ils n'ont pas eu le temps de s'adapter et de craindre les véhicules ou tout du moins de fuir le bitume. L'humain n'a pas eu ou pris le temps de s'adapter aux nouvelles technologies, s'en tenant au principe de la récompense immédiate. L'enfant imitant l'adulte, il n'adoptera pas un comportement de recul et de réflexion propre à l'utilisation de ces outils : il imitera l'adulte, scotché à son smartphone qui ne le quitte plus. Ainsi la démarche de sensibilisation incombe à l'adulte, ne serait-ce que dans un souci de transmission. L'urgence est ici un euphémisme, un jeune recevant son premier outil numérique personnel de plus en plus tôt.

La responsabilité de l'apprentissage

Sensibiliser c'est protéger. Protéger est une obligation inscrite dans le Code de l'action sociale et des familles, plus précisément son article L.112-3 : « La protection de l'enfance vise à garantir la prise en compte des besoins fondamentaux de l'enfant, à soutenir son développement physique, affectif, intellectuel et social et à préserver sa santé, sa sécurité, sa moralité et son éducation, dans le respect de ses droits. » La question des usages numériques des enfants devrait s'interpréter à travers cet article. Parents, enseignants ou membre de l'entourage d'un jeune a donc un rôle clair à jouer sur ce sujet. Néanmoins, lorsque c'est à marche forcée qu'une société se numérise, la responsabilité de l'apprentissage de la sécurité numérique

revient-elle principalement aux parents ? Bien souvent ils sont les premiers désemparés et ignorants de la dangerosité des outils confiés à leurs enfants.

S'impose l'idée que la sécurité numérique doit être enseignée à l'école, là où en « cours de techno » la manipulation des ordinateurs est déjà effective. Des enseignants déjà surchargés, aux faibles moyens et à l'autorité sans cesse discutée s'élèveront contre. Fort heureusement, le pas est immense avec un exemple à donner, un peu de temps consacré et surtout, de la bonne volonté issue des deux côtés, parents et enseignants. Chaque utilisation des outils numériques devrait être enrichie par un échange : as-tu bien activé le VPN (après explication simple de son utilité) ? Regarde si l'antivirus est à jour ; quel moteur de recherche as-tu choisi pour trouver le site ? Les cookies, tu sais ce que c'est ? As-tu bien nettoyé tes données de navigation après ta recherche ? L'enfant, avide de connaissances, posera beaucoup de questions auxquelles des réponses accessibles seront nécessaires. Ainsi, les débuts de la sensibilisation, avec parents et enseignants, se fait à travers un accompagnement dans les usages, au quotidien et non ponctuellement.

Un amendement avait été présenté en 2019 dans le cadre du projet de loi sur l'Ecole de la Confiance, par les députés Sereine MAUBORGNE, Gwendal ROUILLARD, Bertrand SORRE et Stéphane TESTE pour insérer à l'école dès le primaire, une formation dédiée à la sensibilisation, à la prévention et à la gestion des risques liés aux usages numériques (amendement n°877 déposé le 7 février 2019), partant du constat que les enfants naviguent sur Internet, fréquentent les réseaux sociaux et utilisent quotidiennement un smartphone. Il est quelque peu « dommage » qu'il n'ait pas été adopté.

Plus grand, le jeune veut être seul et libre sur l'outil. La question du contrôle parental doit ainsi se poser dès le départ. En ce sens, la loi Studer est extrêmement bienvenue. Rendant obligatoire la pré-installation d'un dispositif de contrôle parental sur les appareils connectés et vendus en France, celui-ci sera gratuit et proposé dès la première utilisation. La responsabilité ici se situe au niveau de la personne qui offre au jeune un outil numérique de type smartphone, souvent pour une question de « sécurité », à l'heure où l'enfant entre au collège par exemple. Il ne se

doute pas qu'au contraire il l'expose ouvertement aux affres du cyberespace. Le jeune lui, voit dans l'outil une façon d'être intégré au groupe et une manière de s'émanciper de la coupe parentale. Dans le contrôle il verra probablement une contrainte lourde, voire un manque de confiance. L'échange sera ici primordial : ce n'est pas au parent de ne pas avoir confiance en l'adolescent mais à celui-ci d'avoir confiance en l'adulte et en sa décision.

La sensibilisation à la sécurité numérique est donc bel et bien l'affaire de tous et dès le plus jeune âge. Elle commence avant même que le jeune ne dispose de son propre outil. Cette acquisition ne devrait pas s'entendre comme la récompense d'un bon bulletin scolaire au risque d'engendrer une relation aussi problématique que celle naissant entre un jeune et le sucre lorsqu'il est « privé de dessert », plaçant l'aliment dans une position qu'il n'a pas à avoir. Les outils numériques doivent rester des outils, être traités pour ce qu'ils sont et avec recul si ce n'est de la méfiance, utilisés avec les règles d'hygiène numérique de base. L'autonomie doit rester le maître mot. N'est-ce pas le premier objectif d'un parent, rendre son enfant autonome, responsable de ses actes et de ses décisions ? Ceci par l'exemple qu'il donne : si l'usage d'un smartphone ou d'un ordinateur n'est pas inné, l'apprentissage par imitation, si.

Parution le 18 Février 2022

Le défi de la sensibilisation des jeunes aux dangers du numérique Constats et propositions

DIANE RAMBALDINI
Présidente cofondatrice
ISSA France

Les élections présidentielles approchant, l'ISSA France travaille à l'écriture d'un rapport pour y formuler, à l'attention des candidats, des propositions concernant le défi de la sensibilisation des jeunes aux dangers du numérique.

En exclusivité pour Parole d'expert, nous en dévoilons quelques idées clés.

Rappelons que l'ISSA France est une association dont la vocation première est d'informer, d'éduquer et d'expliquer le monde numérique afin de sensibiliser différents publics aux dangers mais aussi aux opportunités qu"il représente. L'association se consacre aux publics les plus vulnérables, les enfants, les adolescents et les jeunes adultes.

Distorsion générationnelle

Si parler du défi de la sensibilisation des jeunes aux dangers du numérique semble un sujet ciblé et circonscrit, nos travaux à l'ISSA France ces dernières années et plus particulièrement les trois ans passés, nous ont amenés à faire plusieurs constats, qui nous laissent penser que ce qui se passe dans « le cyber » est peut-être l'arbre qui cache la forêt.

Très tôt, que ce soit à travers nos interventions en établissements scolaires, nos ateliers de parentalité numérique en entreprises, et à nouveau de

manière frappante à l'occasion des interviews et suivis de plusieurs jeunes, nécessaires à la conception de notre dernier ouvrage *Envie de Cyber* et des portraits qui s'y trouvent, il s'est produit un puissant « effet miroir ». Les réactions des jeunes gens face aux conseils de protection en ligne nous ont renvoyés à nos propres contradictions…. celles de ceux, nés et ayant grandi avant l'explosion du monde numérique, la génération d'avant Google, qui pour une part non négligeable a parfois la gâchette facile sur le monde numérique.

Retour sur l'histoire d'une introspection. Ces échanges avec ceux que nous souhaitons protéger nous ont renvoyés de façon assez violente à la façon dont les générations nées ou ayant grandi avant la bulle numérique ont tendance à faire du numérique, un monde à part, non seulement « non essentiel », responsable de bien des maux, tel une sorte de planète de services, dont on peut extraire l'ensemble des ressources sans trop d'états d'âme. En le considérant comme tel… ce monde numérique… comment créer un lien et guider les jeunes face aux dangers qui peuvent les frapper, quand eux ne voient pas deux mondes, mais un parfait continuum entre vies réelle et virtuelle, comme le rez-de-chaussée et l'étage d'une même maison, dans laquelle ils évoluent librement au gré des fonctions de chaque pièce ?

La réponse est « difficilement ». Pour eux, c'est un fait. Le réel et le virtuel forment un parfait prolongement l'un de l'autre. Ils n'y voient pas de différence.

À l'ISSA France, nous avons une devise qui nous est chère « *atteindre avant de convaincre* » et c'est exactement ce qui nous oblige à apprécier l'efficacité et la pertinence de nos messages. C'est pourquoi très vite, nous nous sommes attachés à d'abord écouter et comprendre notre cible pour « tordre » nos discours en les rendant intelligibles et acceptables, un peu à la mode « Inception ».

C'est pourquoi, par exemple depuis bien longtemps lors de nos ateliers, nous ne parlons jamais de « temps d'écran » qui n'a non seulement aucun sens, sauf dans le cas des très jeunes enfants pour des raisons de santé publique, et qui est une malhonnêteté intellectuelle quand on sait le temps

que nous passons tous aujourd'hui devant nos écrans. C'est également aussi le meilleur moyen pour des parents ou figures d'autorité de dévaloriser leurs injonctions auprès des enfants et adolescents en ce qu'ils laissent supposer que leur « temps d'écran » est plus important, plus constructif, que celui des jeunes, quel que soit ce qu'ils y font. Alimenter cette frustration est l'inverse d'une sensibilisation efficace.

Valeurs et concepts bancals

La démonstration ne s'arrête pas là. De la même façon que les enfants et adolescents ont du mal à s'expliquer cette perpétuelle discontinuité que les générations pré-numériques font entre vie réelle et vie virtuelle, ils ne sont pas toujours non plus en mesure de comprendre leurs aînés qui s'échinent à leur expliquer des concepts et des choses de la vie tels qu'ils pouvaient - eux - les vivre dans le monde pré-googlien. Là encore, c'est comme regarder le monde avec une paire de lunettes qui n'est pas à sa vue… les repères deviennent flous.

Le continuum vécu par les jeunes a pourtant modélisé une nouvelle image de nombreux concepts, comme celui de la vie privée. Quand les générations pré-numériques continuent d'apprécier la vie privée en excluant d'office sa réalité (ou plutôt sa non réalité) dans l'espace numérique, elles deviennent là encore totalement incompréhensibles auprès de ceux à qui elles s'adressent. Comment, à leur place, ne pas en déduire qu'on les empêche de pouvoir accéder à l'étage de leur propre maison sans aucune autre explication que parce qu'un escalier les sépare, pour reprendre l'analogie précédente ?

Quel poids peuvent avoir également nos conseils quand le partage des mots de passe est la version moderne du petit mot écrit sur une page margée grands carreaux entre deux écolières des années 80 pour se partager le nom de leurs amoureux respectifs ? Aucun, si on n'explique pas la base de la confiance, la base du respect mutuel et si on ne cesse de considérer le cyber comme une île dont on peut facilement les exiler.

Que ce soit leur rapport à l'information, aux rapports sociaux, à la vie privée, ils les considèrent aussi bien du prisme de la vie réelle que virtuelle

et là encore, à ne pas soupeser ce point, nous nous retrouvons en décalage avec nos jeunes cibles.

Nous ne passerons pas tous les concepts au crible, mais il en va de même de leur rapport à la reconnaissance et à la valorisation. Depuis combien de temps n'a-t-on pas demandé à notre jeunesse ce que signifie pour eux « la réussite » dans une vie, ce que signifie pour eux d'être reconnu et valorisé ?

Vous me direz peut-être que vous ne comprenez pas qu'une association dont le seul but est de faire prendre de bons réflexes aux jeunes se pose de telles problématiques, et vous avez raison de vous poser la question. C'est parce qu'en égrenant au tout début nos discours de prévention sur la sécurité en ligne (mots de passe, données personnelles, cyberharcèlement, attention à la publicité ciblée, arnaques, sextorsion…) nous avons très vite saisi que le compte n'y était pas, que nous ne prenions pas le sujet par le bon bout et qu'il fallait creuser plus loin pour obtenir des résultats satisfaisants et, in fine, oeuvrer à les protéger, les protéger peut-être d'eux-mêmes. Sensibiliser est une bonne action. Le faire avec des résultats, c'est mieux.

Connaissance de façade

Car il ne faut pas s'y tromper, au-delà de tout ce qui a été précédemment dit, ces jeunes ont besoin d'être sensibilisés. Les besoins en éducation cyber sont essentiels et les bonnes volontés sont précieuses. Nous sommes absolument convaincus de la nécessité de construire cette autonomie des jeunes, faire en sorte qu'ils puissent gérer ce continuum vie réelle / vie virtuelle et que nous devons activer leur perception des risques, aussi bien dans l'une que dans l'autre.

Si les jeunes sont pleinement à l'aise avec l'ergonomie des terminaux numériques et des applicatifs, ils n'ont en revanche pas ou peu de connaissances sur l'écosystème et le fonctionnement du monde numérique, ou encore de la géopolitique de l'immatériel, et ce ne sont pas les enseignements numériques qui à ce jour changeront quelque chose. En effet, un rapport de l'Institut Montaigne le soulignait d'ailleurs déjà

dès 2011, le numérique n'est abordé que par son prisme « mathématique ». On ne compte d'ailleurs pas les initiatives faites autour du code, de la dimension technique, au détriment de la dimension stratégique mais également de sa dimension humaine et sociale bien trop souvent éclipsées et qui empêchent le numérique d'être d'ailleurs apprécié comme une perspective d'avenir.

« Cyber », une particule encombrante

Dans le même ordre d'idées, encarter les problèmes qui se passent sous pavillon « monde numérique » a eu l'effet de les rendre tellement spécifiques et hors frontières que ça eu l'effet pendant bien longtemps d'amenuiser leurs effets, de les éloigner de nos préoccupations et d'en faire des maux considérés comme moins indolores. Le cyberharcèlement en est un exemple illustrant.

Il n'a pas toujours été cause de premières dames, ni sujet de campagnes TV. Il a fallu bien des malheurs pour qu'il le devienne. À cela s'ajoute un autre effet néfaste. En estampillant des problématiques bien réelles de « cyber » s'est posée la question de qui devait en être « en charge ». Si aujourd'hui c'est un sujet que l'Education Nationale a fait sien, cela n'a pas toujours été le cas car, qu'on le veuille ou non, la question de le gérer au sein d'un établissement scolaire ou pas s'est posée. Problème du monde numérique ou problème du monde *d'en bas* ? Vaste sujet.

Il est indéniable que le bon choix a été fait en le prenant à bras le corps, mais il est un parmi tant d'autres. … le cyberharcèlement n'est pas le seul fléau du numérique.
C'est dans ces moments-là que faire appel aux sources et à la genèse peut être éclairant.

La cyber, innervée au Parcours citoyen

Si l'école ne peut pas tout et si elle n'a pas le monopole de l'éducation, il faut rappeler tout de même que le code de l'éducation dit ceci : « *La formation scolaire favorise l'épanouissement de l'enfant, lui permet d'acquérir une culture, le prépare à la vie professionnelle et à l'exercice de*

ses responsabilités d'homme et de citoyen. Elle constitue la base de l'éducation permanente. Les familles sont associées à l'accomplissement de ces missions. » et aussi « *Les écoles, les collèges, les lycées et les établissements d'enseignement supérieur sont chargés de transmettre et de faire acquérir connaissances et méthodes de travail. Ils contribuent à favoriser la mixité et l'égalité entre les hommes et les femmes, notamment en matière d'orientation. Ils concourent à l'éducation à la responsabilité civique et participent à la prévention de la délinquance. Ils assurent une formation à la connaissance et au respect des droits de la personne ainsi qu'à la compréhension des situations concrètes qui y portent atteinte. Ils dispensent une formation adaptée dans ses contenus et ses méthodes aux évolutions économiques, sociales et culturelles du pays et de son environnement européen et international. (…) Les écoles, les collèges et les lycées assurent une mission d'information sur les violences et une éducation à la sexualité.* »

En toute honnêteté, nous avons été surpris nous-mêmes à la lecture de cette substantielle mission.

Pour y faire écho, de l'école au lycée, existe le Parcours Citoyen. Le Parcours Citoyen vise à la construction, par l'élève, d'un jugement moral et civique, à l'acquisition d'un esprit critique et d'une culture de l'engagement. La circulaire du 23 juin 2016 en précise les grands objectifs ainsi que les modalités de pilotage et de mise en œuvre.

Il s'adresse à des citoyens en devenir qui prennent conscience de leurs droits, de leurs devoirs, de leurs responsabilités. Adossé aux enseignements, en particulier l'enseignement moral et civique (EMC), l'éducation aux médias et à l'information (EMI), il concourt à la transmission des valeurs et principes de la République en abordant les grands champs de l'éducation à la citoyenneté : la laïcité, les valeurs républicaines, l'égalité entre les sexes et le respect mutuel, la lutte contre toutes les formes de discrimination, notamment la prévention et la lutte contre le racisme et l'antisémitisme, contre les LGBTphobies, l'éducation à l'environnement et au développement durable, la lutte contre le harcèlement, l'éducation aux médias et à l'information ; ou encore l'éducation à la défense et à la démocratie. Ce parcours prend également appui sur la participation de

l'élève à la vie sociale et démocratique de la classe et de l'école ou de l'établissement.

Voici un programme bien dense qui doit cohabiter avec le programme « tronc commun », ce qui n'est d'ailleurs pas du goût de tous les candidats à l'élection présidentielle qui estiment que l'école doit se recentrer sur les fondamentaux. (À relire le code de l'éducation… que penser du fondamental ?)

Voilà une autre façon de dire que dans ce programme déjà chargé doivent se greffer en sus, des interventions de sensibilisation aux bonnes pratiques numériques ou encore au cyberharcèlement. Cela dépend du bon vouloir d'enseignants, de conseillers d'orientation, et autres directeurs d'établissement dont l'initiative est souvent personnelle. C'est en tous les cas souvent ainsi que nos interventions se sont concrétisées avec des établissements perdus ou démunis suite à des problématiques concrètes rencontrées.

Afin non seulement de gagner en temps, mais aussi parce que cela nous semble relever de la plus exemplaire logique, nous revendiquons l'importance d'introduire une dimension cyber au sein même du Parcours Citoyen, en d'autres termes de faire du cyber une transversale à tous les sujets abordés par les thématiques du Parcours Citoyen, ce qui sans aucun doute aura bien davantage de résonance chez des jeunes gens qui n'ont pas connu le monde sans le numérique.

Nous l'avons explicité plus haut, les jeunes ne font pas de différence entre vie virtuelle et vie réelle. À nous d'intégrer cette dimension essentielle.

Comment cela se traduit-il ? Il convient par exemple d'aborder la question du *Revenge Porn* au moment d'évoquer les questions de respect mutuel ou encore de l'égalité entre les hommes et les femmes, comme il est pertinent d'expliquer la sextorsion ou la prostitution de plus en plus préoccupante des jeunes femmes facilitée par l'outil numérique quand on traite de la perception et du respect de son corps. La question du cyberharcèlement est quant à elle tout indiquée au moment de parler du handicap, de la différence, des orientations sexuelles comme identitaires.

De la même façon, aborder les *fake news* quand on traite des questions de démocratie et de contrat social peut avoir tout autant de sens.

Tout à chacun appréciera que dans le Parcours Citoyen, nous abordons le numérique comme outil, et comme continuum existentiel des jeunes.

Ce qui nous amène à préciser que nous revendiquons que le numérique ne doit pas devenir une espèce fourre-tout. Il est important que le numérique tel qu'abordé ici dans le Parcours Citoyen comme outil, et dans sa dimension humaine et sociale ne doit pas se confondre avec le numérique comme savoir fondamental et disciplinaire, auquel il est logique d'associer des enseignements spécifiques et plus techniques (codage, algorithme, cybersécurité, etc.).

Qui sait ? Comme nous le précisons dans le rapport, redonner ses vrais contours au numérique et la place qu'il occupe pour les jeunes, est peut-être la voie pour non seulement mieux les sensibiliser aux dangers mais également révéler le numérique et la sécurité numérique comme des perspectives d'avenir, de développement, d'engagement et de réalisation personnelle.

Parution le 25 février 2022

Favoriser le recrutement et les carrières cyber dans les fonctions publiques territoriales et hospitalières : un impératif de sécurité nationale

PHILIPPE LOUDENOT
Senior advisor
CyberCercle

Si 66% des Français - soit 2 Français sur 3 - attendent aujourd'hui de leur collectivité qu'elles leur proposent des services numériques personnalisés, seul un tiers d'entre eux est prêt à leur confier ses données personnelles. Garantir la confiance numérique est aujourd'hui un enjeu majeur.

La dématérialisation engagée par l'ensemble des acteurs et accélérée par la crise sanitaire participe à la profonde transformation numérique de la société. Mais elle s'accompagne aussi de l'essor des menaces cyber, désormais permanentes et capables de désorganiser de nombreuses structures privées comme publiques, petites comme grandes, que ce soit au niveau national ou de tous les niveaux territoriaux. C'est dans ce contexte que les acteurs concernés doivent faire face à l'explosion de cyberattaques : vol de données confidentielles, interruption des fonctions critiques de l'entreprise ou de la collectivité, actes frauduleux. Ces cyberattaques sont d'ailleurs de plus en plus relayées par les médias.

