Lettre n°48 - mars 2016 - disponible sur omc.ceis.eu

«He led a team of hackers that stole campaign strategies, manipulated social media to create false waves of enthusiasm and derision, and installed spyware in opposition offices, all to help Peña Nieto, a right-of-center candidate, eke out a victory. » ***Article de Bloomberg[1] sur le pirate Andrés Sepúlveda, un colombien qui aurait espionné les concurents du candidat Peña Nieto à l'élection présidentielle mexicaine durant la campagne de 2012.***

Table des matières

[1] http://www.bloomberg.com/features/2016-how-to-hack-an-election/

L'EVOLUTION DES RELATIONS ENTRE LES SOCIETES TECHNOLOGIQUES ET LE GOUVERNEMENT AMERICAIN

Massacre du centre médical de San Bernardino - Source : CNN

Depuis début 2016, une polémique fait rage aux Etats-Unis : le bras de fer entre Apple et le FBI (*Federal Bureau of Investigation*) américain sur le déchiffrement de l'iPhone.

En décembre 2015, un centre médical à San Bernardino (en Californie) a été attaqué par un couple, Syed Rizwan Farook et Tashfeen Malik. Ces derniers ont tué quatorze personnes et en ont blessé une vingtaine d'autres. Suite à une enquête, le FBI a relié le couple à l'organisation terroriste ISIS (*Islamic State of Iraq and Sham*). L'agence américaine a alors aussitôt réclamé à Apple de l'aide pour accéder aux données présentes dans l'iPhone de Syed Rizwan Farook, une requête à laquelle la société américaine a refusé d'accéder.

Le smartphone récupéré par le FBI est un iPhone 5c, équipé de la dernière version du système d'exploitation iOS 9. Depuis les révélations réalisées par Edward Snowden sur l'espionnage généralisé des communications par la NSA, Apple a décidé d'augmenter le niveau de sécurité de son smartphone. La société a ainsi mis en place un chiffrement matériel depuis la version 8 du système d'exploitation (iOS), se basant sur des composants cryptographiques dans le téléphone et l'identifiant unique (UID) de l'iPhone. Les clés de déchiffrement du téléphone s'effacent automatiquement au bout de 10 tentatives infructueuses de déverrouillage par code PIN. Quelques mois plus tard, Google, avec son système Android Lollipop, va aussi promettre le chiffrement par défaut. Finalement, la société californienne a dû reculer, n'ayant pas réussi à convaincre les différents constructeurs de terminaux Android. Google fournit quand même l'option sur tous les terminaux Android.

Bien que les données présentes sur le compte iCloud du terroriste aient pu être récupérées (suite à un mandat, Apple donne accès au FBI aux contenus iCloud), la dernière synchronisation en ligne de l'iPhone datait d'un mois et demi avant la tuerie : il manquait donc beaucoup de données aux enquêteurs.

Le FBI a alors demandé à Apple de développer un fichier image non sécurisé de son système d'exploitation afin de pouvoir l'injecter dans l'iPhone de Farook et contourner toutes les différentes protections mises en place par la société californienne[2]. L'agence américaine avait en effet besoin d'Apple pour faire signer ce système d'exploitation « customisé » afin que le smartphone puisse certifier que le logiciel était viable et accepter la mise à jour. Pour le PDG d'Apple, Tim Cook, une telle action est cependant trop dangereuse[3] : la sécurité de l'iPhone ne serait plus jamais garantie et la société refuse donc de se soumettre à la requête du FBI.

Après des procédures judiciaires, basées sur une loi de 1789, l'*All Writs Act,* obligeant tout citoyen à fournir une aide aux autorités fédérales, l'affaire a pris un nouveau tournant : une source anonyme aurait fourni un moyen de déchiffrer le contenu de l'iPhone au FBI. De nombreux indices pointent vers l'entreprise israélienne Cellebrite[4], un des leaders du forensique numérique qui aurait signé un contrat d'exclusivité avec le FBI. Ce dernier a par la suite abandonné les charges contre Apple, et c'est maintenant Apple qui tente de trouver une solution juridique pour contraindre le FBI à lui fournir la méthode utilisée pour déchiffrer les données de l'iPhone.

