Les DATA, un enjeu de sécurité primordial au sein du cyberespace

Romain HERITIER

Analyste - Commission Sécurité & Défense internationales de l'Institut d'Études de Géopolitique Appliquée - IEGA

Septembre 2021

ISSN : 2739-3283

Comment citer cette publication :

Romain Héritier, « Les DATA, un enjeu de sécurité primordial au sein du cyberespace », Institut d'Études de Géopolitique Appliquée, Paris, 23 septembre 2021.

Institut d'Études de Géopolitique Appliquée - 31 Rue de Poissy 75005 Paris
E-mail : secretariat@institut-ega.org
Site internet : www.institut-ega.org

SOMMAIRE

Introduction

Le terme « *data* » représente un des fondements techniques mais aussi informatif du cyberespace. Cet anglicisme définit un panel large et varié d'outils et d'informations, rendant ses traductions plutôt imprécises. Malgré cet aspect nébuleux, la notion est communément traduite en Français par le terme « données », ce qui ne démystifie pas pour autant le terme. Si le droit français définit aisément certains mécanismes traitant ces données, le concept même de celles-ci n'est pas explicitement mentionné dans les textes juridiques.

Selon le Larousse, plusieurs aspects caractérisent ce terme en fonction de son domaine d'utilisation. Dans le cyberespace, les données s'analysent comme la « représentation conventionnelle d'une information en vue de son traitement informatique »[1]. En ce sens, une *data* serait donc tout type d'information pouvant être analysée informatiquement dans l'objectif de générer d'autres informations.

Sa spécificité par rapport à d'autres ressources pouvant générer de l'information reposerait alors sur sa capacité à être traitée informatiquement, donc à être automatisée par ceux souhaitant l'analyser.

Bien que son développement soit une avancée majeure, sa soumission à une automatisation analytique peut très rapidement engendrer des abus. Il est alors important de rappeler que les *data* peuvent être rangées en plusieurs catégories en fonction de leur provenance, de leur propriétaire initial ou encore de leur utilité première. Ce sont ces catégories qui sont, pour la plupart, définies juridiquement. Des termes plus connus émergent alors comme les *personal data* (données à caractère personnel), mais aussi l'*open data* ou encore le *big data*.

Il est important de préciser que l'objet de cette étude sera restreint aux enjeux de l'exploitation des données à caractère personnel ainsi qu'aux données produites par les personnes morales de droit public ou privé. Le thème des *data* se révélant être un domaine d'étude particulièrement vaste, une limitation à ces deux catégories est importante pour traiter convenablement le sujet.

[1] Donnée. (2021). *Dictionnaire Larousse*. Paris : Société Édition Larousse. l*arousse.fr*

Il convient enfin de distinguer les données à caractère personnel des données produites par les personnes morales. En ce sens et selon la directive 95/46 du 24 octobre 1995, les données à caractère personnel seraient « toute information concernant une personne physique identifiée ou identifiable »[2]. Celle-ci impose un lien évident entre ce terme et les personnes physiques, écartant les personnes morales de toute production ou détention de données à caractère personnel qui leur seraient propres. Si cette distinction semble juridiquement incontestable, sa pertinence sera à remettre en question compte tenu de la portée actuelle des *data* dans le cyberespace.

De manière globale, les différentes catégories de *data* peuvent être étudiées de façon relativement similaire en matière de sécurité. Hormis les moyens mis à disposition et les acteurs concernés, les techniques de protection des *data* ne changent pas fondamentalement en fonction de leur nature.

Comme défini précédemment, les *data* sont des informations. De ce fait elles se révèlent être la base de tous types de renseignements. D'après Gérard Tchouassi [3] , les « entreprises ont besoin de l'information appropriée, au moment opportun, pour la prise de décision », cette information est aussi le fondement de toute analyse géostratégique[4]. La protection des *data* est donc primordiale pour tout acteur en produisant ou en analysant, compte tenu de leur valeur pécuniaire, mais aussi du risque important qu'elles pourraient représenter si elles étaient mises entre de mauvaises mains.

En ce sens, si leur collecte massive représente aujourd'hui un enjeu fondamental pour différents acteurs de par leur grande valeur, la mise en place de moyens effectifs de sécurité au fil du temps, pour en contrôler les abus, reste cependant assez limitée.