Sur l'ensemble des incidents ou attaques numériques, les TPE/PME et collectivités représentent près de 80 % des victimes, souvent sans ressources pour y faire face. A titre d'exemples, plusieurs attaques récentes ont ainsi impacté des administrations territoriales mais également des structures de santé ou médico-sociales révélant un phénomène d'ampleur,

celui de l'oubli par ces structures de la protection des données et de la sécurité numérique de premier niveau.

Cet « oubli » pouvant se révéler dramatique, est induit par une méconnaissance des risques pesant sur la protection des données et des enjeux de la sécurité du numérique. Certes, une pléthore de spécialistes communique sur ce sujet, mais uniquement via des menaces dont l'origine annoncée est située dans des contrées lointaines ou du fait de cybercriminels en recherche d'argent facile et éloignés de la justice : ce sont des méchants et il y en a plein ! Si ce type de discours est toujours écouté très poliment, il est souvent vite oublié face à des interrogations, de fait, légitimes : « pourquoi moi ? », « pourquoi ma structure ? ». Par trop souvent il n'est pas fait état des risques et particulièrement des impacts sur les organisations mêmes.

Pour se prémunir, car, comme en médecine, le préventif coûte moins cher que le curatif (si tant est que l'on puisse traiter), différents acteurs proposent un certain nombre d'actions et particulièrement celle de nommer un responsable de la sécurité des systèmes d'information (RSSI). Si le règlement européen de la protection des données à caractère personnel, le fameux RGDP, fait obligation de nommer un délégué à la protection des données personnelles (DPO), précisant toutefois que celui-ci peut être interne, mutualisé ou externalisé, cette vision ne l'est pas pour le RSSI.

Alors que les entreprises et les administrations françaises prennent conscience de l'enjeu de la cybersécurité, plus de 5 000 postes sont actuellement à pourvoir dans ce domaine dans l'Hexagone. De nouvelles formations se mettent en place, certes, mais cela ne semble pas suffire. Le RSSI est donc une ressource « rare ». Sans paraphraser le sophisme « ce qui est rare est cher », l'énorme difficulté pour certaines structures de proposer un poste de RSSI et de trouver la personne qualifiée est un constat permanent.

Le Livre blanc sur la défense et la sécurité nationale place la sécurité et la défense des systèmes d'information au cœur des priorités stratégiques de la Nation. Néanmoins, au regard des besoins existant sur le terrain, les annonces faites en février 2021 par le Président de la République pour

muscler la filière de cybersécurité française et annoncer un plan national consacré à la cybersécurité se heurtent au manque de moyens des structures des fonctions publiques hospitalières ou territoriales.

En effet, face aux besoins accrus en matière de Ressources humaines cyber, la fonction publique d'État dispose aujourd'hui de deux textes, pour renforcer ou attirer des talents, spécialistes de domaines où les ressources manquent :

La circulaire du Premier ministre du 21 mars 2017 relative à la gestion des ressources humaines dans les métiers du numérique et des systèmes d'information et de communication. Elle se traduit par la création d'un corps des ingénieurs des systèmes d'information et de communication. Elle propose de favoriser le recrutement et la mobilité. A cet effet il est proposé, même en l'absence d'un corps de fonctionnaires, de pouvoir, pour les métiers à compétences rares, procéder directement à un recrutement en CDI.
La note « Référentiel de rémunération des 56 métiers de la filière numérique et des systèmes » du 15 décembre 2021 (annexe 2), co-signée par la directrice générale de l'administration et de la fonction publique, la directrice du budget et le directeur interministériel du numérique d'information et de communication. Cette note vise une meilleure prise en compte de l'expertise et des compétences détenues par les candidats et d'identifier le niveau adapté de rémunération au regard des différents seuils que propose le référentiel, du niveau de complexité du poste, des compétences détenues par le candidat et de son expérience.

En revanche, concernant la fonction publique hospitalière ou territoriale, où les besoins en spécialistes cyber sont criants, force est de constater la pénurie de spécialistes en cybersécurité, renforcée par une faible attractivité : niveaux de salaires incompatibles au regard du marché, postes à durée limitée et aucune visibilité sur un éventuel plan de carrière.

S'il est souhaité une prise en compte et un accompagnement cyber de l'ensemble des échelons de ces fonctions publiques, il peut être envisagé, à l'instar des délégués à la protection des données, la possibilité de disposer de RSSI internes, mutualisés ou externalisés. Sans préjudice de ces deux

dernières possibilités, il pourrait être étudié la mise en place de leviers identiques à ceux existants dans la fonction publique d'État et ainsi favoriser le recrutement de ressources rares, en prenant en compte également les moyens pour garder, maintenir et élever le niveau de connaissance mais aussi de proposer une carrière aux candidats.

Engager une réflexion sur la dimension ressources humaines en cyber pour les fonctions publiques hospitalières et territoriales est un enjeu de sécurité nationale.

Parution le 4 mars 2022

Français, Européens, encore de gros efforts pour être souverains !

PHILIPPE LATOMBE
Député de la Vendée

Ces dernières années, la crise sanitaire, ces dernières semaines, la crise ukrainienne, ont fort malheureusement remis au goût du jour ce propos d'Emile de Girardin : « Gouverner, c'est prévoir ». Il est certes toujours plus facile de dénoncer après coup le manque d'anticipation que de détecter les signes annonciateurs quand ils se manifestent. En revanche, persister dans l'erreur et ne pas tirer les leçons de celles qu'on a commises pose question, le déni constituant une faute grave en politique.

Or, il a fallu deux crises majeures pour que le sujet de notre souveraineté, notamment numérique, revienne au premier plan, au risque d'ailleurs de devenir une tarte à la crème que chacun revisite au gré de ses intérêts, de ses convictions parfois à géométrie variable et pas toujours en conformité avec l'intérêt général. Il a fallu une pandémie et une guerre à nos portes pour que nous réfrénions notre appétence pour une mondialisation béate et débridée, dont nous n'avons que trop occulté les faiblesses et les dangers. Dès le début de mon mandat de député, mon intérêt s'est très vite porté sur les problématiques nouvelles nées de la révolution numérique et de son impact sur l'innovation technologique. Il n'est de spécialité scientifique qui puisse faire abstraction de cet outil qui potentialise les avancées technologiques avec une caractéristique aussi préoccupante qu'enthousiasmante : l'accélération de l'innovation. Le temps scientifique s'est précipité, le temps politique doit suivre, plus encore anticiper, et il a bien du mal.

Or en matière de révolution numérique, force est de constater que non seulement nous n'avons pas anticipé, mais nous n'avons pas, dans notre

pays, accompagné politiquement ce bouleversement technologique, l'un des plus grands de l'histoire de l'humanité, puisqu'il transcende des limites que l'intelligence humaine ne pensait pas possibles ou même envisageables de repousser il y a de cela moins d'un siècle. Nous sommes en la matière devenus dépendants d'opérateurs étrangers dont le pouvoir finit d'ailleurs par outrepasser celui des Etats. Alors que nous excellons dans nombre de domaines de la recherche, nous vivons cette révolution technologique sans protéger notre souveraineté.

Ce déficit de souveraineté numérique, nous le subissons. Nous nous laissons porter et nous ne sommes pas moteurs. Il est trop facile de dire que c'est parce que nous n'avons pas pris le train à temps et qu'il ne sert plus à rien de courir derrière, que nous devons multiplier les compromis et les concessions. La Russie et la Chine, sans doute parce que plus obsédées par leur sécurité intérieure, leur indépendance technologique et leur souveraineté, ont réussi, en mettant les bouchées doubles, à rattraper leur retard en quelques années, à assurer leur souveraineté numérique. Le sujet est surtout éminemment politique, ce que nous avons parfois tendance à oublier.

Pourtant, depuis cinq ans bientôt, je suis obligé de constater le peu d'appétence des politiques pour ce sujet. Peu de mes collègues de l'Assemblée nationale, représentatifs en cela de l'ensemble de nos compatriotes, ont une réelle expertise en la matière. Il est vrai que pouvoir prétendre à une vision politique de cette question demande des compétences juridiques et une connaissance des technologies et de leurs impacts sur la condition humaine et sur l'évolution de nos sociétés. Pourtant il est indispensable, si nous souhaitons pouvoir légiférer avec pertinence dans ce domaine, que nous soyons nombreux, quel que soit notre attachement partisan, à nous approprier ces sujets.

L'événement organisé le 9 mars au Cirque d'hiver par le collectif Convergences numériques, qui regroupe plusieurs associations professionnelles (France Digitale, l'Afnum, Cigref, Fevad…), a été tout à fait révélateur. Sept des douze candidats à l'élection présidentielle y ont en effet présenté leur programme pour le numérique, devant un public d'entrepreneurs, de start-up, d'entreprises du numérique et de journalistes.

Tous sont d'accord (et ils ont tout à fait raison) pour dire qu'il faut développer un cloud souverain, afin de protéger les données personnelles des Français, ou qu'il faut préserver les pépites nationales de la prédation des géants étrangers. Ils ont « coché » ces sujets car ils sont fortement médiatisés ces derniers mois, en raison de leur actualité (Health Data Hub, Gaia X…) mais, à aucun moment, ils n'ont abordé les véhicules autonomes, la 5G, le hardware, les cryptomonnaies, le chiffrement ou la robotique industrielle, autant de domaines qui, si techniques soient-ils et justement parce que, participent eux aussi de notre souveraineté nationale. Faire des propositions au cas par cas, au fil de l'actualité, ne constitue pas une véritable politique de défense de la souveraineté nationale.

Par ailleurs, les chantres de la souveraineté numérique ne forment pas un groupe homogène, souvent parce qu'ils n'en ont pas la même définition. Certains confondent souveraineté et souverainisme. D'autres clament haut et fort qu'il nous faut retrouver notre souveraineté mais succombent par intérêt personnel ou par facilité aux sirènes des Gafam. On ne peut pas crier au loup et en même temps le faire entrer dans la bergerie, sous le prétexte souvent fallacieux qu'on ne peut faire autrement. Quand on laisse Google Cloud ou Microsoft proposer leurs services dans le cadre de licences accordées à des entreprises françaises, on inféode ces dernières et leurs clients à des opérateurs étrangers, dont on sait pertinemment qu'il leur sera difficile, voire impossible, de se séparer par la suite, parce que ce sera trop compliqué et trop cher. On tue par la même occasion l'écosystème numérique national au lieu de le booster.

L'Etat se doit d'être exemplaire et il est loin du compte. Il le peut pourtant de bien des façons. Tout d'abord, il doit privilégier l'écosystème français et européen en cas de commande publique, le recours à une entreprise extérieure ne pouvant se faire que si aucune solution n'a été trouvée et dans des conditions de sécurité et de réversibilité optimales. Il est impératif d'intégrer de façon systématique au sein des arbitrages techniques des projets numériques les enjeux ayant trait à la souveraineté numérique, en particulier concernant la protection des données personnelles et la localisation des données en Europe.

La digitalisation et la modernisation de notre administration doivent être

accélérées. Cela passe par la montée en compétences des ressources humaines internes. Il faut que celles et ceux qui accompagnent ces projets aient à la fois les compétences technologiques adéquates et une parfaite connaissance des besoins de leur administration. Cela passe bien évidemment par une rémunération attractive et la mise en œuvre d'une stratégie de fidélisation pour les conserver au sein de la sphère publique. La difficile mise en adéquation des besoins avec l'offre d'intervenants extérieurs les méconnaissant a été à l'origine de fiascos qui ont coûté cher aux finances publiques.

Il faut imposer au sein de l'administration le recours systématique au logiciel libre, en faisant de l'utilisation de solutions propriétaires une exception. L'exemple le plus flagrant est celui de l'Education nationale : quand l'école biberonne les enfants aux Gafam dès leur plus jeune âge au lieu de les former à l'utilisation de logiciels libres, on développe chez eux des réflexes de consommation qui seront difficiles à déconditionner par la suite et qui influenceront leurs choix personnels et professionnels futurs. L'Education nationale doit développer la formation à l'outil informatique, au codage ainsi que la sensibilisation aux risques qu'en occasionne l'usage. Il s'agit de faire des générations futures des utilisateurs éclairés et non des consommateurs passifs et vulnérables.

L'incendie survenu en mars dans le datacenter strasbourgeois d'OVHCloud a été révélateur de la faible acculturation des entreprises françaises aux enjeux de sécurité de leurs données. Une majorité des clients d'OVH pensaient que leur site et leurs données étaient automatiquement sauvegardées par l'hébergeur, confondant ainsi stockage et sauvegarde.
Le confinement a mis le doigt sur l'intérêt de la numérisation pour les TPE-PME. Pendant cette période, les PME du commerce de détail qui vendent en ligne ont subi une perte de chiffre d'affaires inférieure en moyenne de 25 points comparativement à celles qui ne reçoivent pas de commandes en ligne. Le niveau d'équipement en ordinateurs portables des entreprises a permis d'amortir dans certains secteurs les conséquences de la crise sanitaire grâce au télétravail.

Cependant, comme j'ai pu le constater dans ma circonscription vendéenne, la complexité des démarches pour accéder aux aides

permettant aux entreprises d'améliorer la numérisation et la sécurisation de leurs installations ainsi que la difficulté d'accès à l'information sur ces aides ont un effet contre-productif. Un plan quinquennal de soutien à la numérisation des entreprises et à la cybersécurité permettrait d'obtenir de meilleurs résultats et d'éviter que nombre d'entre elles passent à travers les mailles du filet des aides.

Se pose bien évidemment aussi la réforme des systèmes d'aides au financement des start-up, trop complexes eux aussi et peu réactifs. Nous n'avons pas besoin de faire preuve d'une imagination que nous n'avons pas eue jusqu'à maintenant : peut-être pourrions-nous tout simplement nous inspirer des Etats qui ont fait preuve d'inventivité et peuvent être qualifiés de start-up nations. C'est à ce prix que nous pouvons espérer favoriser l'émergence de nouvelles technologies. Cela peut passer, pourquoi pas, par une participation de l'Etat au capital des entreprises concernées. Il est aussi nécessaire d'aborder sans tabou le sujet sensible de la vente de nos pépites aux Gafam. Il ne s'agit pas de porter atteinte à la libre entreprise. En revanche, il est important qu'une doctrine clairement déclinée et accessible à tout le monde soit formalisée, afin que les décisions soient prises en toute transparence et objectivité. Décider au cas par cas, dans le secret de Bercy, comme c'est le cas actuellement, ne contribue pas à clarifier la lecture des décisions prises. Les outils pour la déclinaison d'une telle doctrine existent déjà, ne serait-ce qu'au niveau européen. L'abandon par NVIDIA du rachat d'ARM ne fait pas couler beaucoup d'encre ni de larmes, beaucoup moins en tout cas que le projet d'acquisition. En matière de libre entreprise, ne soyons donc pas plus royalistes que nos voisins d'outre-Manche qu'on ne peut accuser de laxisme sur ce sujet.

Autant de sujets pour lesquels il faut un pilote dans l'avion,« exfiltré » de Bercy, sans à ses côtés une DGE qui réduit systématiquement l'approche des sujets numériques à des considérations strictement économiques ou financières. Comme j'ai souvent eu l'occasion de m'en expliquer, un secrétariat d'Etat chargé de la Transition numérique et des Communications électroniques, niché dans un recoin de l'administration du ministère de l'Économie, des Finances et de la Relance et disposant d'une équipe réduite, n'a pas le pouvoir de mener des chantiers d'une telle

envergure. Il faut un ministère de plein exercice, doté de pouvoirs étendus pour porter enfin une vision transversale des enjeux du numérique au sein de l'État et construire une véritable stratégie numérique sur le long terme. Il existe un consensus dans les propositions des candidats à l'élection présidentielle sur la nécessité pour notre pays de recouvrer sa souveraineté et sur la conviction que cela passe pour beaucoup par la construction de notre souveraineté numérique, clairement identifiée comme un sujet majeur du prochain quinquennat. Il est temps de mettre en adéquation les paroles et les actes politiques.

Parution le 18 mars 2022

Pour une stratégie offensive de lutte contre la désinformation à l'ère du numérique

OLIVIER CADIC
Sénateur représentant les Français établis hors de France
Vice-président de la commission des Affaires étrangères,
de la Défense et des Forces armées

Si l'on définit la désinformation comme l'art de tromper le jugement d'autrui, la manœuvre est aussi vieille que l'humanité. Des hordes de comptes robotisés pilotés depuis l'étranger s'apprêtent-elles à polluer le débat public sur les réseaux sociaux en diffusant massivement de fausses informations pour influencer l'élection présidentielle des 10 et 24 avril, s'interrogeait le journal Le Monde, le 18 février dernier ?

Quel chemin parcouru depuis la dernière échéance présidentielle ! La société civile a pris conscience qu'elle vivait en pleine guerre froide de l'information.

Une guerre de la communication a été enclenchée, une guerre destinée à réécrire l'histoire et à dénigrer les démocraties pour préparer la reconfiguration du paysage géopolitique de l'après-crise, c'est le constat que je posais avec mon collègue sénateur Rachel Mazuir dans notre rapport « Désinformation, cyberattaques, cybermalveillance : l'autre guerre du Covid-19 », publié en juin 2020, tandis que des millions de Français avaient basculé dans le télétravail. Dans nos recommandations, nous avions appelé à la mise en place d'une « force de réaction rapide » pour contrer les fausses nouvelles, une structure en faveur de laquelle je plaidais depuis des années pour compléter notre dispositif anti-fake news, après le vote de la loi contre la manipulation de l'information en décembre 2018.

Nous avons été entendus par le gouvernement qui a lancé, en février 2021, une stratégie d'accélération de la filière cybersécurité en France et la création de Viginum, opérationnelle depuis décembre 2021.

Cette nouvelle agence gouvernementale a pour mission de détecter les opérations de désinformation sur les plateformes en ligne et d'en informer les pouvoirs publics. Viginum est appelée à jouer un rôle important pendant les périodes électorales en fournissant toute information utile au Conseil supérieur de l'audiovisuel, au Conseil constitutionnel et à la Commission nationale de contrôle de la campagne électorale.

Il s'agit d'une avancée importante, mais je regrette une certaine timidité dans l'approche. Viginum est uniquement chargée de remonter des observations et n'a pas de pouvoir contraignant. Autrement dit, ses agents ont interdiction d'interagir avec les autres utilisateurs : pas question de poster quoi que ce soit sur les réseaux sociaux.

Face à la propagation de fake news par la Chine continentale, les autorités taïwanaises ont mis en place une organisation de « fact-checking » qui permet d'expliquer une fausse nouvelle en moins de deux heures et en moins de 200 mots. J'ai indiqué au directeur du SGDSN que nous devrions nous inspirer de cette expérience taïwanaise pour définir le modus operandi de Viginum.

Autre remarque : demeurer sur la défensive ne devrait pas rimer avec faiblesse de réaction. Lorsque le site de l'ambassade de Chine publie, en pleine crise du Covid, que nous laissons mourir les gens dans les Ephad, on se contente de convoquer l'ambassadeur. Si notre ambassade à Pékin racontait ce qui se passe au Xinjiang, son compte serait immédiatement fermé et l'ambassadeur expulsé, nous a confié un diplomate lors de son audition devant la commission des Affaires étrangères, de la Défense et des Forces armées du Sénat.

On entend souvent dire que la meilleure des protections c'est l'éducation, qu'il faut miser sur l'esprit critique ou bien encore que les plateformes de réseaux sociaux doivent s'autoréguler. Tout cela est vrai, il n'empêche que l'attaquant a toujours un coup d'avance sur sa cible.

C'est pourquoi je prône la création d'une CyberForce qui lutterait de manière offensive. Le but serait d'inverser le jeu. Ainsi, en adoptant cette nouvelle cyber-doctrine, les démocraties pourraient faire passer des messages offensifs aux populations vivant sous dictature en leur laissant entendre qu'un autre monde est possible et souhaitable.

Le temps fera son œuvre. Pour l'heure, je suis heureux de constater que nous avons accompli en 2021 un grand pas vers un « écosystème français » qui place la France en pointe en matière cyber, à l'image de ce que j'ai pu observer à Beer Sheva en Israël en janvier 2019. Je pense au développement de diverses initiatives, comme le Campus Cyber de la Défense ou le pôle de compétences en cyberdéfense à Rennes.