Comme exposé ci-dessus, la relation entre Apple et le gouvernement américain n'est pas des plus simples. Cette dernière a commencé à se compliquer en 2013 suite aux révélations d'Edward Snowden. Ce prestataire de la NSA et de la CIA a rendu public différents programmes des agences américaines, tels que « PRISM » ou encore « DROPOUT JEEP » qui donnent accès à la NSA aux contenus présents sur les iPhones (messages vocaux, listes de contact, textos, fichiers, historique de géolocalisation) ainsi qu'à leur matériel (microphone et appareil photo)[5]. Ces révélations ont eu des conséquences importantes sur l'image des Etats-Unis, et des agences fédérales, principalement la NSA et la CIA. Et ce ne furent pas les seules : en 2013, le FBI fut sur le point d'obtenir de la Maison Blanche une nouvelle législation pour assurer à ses enquêteurs un accès au contenu de téléphones et autres appareils informatiques, sans qu'il soit nécessaire d'avoir un mandat. Les révélations d'Edward Snowden la même année ont réduit à néant ce projet, qui ne verra sûrement jamais le jour, estiment plusieurs hauts fonctionnaires[6].

Ce sont surtout les entreprises de technologies américaines qui ont ressenti cet « effet Snowden », sur le plan économique : selon un rapport[7] de juin 2015 de l'ITIF (*Information Technology and Innovation Foundation*), les pertes pour la seule industrie américaine du Cloud auraient dépassé largement les 35 millions de dollars depuis les révélations de Snowden. De même, selon le cabinet d'étude Forrester[8], 26 % des entreprises ont mis fin à leurs contrats, ou diminué leurs dépenses, avec des entreprises américaines offrant des services Internet, en raison des révélations de Snowden. Ainsi, beaucoup d'entreprises ont décidé de réagir pour regagner la confiance des clients.

En juin 2014, le président d'Apple, Tim Cook, présente lors d'une *keynote* le nouveau système d'exploitation de l'iPhone, iOS 8, avec des ajouts de fonctions de sécurité. Le FBI a ainsi découvert que ce nouveau système allait changer les techniques de collecte de preuves[9] : Apple a fermé un point d'accès important, utilisé pendant des années par les agents pour recueillir des informations sur les suspects. Selon Timothy Edgar[10], ancien directeur entre 2009 et 2010 de l'équipe à la Maison Blanche qui s'occupait des questions

[2] https://blog.trailofbits.com/2016/02/17/apple-can-comply-with-the-fbi-court-order/
[3] https://www.apple.com/customer-letter/
[4] http://www.cellebrite.com
[5] http://guardianlv.com/2013/12/nsa-project-dropout-jeep-hacked-into-apple-iphones/
[6] http://www.bloomberg.com/news/features/2016-03-20/the-behind-the-scenes-fight-between-apple-and-the-fbi
[7] http://www2.itif.org/2015-beyond-usa-freedom-act.pdf?_ga=1.238564416.1356037819.1433920357
[8] http://www.zdnet.com/article/snowden-prism-fallout-will-cost-u-s-tech-vendors-47-billion-less-than-expected/
[9] http://www.bloomberg.com/news/articles/2016-03-16/how-apple-helped-me-crack-iphones-like-clockwork
[10] http://www.bloomberg.com/news/features/2016-03-20/the-behind-the-scenes-fight-between-apple-and-the-fbi

de vie privée et des libertés civiles, « *la raison pour laquelle la relation avec le gouvernement s'est tendue, c'est qu'il attendait des entreprises de technologie un certain degré de coopération. Pour l'essentiel, il se disait que ces sociétés reculeraient et n'ajouteraient pas de nouvelles mesures de sécurité qui rendraient impossible l'accès aux appareils ou à leurs communications. Il a été pris de court lorsque les entreprises lui ont dit non* ». A la suite de ces évolutions de la sécurité d'iOS, des échanges ont eu lieu entre la Maison Blanche et Apple, cette dernière justifiant ces nouvelles mesures par la volonté de protéger les données des clients contre des pirates de plus en plus pointus, alors même que les iPhones recèlent toujours plus de données personnelles ou professionnelles. L'administration Obama fut finalement assez réceptive aux arguments sur le chiffrement : elle a même travaillé avec Apple pour persuader la Chine de ne pas forcer les fabricants de téléphones de donner aux autorités une clé pour les déchiffrer. Ainsi, le gouvernement n'a pas cédé aux requêtes du FBI en octobre 2015 sur l'idée d'imposer aux entreprises de collaborer avec l'agence américaine pour donner un accès à leurs appareils[11]. Les tueries de San Bernardino ont cependant permis au FBI de remettre le sujet sur la place publique en 2016, avec une affaire ayant des implications de sécurité nationale.