[2] Directive 95/46/CE du Parlement européen et du Conseil, relative à la protection des personnes physiques à l'égare du traitement des données à caractère personnel et à la libre circulation de ces données, 24 oct. 1995, *Journal Officiel*, n°L 281, pp. 0031 - 0050.
[3] G. TCHOUASSI, « Les besoins en informations dans les entreprises », *Revue Congolaise de Gestion*, 2017, n°24, pp. 63 - 92.
[4] P. BOULANGER, « Renseignement géographique et culture militaire », *Hérodote*, 2011, n°140, pp. 47 - 63.

I. Une richesse nouvelle abondamment exploitée par différents acteurs du cyberespace

À la manière des *data*, les acteurs interagissant dans le cyberespace peuvent être catégorisés en plusieurs groupes. L'objet de cette étude se centrera sur une liste non exhaustive de certains d'entre eux liés par leur volonté d'en tirer un profit nécessairement pécuniaire.

Ainsi ce propos s'analysera d'abord par l'utilisation commerciale des données à caractère personnel par les entreprises afin de cibler plus précisément leur publicité. Puis il s'analysera au travers d'acteurs explicitement malveillants, usant de failles de sécurité, dans le but d'obtenir la possession de certaines données.

La constitution d'une source de profits considérables pour les entreprises via la collecte de données à caractère personnel

L'utilisation des *data* par les entreprises est particulièrement intéressante d'un point de vue commercial. Elle leur permet d'adapter considérablement leurs dépenses publicitaires afin de réduire les dépenses marketing, tout en espérant prétendre à une augmentation significative de leurs revenus.

Le développement exponentiel d'internet depuis les années 2000 a permis de révolutionner totalement la façon de penser la publicité et l'échange des *data* se révèle en être le fondement. Là où la mise en œuvre d'annonces au sein d'autres médias pourrait s'apparenter à un jeté massif de bouteilles à la mer, celles issues d'internet permettent un ciblage bien plus précis et ainsi une répartition bien moins incertaine des dépenses.

Concrètement, la collecte, l'échange et la confrontation des données personnelles par les machines au sein du cyberespace entraînent une agrégation de profils utilisateurs dont les intérêts se rapprochent. Ces agrégations servent ensuite à proposer aux différents utilisateurs concernés de la publicité ciblée en fonction de leurs besoins, envies ou centres d'intérêt.

Si ce processus peut être l'objet de critiques et dénonciations, il n'en est pas pour autant illicite. Il résulte en réalité d'un contrat dont l'utilisateur est partie, contrat dont il est facilement possible d'en oublier la nature tant sa forme et sa facilité d'exécution se distinguent

des autres. Cette collecte se révèle donc illicite, en France, dans le seul cadre où le cocontractant n'a pas connaissance qu'il contracte, ou si la collecte porte sur des données non expressément mentionnées au sein dudit contrat. Il s'agit des fameuses « politiques de confidentialité ».

Ces politiques ont pour but d'informer l'utilisateur d'un site internet ou d'un logiciel, sur les opérations effectuées avec ses données à caractère personnel. Il s'agit donc de l'acte juridique permettant au propriétaire du site d'obtenir certaines informations pour les analyser, publier, ou encore effacer.

Ce système entraîne cependant un premier obstacle en matière de sécurité. Le cyberespace se trouve être fréquenté par des acteurs du monde entier, utilisant des structures informatiques là aussi implantées dans le monde entier. Si des frontières sont tracées entre les États, dans l'espace numérique celles-ci n'existent plus vraiment. En ce sens, il semble difficile d'articuler chaque système juridique de manière à arriver à un consensus garantissant une sécurité juridique internationale, pleinement effective, en matière de protection des données à caractère personnel.

Ces politiques de confidentialité sont alors critiquables à bien des égards compte tenu de leur nature. Si elles sont nécessaires à l'information et pour exploiter les données des utilisateurs, leur forme actuelle fait débat au sens où elles contrastent particulièrement avec le domaine dans lequel elles s'inscrivent.

L'utilisation du web ou des programmes informatiques permet, en règle générale, de gagner en temps, en efficacité, ainsi qu'en lisibilité par rapport aux procédés classiques. Par exemple, faire ses courses par internet *via* le drive d'un magasin, rédiger sa déclaration d'imposition *via* France Connect, ou, plus simplement, dans le cas d'une simple recherche d'informations. Ce besoin de rapidité contraste alors avec les politiques de confidentialité dans leur forme actuelle. Celles-ci représentent généralement plusieurs pages à lire, avec un langage juridique qui n'est pas nécessairement compréhensible par tous les utilisateurs et qui empêche dans bien des cas l'accès aux ressources en cas de refus. Toutes ces conditions peuvent entraîner une acceptation des politiques sans lecture, causant par la suite une collecte de données à caractère personnel dont le consentement réel, certain et non vicié pourrait être remis en cause.