Dans ce domaine la France est en avance et c'est heureux, car nos sociétés démocratiques sont très perméables aux actions massives et répétées de désinformation et de manipulation de l'opinion. Dans cette bataille des opinions, les démocraties européennes ne doivent pas se montrer naïves. Elles doivent au contraire accroître la défense et la promotion de leurs valeurs en renforçant leur vigilance et en se dotant d'instruments efficaces. Début mai 2018, je m'étais rendu au Pentagone qui avait établi que les fake news étaient clairement la principale menace en termes de guerre hybride.

L'adoption de la Loi de Programmation Militaire par le Sénat, le 29 mai 2018, a inclus ma proposition de prise en compte de « la manipulation de l'opinion publique par l'utilisation massive des médias numériques et des réseaux sociaux avec pour objectif l'altération du fonctionnement normal des institutions démocratiques ».

La présidence française de l'Union européenne doit constituer une fenêtre d'opportunités pour faire avancer les dossiers cyber au plan européen, comme la lutte contre la désinformation.

En mai 2017, le président Macron répondait en ces termes à une journaliste russe de RT qui se plaignait d'avoir été exclue de son QG pendant la campagne présidentielle : « Quand des organes de presse répandent des contrevérités infamantes, ce ne sont plus des journalistes,

ce sont des organes d'influence », a-t-il justifié pour interdire d'accès Russia Today et Sputnik à son quartier général.

La crise ukrainienne aura agi comme un catalyseur : c'est toute l'Europe qui vient de bannir ces organes qu'il convient de qualifier d'ingérence, désormais.

Le prochain quinquennat devra permettre d'armer une cyber-stratégie pro-active, doublée d'efforts législatifs, dont la meilleure échelle est assurément l'Europe. N'attendons pas un « 11-Septembre de la Cyber » pour comprendre que les démocraties doivent s'allier sans tarder pour combattre un ennemi qui se joue des frontières et cherche à les détruire de l'intérieur.

Parution le 8 avril 2022

Sécurité du numérique : moins d'entropie et plus de stratégie ?

CHRISTIAN DAVIOT
Président-fondateur
cdstrat
Senior advisor du CyberCercle

Lettre d'un citoyen engagé au (futur) Premier ministre.

Monsieur le (futur) Premier ministre,

Ce nouveau quinquennat ouvre cinq années cruciales pour la France en matière de sécurité du numérique.

Aussi permettez-moi de porter à votre attention quelques propositions d'orientations relatives à l'action gouvernementale, son organisation, ses priorités, au rôle des régions et succinctement à l'international. Les administrations vous fourniront les multiples mesures techniques à prendre en parallèle.

Le numérique s'est effacé peu à peu des discours de vos prédécesseurs. Cité neuf fois dans la déclaration de politique générale d'Édouard Philippe en 2017, celui-ci n'évoquera le sujet qu'une fois dans sa déclaration de 2019 pour constater notre retard. Dans ce même exercice, Jean Castex ne cite pas une seule fois le numérique en 2020.

Sans sécurité du numérique pas de numérique, pas de développement économique, pas de transition écologique, pas de compétitivité des entreprises, pas de modernisation de l'État ni de services performants pour nos concitoyens.

La sécurité du numérique n'est pas d'abord une affaire d'ingénieurs ou de techniciens. La sécurité du numérique est d'abord une affaire de politique(s). La responsabilité des élus est majeure en ce domaine. Or, force est de constater - le diagnostic n'est que discrètement partagé - que nous avons ces dernières années régressé au niveau stratégique, désorganisé le modèle français, rendu tout à fait illisible une action essentiellement destinée aux « premiers de cordée » et presque disparu de l'international.

La régression stratégique est à la fois le fait de l'hubris de quelques-uns et d'un manque d'intérêt et de prise de conscience des derniers Premiers ministres - même si quelques réunions de rattrapage ont eu lieu ces six derniers mois qui ont donné lieu à la publication d'un décret[1], merveille bureaucratique qui aura sans doute le même avenir que le RGS.

Un peu de chronologie permet de comprendre comment nous en sommes arrivés là.

Le Président de la République avait demandé[2] en juillet 2017 au secrétaire général de la défense et de la sécurité nationale d'élaborer une revue stratégique de cyberdéfense. Ce n'était qu'une partie du sujet large qu'est la cybersécurité, mais il s'adressait alors devant la hiérarchie militaire. En février 2018, le SGDSN publiait une « stratégie nationale de cyberdéfense[3] » qui a voulu traiter de la sécurité du numérique dans son ensemble. Le document, rendu public en la seule présence d'un secrétaire d'État au numérique sur le départ, était certes pédagogique mais peu stratégique. Surtout il a fragilisé l'interministérialité vitale à la cybersécurité en créant quatre « chaînes opérationnelles » confiées à des ministères régaliens, créant ainsi autant de silos. Heureusement ces chaînes n'existent plus aujourd'hui que dans quelques « Powerpoints ».

Dans le texte du SGDSN, Bercy était marginalisé. Cette mise à l'écart a d'ailleurs été souhaitée dès l'origine par les concepteurs de la cybersécurité à la française : pour assurer le développement nécessaire de l'ANSSI en termes d'effectifs et de budget, il fallait éviter à l'agence de passer sous les fourches caudines budgétaires de Bercy. Ainsi, les décisions importantes relatives à l'ANSSI ou à la cybersécurité sont-elles prises depuis 2008 en conseil de défense et de sécurité nationale, qui est le lieu des décisions qui

s'imposent à tous sans contestation possible.

Après le départ de Mounir Mahjoubi, Cédric 0 est devenu secrétaire d'État sans tutelle ou cotutelle d'aucune administration, malgré des décrets d'attribution[4] lui confiant de larges missions qu'il ne pouvait donc remplir de manière autonome et efficace.

Avec le plan de relance d'après crise sanitaire, Bruno Lemaire a lancé une OPA à 700 millions d'euros sur le sujet en préparant avec la DGE, sans concertation, une « stratégie d'accélération de la cybersécurité[5] », essentiellement centrée sur les aspects industriels du sujet, une régression par rapport à la stratégie interministérielle présentée par Manuel Valls[6] en 2015. Préfacée par le ministre de l'Économie et des Finances, elle a de justesse été reprise et présentée par le Président de la République en février 2021[7].

Force est de constater que la mise en œuvre de cette « stratégie » se révèle cacophonique.

Le choix a été fait de subventionner les « premiers de cordée » via des appels à projets, des appels à manifestations d'intérêt dans de multiples domaines, avec des délais souvent très courts[8] ne permettant pas à tous les acteurs de répondre, notamment les moins parisiens. Nulle part n'est disponible une vision d'ensemble de ces initiatives. Il aurait été souhaitable de travailler à de vraies politiques publiques coordonnées qui touchent un large éventail d'administrations, d'institutions et de collectivités, d'acteurs économiques ou de particuliers. Soutenir la filière, bien sûr, mais sous réserve que l'ensemble de l'écosystème en soit bénéficiaire au sein d'un plan d'ensemble suivi et dont l'impact doit être contrôlé. Dans le débat depuis 1993, le levier de la commande publique en faveur des PME-PMI, souvent les plus innovantes, pourrait enfin y être intégré.

Même embarras sur la coordination. Il y a désormais deux coordinateurs de la cybersécurité nationale dans deux de vos (futurs) services : le directeur général de l'ANSSI, acteur historique de la cybersécurité, et le coordinateur national de la stratégie cybersécurité au SGPI. Devant cet embrouillamini, l'ANSSI semble avoir renoncé à la conduite d'une stratégie nationale et à

sa mission interministérielle pour se concentrer sur ses capacités opérationnelles, un domaine d'excellence de l'agence. Quant à la DGE de Bercy, elle ne donne manifestement pas les moyens de remplir pleinement sa mission au coordinateur du SGPI.

Les deux derniers secrétaires d'État au numérique ont décidé d'arrêter la politique : peut-être la manière dont leurs sujets ont été traités n'est-elle pas étrangère à cette décision…

Un signe politique doit être donné à tout l'écosystème.

Plutôt qu'un secrétaire d'État, il serait aujourd'hui plus efficient de nommer un ministre délégué chargé du numérique afin qu'il participe aux conseils des ministres concernés, qui vous serait directement rattaché pour être en mesure d'agir à l'interministériel, et doté d'un décret d'attribution qui lui donne autorité et moyens.

Le choix est vaste. Nombre de parlementaires s'intéressent à la cybersécurité et ont travaillé sur ce sujet.

Deux critères peuvent aider au choix du (ou de la) ministre délégué(e) qui devra :

- d'une part, avoir la capacité à différencier cybersécurité (attention portée aux attaques informatiques) et sécurité de l'information (attention portée à la propagande, aux fausses nouvelles) : ce ne sont ni les mêmes métiers ni les mêmes acteurs. D'ailleurs depuis 2009, dans les instances internationales, la France reproche ce mélange des genres à la Russie comme à la Chine. Il est vrai que, dans la perspective de la campagne électorale officielle, le SGDSN a donné le mauvais exemple en envoyant aux médias fin mars une lettre[9] signée par le directeur général de l'ANSSI qui évoque à la fois la partie cyberattaque (mission de l'ANSSI) et la partie influence (mission de VIGINUM). Une attaque informatique peut permettre d'identifier des éléments utiles à une campagne d'influence : il aurait donc été logique que le SGDSN, auquel est rattaché VIGINUM, endossât cette lettre plutôt que l'ANSSI, dont la mission n'est pas le contrôle politique des réseaux ;

- d'autre part, éviter la fascination pour les capacités sans limite des technologies, quelles que soient les atteintes portées aux libertés ou à la vie privée. L'acceptabilité par les citoyens est un facteur clef pour l'utilisation des technologies en matière de sécurité et l'équilibre délicat libertés publiques-performances sécuritaires est ici un enjeu démocratique fondamental.

Voilà pour l'échelon politique.

Vous devrez également veiller aux nominations à la tête des administrations qui traitent du numérique et de sa sécurité.

Le désintérêt d'Édouard Philippe et surtout de son dircab pour le numérique avait entraîné le renvoi dos à dos du secrétaire d'État et du directeur interministériel du numérique et du système d'information de l'État (DINUM) qui avait pourtant engagé une dynamique très innovante de transition numérique de l'État. La DINUM s'est effondrée en perdant nombre de ses talents après le choix, pour le remplacer, d'un dirigeant pour le moins controversé. Récemment, le directeur général de l'ANSSI a annoncé son départ de l'agence. Le secteur privé sera évidemment ravi de l'accueillir, mais il y aurait sans doute d'autres missions à lui confier au sein de l'État. Accompagner le ministre délégué par un Haut-commissaire dédié au travail avec les administrations est certainement une option. Il pourrait par exemple étudier le moyen d'attirer, de rémunérer au bon niveau et de garder les ressources humaines les plus performantes et les plus utiles pour accomplir les missions défensives et offensives. Dans certaines administrations sensibles, le turnover est en effet dangereusement élevé. Favoriser la mobilité des effectifs entre les différentes fonctions publiques serait également déterminant.

Plus largement, les ressources humaines sont critiques pour garantir la cybersécurité du pays. L'apprentissage du code au collège ne suffira pas. Donner les clefs de compréhension du numérique et éduquer les citoyens dès le plus jeune âge aux usages sécurisés du numérique est devenue une urgence – comme l'avait d'ailleurs identifié la Stratégie nationale pour la sécurité du numérique de 2015. Vous pourriez vous inspirer d'Israël dans l'identification des jeunes talents. De plus, le numérique comme la

cybersécurité ne se limite pas au code informatique. Toutes les disciplines, notamment le droit et les relations internationales, y concourent.

J'en viens à quelques priorités qui pourraient animer votre action.

D'abord, la mise en évidence à l'occasion de la crise sanitaire de l'importance d'une vraie souveraineté qui permet de gérer les dépendances, au-delà des discours simplificateurs. Ainsi faut-il tirer les enseignements de l'échec français et européen en matière d'informatique en nuage. Après le fiasco Cloudwatt et Numergy - quel autre État aurait eu l'idée de créer deux concurrents pour ne pas froisser la Commission européenne ? -, nous nous sommes mis en situation de dépendance à long terme vis-à-vis des acteurs américains sans avoir laissé une chance aux PME françaises du domaine. Après leur entrisme dans Gaia-X, les leaders américains du cloud ont piégé les grands acteurs français dans un scénario connu : dépendance aux licences dont le coût augmentera, version n-1 des technologies et rachat lorsque les acteurs français étranglés auront acquis les parts de marché.

Ensuite, le constat qu'il n'y a pas de perspective d'émergence d'acteurs français de niveau mondial à courir après des technologies numériques développées par d'autres. D'une part, parce que dans ce domaine, le premier arrivé prend instantanément une part conséquente du marché, mais également parce que l'effort de rattrapage est généralement hors de portée - voir la mésaventure d'un moteur de recherche « français ». La lecture de la dernière livraison du tableau de bord de la recherche[10] élaboré par la Commission européenne est explicite. Deux exemples : aux États-Unis, les cinq budgets annuels de recherche les plus importants sont investis par des entreprises du numérique (de 10 à 20 milliards de $) ; dans le classement européen, la première entreprise du numérique n'arrive qu'en 8ème position (4 milliards d'€) ; Alphabet, Huawei, Microsoft investissent chacun en recherche environ 20 milliards de $ chaque année !

Nous sommes d'un point de vue industriel vis-à-vis du numérique comme était la France en 1945 vis-à-vis de l'atome. Il suffit de lire, pour s'en convaincre, l'ordonnance de création du CEA[11]. Plutôt que de tenter de rattraper notre retard sur des technologies existantes, inventons les

technologies et les services de demain, pour le numérique et sa sécurité. Nous avons les chercheurs, les ingénieurs, les entrepreneurs nécessaires. Le fait que l'entreprise qui a déposé le plus de demandes de brevets en 2021[12] en Europe soit Huawei n'est pas une fatalité. Une dynamique a été initiée au sein du Campus Cyber qui rassemble des ressources publiques et privées. Pourrait-être étudiée l'opportunité de créer un Commissariat au numérique[13] qui rassemblerait les forces de recherche publiques de l'ensemble du territoire national et les communautés du logiciel libre. Une des premières missions de ce commissariat - virtuel dans un premier temps pour contourner les obstacles administratifs -, consisterait à établir la cartographie de la recherche nationale dont nous ne disposons que partiellement aujourd'hui. C'est un des effets délétères de la logique de guichets, d'appels à projets ou à manifestation d'intérêt : la méconnaissance du tissu national.
Un think tank dédié au numérique, d'ailleurs prévu par la revue stratégique du SGDSN en 2018, pourrait accompagner cette création.

J'en viens à l'articulation entre ce qui relève des administrations centrales et ce qui devrait être délégué.

C'est une des leçons que nous devons tirer de la gestion de la crise sanitaire : lorsque les régions ont été impliquées dans la lutte contre la COVID-19, tout est devenu plus efficace. Ainsi des vaccinations plus nombreuses grâce à la création de « vaccinodromes » au plus près des citoyens. Il nous faut envisager une crise virale informatique et la possibilité que nombre de particuliers, d'acteurs économiques, de collectivités territoriales et d'administrations soient infectés, par exemple par un rançongiciel. Nos modes d'action devraient également être décentralisés pour être plus efficaces.

En 2015, le Premier ministre a annoncé la création d'un GIP qui accompagnerait dans la sensibilisation et le traitement des attaques informatiques les publics que l'ANSSI ne pouvait assister directement. Maladroitement baptisé « Cybermalveillance.gouv.fr » par le SIG - encore un de vos (futurs) services -, suggérant que l'État crée une plate-forme de cybercriminalité, le GIP ACYMA est constitué début 2017 et rassemble des représentants de l'État, des utilisateurs, des prestataires et des offreurs

de solutions et de services. Il a créé une plate-forme de sensibilisation et d'assistance aux victimes d'actes de cybermalveillance en leur proposant une assistance de proximité construite sur l'adhésion à une charte de prestataires informatiques répartis sur tout le territoire national.

Dans le cadre du Plan de relance, l'ANSSI, qui bénéficie d'une enveloppe de 136 Millions d'euros, écrit aux présidentes et présidents de régions, quelques jours avant les élections régionales (!), pour leur proposer de créer un CSIRT, « *un centre de réponse aux incidents cyber au profit des entités implantées sur le territoire régional* », destiné à traiter « *les demandes d'assistance des acteurs de taille intermédiaire (ex : PME, ETI, collectivités territoriales et associations) et les [mettre] en relation avec des partenaires de proximité : prestataires de réponse à incident et partenaires*[14]». L'agence s'engage à subventionner les régions volontaires pendant trois ans, à charge de ces régions d'inventer le modèle économique susceptible de prolonger la vie du CSIRT. Outre le fait que seules sont aidées les régions candidates, que le financement n'est assuré que pour trois ans, ce dispositif, lorsqu'il sera opérationnel, fera doublon avec celui créé en 2017.

Ce n'était apparemment pas suffisamment entropique. En janvier dernier, a ainsi été annoncée la « *mise en place d'un équivalent numérique de « l'appel 17 » afin que chaque citoyen puisse signaler en direct une attaque cyber et être mis immédiatement en relation avec un opérateur spécialisé*[15] ».
Il est difficile de proposer une action publique plus illisible et moins économe de l'argent des Françaises et des Français ! Là encore une action d'ensemble, coordonnée et lisible par tous, s'impose.

Plus largement, nous devons mieux impliquer nos régions - toutes nos régions - dans ce domaine de la cybersécurité, notamment au nom de leur mission de développement économique. En s'appuyant sur Cybermalveillance.gouv.fr et les préfectures, elles sont le bon niveau administratif pour mettre en place les politiques qui prennent en compte les caractéristiques humaines, industrielles et universitaires de leur territoire. Elles ont également la clé de notre résilience. Ce sont elles qui devront faire face demain aux conséquences en termes de sécurité du développement des villes et territoires « intelligents » dont l'État ne se

préoccupe pas aujourd'hui malgré les concrétisations rapides de ces projets - voir le dispositif ONDIJON porté par la Métropole de Dijon.

Pour conclure cette lettre trop longue, quelques mots sur l'Europe et l'international qui mériteraient également un développement important.

La guerre en Ukraine a obéré la visibilité de la présidence française du Conseil de l'Union européenne dans d'autres domaines que celui de la diplomatie. Or les initiatives en matière de cybersécurité et de numérique sont désormais davantage portées par la Commission que par la France. L'action à mener dans les années à venir devrait également porter sur la redéfinition des aides publiques au niveau européen pour que soit soutenue une véritable politique industrielle, à l'image de ce que font les États-Unis ou la Chine.

À l'international, a été lancé en 2018 « l'Appel de Paris[16] » issu d'une conférence internationale organisée par l'ANSSI à l'UNESCO en 2017. Les diplomates ont réussi à faire signer ce début d'engagement au respect de certaines règles à plus de 80 États, dont les États-Unis, 700 acteurs économiques et près de 400 ONG. Mais, en cinq ans, seuls des groupes de travail ont été créés, et encore, début 2021 seulement. La France dispose avec cet appel d'un instrument qui peut pacifier le cyberespace, à un moment de l'Histoire où tout est possible et où une attaque informatique serait susceptible de conduire à la mort de vastes populations, à la destruction d'infrastructures vitales, à l'arrêt d'économies entières. Il y a quelques années, le chef du Conseil de sécurité russe, Nikolaï Patrouchev, avait indiqué au secrétaire général de la défense et de la sécurité nationale que tant qu'il n'y aurait pas de traité international encadrant et limitant l'action offensive des États dans le cyberespace, la Russie ne s'interdirait rien. Il est temps d'agir aussi pour redynamiser les actions dans le cadre de l'Appel de Paris.

L'OCDE, avec l'animation active de l'ANSSI, a réalisé un travail de fond sur les vulnérabilités logicielles[17], qui a fait consensus parmi ses 38 pays membres. Nous avons la chance d'avoir parmi les entreprises françaises des championnes de ce sujet qui, bien mené, par exemple en abordant la question du marché gris, peut avoir un impact significatif sur la

cybersécurité mondiale et ainsi renforcer la place de la France.

Vous le voyez, la cybersécurité recouvre des sujets bien plus larges que « seulement techniques ».

Elle est aujourd'hui un pilier de nos sociétés dans lesquelles s'accélère la fusion entre le numérique et l'activité humaine - et demain avec le corps humain. Dans ses aspects défensifs et offensifs, la cybersécurité est un enjeu majeur pour notre développement économique, social, pour notre sécurité globale, pour notre place sur la scène internationale.

Monsieur le (futur) Premier ministre, votre fonction vous oblige.