D'autres sociétés tentent aussi de faire amende honorable sur les questions de chiffrement et de vie privée, comme Google ou Microsoft après les révélations de Snowden de 2013.

Tout d'abord, elles décident de jouer la transparence : avant que l'image de ces sociétés soit écornée, seuls Twitter et Facebook publiaient des rapports annuels sur les demandes légales du gouvernement d'accéder à des informations personnelles d'utilisateurs, dans le cadre d'enquêtes. Quelques mois après le début de l'affaire Snowden, Apple et Facebook[12] décident de publier eux aussi ces rapports. En 2014, Apple, Google, Microsoft et Facebook ont fait le choix de prévenir personnellement l'utilisateur si ses informations personnelles sont transmises au gouvernement américain[13].

[11] http://www.wired.com/2015/10/cops-dont-need-encryption-backdoor-to-hack-iphones/
[12] http://www.techtimes.com/articles/6427/20140503/apple-facebook-microsoft-google-silence-government-data-collection.htm
[13] http://www.cultofmac.com/277085/apple-will-now-alert-nsa-asks-data/

Etat des lieux de 2013 faisait le point sur la politique des grandes sociétés de la Silicon Valley face aux demandes du gouvernement – Source : EFF

Etat des lieux de 2015 faisait le point sur la politique des grandes sociétés de la Silicon Valley face aux demandes du gouvernement – Source : EFF

En juillet 2015, un groupe d'experts internationalement reconnus dans le domaine de la sécurité informatique et de la cryptographie ont publié un manifeste « *Keys Under Doormats* »[14] contre la mise en place de faiblesses au sein du chiffrement des communications par les gouvernements américains et anglais. Parmi ces 14 auteurs, Susan Landau est employée chez Google et Josh Benaloh, chez Microsoft.

Les sociétés technologiques se mêlent aussi aux débats politiques sur ce type de sujets. Elles publient des lettres communes pour dénoncer des projets de loi qui vont contre leurs principes et intérêts. Par exemple, lors des débats de mai 2015 autour d'un projet de loi prévoyant le déchiffrement des communications par les forces de l'ordre américaines, ces sociétés ont, avec d'autres personnalités du monde de la sécurité, publié une lettre commune[15] de 6 pages à destination du président Obama pour dénoncer ce projet. Elles se regroupent pour avoir plus de poids dans le débat politique, ainsi que pour protéger leurs intérêts : leur

[14] http://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf?sequence=8
[15] https://static.newamerica.org/attachments/3138--113/Encryption_Letter_to_Obama_final_051915.pdf

groupement le plus connu, le CCIA (*Computer and Communications Industry Association*), comprend plus de 25 sociétés telles que Microsoft, Google, Facebook, Amazon, Nvidia, eBay, et Yahoo! Il est très présent sur les sujets de la propriété intellectuelle et sur la vie privée. Il joue aussi le rôle de lobby pour ces sociétés : lors des échanges en 2014 sur le droit à l'oubli entre Google et la Commission Européenne, la CCIA a publié un avis contre le droit à l'oubli, en le rapprochant de « censure de l'Internet »[16].

L'engagement des sociétés technologiques sur le thème de la protection des données de ses utilisateurs peut aller parfois jusqu'au tribunal. Ainsi, en juin 2014, le gouvernement américain engagea une procédure devant les tribunaux contre Microsoft[17] : la justice avait sommé la firme de mettre à la disposition du gouvernement l'accès aux emails d'un utilisateur stockés dans son Datacenter de Dublin en Irlande. Microsoft s'y était opposé, affirmant que les données en question étaient gérées par l'une de ses filiales étrangères et que les lois américaines ne devaient donc pas s'appliquer dans ce cas. La juge alla cependant dans le sens des autorités, en considérant que c'était le lieu de contrôle des informations, et non leur emplacement, qui comptait. L'affaire fut de nouveau jugée en appel en 2015, mais avec un verdict identique.