La collecte de ces données se concrétise par l'usage de programmes informatiques tout aussi connus puisqu'il s'agit des « Cookies ». À l'origine ce mécanisme fut créé par la société Netscape afin de sauvegarder le contenu des paniers utilisateur sur les marchés en lignes, dans le cas d'une fermeture soudaine de la page web. Ce mécanisme fut exclusivement conçu dans le but de pouvoir retracer les utilisateurs à chaque connexion et ainsi faciliter leur utilisation.

Comme le souligne Benjamin Poilvé « L'idée était simple : permettre au serveur de transmettre un fichier texte au client, celui-ci lui renvoyant ce même fichier à chaque requête subséquente, permettant ainsi d'identifier l'utilisateur et donc, par exemple, de se rappeler du contenu de son panier au niveau du serveur »[5]. Toutefois, cette méthode n'est pas dépourvue d'inconvénients. Dans le cas où ces cookies servent de relais entre le terminal utilisateur et le serveur du site, alors l'utilisateur comme le serveur peuvent rédiger des informations sur ce relais. Cela signifie que si le serveur du site héberge d'autres serveurs en son sein, alors ces derniers ont aussi accès au relais. Il s'agit des « cookies tiers ».

Concrètement cela s'illustre par la présence de liens de redirection ou d'images de publicités sur les sites visités. Lorsqu'une entreprise autorise des publicités tierces sur son site, celle-ci n'héberge pas directement les publicités mais passe par un serveur publicitaire qui gérera les publicités à présenter. Le serveur publicitaire ayant accès au relais, il peut alors analyser non seulement les actions réalisées sur le site, mais aussi toutes les autres actions présentes dans le relais sans lien avec le site. Le site et l'hébergeur publicitaire ont donc accès à une quantité importante d'informations privées de l'utilisateur, notamment les différents liens URL visités précédemment. L'hébergeur de publicité pourra connaître plus précisément les centres d'intérêt de l'utilisateur en analysant les différents liens présents dans le relais. Il pourra alors proposer une publicité plus ciblée à chaque profil, à chaque nouvelle connexion. Le site pourra, quant à lui, monnayer à la hausse les différentes places accordées à l'hébergeur publicitaire. Cette mécanique se révèle donc être extrêmement lucrative pour les entreprises, au détriment de la vie privée des utilisateurs.

[5] B. POILVÉ, « Une petite histoire du cookie », *linc.cnil.fr*, 14 jan. 2020, p. 1.

Ainsi, de nombreux abus comme le scandale de Facebook et Cambridge Analytica en 2018 ont été dévoilés. En l'espèce, les données de près de 87 millions de personnes auraient été illégalement récupérées par l'entreprise grâce au réseau social[6].

En revanche, si l'échange de données personnelles permet aux entreprises de générer de grands profits, elles ne sont pas les seules à profiter de ce système. Avec le développement important du cyberespace dans la sphère publique, bon nombre d'acteurs malveillants exploitent les failles de sécurité informatiques afin de détourner les *data* à leur avantage.

Des utilisations détournées constamment adaptées par les acteurs malveillants

À la manière de toute activité lucrative, le secteur des *data* n'échappe pas aux acteurs malveillants. Ils peuvent s'identifier comme des personnes, ou groupes de personnes, tierces au processus de génération et d'échange des *data*, souhaitant le détourner pour leur propre profit.

La particularité notable des acteurs malveillants au sein du cyberespace résulte de leur nature. En ce sens, les personnes concernées peuvent tout aussi bien être de solides directions de renseignement étatiques, de grands groupes criminels organisés, ou encore de simples particuliers. Cette grande hétérogénéité s'explique par la facilité d'accès aux outils informatiques, aussi bien techniquement que financièrement. Cette pluralité de profils n'est pas à négliger car elle permet le développement de techniques variées, s'actualisant plus rapidement que d'autres activités criminelles.

Toutefois, bien que ce milieu compte une hétérogénéité d'acteurs, les modes opératoires suivent un modèle assez similaire. Premièrement l'exploitation d'une faille de sécurité est nécessaire afin de pouvoir collecter les données. Ensuite, l'utilisation d'outils va être indispensable pour exploiter ladite faille. Enfin, la mise en œuvre de moyens pour traiter les *data* collectées et en tirer un quelconque profit clôturera le processus.

[6] C. CRIDDLE, « Facebook Sued Over Cambridge Analytica Data Scandal », *bbc.com*, 28 oct. 2020, p. 1.