Parution le 15 avril 2022

[1] https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000045537693
[2] https://www.elysee.fr/emmanuel-macron/2017/07/13/discours-d-emmanuel-macron-a-l-hotel-de-brienne
[3] http://www.sgdsn.gouv.fr/evenement/revue-strategique-de-cyberdefense/
[4] Décrets du 10 avril 2009 : https://www.legifrance.gouv.fr/loda/id/JORFTEXT000038359072/ et du 14 août 2020 : https://www.legifrance.gouv.fr/loda/id/JORFTEXT000042237946/
[5] https://www.gouvernement.fr/sites/default/files/contenu/piece-jointe/2021/02/210218_dp_cyber_vfinale.pdf?v=1645019943
[6] https://www.gouvernement.fr/actualite/strategie-nationale-pour-la-securite-du-numerique-un-bon-equilibre-entre-prise-en-compte-de-la-3075
https://www.ssi.gouv.fr/actualite/la-strategie-nationale-pour-la-securite-du-numerique-une-reponse-aux-nouveaux-enjeux-des-usages-numeriques/
[7] https://www.elysee.fr/emmanuel-macron/2021/02/18/strategie-nationale-cybersecurite
[8] La palme revient sans doute à l'AMI sur l'identité numérique ouvert sur une période de 14 jours ! https://www.entreprises.gouv.fr/fr/aap/numerique/politique-numerique/appel-manifestation-d-interet-sur-l-identite-numerique
[9] Réf : 758/ANSSI/DIR/NP du 24 mars 2022.
[10] The 2021 EU industrial R&D investment scoreboard
https://iri.jrc.ec.europa.eu/sites/default/files/contentype/scoreboard/2021-12/EU%20RD%20Scoreboard%202021%20FINAL%20online.pdf
[11] https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000521964/
[12] https://www.epo.org/news-events/news/2022/20220405_fr.html
[13] Je sais que cette proposition avait été portée sans succès au cabinet de Lionel Jospin alors Premier ministre.
[14] https://www.ssi.gouv.fr/agence/cybersecurite/france-relance/programme-dincubation-de-csirt/
[15] https://www.elysee.fr/emmanuel-macron/2022/01/10/deplacement-du-president-de-la-republique-a-nice
[16] https://pariscall.international/fr/
[17] https://www.oecd.org/fr/numerique/ieconomie/securite-numerique/

Le pilotage au cœur de la gestion de la crise cyber

JEROME SAIZ
Président-fondateur
OPFOR Intelligence
Senior advisor du CyberCercle

L'ingrédient secret au cœur de la crise, c'est le pilotage ! Le séquençage des multiples actions - souvent interdépendantes - et l'alignement d'objectifs parfois opposés exige en effet une vision transverse, unifiée ainsi que la capacité d'alterner sans cesse entre une grande attention aux détails et la prise de décisions rapides, forcément « à la serpe ». Et le tout, généralement, alors qu'aucune de ces décisions n'est véritablement satisfaisante.

C'est pourquoi le casting du pilote, et notamment sa capacité à coordonner les opérations de manière transverse, sera l'un des éléments déterminants du succès de la gestion de crise.

Bien sûr, chaque acteur du dispositif de crise participe activement à son succès. Mais le rôle du pilote est à part : ni expert technique, ni spécialiste métier, ni dirigeant, il doit pourtant faire preuve de bonnes connaissances dans tous ces domaines afin d'organiser l'effort collectif, saisir les enjeux globaux aussi bien que spécifiques, séquencer les opérations ou encore éclairer les risques, autant sur les plans techniques, juridiques ou de la communication.

Le tout au sein du chaos que peut représenter l'état de crise.

Aussi convient-il de se pencher sur le profil et les responsabilités de ce chef d'orchestre qui sera au cœur de la gestion de crise cyber.

Le profil du pilote

Pour l'Agence nationale de la sécurité des systèmes d'information (ANSSI), qui l'a baptisé Responsable des Opérations de Cyberdéfense (ROC), il s'agit d'un rôle relativement récent dont la création a été motivée par la complexité croissante des cyberattaques[1]. Sa mission est alors « *d'accompagner la victime dans son processus de gestion de crise jusqu'au rétablissement de son activité* ».

La complexité croissante des attaques est donc la raison d'être du pilote de crise. Face à une malveillance numérique de plus en plus souvent transverse, et dont l'impact sur l'entreprise l'est tout autant, la réponse ne peut qu'être, elle aussi, transverse. Cette transversalité est le socle même de la valeur ajoutée du pilote de crise. Celui-ci doit être autant à l'aise au sein de la DSI lors des points d'étapes techniques que dans ses échanges avec l'équipe de réponse à incident en charge de l'investigation numérique, qu'auprès du RSSI qu'il conseillera sur le déploiement de nouvelles solutions de cybersécurité, ou encore face au comité de direction de l'entreprise, où il devra faire preuve de pédagogie afin de présenter les situations, les options et les risques. Car, *in fine*, son rôle est de fournir aux dirigeants les moyens de prendre des décisions éclairées dans une situation qui ne l'est pas !

Priorité aux « soft skills »

À un socle de solides connaissances techniques (probablement issues d'un parcours préalable dans le conseil en cybersécurité), le pilote de crise doit ajouter une forte capacité organisationnelle et surtout une série de « *soft skills* », des compétences interpersonnelles et de communication plus difficiles à évaluer de manière formelle. Parmi celles-ci, l'on retrouve notamment les capacités d'écoute, de synthèse, de communication, ainsi que l'empathie, la ponctualité, l'attention aux détails, la capacité à résoudre les conflits, à organiser le chaos, à mener plusieurs tâches de front… et tant d'autres pour lesquelles n'existe aucun diplôme !

Bien que difficiles à évaluer, ces caractéristiques sont pourtant essentielles tant la journée du pilote de crise se déroulera au contact d'interlocuteurs variés aux attentes diverses et aux niveaux de connaissance (technique, no-

tamment) hétérogènes. Pire : chacun aura à cœur de résoudre au plus vite les problèmes sur son propre périmètre, parfois au détriment des autres et surtout en dehors de toute logique de séquençage (certaines activités doivent être opérationnelles avant d'autres). C'est alors le rôle du pilote non seulement de proposer les méthodes et l'organisation qui permettront d'atteindre les objectifs de la gestion de crise sans s'égarer (notamment le redémarrage de l'activité en toute sécurité), mais aussi d'aligner les attentes de chacun et, parfois, de calmer les ardeurs.

Les responsabilités du pilote au déclenchement de la crise

À l'activation du dispositif de crise, le pilote aura la responsabilité de suivre la montée en charge du dispositif, du gréement des différentes cellules au suivi des premières actions techniques, en passant par la compilation des premières synthèses managériales. Il n'est certes pas en charge de ces différentes actions (le plan de gestion de crise en a identifié chacun des responsables au préalable), mais il doit s'assurer qu'elles ont bien lieu, et alerter si ce n'est pas le cas. Ainsi, dès les premiers instants de la crise, le pilote est le garant de la structure du dispositif, quelle que soit la situation sur le terrain. C'est lui qui fait toute la différence entre la théorie (le plan de gestion de crise) et la réalité (composer avec absences, les indisponibilités de solutions techniques essentielles, les erreurs inévitables, l'effet de sidération dû à un impact majeur, etc.)

Enfin, son positionnement hiérarchique est important : si une certaine séniorité est un atout, il est préférable que le pilote ait un statut d'expert autonome et ne soit pas *dans* la hiérarchie, où il pourrait se heurter alors à des conflits d'intérêts ou subir des pressions inutiles. C'est pourquoi le rôle est souvent confié à un expert externe, un consultant soit intégré au dispositif de réponse à incident tiers (l'avantage d'un regard neuf), soit partenaire régulier de l'entreprise (l'avantage de déjà bien connaître le contexte d'intervention).

Le pilote est prêt ? Il est temps de plonger dans la crise…

Parution le 6 mai 2022

[1] https://www.ssi.gouv.fr/agence/cybersecurite/plans-gouvernementaux/stephane-sans-responsable-doperation-de-cyberdefense-au-sein-du-centre-operationnel-de-lanssi/

Institution judiciaire et lutte contre la cybercriminalité : orientations et perspectives

MYRIAM QUEMENER
Avocat général
Docteur en droit

La cybercriminalité est devenue un véritable fléau et a coûté plus de 6000 milliards de dollars (5.700 milliards d'euros[1]) au monde l'an dernier selon le patron du géant italien de l'aéronautique et de la défense Leonardo, Alessandro Profumo. Le nombre d'attaques informatiques signalées à l'ANSSI[2] (Agence nationale de la sécurité des systèmes d'information) a augmenté de 37% entre 2020 et 2021.

Par ailleurs, la cybercriminalité est de plus en plus une délinquance financière et organisée. Cet aspect est d'ailleurs souligné par le dernier rapport du GAFI[3] : la transformation technologique du secteur financier, notamment avec l'apparition de nouveaux produits comme les actifs numériques, crée de nouvelles vulnérabilités. La nature transfrontalière de ces nouveaux services et la digitalisation complète des relations d'affaires continuent aussi de poser des défis en constante évolution, en particulier dans un contexte où le recours à ces nouveaux dispositifs se matérialise de manière croissante dans les affaires de blanchiment et de financement du terrorisme.

Outre la lutte contre les cyberattaques qui portent atteinte aux intérêts fondamentaux de l'État, le rapport relève que l'on assiste au développement d'une cybercriminalité de masse. La traditionnelle économie souterraine se trouve complétée par une cyber économie parallèle qui constitue une menace criminelle certaine, mais également un trouble à l'ordre public et

judiciaire tant le nombre de particuliers victimes est en augmentation, comme l'ont démontré les attaques dont certains hôpitaux ont été victimes en février 2022.

Dans ce contexte, il convient de présenter les dernières orientations de l'institution judiciaire en matière de lutte contre la cybercriminalité ainsi que les perspectives à envisager.

Une politique pénale pour la lutte contre la cybercriminalité

Le nouveau rapport de politique pénale du garde des Sceaux[4] déposé au Parlement en mai 2022[5] aborde la lutte contre la cybercriminalité dans la partie du document concernant l'accompagnement des évolutions de la société. Compte tenu de l'ampleur de ce fléau, il gagnerait même à l'avenir à figurer dans la partie du rapport sur le renforcement des politiques pénales prioritaires.

Il faut également noter que la direction des affaires criminelles et des grâces (DACG) avait déjà en 2021[6] fixé les axes stratégiques afin que soient regroupées à la juridiction parisienne les cyberattaques par rançongiciel.
L'ANSSI et le ministère de la justice ont aussi publié un guide pour sensibiliser les entreprises et les collectivités[7] .

Le ministère de la Justice a mis en place une politique pénale dynamique afin de répondre aux évolutions des phénomènes cybercriminels, en s'engageant notamment, avec les partenaires interministériels, auprès du Secrétariat général de la défense et de la sécurité nationale (SGDSN) pour contribuer aux travaux stratégiques en matière d'atteintes cyber aux intérêts fondamentaux de l'État et pour consolider chacun des acteurs dans la poursuite de ses finalités, en particulier, pour ce qui concerne l'autorité judiciaire, l'action de la section J3 du parquet de Paris composée de magistrats spécialisés en la matière.

En plus du développement des plateformes de signalement en ligne de ces infractions gérées par le ministère de l'Intérieur, les services du ministère

de la Justice accompagnent la création d'un observatoire de la menace cyber afin de mieux connaître l'ampleur de cette cybercriminalité. Concernant la cybercriminalité de haute intensité, le parquet de Paris, au titre de sa compétence concurrente, a connu une augmentation qui donne lieu à des développements inquiétants et nécessite à la fois des actions de sensibilisation et des travaux à l'international.

Enfin, il faut souligner que des magistrats « cyber-référents » formés et identifiés au sein de chaque parquet sont régulièrement réunis par la chancellerie (DACG) et fonctionnent en réseau, ce qui permet de renforcer le niveau de spécialisation et de prise en compte judiciaire de ce contentieux en évolution permanente.

La lutte contre la haine en ligne

Le rapport de politique pénale du garde des Sceaux présente le pôle national de lutte contre la haine en ligne[8] (PNLH) créé en janvier 2021 au sein du tribunal judiciaire de Paris, chargé de centraliser, sous la direction du procureur de Paris, le traitement des affaires significatives de cyber-harcèlement et de haine en ligne[9] . Ce pôle a établi un véritable dialogue avec les opérateurs de réseaux sociaux. Doté de deux magistrats, trois greffiers, deux juristes-assistants et d'un assistant spécialisé, il doit permettre d'apporter une réponse visible et unifiée là où ce type de phénomène amenait souvent chaque parquet territorial à répondre aux seuls faits commis par les auteurs identifiés sur son ressort. Durant l'année 2021, le pôle a été saisi de 502 procédures, provenant en partie de la plateforme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements (PHAROS), rattachée à l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC).

Outre la création de ce pôle et la participation de la direction des affaires criminelles et des grâces à l'observatoire de la haine en ligne, l'engagement du ministère de la Justice pour lutter contre cette haine en ligne s'est aussi traduit par l'adoption du décret n° 2020-1444 du 24 novembre 2020 pris pour l'application de l'article 15-3-3 du code de procédure pénale qui a désigné le tribunal judiciaire de Paris comme juridiction compétente

disposant d'une compétence nationale concurrente pour les délits de harcèlement sexuel ou moral à caractère discriminatoire.

Les actions de coordination avec les associations, comme par exemple Respect zone[10], en matière de prévention sont également essentielles et doivent encore se développer.

De plus, la loi du 24 août 2021 confortant le respect des principes de la République a notamment créé un nouveau délit de mise en danger par la diffusion sur les réseaux sociaux de messages vindicatifs comportant des éléments permettant d'identifier ou de localiser une personne pour qu'il lui soit porté une atteinte grave (article 223-1-1 du code pénal), et a rendu applicable les poursuites accélérées pour les abus les plus graves de la liberté d'expression (comparution immédiate et convocation par procès-verbal). Enfin, les bonnes pratiques développées par les juridictions et les services déconcentrés sur cette thématique sont à relever.

L'accent sur les opérations internationales

La spécificité des cyber-enquêtes nécessite très fréquemment des investigations à l'étranger et donc de la coopération internationale, en particulier avec les États-Unis, afin d'accéder aux données de souscription de trafic ou de contenu nécessaires pour l'enquête.

Récemment, une opération de police internationale dénommée Tourniquet a permis d'arrêter les gérants du plus important site de revente de données piratées, RaidForums. Les investigations poussées des cyber-enquêteurs du Royaume-Uni, des États-Unis, d'Allemagne, de Suède, du Portugal et de Roumanie ont abouti au démantèlement total de cette plateforme criminelle.

RaidForums vendait en accès libre des bases de données volées appartenant à un certain nombre de sociétés américaines. L'infrastructure du réseau a été saisie et l'administrateur de la plateforme ainsi que deux de ses complices ont été arrêtés, affirme le site d'Europol.[11]

Le commerce du trafic de données sur RaidForums est apparu en 2015

et, très vite, ce site a accédé à une notoriété internationale en raison de la facilité avec laquelle ses utilisateurs récupéraient les informations subtilisées. N'importe qui, en fait, pouvait se les procurer contre une somme d'argent évidemment, et de préférence en monnaie virtuelle de type bitcoin.
L'institution judiciaire est très active au niveau des négociations à l'international. On peut citer par exemple le Protocole Additionnel à la Convention sur la cybercriminalité (« Convention de Budapest »), destiné à renforcer la coopération et la divulgation des preuves électroniques, qui a été ouvert à la signature lors d'une conférence internationale organisée les 12 et 13 mai à Strasbourg - sous la Présidence italienne du Comité des Ministres du Conseil de l'Europe. Le Protocole additionnel répond à ce défi et fournit des outils comme la coopération directe avec les fournisseurs de services et les bureaux d'enregistrement, des moyens efficaces d'obtenir des informations sur les abonnés et des données relatives au trafic, une coopération immédiate en cas d'urgence ou des enquêtes conjointes - qui sont soumis à un système de droits de l'homme et d'état de droit, y compris des garanties en matière de protection des données.

Perspectives

Il apparaît nécessaire que l'institution judiciaire continue dans cette voie en étoffant ses services spécialisés et ses compétences de façon encore plus lisible, non seulement en première instance mais également en appel. Il conviendrait aussi de désigner des magistrats du siège cyber-référents pour que la cybercriminalité soit systématiquement traitée comme un véritable contentieux à part entière. A cet égard, l'ouverture du Campus Cyber de la Défense[12], qui réunit entreprises, services de l'État, organismes de recherche et de formation dans un même lieu, crée un écosystème de cybersécurité où l'institution judiciaire a toute sa place et pourra échanger et mieux connaître ses interlocuteurs.

Parution le 27 mai 2022

[1] https://www.lefigaro.fr/secteur/high-tech/la-cybercriminalite-a-coute-plus-de-6000-milliards-de-dollars-en-2021-20220510
[2] https://www.ssi.gouv.fr/uploads/anssi_rapport_activite_2021_fr.pdf
[3] hhttps://www.fatf-gafi.org/media/fatf/documents/reports/mer4/Rapport-Evaluation-Mutuelle-France-2022.pdf
[4] hhttp://www.justice.gouv.fr/publications-10047/rapports-thematiques-10049/rapport-de-politique-penale-du-garde-des-sceaux-2021-34404.html
[5] hRapport établi conformément à l'article 30 du code de procédure pénale
[6] hDépêche relative à la lutte contre la cybercriminalité de la Direction des affaires criminelles et des grâces DACG, ref / 2020 : 0064 /M12C
[7] hAttaques par rançongiciels, tous concernés, https://www.ssi.gouv.fr/actualite/rancongiciels-face-a-lampleur-de-la-menace-lanssi-et-le-ministere-de-la-justice-publient-un-guide-pour-sensibiliser-les-entreprises-et-les-collectivites/
[8] hhttps://www.lemonde.fr/societe/article/2021/07/08/les-debuts-discrets-du-pole-national-de-lutte-contre-la-haine-en-ligne_6087529_3224.html
[9] hCirculaire relative à la lutte contre la haine en ligne, N° NOR : JUSD2032620C, 24 novembre 2020
[10] hhttps://www.respectzone.org/
[11] hhttps://www.europol.europa.eu/media-press/newsroom/news/one-of-world%E2%80%99s-biggest-hacker-forums-taken-down
[12] hhttps://campuscyber.fr/

Renforcer la cyber résilience du secteur public : un enjeu crucial

ELENA POINCET
Co-fondatrice et CEO
TEHTRIS

Le secteur public est, comme le secteur privé, confronté de manière croissante aux cyberattaques, et ce d'autant plus avec la crise liée à la COVID-19 qui a impliqué un recours au télétravail et une digitalisation des services publics. Les administrations, les métropoles, les collectivités et les structures hospitalières, quelle que soit leur taille, sont particulièrement exposées à ces actes de cybercriminalité. L'obsolescence de leur parc informatique, la plus faible acculturation au numérique, l'utilisation croissante d'outils connectés engendrent un élargissement de la surface d'attaque qu'il est plus complexe à défendre… Autant d'enjeux à relever pour que le secteur public devienne cyber résilient.

Regardons de plus près les menaces et enjeux liés aux structures hospitalières, aux métropoles et collectivités locales. Le secteur de la santé a été particulièrement touché depuis 2017 avec les attaques Wannacry et NotPetya. Le système de santé britannique a notamment été paralysé. En France, les hôpitaux de Dax, d'Oloron-Sainte-Marie, de Villefranche-sur-Saône, Saint-Gaudens ou encore l'Assistance Publique - Hôpitaux de Paris (AP-HP) ont été touchés. Il est estimé qu'un établissement de santé est victime chaque semaine d'une cyberattaque. Quant aux métropoles et collectivités locales affectées par de telles attaques, la liste s'allonge si bien qu'il est plus difficile de la suivre…

Les acteurs sont particulièrement vulnérables pour plusieurs raisons.

Les métropoles, collectivités et les structures hospitalières sont en pleine transformation digitale avec une numérisation rapide des parcours « citoyens » et « patients ». Le recours aux dispositifs médicaux connectés, à la télémédecine, à la télésurveillance médicale, ou encore aux chatbots est croissant… Ces acteurs collectent et stockent une très grande quantité de données à caractère personnel. Ils disposent par ailleurs d'un parc informatique vaste et hétérogène au service des agents de la collectivité, des écoles et maternelles, des médiathèques, du public, des patients...
La chaîne logistique de ces écosystèmes devient dès lors plus complexe et engendre ainsi un élargissement de la surface d'attaque, rendant ces acteurs publics attractifs pour les cybercriminels.