Lorsqu'il est question de failles de sécurité, celles relevant du domaine informatique et plus précisément du code se distinguent particulièrement. En revanche, si Rabbin des bois présente de manière explicite son expérience de hacker informatique au sein de son premier livre *Lève-toi et code*[7], il expose surtout la principale faille de sécurité commune à chaque attaque informatique : l'humain. Son ouvrage permet de s'interroger sur la réelle cause de l'insécurité constante planant sur les *data* et le facteur humain en est incontestablement l'origine.

Afin de mieux cerner cette affirmation, il est possible de prendre l'exemple d'une technique appelée le *social engineering.* D'après la National Security Agency, elle consiste en une « manipulation psychologique d'une personne par un acteur menaçant pour effectuer des actions ou divulguer des informations »[8]. Ici, l'acteur malveillant use d'erreurs humaines telles que la divulgation maladroite de données personnelles, ou encore l'utilisation de mots de passe composés d'informations facilement identifiables[9].

Le facteur humain est moins bien identifiable sur les attaques exclusivement informatiques, mais pas nécessairement indémontrable. Si l'on considère qu'un humain se trouve derrière chaque codification informatique et donc derrière chaque ligne de code de chaque système, alors toutes les failles identifiables au sein de ces systèmes peuvent être imputables à un être humain. La faute est alors soit volontaire si elle résulte d'un comportement conscient de la personne, soit involontaire et totalement imprévisible si elle résulte d'une erreur inconsciente ou d'une mauvaise articulation *a posteriori* des différents systèmes. Cette origine commune aux failles de sécurité pose alors un problème de taille pour la sécurisation des *data*, mais aussi une véritable mine d'or pour les acteurs malveillants.

On ne peut assurer avec certitude l'infaillibilité absolue d'un système de stockage ou d'échange de *data*. De ce fait, ces acteurs malveillants disposent d'une multitude d'outils pour parvenir à déstabiliser, casser et exploiter ces systèmes en vue d'une récupération de données. De plus, la facilité d'accès à ces outils permet un

[7] RABBIN DES BOIS, *Lève-toi et Code*, Paris, ed. de La Martinière, 2018, 112p.
[8] NSA - CYBERSECURITY PRODUCTS AND SHARING DIVISION, *NSA/CSS Technical Cyber ThreatFramework V2*, *nsa.gov*, 13 nov. 2018, p. 13.
[9] Il s'agit d'informations originellement personnelles intentionnellement divulguées en ligne, tel qu'une date d'anniversaire, le nom d'un animal de compagnie, etc.

développement important du nombre de ces acteurs, entraînant ainsi une insécurité grandissante en matière de protection des *data*. À titre d'exemple l'existence de nombreux codes open-sources destinés au partage d'outils informatiques illustre plutôt bien cette accessibilité. Ils sont disponibles *via* des plateformes hébergeant du code tel que Github et peuvent notamment permettre d'obtenir les données personnelles relatives aux identifiants de connexion des appareils infectés. Théoriquement, n'importe qui peut donc avoir accès à ces outils et les utiliser à partir d'un terminal.

Enfin, les acteurs malveillants se multipliant et les outils informatiques se développant, une boucle se crée alors permettant de nombreuses innovations en la matière.

C'est aussi ce qui fait la particularité de ces acteurs par rapport à d'autres secteurs criminels. Cette facilité de partage de l'information se répercute aussi sur la préparation de l'attaque, permettant une mise en liaison bien plus rapide des acteurs entre eux *via* des espaces d'échanges comme les forums.

Cela peut s'analyser à la lumière de l'histoire de Marcus Hutchins dit MalwareTech. Il est notamment connu pour avoir participé activement au démantèlement du virus WannaCry, mais aussi à la création du virus Kronos, un célèbre ransomware[10] de vol de données bancaires. La mise en service de Kronos a pu se concrétiser par la mise en relation de différents acteurs malveillants, dont MalwareTech, par le biais de forums de partage de connaissance informatique. Son parcours se révèle très intéressant pour cet article car il se positionne du côté malveillant à ses débuts, puis du côté de la sécurité dans la suite de sa carrière. Sa connaissance importante des virus informatiques et notamment des rançongiciels lui a permis de se reconvertir et ainsi participer activement à la sécurisation des *data*.

Seulement, si le cas de MalwareTech n'est pas isolé au sein de la communauté des pirates informatiques, la sécurisation des *data* n'en devient pas pour autant aisée. Si un environnement de protection juridique a commencé à s'imposer au fil du temps pour contenir les abus de collectes par les sociétés précédemment évoqués, celui-ci reste à relativiser compte tenu de son efficacité limitée. De la même façon, si

[10] Le ransomware, ou rançongiciel en français, est un logiciel de cryptage de donnée. Il permet alors à l'attaquant de d'exiger certaines choses de la victimes en échange de la clé de décryptage.

les campagnes de prévention et de sécurité au niveau humain et matériel se sont multipliées au cours de cette décennie, les attaques visant les *data* n'en ont pas pour autant disparu.

II. Un déploiement exponentiel de moyens de sécurités à l'efficacité encore limitée

Si un cadre juridique européen en matière de protection des données personnelles s'est particulièrement développé au cours des années 2000, la mise en œuvre d'une protection effective de ce type contre les collectes abusives des sociétés se trouve néanmoins limitée de nos jours. Ces limites sont compensées en matière criminelle grâce aux entités de sécurité nationales et internationales, nécessitant toutefois un renforcement important de leurs moyens pour améliorer davantage cette protection.

La progression d'un cadre juridique communautaire de protection des données nécessitant un prolongement international

La sécurité juridique consacrée à la collecte des données personnelles en droit interne a souffert de retards significatifs[11].

Les premières traces de protection émanent de la loi du 6 janvier 1978, notamment connue pour avoir institué la Commission Nationale Informatique et Liberté. Si cette loi peut être considérée comme une base solide du fait de son renvoi exprès aux libertés fondamentales, le caractère général de celle-ci pourrait expliquer les carences ultérieures en la matière. En effet, il faudra ensuite attendre l'intervention du droit communautaire avec une directive du 24 octobre 1995[12], aujourd'hui abrogée mais dont le contenu sera repris au sein du Règlement Général sur la Protection des Données (RGPD)[13], pour connaître de notables évolutions.

Déjà à l'époque les priorités de l'État français semblaient ne pas prendre au sérieux cette protection, en témoigne la transposition de cette

[11] C. FÉRAL-SCHUHL, *Cyberdroit 2020/2021*, Paris, ed. Dalloz, 2020, 8ème ed, 1888p.
[12] Directive 95/46/CE du Parlement européen et du Conseil, relative à la protection des personnes physiques à l'égare du traitement des données à caractère personnel et à la libre circulation de ces données, 24 oct. 1995, *Journal Officiel*, n°L 281, pp. 0031 - 0050.
[13] Règlement 2016/679 du Parlement européen et du Conseil, relatif à la protection des personnes physiques à l'égare du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), 27 avr. 2016, *Journal Officiel*, n°L 119, pp. 1 - 88.

directive au sein d'une loi du 6 août 2004 soit six années après la limite de transposition posée par les institutions européennes. Bien qu'un problème d'inconstitutionnalité partielle vint entraver la bonne transposition de cette directive, il faut tout de même souligner qu'il aura fallu attendre la mise en place du gouvernement Jospin pour assister à une évolution en la matière.

Ce retard n'est cependant pas exclusivement français, puisque seules la Grèce et la Suède sont parvenues à transposer la directive dans leur droit interne à la fin de l'année 1998[14]. Si cela témoignait d'une faiblesse pouvant limiter l'efficacité du droit communautaire en matière de protection des données, la refonte de cette directive au sein du RGPD fut le symbole d'une évolution juridique majeure pour la protection des données personnelles. L'utilisation d'une directive fut la première erreur du conseil européen puisque ses particularités juridiques en font un texte moins contraignant pour les États. L'entrée en vigueur du RGPD le 25 mai 2018 a pallié ce problème en élevant au rang de règlement les mesures reprises. En ce sens, les États furent obligés de construire leur droit interne en fonction du règlement, quitte à écarter des lois contraires, ce qui ne s'imposait pas pour un texte transposant une directive.

En substance, c'est une mesure importante pour les libertés individuelles car elle permet de réguler plus fermement la réglementation des États membres. Cependant, se prononcer sur l'efficacité globale du RGPD reste actuellement difficile compte tenu de sa relative jeunesse. Comme souligné par Alexandra Mendoza-Caminade, le RGPD semble tout de même avoir eu un impact important sur la politique numérique des entreprises sur le territoire de l'UE. Elle remarque alors qu'un an après l'entrée en vigueur du règlement, environ 80% des entreprises locales ne seraient pas parvenues à entrer en conformité avec les dispositions qu'il contient[15]. La pratique permet alors de distinguer deux types de conduites face à ce règlement. D'une part les entreprises respectant ces dispositions en acceptant les nombreux désavantages, et celles contournant ou violant simplement le règlement, d'autre part.