La prise de conscience des risques cyber est aussi relativement limitée dans le secteur. Selon Cybermalveillance[1], 65% des communes de moins de 3 500 habitants pensent que le risque est faible, voire inexistant, ou ne savent pas l'évaluer. Seules 35% identifient un risque numérique élevé, voire très élevé, mais s'interrogent sur les moyens pour y pallier (budgets, outils, ressources humaines). L'utilisation d'outils personnels dans ces petites structures est aussi répandue.

Les menaces sont quotidiennes, qu'ils s'agissent d'une clé USB infectée, d'e-mail de phishing, d'attaques DDOS, de rançongiciels ou encore de vol de donneés combinée à du doxing[2].

Les attaques par phishing sont très efficaces. Ces attaques par ingénierie sociale visent à perturber le fonctionnement des structures, à voler les données, à récupérer une rançon en dupant les utilisateurs (médecins, tiers de confiance) qui sont de plus en plus pressés. Les ransomware constituent la menace la plus fréquente. Ces attaques contre les hôpitaux ont augmenté de 123% en 2021 par rapport à l'année précédente. Le coût par attaque de ransomware est en moyenne de 8 millions USD. Les attaques par déni de service (DDOS), qui visent à couvrir généralement une seconde attaque, sont aussi redoutables.

Le vol de données est répandu. Les données constituent notre patrimoine et valent de « l'or » pour les cybercriminels. Les métropoles, collectivités locales et hôpitaux regorgent d'informations sensibles : données personnelles (noms, dates de naissance, numéros de sécurité sociale, adresses, numéros de téléphone), documents de recherche, informations sur la propriété intellectuelle… L'espionnage est une réalité et ces données récupérées alimentent le marché du darkweb. Un dossier médical peut valoir par exemple jusqu'à 350 USD sur le marché noir, soit 50 fois plus qu'un dossier bancaire[3].

Les conséquences de telles attaques sont de plusieurs ordres.
Financières d'abord. Ces actes nécessitent la remise en service des systèmes informatiques et la récupération des données, avec potentiellement le paiement d'une rançon. Le secteur public est néanmoins moins disposé à la payer que les entreprises qui disposent de plus de moyens. Les coûts sont aussi liés à l'inactivité du personnel qui ne peut poursuivre son travail.

Humaines ensuite. D'une part, les cyberattaques affectent directement les citoyens qui se retrouvent privés de services et qui sont susceptibles de voir leurs données utilisées à mauvais escient (divulgation, suppression). Cela porte atteinte à la vie privée des individus. Le lien de confiance entre le citoyen et l'entité publique, dont l'image est dégradée, s'en trouve rompu. D'autre part, dans le secteur de la santé, les attaques peuvent impliquer en quelques secondes une paralysie du système d'un hôpital : SI, système de communication, scanners, IRM, pompes à perfusion. La vie des patients est dès lors en jeu. Imaginez que demain un robot de chirurgie soit contrôlé par un cybercriminel…

La question est désormais de savoir « quand » ces acteurs seront la cible d'une attaque, et non plus « si ». Le système d'information est au cœur du bon fonctionnement des opérations et doit être constamment en état de marche. Certes, on parle de sensibilisation et la dimension cyber doit être intégrée à la culture de ces structures. Mais la problématique de la cybersécurité ne peut pas porter uniquement sur l'utilisateur. Nous sommes actuellement dans une jungle numérique, constituée de matériels et de logiciels provenant la plupart du temps de l'étranger. Les systèmes d'informations et d'exploitations pour ordinateurs ou serveurs (Windows,

iOS ou encore Linux) présentent des failles ouvrant la voie à des cyberattaques.

Parallèlement, la surface d'attaque s'élargit, comme mentionné précédemment. Or, la chaîne des acteurs que composent ces écosystèmes complexes doit être sécurisée de bout en bout.

Dans ce contexte, les solutions qui reposent sur l'hyperautomatisation sont clés pour se protéger de ces cyberattaques fulgurantes.
Les métropoles, collectivités et hôpitaux souhaitent de plus en plus faire évoluer et moderniser leur dispositif de cybersécurité afin d'y apporter une couche de sécurité supplémentaire. Pour se protéger de ces cyberattaques et des conséquences engendrées, ils recherchent des solutions performantes, souples, faciles à opérer et compatibles avec un antivirus existant. La préservation de la souveraineté et de l'intégrité des données (aussi bien des collaborateurs, des citoyens que des patients) est par ailleurs une préoccupation croissante. Enfin, lutter contre des attaques de plus en plus nombreuses et évoluées avec des équipes limitées est un enjeu clé pour ces acteurs. Rappelons qu'il est particulièrement difficile de recruter du personnel qualifié en sécurité informatique.

Il a été démontré qu'une attaque pouvait ne durer que 37 minutes, entre l'intrusion, l'exfiltration des données et le déploiement du ransomware sur un parc numérique. Face à ces menaces, les équipes responsables des systèmes d'information ne peuvent pas s'en sortir en recourant seulement à de la détection pour certains et à de la neutralisation gérée par l'humain pour d'autres. Aujourd'hui, les outils traditionnels, les anti-virus, ne suffisent plus pour se protéger. Adopter une technologie pensée et conçue pour simplifier, centraliser et orchestrer permet aux analystes de se concentrer sur des tâches à haute valeur ajoutée.

Pour assurer la protection en temps réel de son parc informatique, la proactivité et la réactivité sont désormais cruciales. Il est alors important d'intégrer une solution hyper automatisée qui permet d'effectuer la détection, l'analyse, la mise en quarantaine et la remédiation en temps réel. Grâce au machine learning et au deep learning, les aspects subtils des menaces qui seraient invisibles à l'œil nu sont détectés. Ces techniques

permettent de mieux connaître les comportements des cybercriminels et de prévenir les attaques.
En 2022, le secteur public doit pouvoir se défendre et être protégé du cyber espionnage et du cyber sabotage. Recourir à une solution de sécurité efficace, hyper automatisée permettant une visibilité à 360° et une couverture globale est primordiale. Pour une protection optimale des données, il convient enfin de s'assurer que les solutions de cybersécurité utilisées soient « secure and ethics by design ». Il est effectivement crucial que les logiciels soient conçus, produits, configurés en tenant compte, dès la conception et par défaut, de la vie privée et de la sécurité du contenu des fichiers protégés.

C'est en prenant en compte ces enjeux et en recourant à des technologies performantes et souveraines, de détection et de neutralisation en temps réel et sans action humaine, que le secteur public sera en mesure de renforcer sa résilience.

Parution le 17 juin 2022

[1] Etude : la sécurité numérique dans les collectivités françaises de moins de 3 500 habitants (mai 2022)
[2] Divulgation de données personnelles
[3] Proofpoint, paysage des menaces dans le secteur de la santé (2020)

Les ports, nouvel enjeu de la cyber résilience de la chaine d'approvisionnement logistique !

JEROME BESANCENOT
Directeur de projet transition numérique
HAROPA PORT

Le secteur portuaire : une interdépendance mondiale face au risque cyber

Les différentes et récentes crises internationales (Covid, Ever Given, conflit en Ukraine) ont illustré de manière diverse la fragilité de nos chaines d'approvisionnement et l'importance des ports pour garantir le ravitaillement des nations.

Ces crises génèrent des désorganisations chroniques dans les chaines logistiques qui peinent à revenir à leur vitesse de croisière du fait de pénuries sur certaines matières premières et de congestions portuaires faisant suite à une reprise soutenue des exportations.

Ces congestions induisent des difficultés de planification des escales dans les ports et notamment dans le fonctionnement des opérateurs terminaux qui font face à de très forts surcroits d'activité.

Les ports entrainés dans cette spirale doivent recourir à des outils numériques toujours plus sophistiqués pour préparer l'arrivée des navires, assurer leur navigation en sécurité, synchroniser les actions des différents acteurs intervenant sur les opérations portuaires et faciliter le passage des marchandises en interconnexion avec les acteurs du pré post acheminement.

L'usage de données numériques massives comme le Big Data, les développements de nouveaux services à valeur ajoutée grâce à l'Intelligence Artificielle (IA), le « deep learning », l'IoT ou des moyens de communication toujours plus puissant comme la 5G, conduisent les ports à se doter d'environnements virtuels comme les jumeaux numériques (Digital Twin), pour optimiser leurs activités toujours plus complexes et s'adapter rapidement aux enjeux économiques, politiques et environnementaux.

Cette accélération numérique vertigineuse s'inscrit dans une exigence pour les ports, d'offrir une meilleure qualité de services à leurs clients notamment en garantissant une traçabilité complète sur les marchandises, leurs statuts et les moyens de transport au bénéfice d'une chaine d'approvisionnement plus performante et qualitative. Cette volonté pousse ainsi les ports à s'intégrer toujours plus loin avec les outils numériques des logisticiens, en ouvrant en particulier leurs interfaces applicatives pour systématiser les interconnexions nécessaires aux échanges d'informations. Depuis quelques années, la cybersécurité portuaire et maritime est devenue un enjeu majeur qui interroge l'ensemble des organisations internationales sur la nécessité d'assurer une cyber résilience globale du commerce maritime, et en particulier la cyber résilience de la chaine d'approvisionnement. Dans ce contexte, les ports devenant tributaires de la sophistication de leurs outils numériques, deviennent des maillons cyber sensibles de la logistique.

En effet les acteurs ne peuvent plus travailler seulement en silo, il est nécessaire d'intégrer le risque cyber avec une vision élargie des processus d'activités et leur criticité. Les ports ne doivent plus considérer que le risque cyber n'est qu'affaire de stratégie individuelle, il faut adresser ce risque collectivement. Un port lourdement impacté par une crise cyber va engendrer inévitablement des désorganisations d'escales sur les autres ports auxquels il est connecté, voire un risque de propagation de la cybermenace via les systèmes et données partagés entre les parties prenantes.

Le risque cyber se dissémine au-delà des organisations ou des Etats, la chaine d'approvisionnement est un réseau propice à la circulation de la

menace. Un port ne pouvant être considéré comme « étanche », il faut donc bien renforcer la cybersécurité de l'ensemble des ports.
L'IAPH (Association Internationale des Ports) a souligné récemment au travers d'un guide spécifique[1] sur la cybersécurité portuaire l'ampleur de ce nouveau risque mondial, où certains ports accélèrent leur numérisation au détriment de la prise en compte du risque cyber, pouvant ainsi conduire à une fracture entre des ports mieux armés et ceux qui resteront ultra vulnérables.

Pour construire une cyber résilience globale, il est légitime pour chaque port de se pencher d'abord sur sa propre résilience, toutefois il est primordial d'être attentif à favoriser aussi la sécurité des ports auxquels il est relié, et ainsi contribuer au maintien du bon fonctionnement de la chaine d'approvisionnement logistique mondiale.

Cette considération élargie n'est pas simple à mener, car l'activité mondiale du commerce maritime est assurée par une succession d'acteurs, de nombreux systèmes hétérogènes interconnectés et des données massives transitant au travers de ces systèmes et applications, constituant plutôt une toile de systèmes qu'un système unitaire homogène. En poussant ce raisonnement, il devient presque illusoire de vouloir maitriser et identifier globalement l'ensemble de ces actifs. Cela revient un peu à faire face à une architecture informatique, dont personne ne peut maitriser la vision d'ensemble et donc les risques qui pourraient survenir.

Comment s'organiser mondialement pour renforcer globalement la cybersécurité portuaire ?

Les cyberattaques contre les ports sont souvent perturbatrices et coûteuses. Elles peuvent générer des dégâts matériels en perturbant les processus métiers mais aussi des dégâts immatériels en perturbant le fonctionnement des systèmes numériques IT ou OT.
Ces perturbations peuvent même affecter le fonctionnement d'un pays et entraîner des répercussions politiques et économiques majeures.
Les dirigeants d'entreprises portuaires, d'installations portuaires ou de ports doivent prendre en compte la gestion des risques cyber au premier niveau, et définir une stratégie de résilience pour maintenir des conditions

de fonctionnement opérationnel.

Sur le plan international, il existe dorénavant des guides et des méthodes pour aider les ports à progresser et à s'organiser pour traiter les menaces cyber. L'ENISA[2] (Agence européenne chargée de la sécurité des réseaux et de l'information), l'IAPH avec l'OMI (Organisation Maritime Internationale) proposent ainsi des outils méthodologiques qui permettent aux dirigeants de travailler sur ce sujet avec efficience et de se concentrer sur des étapes clés favorisant une montée en charge rapide : identification des risques et vulnérabilités, les parties prenantes, les systèmes informatiques et industriels, l'importance des données, etc.

La notion d'opérateur de services essentiels proposée par la directive NIS de l'Union Européenne amène un premier niveau d'incitation des ports à travailler globalement à l'échelle internationale sur le sujet et à suivre une certaine méthodologie, notamment pour identifier le caractère critique d'un système numérique et définir un plan d'action au regard des risques inhérents. L'OMI réfléchit aussi pour qu'au niveau mondial, le cyber risque soit désormais appréhendé sous l'angle de la conformité. Cela a conduit à l'évolution en 2021 pour les navires du code ISM, et fait l'objet de réflexions autour du code de sûreté ISPS pour une prise en compte par les ports d'une politique de cybersécurité plus affirmée.

Néanmoins, ces différents guides ne peuvent adresser toutes les particularités des systèmes et des risques associés. Afin de garantir aux ports dans l'avenir une interconnexion et une interopérabilité mondiales accrues et sécurisées, il convient de travailler en premier lieu sur les systèmes communautaires portuaires qui assurent les échanges d'informations au niveau local pour une communauté ou au niveau international pour le commerce maritime.

Un premier sujet d'investigation porte donc légitimement sur les systèmes communautaires informatiques dits PCS (Port Community System) qui restent la véritable pierre angulaire de l'organisation prévisionnelle et opérationnelle de l'escale, son suivi, et du passage des marchandises et des passagers. Ces outils sont également la source principale des données numériques utilisées par les jumeaux numériques portuaires.

Ces systèmes assurent un fonctionnement optimisé du port sur le plan opérationnel mais aussi administratif. Sur ce dernier volet, les PCS jouent un rôle essentiel pour faciliter la transmission des informations réglementaires obligatoires aux Guichets Uniques (GU) maritimes ou douaniers de chaque Etat. Ces derniers sont des instruments fondamentaux dans la facilitation du commerce international et de la sécurité du transport par voie maritime. De fait, les PCS et les GU offrent une interconnexion et une interopérabilité accrues entre les acteurs du transport maritime, et la réutilisation de données massives électroniques. Les PCS gèrent des milliers de connexions et échangent des millions d'informations. Ils sont reconnus comme des outils référents nécessaires à l'interfaçage du monde maritime, portuaire et logistique. Leur forte expansion dans les ports (voire aéroports) démontre leur pertinence pour la chaine d'approvisionnement.

La cybersécurisation globale des systèmes portuaires, un enjeu de résilience et de souveraineté

Les PCS sont principalement développés par des sociétés de services informatiques ou par des autorités portuaires. Ils permettent d'automatiser, de sécuriser, de fluidifier les processus métiers liés aux escales ou aux marchandises, et sont les traits d'union avec les chargeurs, les commissionnaires de transport, les opérateurs de terminaux, les compagnies maritimes et les plateformes logistiques multimodales qui utilisent les ports. Ils jouent un rôle majeur dans la chaine de valeur au titre des importations et exportations.
Pour cette raison, il parait important d'orienter les travaux de cybersécurité sur le rôle et la place de ces systèmes dans les écosystèmes portuaires, d'avoir un regard à 360° pour examiner l'existence de menaces cyber et anticiper les risques relatifs.

Un travail préalable doit porter sur les interfaces et interconnexions des PCS avec les systèmes des acteurs portuaires, maritimes ainsi que les GU. L'objectif est clairement de sécuriser les échanges de données en sanctuarisant certains canaux de connexion (emails, interfaces hommes machines, EDI, API etc.). Ces derniers restent encore très diversifiés et

reposent trop souvent sur des protocoles plus ou moins sécurisés. L'idée ici est d'harmoniser les méthodes d'échanges en tenant compte du caractère de sensibilité de l'information et l'importance de sa disponibilité. Il serait illusoire et coûteux de vouloir tout surprotéger, il faut aussi considérer les capacités technologiques, la complexité des solutions et la capacité des acteurs à les mettre en œuvre. Autrement dit, éviter de compliquer l'organisation des clients avec des solutions complexes et contraignantes quand cela n'est pas nécessaire. L'important est d'assurer une démarche progressive et ciblée en fonction des besoins et des risques associés. Généralement, les échanges peuvent s'appuyer sur des réseaux privés virtuels (VPN) entre acteurs qui se connaissent et échangent régulièrement des informations. Ces solutions ne sont malheureusement pas toujours adaptées quand les acteurs échangent de manière plus sporadique. Comment maintenir l'accès aux PCS sans imposer systématiquement une protection additionnelle délicate. Les PCS évoluent et intègrent de plus en plus ces composantes au sein de leur offre de service pour sécuriser les clients graduellement en fonction de leurs besoins. Il convient à présent de normer plus formellement ces services en fonction de la nature des échanges, afin de partager ces bonnes pratiques entre les ports.

Un autre axe de travail doit utilement s'orienter sur les données dites essentielles à l'activité portuaire. Pour sécuriser les systèmes au-delà des interfaces, une approche complémentaire porte sur l'accès à la donnée elle-même qui doit faire l'objet d'une stratégie de renforcement plus poussée selon la nature sensible de la donnée, avec notamment des mécanismes de vérification de l'identité numérique de l'accédant et de ses droits d'accès assortis. Comment s'assurer que ces données restent suffisamment sécurisées pour être utilisées sans risque dans des activités sensibles tel le guidage du navire et sa mise à quai ? Les PCS s'appuient toujours davantage sur les outils de navigation électronique maritime fournissant des données de positionnement AIS/GNSS ou encore de bathymétrie par le biais de cartes électroniques côtières. Au-delà de la sensibilité de la donnée, il est aussi intéressant de se pencher sur sa temporalité notamment quand elle est critique mais qu'en plus elle varie fréquemment. Une fragilité potentielle peut survenir du fait d'une désynchronisation sur la valeur de la donnée entre les systèmes des acteurs. Un constat récurrent

montre que certaines données électroniques sensibles, quoique partagées, sont parfois dupliquées et stockées dans chaque système des parties prenantes, afin de préserver une forme de résilience de fonctionnement quand les interfaces sont indisponibles. Cette pratique augmente les risques d'incohérence sur les données, et donc les risques de voir se propager aisément des informations corrompues volontairement ou involontairement entre les acteurs. Des technologies de contrôle sur la valeur de la donnée pourraient être profitables sur des informations critiques, obligeant par exemple une resynchronisation pour un usage sensible. En s'inspirant de technologie telle la blockchain, on pourrait dans certains cas favoriser un contrôle renforcé de cohérence sur la dernière valeur qualifiée (hauteur sous quille, position d'un navire, tirant d'eau, profondeur d'eau, etc.).

Enfin, le dernier axe porte sur la détection d'activités frauduleuses. Les développements en matière de cyber sécurisation doivent également s'orienter vers la recherche d'opérations douteuses ou fallacieuses afin de lutter contre les trafics illicites. Les systèmes portuaires sont de plus en plus la cible de pirates cyber pour justement faciliter l'organisation de ces opérations illégales. La détection de ces activités est très difficile et peut conduire à la recherche de signaux faibles dans l'environnement direct des systèmes portuaires ou de manière très indirecte dans l'activité foisonnante de la toile internet. L'innovation à base de IA pourrait aider à favoriser des recoupements permettant aux ports de mener des investigations complémentaires, d'améliorer leur système de protection, ou encore de sécuriser davantage les usages de leurs systèmes. Ce volet aujourd'hui n'existe pas réellement, car il reste très expérimental. Il offrirait une vision additionnelle des menaces identifiées et avérées par le M-CERT national. Il s'agirait ainsi de repérer la naissance d'un risque pour le PCS particulier d'un port.

En conduisant des efforts selon plusieurs axes, il devient possible d'améliorer la cybersécurité de bout en bout de l'ensemble des données publiques ou privées qui transite dans les systèmes portuaires ou qui est échangé entre les états membres au titre des missions de sureté et sécurité du territoire.

Dans cet esprit d'amélioration de la cybersécurité portuaire, HAROPA PORT, le Grand Port Maritime de Marseille, le Port de Toulon, le Grand Port Maritime de la Guadeloupe et France PCS (SOGET et MGI) ont été lauréats en novembre 2021 de l'appel à manifestation d'intérêt « sécuriser les territoires » grâce au projet d'innovation CYSPEO (Cyber sécurisation des sYStèmes PortuairEs Opérationnels). Ce consortium offre une large expertise en matière de systèmes d'information portuaires ainsi qu'en dématérialisation des processus métiers des ports de commerce.

Le projet repose sur des démonstrateurs opérationnels illustrant la capacité à innover dans le domaine de la cybersécurité portuaire pour améliorer la sécurité des ports français et renforcer leur position comme tiers de confiance numérique au sein de la chaine d'approvisionnement. Ces démonstrateurs, une fois validés, pourront être répliqués selon les besoins sur les territoires portuaires français.

La démarche initiale sera de définir un document de Politique de Sécurité des Systèmes d'Information (PSSI) mutualisé pour l'ensemble des ports français et leur écosystème d'acteurs. Ce document général favorisera une déclinaison opérationnelle pour chaque territoire en alignement avec les orientations de la Stratégie Nationale de Cybersécurité des Secteurs Maritime et Portuaire.

Par ailleurs, le projet contribuera à l'élaboration d'un Security Operation Center (SOC) mutualisé au bénéfice des places portuaires françaises. Ce SOC pourra superviser l'ensemble des PCS utilisés par les ports français et aider à repérer des comportements anormaux précurseurs de vulnérabilités ou d'attaques cyber. Il identifiera les menaces, recherchera les marqueurs de cyberattaques et veillera de manière globale à la sécurisation des échanges d'informations entre les acteurs et places portuaires.
Ce SOC contribuera à la fourniture d'informations clés pour le M-CERT national en charge de centraliser et de coordonner les réponses aux incidents portuaires et maritimes.

Les ports et le secteur portuaire s'organisent pour lutter contre la menace cyber en très forte augmentation. Les démarches isolées sont aujourd'hui

dépassées : il s'agit de gérer un risque qui ne se limite plus aux limites territoriales ni aux frontières. L'interconnexion des outils portuaires PCS aux outils informatiques des acteurs logistiques compose une architecture informatique polymorphe difficile à sécuriser globalement. C'est grâce à la capacité à travailler collectivement entre les ports pour renforcer la sécurité des PCS et la veille sur ces outils, qu'il sera possible d'anticiper et de réagir face aux attaques cyber. Le projet CYSPEO est une première démarche qui vise à mettre en œuvre une stratégie commune et à suivre une méthodologie unifiée pour assurer une gestion de risque adaptée et pertinente face aux enjeux de cybersécurité portuaire, et ainsi contribuer au renforcement de la souveraineté de l'Etat français en matière d'approvisionnement stratégique.

Parution le 24 juin 2022

[1] IAPH Cybersecurity Guidelines for Ports and Port facilities Version 1.0 (2021)
[2] Port Cybersecurity : Good practices for the Maritime Security (2019)
Cyber Risk Management for Ports (2020)

La BITD dans le cy(ber)clone

GENERAL DE CORPS D'ARMEE ERIC BUCQUET
Directeur du Renseignement et de la Sécurité de la Défense
Ministère des Armées

Le rapport d'information du Sénat[1] n°605 exposait mi-2020 les difficultés traversées par les entreprises de la BITD et celles qu'elles devraient encore affronter, principalement dans le champ des investissements indispensables à leur croissance. Ce rapport s'intitulait « l'industrie de défense dans l'œil du cyclone ». Face à la menace croissante et aux attaques régulièrement constatées, les 4 000 entreprises de la base industrielle et technologique de défense (BITD) mais aussi les 10 000 entités suivies par la DRSD au titre de la protection du potentiel scientifique et technique de la nation (PPST) ne connaissent pas le calme relatif et précaire de l'œil du cyclone. Elles sont dans le cy(ber)clone.

Cybercriminalité et cyberespionnage sont entrelacés et rendent cette menace particulièrement dangereuse car plusieurs effets néfastes peuvent se cumuler pour non seulement piller mais aussi, *in fine*, détruire leurs cibles.

Quelles peuvent être les conséquences principales de ces attaques ?

Je placerai deux conséquences comme étant les plus graves possibles.
La première est le coût économique pour l'entreprise qui peut subir toute une gamme de pertes financières, depuis la « simple » escroquerie de type arnaque au président ou FOVI[2] jusqu'à la double voire triple extorsion de type rançonnage à laquelle peut venir s'ajouter non seulement le

blocage de l'outil de production mais également l'exfiltration de données stratégiques et/ou personnelles (avec éventuellement une pression en cascade sur les victimes tierces). Cela peut conduire à la faillite d'une entreprise possiblement critique dans notre écosystème de défense. Sa mise en péril industriel pendant plusieurs semaines ou plusieurs mois, en raison de difficultés à assurer la livraison des commandes ou à facturer correctement ses clients, pourrait également fortement perturber en fin de chaîne de valeur la production d'un équipement stratégique.

La seconde est la compromission du secret de la défense nationale. Les niveaux de classification entrés en vigueur avec la nouvelle instruction générale interministérielle 1300 sur la protection du secret de la défense nationale il y a un an ont consolidé la notion de protection de l'information et rappelé le rôle essentiel qu'elle joue pour l'exercice des activités régaliennes de l'État. Si les textes particuliers régissant l'aptitude d'un réseau à accueillir des informations secrètes imposent un cadre qui rend particulièrement difficile leur accès, la compromission du secret est d'une gravité majeure car elle étend les conséquences de l'attaque cyber au-delà du périmètre de l'entreprise, pouvant même se porter jusque sur les équipements de nos forces armées.

A qui profite le crime ?

Qui sait si les données exfiltrées par des criminels l'ont été afin d'obtenir le paiement d'une rançon ou pour répondre à la demande d'un commanditaire, qu'il s'agisse d'un concurrent malveillant ou d'un service d'espionnage étatique ?

La mission de la DRSD, qu'elle soit de protection du secret de la défense ou de service enquêteur[3], l'oblige à répondre à ce type d'interrogation. Il est donc important qu'elle soit rapidement informée des incidents cyber touchant les entreprises de la BITD. La rapidité de réaction facilite en effet la mise en place du processus de levée de doute et permet d'aider l'entreprise à faire face efficacement aux conséquences.

Comment mieux protéger l'écosystème de défense et faire face aux attaques ?

Depuis 150 ans[4], la DRSD travaille à protéger le pays contre les menaces à l'encontre de la sécurité des militaires et de l'industrie de défense. Le Service a historiquement pour cœur de métier la contre-ingérence des forces et la contre-ingérence économique auxquelles s'ajoute depuis déjà plusieurs années la contre-ingérence cyber.

C'est à ce titre et pour compléter le dispositif national qu'il a été décidé en 2021 d'initialiser un projet de CERT[5] sectoriel dédié à la protection des entreprises du périmètre défense : le CERT-BITD[6]. Appuyé par les plus hautes instances du ministère des armées, ce projet bénéficie par ailleurs du programme d'incubation de l'ANSSI.

Quid de la protection dans les territoires ?

Une des forces de l'organisation de la DRSD repose sur son maillage territorial qui lui permet une proximité et une réactivité d'intervention locale, indispensable face aux attaques de plus en plus fulgurantes. Par ailleurs, les échanges quotidiens entre les entreprises de la BITD et les agents de la DRSD, que ce soit au cours des sensibilisations, inspections, audits, processus d'habilitation…, favorisent un climat de confiance utile à l'alerte en cas d'attaque cyber. Les équipes cyber de la DRSD en région seront ainsi progressivement dimensionnées pour répondre aux exigences du CERT-BITD et disposeront également de formations complémentaires adaptées. Elles seront ainsi pleinement en mesure d'assurer la primo-intervention, la levée de doute et le conseil adapté au durcissement de la sécurité du système compromis, particulièrement utile pour les petites et très petites entreprises, souvent les plus démunies en capacité cyber. Lorsque cela sera nécessaire, elles seront appuyées par les experts de la direction centrale.

A terme, le CERT-BITD offrira plusieurs services.
Le service le plus visible sera la réponse à incident. Ce dispositif permettra aux entreprises du périmètre de déclarer leurs incidents cyber grâce à une plate-forme spécifique et à la DRSD de réagir et de déclencher si besoin

l'envoi d'un élément d'intervention cyber.

Un autre service sera la veille en vulnérabilités. Le maintien d'une veille réactive est en effet indispensable pour être en mesure de détecter au plus tôt une propagation cyber malveillante.

Cela conduit naturellement au troisième service : la connaissance de la situation cyber[7]. La présence de la DRSD au Campus Cyber inauguré en février 2022 à La Défense favorisera naturellement cet aspect.

Enfin, le quatrième service recouvrira la formation et la sensibilisation. Comme sur la route, respecter les règles et rouler dans un véhicule bien entretenu permet d'éviter beaucoup de problèmes ! La DRSD a déjà une capacité éprouvée de sensibilisation et je reste persuadé que l'effort doit être permanent sur cet axe.

Le CERT-BITD a déjà passé une phase de POC[8] sous l'égide de l'ANSSI et fera l'objet au second semestre 2022 d'une mise en œuvre limitée à une région pilote. Il a vocation à être étendu à tout le territoire métropolitain au second semestre 2023.

Ce CERT-BITD sera parfaitement intégré dans la stratégie nationale pour la cybersécurité lancée en 2021 par le Président de la République et représentera une brique « BITD » majeure dans le dispositif national de protection cyber des entreprises. Dès que le CERT-BITD sera effectif sur tout le territoire, les entreprises en lien avec la défense seront toujours sous la menace cyber… mais mieux armées pour résister aux cyclones !

Parution le 15 juillet 2022

[1] Rapport d'information de MM. Allizard et Boutant, fait au nom de la commission des Affaires étrangères, de la Défense et des Forces armées du Sénat, déposé le 8/7/2020.
[2] Faux ordres de virement – escroquerie avec usurpation d'identité.
[3] Code de la défense et IGI 1300 - protection du secret de la défense nationale - Légifrance
[4] Créée en 1872, la DRSD a fêté en présence du ministre des armées le 150ème anniversaire de la création de la section de statistiques qui est à l'origine du contre-espionnage et de la contre-ingérence militaire.
[5] *Computer Emergency Response Team*
[6] CERT sectoriel de la base industrielle et technologique de défense.
[7] Service aussi connu sous l'acronyme anglais CTI, *Cyber Threat Intelligence*.
[8] *Proof of concept*

La certification, un vecteur de confiance adapté aux multiples enjeux du numérique

ARTHUR RIBEMONT
Responsable du Pôle Confiance Numérique
AFNOR Certification

Incertitude et besoin de confiance

Les crises se multiplient. COVID, climat, guerres, inflation : il est extrêmement difficile dans ce contexte pour une entreprise de pouvoir planifier faute d'une vision claire. Elles doivent faire face à de nombreuses incertitudes et cela pourrait impacter leur chaîne de valeur. Ces difficultés ne sont pourtant pas les seules auxquelles elles font face. Le risque numérique est incontournable comme le démontre de nombreuses études et baromètres dont celui d'Allianz - AGCS qui fait du risque cyber la 3e source d'inquiétude pour les chefs d'entreprise[1].

Sécuriser son activité dans ce contexte devient fondamental. Pour cela, il est nécessaire de réduire le risque en minimisant les aléas quand cela est possible. Dans une chaîne de valeur, les partenaires qu'ils soient sous-traitants, fournisseurs, distributeurs, etc. ont une place importante. S'appuyer sur des partenaires de confiance est essentiel ; pourtant cette dernière est intangible. La certification apparaît dans ce cadre comme un levier incontournable pour concrétiser cette confiance.

Qu'est-ce que la certification ?

La certification est la reconnaissance par une tierce partie qu'une entreprise, un produit, un service ou une personne est bien conforme à un ensemble

de critères définis. La certification est une marque de garantie et son utilisation est encadrée par le code de la Consommation notamment pour ce qui concerne les produits et services. L'article L433-3 la définit comme suit : « *Constitue une certification de produit ou de service [..] l'activité par laquelle un organisme, distinct du fabricant, de l'importateur, du vendeur, du prestataire ou du client, atteste qu'un produit, un service ou une combinaison de produits et de services est conforme à des caractéristiques décrites dans un référentiel de certification.* ». L'article L433-5 précise *« Peuvent seuls procéder à la certification de produits ou de services les organismes qui bénéficient d'une accréditation ».*

Les deux précédents extraits illustrent trois aspects élémentaires d'une certification : le référentiel, l'audit et l'accréditation. Dans le cadre d'une certification, le référentiel ou règlement d'usage détermine un ensemble de critères auxquels doit se conformer l'organisme souhaitant obtenir une certification. La reconnaissance d'une certification, au niveau réglementaire et par le marché, nécessite que ses critères aient fait l'objet d'une concertation des parties intéressées. C'est notamment en France le rôle de l'AFNOR (Association française de normalisation) qui réunit au sein de commissions de normalisation, les parties intéressées pour obtenir un consensus sur les normes.

L'audit est l'étape incontournable d'un processus de certification. Celui-ci doit être réalisé par une tierce partie indépendante de l'organisme audité aussi appelé organisme certificateur. Après avoir déterminé le périmètre des activités à auditer, un premier audit documentaire est souvent réalisé pour déterminer la capacité de l'organisme à réaliser l'audit. S'en suit alors la visite sur site d'un auditeur compétent et qualifié qui va interroger les équipes, observer les pratiques et étudier les pièces documentaires. Un rapport est ensuite remis à un expert décisionnaire qui peut rendre un avis favorable ou non sur la délivrance de la certification.

Légitimité et impartialité

L'accréditation complète ce triptyque de la certification et permet à un organisme certificateur de délivrer des certifications. En France, le Cofrac

(Comité français d'accréditation) est l'instance nationale désignée et reconnue par l'Etat pour attester des compétences d'un organisme de contrôle que sont les organismes certificateurs. Ces contrôles sont réalisés sur la base de normes, référentiels ou réglementations en vigueur. L'accréditation démontre le savoir-faire d'un organisme certificateur et apporte de la réassurance à l'audit réalisé par ce dernier.

Il est important de noter que lorsqu'un client manifeste sa volonté d'entrer dans une démarche de certification, il n'a aucune garantie quant à l'obtention de celle-ci. L'organisme certificateur est impartial. Pour résumer, AFNOR Certification définit la certification comme étant « *une preuve irréfutable, délivrée suite à un audit mené par un organisme certificateur impartial et objectif, qu'un produit, service ou une organisation, respecte les exigences d'un cahier des charges strict.* »

Quels sont les enjeux de la certification pour les organisations et personnes certifiées ?

Les enjeux de la certification peuvent être synthétisés en quatre grands axes : se conformer, conquérir, sécuriser et valoriser. Dans le cadre de certains marchés, la certification est obligatoire. C'est le cas par exemple des hébergeurs de données de santé qui doivent être certifiés selon le Décret n° 2018-137 du 26 février 2018 relatif à l'hébergement de données de santé à caractère personnel. La seconde motivation est d'ordre commerciale et notamment de pouvoir concourir à des appels d'offres. Et la tendance est à la généralisation de telles pratiques.

Le troisième aspect concerne la sécurité de l'entreprise. La certification permet de garantir que des mesures répondant à un ensemble de critères définis sont mises en œuvre. Cela génère de la réassurance vis-à-vis de ses partenaires économiques. Enfin la certification peut également être le moyen de valoriser et fédérer les équipes grâce à une reconnaissance. C'est la récompense de tout un travail collectif. S'interroger sur les raisons de l'acquisition d'un signe de confiance est important pour maintenir dans le temps l'engagement des équipes.

La certification comme marque de garantie présente bien des atouts. A ce

titre, c'est un puissant instrument pour répondre aux nombreux défis induits par le numérique. Le champ d'action est vaste et presque sans limite et concerne tout à la fois : l'innovation et ses risques critiques de dérives, l'explosion de la cybermenace dans un contexte de décentralisation des SI, la protection des libertés individuelles, la compétitivité des entreprises et bien d'autres encore. Panorama de ces enjeux illustrés par les certifications afférentes.

La certification, une réponse possible au défi technologique

Les innovations dans le numérique sont constantes et rapides. Certaines pouvant entraîner des dérives. Pour n'en citer qu'une : l'affaire Cambridge Analytica, du nom de l'entreprise qui a été accusée d'utiliser des données Facebook pour influencer l'élection américaine. Le risque de dérive est d'autant plus important que les sujets sont intangibles et non maîtrisés par la grande majorité des personnes. Pour accompagner ces innovations, la Commission européenne a notamment dans le cadre de l'intelligence artificielle (IA) proposé une approche par les risques. Les systèmes d'IA présentant un risque classé comme « inacceptable » seront interdits. Pour les autres niveaux risques, cette réglementation devrait imposer : le marquage CE.

Ce dernier ne peut être considéré comme une certification. Le marquage CE indique qu'un produit a été évalué conforme par son fabricant conformément à un ensemble d'exigences. Le marquage CE n'est toutefois pas une certification mais une attestation. L'évaluation peut être réalisée par le fabricant lui-même (déclaration de conformité) ou dans d'autres cas, il doit recourir à un organisme notifié. Dans ce dernier cas, la notification peut être considéré comme une accréditation et le marquage CE comme une certification. Son obtention peut être corrélée à des normes harmonisées.

Les normes harmonisées décrivent les spécifications techniques permettant éventuellement de pouvoir démontrer le respect des exigences techniques de la législation européenne. Elles sont élaborées à la demande de la Commission européenne par une organisation européenne de normalisation.

Pour une entreprise, être certifiée sur une norme harmonisée s'inscrit pleinement dans la démarche d'obtention du marquage CE associé. En la matière, la France par l'intermédiaire du Secrétariat général pour l'investissement (SGPI) a initié un grand défi, sous animation AFNOR : « Comment sécuriser, certifier et fiabiliser les systèmes qui ont recours à l'intelligence artificielle ? ». Toutes ces démarches visent à instaurer un cadre de confiance.

La certification, un enjeu de sécurité et de souveraineté

Pour des enjeux politiques, comme celui de la souveraineté, la certification est également présentée comme un critère de garanti notamment pour les infrastructures critiques. C'est tout l'intérêt de la qualification SecNumCloud de l'ANSSI qui est au cœur de la stratégie du cloud de confiance. A fin septembre 2022, seules cinq entreprises ont obtenu cette qualification de très haut niveau[2]. Toutefois, la stratégie du gouvernement, et notamment les aides proposées par l'Etat, devrait encourager la mise en conformité des industriels.

Ce référentiel est construit sur la même base que l'annexe A « Objectifs et mesures » de la norme ISO/IEC 27001 - Management de la sécurité de l'information. La certification ISO/IEC 27001 est l'une des certifications les plus recherchées et demandées par les entreprises. La dernière étude de l'ISO Survey parue en 2022 révèle une accélération de la croissance du nombre de certifiés 27001 en France de près de 55% en 1 an (606 en 2021 vs 392 en 2020). De nombreux autres signes de reconnaissance comme les certifications HDS – Hébergeur de données de santé, NF Service - systèmes d'archivage électronique ou encore TISAX dédiée à l'industrie automobile s'appuient sur cette norme de référence. Ce standard pourrait prochainement devenir un incontournable pour toutes les entreprises. Initier dès à présent une démarche de certification pourrait être à court terme un avantage compétitif significatif pour les entreprises. Et cela pourrait rapidement arriver. Dans un récent discours dédié au cloud de confiance, le Ministre de l'Economie et des Finances, Bruno Lemaire, a avancé la possibilité d'une certification pour les industriels ne sécurisant pas assez leurs infrastructures : « *Et je pense qu'il faut d'abord partir sur une base volontaire. Mais je le dis avec beaucoup de gravité, si*

jamais nos entreprises qui ont des données extraordinairement sensibles ne se saisissaient pas librement de cette offre de sécurisation de leurs données, je ne peux pas exclure que, à un moment ou à un autre, nous en venions à une norme obligatoire pour protéger notre souveraineté industrielle et protéger notre indépendance. ».

La certification, un vecteur de réassurance pour ses partenaires économiques

Cette déclaration du Ministre s'inscrit dans un contexte où la menace cyber explose. La question n'est plus de savoir si une entreprise va être attaquée, mais quand. Dans son rapport d'activité 2021, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) recense 1057 incidents vs 759 incidents en 2020 (+40%). Parmi ces attaques, certaines sont orchestrées par rebond, utilisation d'un système intermédiaire pour attaquer un système. S'appuyer sur un partenaire non fiable peut contribuer à l'ouverture d'une brèche même au sein d'un système d'information sécurisé et les conséquences peuvent être importantes pour l'entreprise. A ce titre, la certification telle que l'ISO/IEC 27001 constitue un excellent vecteur de réassurance quant aux pratiques et mesures mises en œuvre au sein d'une organisation.