[14] Seizième rapport annuel, sur le contrôle de l'application du droit communautaire (1998), 7 déc. 1999, *Journal Officiel*, n°C 354, p. 0001.
[15] A. MENSOZA-CAMINADE, « L'impact du RGPD sur l'activité des plates-formes en ligne », *Petites affiches*, 2019, n°122, p. 7.

Concernant celles s'étant confortées au RGPD, le résultat reste mitigé. Certes les politiques de cookies présentées précédemment furent l'objet d'une régulation très importante, mais cela ne signifie pas pour autant l'aboutissement à une protection effective des données personnelles. Les cookies restent automatiquement définis par la plateforme en ligne, l'apport du RGPD a cependant permis une meilleure visibilité du système de désactivation de ces derniers pour l'utilisateur. Deux problèmes majeurs en découlent.

Tout d'abord les cookies dits « indispensables » au fonctionnement du site restent obligatoires. Il s'agit en règle générale des cookies dans leur forme originaire présentés précédemment. Ces cookies étant indispensables, le désaccord de l'utilisateur entraîne souvent une impossibilité à bénéficier du contenu de la plateforme. Ensuite, la gestion des cookies s'avérant être une tâche relativement répétitive et chronophage si répétée sur une longue durée, il n'est pas improbable que de nombreux utilisateurs acceptent tous les cookies par gain de temps ou par facilité. Comme les cookies sont parfois pré-remplis par la plateforme, le RGPD s'avère assez peu efficace dans ce cas-la.

Il convient toutefois de préciser que la portée de ce règlement reste limitée aux États de l'Union européenne l'ayant ratifiée, ce qui pose un certain problème puisque qu'aucun autre grand acte juridique notable rassemblant des pays à l'échelle internationale ne semble avoir vu le jour.

Cela peut s'expliquer par de nombreux facteurs. Par exemple l'influence des GAFAM[16], ainsi que leurs ressources considérables leur permettent de pouvoir s'affranchir des juridictions locales. En ce sens, Google et Amazon furent condamnés par la CNIL à des amendes de plusieurs dizaines de millions d'euros pour non-respect de la législation sur les cookies publicitaires, en décembre 2020. La branche française de Google ayant réalisé à elle seule un chiffre d'affaires de 483 millions d'euros en 2019[17], le fait de payer l'amende pourrait potentiellement s'avérer plus intéressant pour elle que brider ses revenus en limitant la collecte de données.

Sans législation internationale globale, il semble alors difficile d'imposer par contrainte politique ou financière une pression suffisante

[16] Le mot GAFAM est une anagramme représentant 5 sociétés du numérique : Google, Amazon, Facebook, Android et Microsoft.
[17] *https://www.societe.com/societe/google-france-443061841.html*

sur certaines sociétés. D'autant qu'une législation de ce type semble plutôt illusoire au sens où certains de ces acteurs coopèrent activement avec certains États, entraînant alors un important conflit d'intérêts.

Si la protection concernant la collecte des données personnelles semble trouver des limites par rapport au commerce entre sociétés, celle-ci semble cependant se renforcer en matière de lutte contre la fraude et la cybercriminalité.

L'apport d'un soutien essentiel par les organisations de sécurité locales et internationales à développer davantage

Avec l'apparition de la Covid-19 et le développement rapide de la pandémie, bon nombre d'emplois ont connu une mutation de leur fonctionnement. Ceci s'explique au prisme de la mise en œuvre de confinements par la plupart des États touchés et la nécessité de continuer à exercer sa profession depuis chez soi. Avec l'augmentation de la dématérialisation des communications et la multiplication du nombre d'intermédiaires, la cybercriminalité a pu connaître des conditions extrêmement favorables à la mise en œuvre et à la réussite de ses opérations.