Autre domaine, mêmes enjeux. Pour répondre aux enjeux de protection des données, le Règlement général sur la protection des données (RGPD) prévoit plusieurs mécanismes. De manière transverse, c'est-à-dire pouvant concerner presque tous les traitements, des certifications reconnues par les autorités compétentes ayant une portée nationale et/ou européenne commencent à apparaître sur le marché. Ces certifications peuvent être complétées sectoriellement par des codes de conduite visant à contrôler des traitements réalisés dans un cadre spécifique comme par exemple le CISPE dédié aux fournisseurs de services d'infrastructure cloud (IaaS). Ces instruments volontaires parmi d'autres concourent à une meilleure prise en main de la conformité RGPD par les responsables de traitement et sont encouragés par la CNIL[3].

La dynamique de la certification à travers quelques exemples

Tous ces exemples montrent que la certification est un mécanisme important sinon incontournable au sein de l'Union européenne et que son utilisation tend à augmenter au fil des ans tant les enjeux dans le secteur numérique sont divers et complexes. Les travaux en cours, dans le cadre du règlement sur la cybersécurité[4], pour créer des schémas de certification européens sur le cloud (EUCS), les produits (EUCC) et la 5G (EU5G) sont autant d'indicateurs de cette tendance. Point intéressant à noter pour les industriels, les travaux initiés dans le cadre de EUCS visent une harmonisation des certifications nationales comme SecNumCloud en France ou C5 en Allemagne.

L'ensemble de ces certifications ou équivalents, initiés par des acteurs de référence légitime concourent à créer un numérique de confiance pour les entreprises, les consommateurs et les citoyens. Loin de refléter toute la dynamique sur le sujet, elles sont représentatives de la dynamique actuelle. L'ANSSI propose par exemple des solutions à destination des prestataires de vérification d'identité (PVID), Cybermalveillance.gouv.fr valorise les professionnels en sécurité numérique grâce au label ExpertCyber. Le ministère de la Justice a développé Certilis, la marque de garantie pour les plateformes de résolution des litiges en ligne : conciliation, médiation et arbitrage. Enfin d'autres projets sont en discussion ou en attente de décret d'application comme la certification concernant les logiciels de contrôle parental ou la certification de cybersécurité des plateformes numériques destinées au grand public.

Quel futur pour la certification dans le domaine du numérique ?

Déjà nombreux, les sujets liés au numérique ne devraient pas manquer dans les années à venir : metavers, edge computing, web3, quantique, NFT, industrie 4.0, etc. Les besoins de sécurité et de réassurance vont plus que jamais être nécessaires. Dans un tel environnement, marqué par de nouvelles pratiques de travail (télétravail, cloud, etc.) et l'explosion des cybermenaces : la confiance est un élément incontournable et en constante

progression dans les relations inter-entreprises. De par ces caractéristiques, la certification dispose de solides arguments pour accompagner l'essor de cette confiance. Elle apporte des garanties et un levier de différenciation aux acteurs qui y recourent.

En France la dynamique autour de la certification ISO/IEC 27001 est particulièrement intéressante. Couplée à une politique publique ambitieuse en matière de sécurité et résilience des entreprises françaises, ce standard de la confiance numérique pourrait contribuer à renforcer l'attractivité des entreprises françaises en Europe et à l'international. Tout en contribuant à faire de la cybersécurité un axe majeur de notre souveraineté numérique.

Pour faire face aux défis réglementaires, politiques ou encore technologiques, la certification apparaît comme une marque de garantie incontournable. Pour autant, la multiplicité des signes de reconnaissance non encadrés induisant des informations contradictoires aussi bien pour les consommateurs que pour les entreprises pourrait être préjudiciable et mener à la défiance des consommateurs. C'est ce que rappelle un récent rapport d'information du Sénat : « *Labels, scores, allégations, mentions valorisantes, informations obligatoires, simple marketing : la profusion semble mener à la confusion.* »[5]. Ne pas briser cette confiance, tel est l'enjeu de la certification pour les années à venir.

Parution le 30 septembre 2022

[1] https://www.agcs.allianz.com/news-and-insights/news/allianz-risk-barometer-2021-fr.html
[2] https://www.ssi.gouv.fr/uploads/liste-produits-et-services-qualifies.pdf
[3] https://www.cnil.fr/fr/la-cnil-publie-son-plan-strategique-2022-2024
[4] Règlement (UE) 2019/881 - relatif à l'ENISA […] et à la certification de cybersécurité des technologies de l'information et des communications
[5] http://www.senat.fr/notice-rapport/2021/r21-742-notice.html

Les lois de la protection des données personnelles au service de la planète

ISABELLE DU CHATELIER
Group DPO
Dassault Systems
&
JAWAHER ALLALA
CEO
Systnaps Software

Le numérique est de façon simpliste pensé comme un outil des sociétés modernes permettant, à travers l'exploitation massive des données, des services dématérialisés toujours plus rapides et personnalisés.

Toutefois, pendant de nombreuses années, le sempiternel « si c'est gratuit, vous êtes le produit » est devenu si commun qu'il est apparu nécessaire pour les législateurs de porter leurs efforts sur le renforcement de la protection individus dans le but d'éviter que l'algorithmisation du numérique n'engendre des atteintes disproportionnées et incontrôlables aux droits de l'homme, et notamment aux droits à la vie privée.

Aujourd'hui, face à l'intensification des crises climatiques, la question des traitements massifs de données se pose en des termes nouveaux et interroge avec insistance l'impact du numérique sur les ressources planétaires. La dimension « virtuelle » du numérique est de nature à nourrir l'illusion d'une déconnexion de la réalité matérielle des traitements de données.
Et si la bonne application des lois de protection des données permettait d'agir en faveur de la sobriété numérique ?

Et si le respect des droits humains combiné à une exploitation éthique et économique responsable des données pouvait avoir un impact direct, positif et mesurable dans la réduction de l'empreinte énergétique et spatiale du numérique ?

La protection des données en quête d'un équilibre entre intérêts économiques et protection des personnes, la question environnementale absente.

La directive 95/46/CE du Parlement européen et du Conseil visait à harmoniser la protection des libertés et droits fondamentaux des personnes physiques en ce qui concerne les activités de traitement des données tout en garantissant un équilibre dans la libre circulation des données entre les Etats membres. Il n'était alors nullement question d'impact environnemental ; bien au contraire, l'industrie du numérique était alors considérée comme l'une des plus propres et durables comparée à des industries plus traditionnelles nées lors de la révolution industrielle par exemple.

Aujourd'hui, le développement du numérique a ouvert la voie à des modèles à fort potentiel économique portés par des plateformes alimentées par l'exploitation massive de données. La géopolitique de la gouvernance des données a permis de mettre en lumière l'hyper-puissance des GAFAM, aux risques associés à la surveillance de masse et à la perte de contrôle sur l'usage des données.

Ces challenges ont conduit à la refonte de cette réglementation et à la préparation du RGPD afin de réaffirmer et renforcer les droits et obligations des parties prenantes afin que :

- Les personnes concernées puissent en effet exprimer leur consentement ou s'opposer à des traitements, et que ces choix clairement exprimés soient respectés par toute organisation traitant des données ;
- Les organismes qui tirent un profit économique des données soient responsabilisées ;
- Les chaines de sous-traitance partagent les risques opérationnels liés au traitement de données ;

- Les organismes de contrôle puissent être équipés d'un arsenal de sanctions coercitives et crédibles proportionnés aux pouvoirs économique, technique et politique des géants du numérique.

Ainsi, la réglementation en matière de protection des données a été construite pour orchestrer les relations entre les personnes, les entreprises et les machines autour de la donnée. Il n'a jamais été question de l'impact environnemental de l'exploitation.

De l'hyper responsabilisation des entreprises numériques pour une éthique des traitements de données à la RSE

Depuis l'adoption du RGPD, les entreprises, selon leurs ambitions, leur niveau de maturité, le niveau de pénétration du numérique dans leur marché et au sein de leur structure, ont pu choisir leur orientation face à la protection des données : appliquer strictement la loi ou entreprendre une démarche plus globale en prenant en considération non seulement leur obligation de conformité à la loi mais également en adoptant une démarche éthique socio-environnementale.

Pour celle qui sont passées à l'action, les programmes de conformité se sont déroulés en plusieurs étapes :

- La définition d'un projet d'entreprise reflétant une ambition traduite en un programme opérationnel structuré et démontrable (preuve de la conformité) ;
- La mise en place d'une gouvernance dédiée pour animer la gestion des données à tous les niveaux (exécutif et opérationnel) ;
- L'incarnation d'engagements et de valeurs fortes dans les relations avec l'écosystème (partenaires, clients, sous-traitants).

Peu à peu autour des chartes éthiques et de la responsabilité socio-environnementale des entreprises, s'est construite une prise de conscience de l'impact des activités numériques.

La RSE devient alors un outil incontournable pour communiquer autour de l'impact des entreprises afin d'évaluer et promouvoir leurs engagements. Aujourd'hui ces engagements ne peuvent plus se limiter à des effets

d'annonce, la chasse au « greenwashing » étant lancée. Dès lors, les entreprises doivent produire et partager des résultats positifs mesurables au regard de l'impact de leur activité sur la planète afin notamment d'attirer les talents en quête de sens dans un contexte de pénurie de profils qualifiés.

Les temps de crises pour changer de paradigme : le besoin de sobriété organisée des données !

A la suite de la pandémie du covid19, le monde a dû faire face à une nouvelle accélération de la digitalisation des entreprises : la transformation des processus RH qu'ils concernent les employés ou les recrutements, les nouveaux modèles collaboratifs immersifs, la mise à disposition d'interaction virtuelles avec les clients, etc.
En parallèle, de nouvelles perspectives ont émergé avec l'accélération de nombreux projets transformatifs : les smart cities, les industries 4.0, les jumeaux numériques, les NFT, les cryptomonnaies ou encore le métavers. Tout ceci implique de traiter des volumes de données toujours plus colossaux au travers d'infrastructures et de data centers très énergivores et plus ou moins consommateurs en ressources naturelles. Le numérique consomme près de 10% de l'énergie électrique mondiale et cette consommation augmente chaque année. Les traitements des données ont une empreinte physique, spatiale, énergétique et donc environnementale !

Les données sont parfois appelées le nouvel « or noir » du 21ème siècle. Contrairement aux ressources pétrolières qui diminuent, la quantité de données augmente de manière exponentielle. Les données sont dites « non rivales « car contrairement aux matières premières fossiles, elles se démultiplient et peuvent être utilisées et réutilisées à l'infini pour toutes sortes de finalité. Cette nouvelle source de valeur nécessite des infrastructures qui en 2022 vont consommer 90 milliards de kilowattheures d'électricité par an, soit la production équivalente d'environ 34 centrales électriques au charbon.

Cette inflation n'est pas près de s'arrêter si l'on constate le nombre de projets en cours d'élaboration pour encadrer, ouvrir et faciliter l'usage de la donnée (ePrivacy, DSA, Data Act, DMA, DGA et IA Act) à des fins de

compétitivité ou d'altruisme, pour faire bénéficier au plus grand nombre du pouvoir et du savoir des données.

Comme dans tous les domaines de consommation, il devient urgent de changer de paradigme et de consommer mieux des données pertinentes. Place à la sobriété organisée qui se doit d'être plus vertueuse et applique strictement et rationnellement les principes de minimisation des données et de Privacy By Design !

Le droit de la protection des données au service de la sobriété organisée des données

Ancrer la sobriété dans le traitement des données permettrait d'avoir un impact positif direct sur l'empreinte carbone par la suppression d'immenses volumes de données inutiles, la libération des espaces de hautes disponibilités et la réduction de la consommation énergétique et spatiale associée.

Le droit de la protection des données dispose de 5 leviers permettant d'atteindre en pratique une sobriété organisée des données :

- La qualité des données : En agissant sur la qualité et mobilisant uniquement le « juste patrimoine des données », il est possible de focaliser uniquement sur les données qui ont du sens et de la valeur et ainsi de supprimer toutes les données inutiles ou incorrectes. Malheureusement aujourd'hui, la destruction des données est encore source d'anxiété pour les entreprises et de nombreux freins sont observés pour des motifs plus ou moins légitimes. Cette obligation légale de conserver les données personnelles pour une durée de conservation identifiée est incontournable en Europe au titre du RGPD. Mais il ne s'agit pas de données non-personnelles. En appliquant les principes de qualité de données que celles-ci soient couvertes au titre du RGPD ou non, il sera possible de réduire de façon considérable les volumes de données inactives et inutiles.
- La minimisation des données : En appliquant des principes de collecte légitime et proportionnelle des données, il devient naturel pour une organisation de ne traiter que le juste patrimoine informationnel des données et de bénéficier de données de qualité dans des volumes maitrisés.

- Les droits des personnes : En exerçant leur droit, les individus peuvent stopper la collecte massive des données les concernant. Les entreprises respectueuses des droits des personnes veillent à mettre en place et maintenir dans le temps des processus de traitement loyaux et transparents, contribuer à la constitution d'un juste patrimoine informationnel des données.
- L'effacement des données : En procédant à l'effacement des données à l'issue de la durée de la finalité pour laquelle elles ont été collectées, les entreprises peuvent agir rapidement et simplement pour diminuer l'empreinte carbone produite par d'immenses volumes de données stagnant dans les bases de données de production et les centres de données. Cette croissance de données inactives ayant mécaniquement un effet sur l'augmentation du temps de traitement et l'accès aux données.

Nous devons désormais entrer dans une économie circulaire qui vise à changer le paradigme de l'économie dite linéaire, à limiter le gaspillage des ressources et l'impact environnemental, à augmenter l'efficacité à toutes les étapes de l'économie numérique. Il est possible d'y parvenir en adressant le cycle de vie des données.

Une nouvelle piste avec le recyclage des données pour faire entrer la donnée dans l'économie circulaire !

Appliquer les logiques de recyclage à la donnée revient à mettre en musique des principes juridiques existants : la collecte, le traitement et l'effacement et à transposer un modèle qui a été conçu pour les actifs matériels à des actifs immatériels comme la donnée.
Il est de la responsabilité de chaque entreprise de mettre en place une telle logique et d'élargir les principes du RGPD à toutes les données qu'elle peut être amenée à collecter et utiliser.

Parution le 7 octobre 2022

Pour les sciences, un devoir de mémoire

FLORENCE ESSELIN
Senior advisor
CyberCercle

Depuis 2009, chaque deuxième mardi d'octobre, un événement à ambition internationale initié au Royaume-Uni, le « jour Ada Lovelace », rend hommage à Augusta Ada King, Comtesse de Lovelace. Mathématicienne britannique née en 1815 et décédée moins de trente-sept ans plus tard, Ada Lovelace est considérée comme une pionnière de l'informatique pour ses travaux sur le prototype de calculateur numérique conçu par Charles Babbage, et de surcroît inspiratrice de l'intelligence artificielle pour son extraordinaire intuition des capacités et des applications futures des descendants de la Pascaline associée au métier Jacquard.

L'objectif de cette célébration est une mise en valeur des femmes travaillant dans les « sciences, technologies, ingénierie et mathématiques ».
Cette année, La Poste fait écho à cette célébration, en sortant, pour le « jour Ada Lovelace », un timbre à son effigie, qui évoque les « boucles conditionnelles » censées être réalisées par le prototype de Babbage dans les « sous-programmes » écrits par Ada pour le calcul des « nombres de Bernoulli ».

Cette initiative s'inscrit également dans la semaine de la science, manifestation nationale créée en 1991 et organisée cette année du 7 au 17 octobre 2022 en métropole par le ministère de l'Enseignement Supérieur, de la Recherche et de l'Innovation, ayant pour but de promouvoir la science auprès du grand public. Cet événement, comme le mois européen de la cybersécurité organisé en octobre depuis 2012, s'est installé progressivement dans la vie de nos concitoyens, mais certainement

encore trop discrètement.

Car il est indispensable pour la compétitivité et l'indépendance de notre pays, de susciter les vocations scientifiques chez les filles et les garçons ; le rappel de la vie et des inventions des ingénieurs qui nous ont précédés est un bon moyen de stimuler l'engouement pour les sciences, dans tous les domaines.

Cet engouement n'est pas nouveau ; il y a exactement trois-cent-cinquante ans Molière créait Les Femmes savantes, comédie qui mettait en lumière l'intérêt de ses contemporaines (et contemporains) pour les mathématiques, la grammaire, la philosophie et la poésie notamment. Cette comédie évoquait déjà la recherche d'émancipation de certaines femmes par une instruction de haut niveau, en soulignant les déboires conjugaux et financiers auxquels un zèle excessif, mué parfois en pédanterie, pouvaient les mener.

Sans s'étonner alors qu'une femme, née presque deux-cents ans après Molière, se soit passionnée pour un prototype de machine capable de calculs complexes tels celui des nombres de Bernoulli (1700-1782) que l'on enseigne de nos jours en université, on peut toutefois être admiratifs de ses compétences scientifiques, sachant qu'en France, l'accès à l'enseignement supérieur était interdit aux femmes avant le Second Empire.

«La machine analytique n'a nullement la prétention de créer quelque chose par elle-même. Elle peut exécuter tout ce que nous saurons lui ordonner d'exécuter. Elle peut suivre une analyse ; mais elle n'a pas la faculté d'imaginer des relations analytiques ou des vérités. Son rôle est de nous aider à effectuer ce que nous savons déjà dominer.»
Ada Lovelace mit plusieurs mois à documenter le fonctionnement de cette machine analytique ; sa « note G » est considérée comme le premier programme informatique au monde.
Passionnée et déterminée, elle sacrifia sa fortune et sa santé pour tenter d'achever le calculateur numérique de Babbage qui ne trouvait alors pas de financement.

« La machine analytique tissera des motifs algébriques comme les métiers de Jacquard tissent des fleurs et des feuilles. »
Associant à ses recherches techniques une vision poétique de l'évolution des calculateurs et de leurs applications, Ada Lovelace, fille du poète Lord Byron, est certainement un modèle d'ingéniosité, d'imagination scientifique et poétique, de persévérance et d'abnégation.
« I never am really satisfied that I understand anything; because, understand it well as I may, my comprehension can only be an infinitesimal fraction of all I want to understand about the many connections and relations which occur to me, how the matter in question was first thought of or arrived at, etc., etc. »

C'est un bel hommage alors qui lui est rendu par le timbre-poste français. Concept créé trois ans avant le décès d'Ada Lovelace, son usage est pourtant en train de disparaître par la concurrence de la messagerie électronique, une application des lointains descendants du calculateur de Babbage.

La Poste a aussi célébré cette année au titre des personnalités scientifiques, un grand homme injustement méconnu, qui participa activement à l'invention de la Poste pneumatique de Paris que de nombreux historiens considèrent, dans l'esprit et le principe, comme l'un des ancêtres de l'Internet.

Henri Rouart (1833-1912), fut non seulement un ingénieur polytechnicien des plus talentueux, mais également un entrepreneur et industriel apprécié, un maire dévoué à sa ville (La Queue-en-Brie, dans le Val-de-Marne), un pionnier de la photographie familier de Nadar, un collectionneur mécène des Impressionnistes, ami intime d'Edgar Degas et peintre impressionniste lui-même, amoureux de la nature surnommé « le peintre des arbres »... Patriote, par ses inventions il a rendu la France indépendante du Royaume-Uni pour le développement des usages des fluides. A l'origine de nombreuses inventions en collaboration avec d'autres ingénieurs de diverses écoles et domaines (tels Jean-Baptiste Mignon, Clément Ader et Gustave Eiffel), il était aussi capable de les industrialiser et d'en assurer l'exportation jusqu'en Russie ou aux Etats-Unis. Il finança un procès contre un ressortissant allemand ayant

abusivement déposé un brevet sur un principe de moteur inventé par un ingénieur français désargenté, qui fut alors finalement rétabli dans ses droits.

Un véritable honnête homme comme on en rencontre peu, que Paul Valéry, ami des fils d'Henri Rouart, a ainsi dépeint dans « Henri Rouart - Dans le sillage de Corot » : « Ceux qui ont connu M. Henri Rouart - sa belle vie, ses nobles goûts, la largesse et la délicatesse de son accueil, sa maison, qui depuis le seuil jusqu'à la chambre la plus haute n'était que peintures exquises - ont connu ce que la seconde moitié du siècle dernier a pu produire en France de plus accompli, de plus solide, de plus raffiné, de plus respectable - une existence fortement construite et magnifiquement ornée.
J'admirais, je vénérais en M. Rouart la plénitude d'une carrière où presque toutes les vertus du caractère et de l'esprit se trouvaient composées. Ni l'ambition, ni l'envie, ni la soif de paraître ne l'ont tourmenté. Il n'aimait que les vraies valeurs, qu'il pouvait apprécier dans plus d'un domaine. »

L'histoire d'Henri Rouart et celle d'Ada Lovelace, témoignent de la nécessité de la collaboration scientifique à travers le monde et plus encore, à travers les siècles, ainsi que de l'intime relation entre les arts, les lettres et les sciences.
« « *Nam sine doctrina vita est quasi mortis imago.* » Cela veut dire que Sans la science, la vie est presque une image de la mort. » (Molière, Le Bourgeois Gentilhomme, acte II sc.IV)

Il nous reste à réinventer un André Léveillé, un Jean Perrin ou un André Malraux, pour convaincre l'Etat de faire sauter les obstacles qui s'opposent à la diffusion de la connaissance.

Rares sont les inventions qui sont l'œuvre d'une seule personne. L'innovation hérite du passé. C'est pourquoi il est nécessaire de l'enseigner, même dans des domaines d'apparence récents tels que l'informatique, la cybersécurité ou l'intelligence artificielle.

Rappelons-nous que le premier micro-ordinateur (le Micral) fut créé au sein d'un bureau d'études français (R2E) ; que les travaux de Louis Pouzin

et de ses collaborateurs sur le réseau Cyclades furent précurseurs de l'Internet ; que la carte à puce est aussi une invention française, etc. La liste des apports des ingénieurs français au monde cyber actuel est trop longue pour être développée ici.

Rendons-leur hommage car l'humilité est souvent leur grand « défaut ». Remercions les associations qui travaillent à entretenir le souvenir des ingénieurs remarquables disparus, telle l'ARCSI (Association des Réservistes du Chiffre et de la Sécurité de l'Information) qui mettra en lumière à l'occasion de ses 14èmes rencontres sur « L'épopée de la carte à puce et son avenir », l'ingénieur Michel UGON, disparu en fin d'année 2021 et dont le rôle fut déterminant dans le développement de la carte à puce.

Remercions enfin La Poste pour avoir honoré ces personnalités remarquables et enrichi ainsi l'encyclopédie vivante, accessible à tous, objet de la vie quotidienne, que constitue la collection des timbres postes français.

Parution le 14 octobre 2022

Et si l'ENISA devenait le vrai NIST Européen ?

GUILLAUME COLLARD
Associé fondateur
CSB.SCHOOL

Le National Institute of Standards and Technology (NIST), ce nom ne vous dit sûrement rien si vous ne travaillez pas dans le domaine de la recherche, de l'industrie ou des technologies. Mais si, à l'inverse, vous évoluez dans un de ces mondes et notamment celui de la Cybersécurité, ce nom doit vous être extrêmement familier.

Le NIST dans le monde de l'informatique et de l'informatique industrielle, qu'est-ce que c'est ?

Une agence d'Etat américaine rapportant au Département du Commerce qui développe, entre autres, des normes de concert avec l'industrie du secteur des Technologies, de l'Information et des Communications (TIC).

Ces normes ayant deux objectifs principaux :
- donner un support compréhensible de règles permettant de bien concevoir, déployer et gérer ses systèmes avec une vision à la fois « technologie » et « process » ;
- apporter un support documentaire pour soutenir efficacement les réglementations fédérales ou sectorielles des Etats-Unis.

Les Etats-Unis ont donc une institution qui soutient les organisations dans leur démarche de conformité réglementaire tout en préservant l'intérêt des Etats-Unis et de son économie.

Qu'en est-il de l'Europe ?

L'équivalent Européen de NIST est l'ENISA (The European Union Agency for Cybersecurity). Cette agence européenne constitue l'organe central pour tous les sujets Cyber de l'Union Européenne en portant par exemple le Cybersecurity Act de 2019 qui lui confère sa capacité d'action. Sur papier, l'ENISA est officiellement le NIST Européen.

L'ENISA émet donc des publications permettant d'accompagner les Etats membres et les organisations dans leur démarche de conformité et de sécurisation de leur environnement numérique.

Pour autant, à date, le NIST fait office de référence au niveau Européen devant l'ENISA. Mais pourquoi ?

Pour comprendre cela, prenons un exemple concret et intéressons-nous au sujet de la cryptographie. La cryptographie est un sujet intéressant car il est souvent au cœur de sujets extrêmement sensibles comme les réglementations portant sur la sécurisation des données militaires, doubles usages, personnelles, de santé, financière etc. Il est souvent utilisé comme un argument (marketing) permettant de rassurer les organisations et les États sur la sécurité d'un système et des données qui lui sont associés.

Le NIST Special Publication 800-175A[1] est une publication qui présente les Standards Cryptographiques à utiliser par les organisations fédérales américaines et sur base du « volontariat » pour les autres organisations. Le mot volontariat est à pondérer sachant que la section 2 du Standard présente l'ensemble des lois américaines qui sont impactées par cette publication et donc qui obligent, *de facto*, à suivre ces règles. Cette publication explique de manière détaillée les mesures de sécurité applicables dans le domaine de la cryptographie, les techniques à utiliser, etc. Elle est soutenue par un programme de validation des modules cryptographique (CMVP)[2] et un programme de validation des algorithmes cryptographiques (CAVP)[3]. Le CAVP est lui-même soutenu par une publication, la série 140 du Federal Information Processing Standards, plus connue sous le nom FIPS 140. Le processus est simple,

chaque organisation peut soumettre un module de chiffrement et / ou un algorithme de chiffrement qui sera analysé par le NIST (dont le code source et les commentaires du code source expliquant en détail son fonctionnement) afin de savoir s'il répond ou non aux exigences de sécurité imposées par les Etats-Unis. Si c'est le cas, l'algorithme et ou le module est référencé dans la base de données accessibles[4] et devient ou peut devenir FIPS approved et NIST recommended. Ceci permettant aux organisations impactées par une réglementation les obligeant à utiliser une technologie cryptographique certifiée de pouvoir choisir librement dans la base de données.

Dans le cas des algorithmes de chiffrement symétrique, le NIST organise des concours appelés Advanced Encryption Standard (AES) permettant de sélectionner l'algorithme qui fera référence dans cette catégorie. L'algorithme gagnant récupère d'ailleurs le nom du concours. Exemple : l'AES très connu dans le monde cryptographique est un algorithme nommé Rijndael qui a remporté le concours de 2001 et qui porte désormais le nom du concours, comme pour effacer son passé et rappeler au monde que cet algorithme est désormais américain.

NIST travaille également de concert avec la NSA (National Security Agency) pour émettre des fonctions de hachage robustes connues sous le nom de Secure Hash Function (SHA). Le NIST organise également des concours pour les Signatures Digitales (RSA), etc. Par le biais de ce programme, le NIST contrôle le monde cryptographique en dictant quels seront les algorithmes et modules qui régneront dans le monde Cyber. En effet, quand bien même un algorithme soit performant, tant qu'il ne sera pas reconnu par NIST, très peu d'organisations prendront le risque de l'utiliser, ceci afin d'éviter les lourdes sanctions liées à un défaut de conformité.

A ce jour, il n'existe aucun programme de ce genre en Europe.

Si nous nous concentrons sur les publications de l'ENISA, ces dernières mettent l'accent sur les techniques de chiffrement, leurs forces et faiblesses en évoquant par ailleurs AES et SHA de façon théorique à l'image d'un

module scolaire. Mais, à aucun moment, ils ne mettent l'accent sur le caractère stratégique de détenir le pouvoir de sélection des algorithmes à appliquer au sein de l'Union Européenne.

Attention, ne nous méprenons pas sur les intentions de ce papier.
En aucun cas nous remettons en cause la qualité de l'AES (Rijndael), de SHA 3 ou encore RSA. Nous attirons l'attention sur le fait qu'aucune technologie européenne ne peut ou ne pourra exister de manière « sérieuse » au niveau International / Européen sans le fameux tampon du NIST et donc, par conséquent, des Etats-Unis. Le dernier exemple en date est l'algorithme Falcon développé par Thalès pour répondre aux enjeux du post quantique qui vient d'être sélectionné par le NIST comme standard cryptographique post-quantique pour les signatures digitales. Un succès français qui n'est un succès que parce que le NIST a donné son accord. Pas l'ENISA, mais bien le NIST. Est-ce que cet algorithme répondra aux enjeux de sécurité des Européens ? Nous n'en savons rien car à l'inverse du NIST, nous ne testerons pas et nous suivrons les recommandations américaines les yeux fermés.

A ce jour, l'AES est considéré par la communauté cyber comme un algorithme fiable et sécurisé entre autres car les Etats-Unis l'autorisent toujours. Pour autant en 2003, le gouvernement américain avait annoncé : « L'architecture et la longueur de toutes les tailles de clés de l'algorithme AES (128, 192 et 256) sont suffisantes pour protéger des documents classifiés jusqu'au niveau « SECRET ». Le niveau « TOP SECRET » nécessite des clés de 192 ou 256 bits. L'implémentation de l'AES dans des produits destinés à la protection des systèmes et/ou documents liés à la sécurité nationale doit faire l'objet d'une analyse et d'une certification par la NSA avant leur acquisition et leur utilisation ».

Rappelons que la NSA travaille à détecter des faiblesses dans les algorithmes de chiffrement et qu'elle a accès aux codes sources ainsi qu'aux commentaires. Lorsqu'elle en détecte, elle choisit généralement de ne pas les communiquer mais demande aux institutions américaines traitant des données hautement confidentielles de ne pas les utiliser ou alors de faire valider leur usage. Il y avait eu des précédents entre autres sur l'algorithme de chiffrement DES. En suivant aveuglément le NIST, les Européens font

le choix de décentraliser leur capacité de contrôle et de maîtrise de la protection de leur données et éventuellement de leurs données stratégiques. Si jamais la NSA avait trouvé un moyen de déchiffrer un message protégé en AES via une faiblesse de ce dernier, nous n'en saurions rien pendant un certain temps jusqu'à un énième scandale PRISM et Upstream Collection.

Cette posture ne serait pas gênante si les dernières réglementations européennes ne cherchaient pas à effectuer une forme de protectionnisme européen et si le débat public et politique n'était pas un concentré de souverainisme.

Pour conclure, toutes ces volontés ne pourront être couronnées de succès tant que l'Europe ne possédera pas une organisation à la hauteur du NIST.

Il existe une dichotomie de posture en Europe. Certains pays ont d'ailleurs fait un choix stratégique pour répondre à cette problématique comme la Chine qui s'arme et se structure comme les Etats-Unis avec le National Information Security Standardization Technical Committee (TC260) afin de déterminer quelles sont les mesures de sécurité les plus pertinentes pour répondre à ses enjeux stratégiques[5]. Le TC260 a approuvé en 2020 huit standards de Cybersécurité.

Pour revenir à notre exemple, vous vous en douterez en matière de chiffrement, les recommandations chinoises ne sont pas obligatoirement les mêmes que celles des Américains. Ce qui inquiète fortement ces derniers, surtout pour tout ce qui concerne le domaine des nouvelles technologies (NTIC) et en particulier les télécommunications (5G et 6G). Ceci les a d'ailleurs amenés à diligenter l'étude suivante : « L'article 9414 de la loi sur l'autorisation de la défense nationale (NDAA) de 2021 qui ordonne au NIST de conclure un accord avec une entité appropriée pour mener une étude et fournir des recommandations concernant l'effet des politiques de la République Populaire de Chine (RPC) et la coordination entre les entités industrielles au sein de la RPC sur les organismes internationaux engagés dans le développement et l'établissement de normes internationales pour les technologies émergentes ».[6]

Force est de constater que l'ENISA et l'Europe ne représentent pas à ce jour une source d'inquiétude pour les Etats-Unis ou la Chine compte tenu de l'approche et de la gouvernance adoptée sur le sujet.

Parution le 25 novembre 2022

[1] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-175A.pdf
[2] https://csrc.nist.gov/projects/cryptographic-module-validation-program
[3] https://csrc.nist.gov/Projects/cryptographic-algorithm-validation-program#:~:text=The%20NIST%20Cryptographic%20Algorithm%20Validation,prerequisite%20of%20cryptographic%20module%20validation.
[4] https://csrc.nist.gov/Projects/cryptographic-module-validation-program/validated-modules/Searc
[5] Chinese Central Strategy National Security Publication http://www.gov.cn/zhengce/2021-10/10/content_5641727.htm
[6] https://www.federalregister.gov/documents/2021/11/04/2021-24090/study-on-peoples-republic-of-china-prc-policies-and-influence-in-the-development-of-international

Il est temps de « désexpertiser » la cybersécurité !

XAVIER LEONETTI
Magistrat
&
CHRISTIANE FERAL-SCHUHL
Avocate
Co-auteurs de « Cybersécurité, mode d'emploi » (PUF, 2022)

Le 16 novembre 2022, le ministre délégué à la transition numérique a annoncé une série de mesures visant à renforcer la sécurité des PME et des collectivités publiques.

Au-delà des trente millions d'euros qui seront alloués à la protection des entreprises et des collectivités, il s'agit de positionner les questions cyber au cœur des stratégies des comités de direction. En effet, dans les entreprises et dans un grand nombre d'administrations, les questions de cybersécurité relèvent encore trop souvent de la technique au lieu de faire partie intégrante de la stratégie. En quelque sorte, les enjeux de cybersécurité et de cyberdéfense au sens large sont perçus comme l'émanation de problématiques liées au service informatique. Or, le numérique comporte à la fois une dimension structurelle, sous la forme de l'architecture technique qui supporte l'activité d'une entreprise ou d'une collectivité, mais également une dimension stratégique en lien avec l'usage qui en est fait : la protection des ressources, la gestion des données internes et des clients, la communication externe… Le cyber est aujourd'hui aussi présent et vital pour les entreprises que l'air que l'on respire. C'est pourquoi il est impératif que ce sujet ne reste pas l'affaire des seuls techniciens.

La sécurité est un sujet qui a toujours existé dans nos sociétés, mais qui a pris une dimension nouvelle avec l'ère du numérique. La seule évocation du RGPD permet de comprendre que la sécurité des données personnelles est devenue un enjeu au plan national, comme au plan international. Il doit désormais être au cœur des préoccupations des entreprises et des collectivités. De surcroît, les enjeux de cybersécurité nécessitent le suivi et l'anticipation des règles européennes, telles que les récentes publications du Digital Service Agreement (DSA) et du Digital Marketing Agreement (DMA), venus réguler l'offre de produits et de services en ligne.

Pour cela, chacun doit s'approprier les questions cyber.

Aussi, la sécurité des systèmes d'information, la gestion des données ne doivent plus se limiter aux seuls aspects techniques, mais doivent désormais s'intégrer dans un plan global de stratégie de développement positionné au plus près des décideurs, qu'ils soient chefs d'entreprises ou élus locaux. A défaut, lorsque le pilote ne s'interroge pas sur les évolutions de son écosystème, il se condamne à progresser dans « un brouillard décisionnel » au risque de subir des surprises stratégiques et de perdre en termes de compétitivité et d'image.

Le récent crack de la plateforme FTX, l'une des principales plateformes mondiales d'échanges de cryptomonnaies, illustre ce type de surprise survenue faute d'anticipation et de clairvoyance. Cette faillite est le résultat d'un cocktail classique entre aveuglement et négligences. Au cœur du scandale, une partie de l'argent confiée à FTX par ses clients aurait été aspirée par le fonds Alameda Research et détournée au profit du fondateur et des dirigeants de la plateforme. Si le secteur bancaire traditionnel a gardé ses distances avec cette plateforme, d'autres tels que des fonds d'investissement ayant pignon sur rue comme Sequoia, la caisse de retraite des enseignants de l'Ontario, ou le japonais Softbank ont investi massivement dans cette plateforme. Il convient donc de s'interroger sur la légèreté avec laquelle ces établissements ont pu investir dans un placement aussi risqué.

L'appât du gain vers des placements risqués n'est pas sans rappeler la crise de 2008. De même, l'apparente complexité des « subprimes » et de leurs

produits financiers dérivés a souvent facilité l'ignorance du plus grand nombre en réservant la connaissance à un cercle de sachants, plus ou moins bien intentionnés.

Ne commettons pas la même erreur en matière numérique en nous désintéressant de ces questions ! Les enjeux cyber ne doivent pas rester concentrés entre les mains des seuls experts !

En interne cela reviendrait à laisser les clefs entre les mains d'une seule personne. Au contraire, une vision à 360° doit permettre de positionner les questions numériques et cyber au centre des compétences partagées par la technique informatique, le droit, le marketing, la finance, les ressources humaines… C'est à cette condition qu'une stratégie efficace pourra être développée et déployée. D'autant que les entreprises et les collectivités sont arrivées au milieu du guet, au « turning point », à partir duquel l'ensemble de leur stratégie doit impérativement évoluer, notamment pour faire face à la recrudescence des cyberattaques. On relèvera que, en 2021, 5037 notifications ont été reçues par la CNIL dont 59% résultaient d'un piratage informatique. L'ampleur de ce phénomène doit être prise en compte par chacun, tout particulièrement les RSSI et les Délégués aux données personnelles mais pas seulement. Tous les acteurs doivent se poser les bonnes questions.

En premier lieu, quelles sont les mesures à prendre en cas de cyberattaque ?

Les premiers réflexes à adopter sont ceux du « cyber bon sens » qui mêle technique, juridique et communication. Il convient notamment d'alerter immédiatement le support informatique, d'isoler le système attaqué afin que l'attaque ne se propage pas à d'autres équipements, de constituer une équipe de gestion de crise, de déposer plainte, de conserver les preuves de l'attaque, de procéder à une analyse pour identifier les failles et prévenir les éventuelles répliques… Par ailleurs, une cyberattaque aura bien souvent pour conséquence une violation des données au sens du RGPD. Dans ce cas, une violation de la confidentialité, de l'intégrité ou de la disponibilité des données, fait naître, dans un délai très court, un certain nombre d'obligations à la charge du responsable de traitement. Ce dernier devra

par exemple notifier la violation à la CNIL dans un délai de 72 heures. De même, il devra notifier la personne concernée par la violation des données dans le meilleur délai et documenter cette violation en indiquant les faits, les effets et les mesures prises pour y remédier (article 35 du RGPD).

En amont d'une crise, quels sont les points de vigilance sur lesquels se pencher prioritairement ?

Il faut définir le bon niveau de sécurité des données et hiérarchiser les accès. S'agissant plus particulièrement des données à caractère personnel, la désignation d'un Délégué aux données personnelles est souvent une mesure de précaution. Elle peut être obligatoire dans un certain nombre de cas, par exemple pour les collectivités. La CNIL a d'ailleurs récemment mis en demeure 22 collectivités qui n'avaient pas désigné de DPO. Ce dernier joue en effet un rôle essentiel dans la conformité des traitements de données mis en œuvre par les autorités publiques. Il constitue l'interlocuteur privilégié des agents et des administrés sur l'ensemble des sujets relatifs à la protection des données.

Enfin, comment renforcer le dispositif sécuritaire face aux risques cyber ?

Un outil d'auto-diagnostic devrait être prochainement développé permettant notamment aux 750 entreprises issues des secteurs stratégiques (définis par la directive européenne NIS2) de contribuer au bouclier cyber qu'elles devront bientôt mettre en œuvre. Concrètement, à la suite de l'adoption de la directive NIS en 2016, les opérateurs de services essentiels (OSE), tels que dans les secteurs bancaires, de la santé ou de l'énergie, ont dû adopter des mesures spécifiques de cyber protection. La directive NIS2 étendra ces obligations à de nouveaux acteurs.

Pour les collectivités territoriales, le plan annoncé par le secrétaire d'Etat au numérique leur permettra de renforcer leur cybersécurité au travers de parcours différenciés. Le plan prévoit qu'à la fin de l'année 2023, plus de 1000 collectivités et administrations auront suivi l'un ou l'autre des parcours de cybersécurité. Les plus petites communes disposeront quant

à elle d'un accompagnement sous la forme d'outils de cybersécurité « clé en main » mis à leur disposition.

La cybersécurité doit désormais être considérée comme partie intégrante des enjeux stratégiques des entreprises ou des collectivités. Elle doit mettre en réseau la technique et la stratégie, en quelque sorte, à l'image d'un développeur qui devra intégrer une solution technique dans un cadre juridique et stratégique préalablement défini.

Parution le 9 décembre 2022

Table des matières

CyberCercle - 92 Cours Lafayette, 69003 Lyon
contact@cybercercle.com - cybercercle.com

Réalisation : S.I.M. Publicité - Photo d'illustration ©bestfoto77 - Shutterstock

Directeur de la publication : Bénédicte PILLIET
CyberCercle – 92 Cours Lafayette, 69003 Lyon
contact@cybercercle.com – cybercercle.com