Afin de limiter le plus possible l'aboutissement de ces attaques, les agences de renseignement et d'information nationales ainsi que certaines organisations de coopération inter-étatiques ont développé des campagnes et outils de prévention. Cela fut l'objet d'un développement précis par Axel Castadot, chef de la division connaissance et anticipation au sein de l'ANSSI, lors de la conférence de l'AEGE : *La menace cyber au cœur de la transition numérique*[18]. Il détaille notamment la multiplication par quatre entre 2019 et 2020 des attaques de types rançongiciels, destinées à la prise en otage de *data*, dont la pandémie fut un catalyseur notoire. L'ANSSI intervient alors auprès des personnes physiques et morales en coopération avec les directions étatiques afin de prévenir les risques de cyberattaques. Serge Lefranc, conseiller au Commandement de la cyberdéfense, mentionnait que cette prévention débute avec des réflexes et attitudes à adopter relativement accessibles mais souvent oubliés. Il s'agit notamment de se demander s'il est réellement nécessaire de connecter certaines *data* à internet, mais aussi d'avoir une bonne vision des infrastructures matérielles et réseaux

[18] L'AEGE est « l'association des anciens de l'école de guerre économique » et dispense notamment de nombreuses conférences en relation avec les domaines stratégiques et ceux en lien avec l'intelligence économique.

dont les personnes disposent, ou encore se préparer en formant et en recrutant des personnes qualifiées pour répondre à certaines attaques.

Toutefois, ces campagnes de renseignement semblent avoir du mal à freiner l'effectivité des attaques, en témoignent notamment celles ayant touché différents hôpitaux français au cours de l'année 2020. Cela peut en partie s'expliquer par la visibilité relativement faible des campagnes d'informations liées au cyberespace par rapport à d'autres. En effet, si certaines campagnes comme celles de la sécurité routière s'imposent assez aisément grâce à une divulgation étendue sur plusieurs médias, celles concernant la cybersécurité semblent avoir du mal à sortir des médias web. Par exemple, les informations de l'ANSSI concernant les failles de sécurité des logiciels peuvent se retrouver facilement *via* leur compte twitter dédié : @CERT-FR. En revanche, les partages et relais se révèlent très faibles face à l'ampleur de certaines menaces et les indications fournies nécessitent de consulter régulièrement le site web de l'ANSSI[19], chose qui n'est certainement pas évidente pour ceux extérieurs au domaine du cyber. L'humain ayant un rôle majeur dans l'exploitation des failles de sécurité, sensibiliser les individus à la sécurité informatique est donc une base primordiale pour réduire les vols de *data*.

Cela s'explique aussi par le caractère relativement récent de ce type de criminalité. Toujours lors de cette conférence dispensée par l'AEGE, Vincent Desroches, chef de la division management et sécurité numérique, précisait que la prolifération massive des cyberattaques n'avait vu le jour qu'à partir des années 2010. Par rapprochement avec le caractère d'évolution rapide des outils et techniques disposés par les acteurs malveillants, il est encore assez difficile pour une personne d'assurer une sécurité effective de ses équipements.

Ces différents aspects ont alors permis le développement d'une répression qui s'améliore de jour en jour. En ce sens, de nombreuses agences et organisations internationales de lutte contre la criminalité ont développé au cours des dernières décennies des services exclusivement affectés au cyberespace. C'est le cas d'Europol qui, après sa création en 1995[20], développa progressivement son domaine d'action au sein du cyberespace pour finalement mettre en place le Centre européen de lutte contre la cybercriminalité durant l'année 2013.

[19] https://www.cert.ssi.gouv.fr

[20] Convention C 316 du Conseil, sur la base de l'article K.3 du traité sur l'Union européenne portant création d'un Office européen de police (convention Europol), 27 nov 1995, *Journal Officiel*, n°C 316/01, p. 2.

Cette évolution est démontrée par Jessica Eynard qui, au sein du Repertoire IP/IT et Communication, rappelle la fonction initiale motivant la création d'Europol à savoir la lutte « contre le terrorisme, le trafic illicite de stupéfiants et d'autres formes graves de la criminalité internationale »[21].

De ce fait, la création de ce centre fut une nécessité pour répondre à l'expansion de la criminalité dans le cyberespace au début des années 2010.

En l'espèce, plusieurs opérations menées par Europol en matière de cybersécurité ont pu aboutir au démantèlement de virus informatiques et groupes criminels. L'organisation de coopération a notamment participé à l'enquête sur le virus WannaCry. La pertinence de cette affaire réside dans le fait qu'une grande coopération internationale a pu voir le jour. Bien que Marcus Hutchins parvint à trouver la faille informatique ayant permis une destruction du logiciel, d'autres acteurs privés spécialistes en cybersécurité participèrent à la mise en œuvre de solutions partielles dans l'attente dudit démantèlement. C'est ainsi que les travaux de Benjamin Delphy[22] et Matthieu Suiche[23] aboutirent à la création d'un outil informatique de décryptage des *data* encodées par WannaCry, fonctionnant grâce à la récupération, par Adrien Guinet[24], de la clé privée de chiffrement après que ce dernier ait exploité les failles issues de la relation entre le virus et l'OS[25] de Windows XP[26].

Si cette coopération témoigne d'une capacité de coordination efficace des acteurs mondiaux en matière de récupération de *data* volées, celle-ci présente toutefois un revers à la médaille. En effet, elle atteste de la nécessité d'employer un certain nombre de moyens et de personnes, dont certains peuvent être d'origine privée ou même indépendants de toutes structures. Cela pose des problèmes de fiabilité mais aussi de souveraineté. En ce sens, la protection des données stratégiques ou sensibles devrait nécessiter une mainmise totale de la part de l'État ou de l'Union européenne sur le processus de sécurisation et de récupération de ces données, dans le cas où elles viendraient à être

[21] J. EYNARD, « Cybersécurité », *Répertoire IP/IT et Communication*, jan. 2021, 42.
[22] Responsable du Centre de Recherche & Développement en Sécurité pour la Banque de France.
[23] Spécialiste informatique et entrepreneur, fondateur de Comae Technologie entre autre.
[24] Ingénieur logiciel Recherche & Développement pour Quarkslab.
[25] Operating System, ou système d'exploitation est l'outil permettant de coordonner les communications entre la machine, l'utilisateur et les programmes informatiques.
[26] M. Untersinger, « « Rançongiciel » : trois Français trouvent un remède partie à WannaCry », *Le Monde*, 22 mai. 2017, p. 1.

la cible de ce genre d'attaque. Il est alors nécessaire de renforcer les moyens mis à disposition d'Europol ou des services de sécurité nationaux pour assurer de meilleures garanties de sécurité et ne pas dépendre d'acteurs privés ou indépendants.

Ces problématiques sont d'autant plus importantes que le cyberespace connaît actuellement un bouleversement technologique important. Avec l'arrivée de la 5G, le développement grandissant des intelligences artificielles et à l'aube de la première génération d'ordinateurs quantiques, les enjeux de sécurité informatiques vont prendre une dimension de plus en plus vitale. Ne pas assurer une protection suffisante des *data* de nos jours c'est prendre le risque d'accumuler un retard qui sera très difficile à rattraper dans le futur.

Bibliographie

- Donnée. (2021). *Dictionnaire Larousse*. Paris : Société Édition Larousse. *larousse.fr*

- Directive 95/46/CE du Parlement européen et du Conseil, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, 24 oct. 1995, *Journal Officiel*, n°L 281, pp. 0031 - 0050.

- Règlement 2016/679 du Parlement européen et du Conseil, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), 27 avr. 2016, *Journal Officiel*, n°L 119, pp. 1 - 88.

- G. TCHOUASSI, « Les besoins en informations dans les entreprises », *Revue Congolaise de Gestion*, 2017, n°24, pp. 63 - 92.

- P. BOULANGER, « Renseignement géographique et culture militaire », *Hérodote*, 2011, n°140, pp. 47 63.

- B. POILVÉ, « Une petite histoire du cookie », *linc.cnil.fr*, 14 jan. 2020, p. 1.

- C. CRIDDLE, « Facebook Sued Over Cambridge Analytica Data Scandal », *bbc.com*, 28 oct. 2020, p. 1.

- RABBIN DES BOIS, *Lève-toi et Code*, Paris, ed. de La Martinière, 2018, 112p.

- NSA - CYBERSECURITY PRODUCTS AND SHARING DIVISION, *NSA/CSS Technical Cyber ThreatFramework V2*, *nsa.gov*, 13 nov. 2018, p. 13.

- C. FÉRAL-SCHUHL, *Cyberdroit 2020/2021*, Paris, ed. Dalloz, 2020, 8ème ed, 1888p.

- Seizième rapport annuel, sur le contrôle de l'application du droit communautaire (1998), 7 déc. 1999, *Journal Officiel*, n°C 354, p. 0001.

- A. MENSOZA-CAMINADE, « L'impact du RGPD sur l'activité des plates-formes en ligne », *Petites affiches*, 2019, n°122, p. 7.

- Convention C 316 du Conseil, sur la base de l'article K.3 du traité sur l'Union européenne portant création d'un Office européen de police (convention Europol), 27 nov 1995, *Journal Officiel*, n°C 316/01, p. 2.

- J. EYNARD, « Cybersécurité », *Répertoire IP/IT et Communication*, jan. 2021, 42.

- M. Untersinger, « « Rançongiciel » : trois Français trouvent un remède partie à WannaCry », *Le Monde*, 22 mai. 2017, p. 1.