Des solutions plus techniques ont aussi été mises en place pour redonner confiance aux clients mondiaux. Microsoft a par exemple annoncé en novembre 2015 la construction de datacenters en Allemagne en partenariat avec Deutsche Telekom[18]. Pour éviter d'être sous le joug du *Patriot Act*[19] et du *Safe Harbor*, les données ne sont accessibles que par Deutsche Telekom, société allemande.

Fin 2014, quelques mois après son rachat par Facebook, l'application WhatsApp met en place un système de chiffrement de bout en bout de ses communications : il est ainsi impossible de connaitre le contenu des échanges des utilisateurs. Conséquence, le vice-président de Facebook pour l'Amérique Latine est arrêté début mars 2016 car WhatsApp a refusé de donner des informations à la police brésilienne dans le cadre d'un réseau de crime organisé présumé.

On observe ainsi que les GAFA ont évolué suite aux révélations de Snowden. Ils se sont émancipés du gouvernement américain et n'hésitent plus à affirmer publiquement, ou techniquement, leurs divergences d'opinion avec leur administration. On constate aussi que ces sociétés ne se contentent plus uniquement d'agir aux Etats-Unis. On a pu le mesurer en Europe lors des débats sur le *Safe Harbor* ou sur le droit à l'oubli auxquels elles n'ont pas hésité à participer pour protéger leurs intérêts.

Ainsi, en décembre 2015, Apple, Google ou encore Yahoo! ont milité contre la proposition de loi du gouvernement britannique « *Investigatory Powers Bill*[20] » traitant de la surveillance. Ce texte prévoit différentes mesures telles que l'obligation pour les entreprises technologiques de retirer tout chiffrement à la demande des autorités ou encore la mise en place de portes dérobées au sein des différents systèmes. A la suite des différents attentats qui ont frappé l'Europe, le chiffrement soulève ainsi une question beaucoup plus globale : comment régler le curseur entre liberté et sécurité ? Une partie de la réponse des sociétés technologiques consiste à rappeler qu'il est dangereux d'affaiblir les systèmes. Les pirates peuvent en effet utiliser ces mêmes vulnérabilités comme cela a pu être le cas avec les portes dérobées « d'administration » existantes, sur différents routeurs comme ceux de la marque Linksys, Netgear ou encore Cisco[21].

---

[16] http://www.ccianet.org/2014/05/ccias-response-to-european-court-of-justice-online-privacy-ruling/
[17] http://www.theguardian.com/technology/2015/sep/09/microsoft-court-case-hotmail-ireland-search-warrant
[18] https://www.rt.com/usa/321634-microsoft-germany-snowden-spying/
[19] Pour rappel, le Patriot Act autorise l'administration américaine à accéder à tout moment et sans autorisation judiciaire aux données informatiques des entreprises ou des particuliers qui ont un lien, quel qu'il soit, avec les États-Unis.
[20] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473770/Draft_Investigatory_Powers_Bill.pdf
[21] http://www.theregister.co.uk/2014/01/06/hacker_backdoors_linksys_netgear_cisco_and_other_routers/

Le refus d'Apple de transmettre ses clés au Gouvernement américain aura donc finalement permis à Apple de redorer son blason en s'épargnant une campagne de communication sur la « privacy ». Reste enfin à voir quelle sera la réaction d'Apple face à la toute récente requête d'un père de famille italien qui a demandé à la firme d'accéder aux données de son fils de 13 ans récemment décédé d'un cancer[22]. Les arguments juridiques ou techniques ne sont pas faciles à manier sur un terrain émotionnel…

[22] http://www.zone-numerique.com/iphone-il-demande-a-apple-de-debloquer-le-smartphone-de-son-fils-decede.html

LE DEBAT SUR LE CHIFFREMENT DANS LE MONDE

« Le Rapporteur spécial, reconnaissant que les outils de chiffrement et d'anonymisation, pour être valables, doivent être adoptés largement, encourage les Etats, les organisations de la société civile et les entreprises à s'engager dans une campagne visant à fournir aux utilisateurs du monde entier des technologies de chiffrement par choix ou par défaut et, si nécessaire, à garantir que les utilisateurs les plus vulnérables soient dotés des outils nécessaires pour exercer leur droit à la liberté d'opinion et d'expression en toute sécurité »[23].

Le 16 février 2016, un jugement[24] d'une cour fédérale américaine (*Federal District Court for the District of Central California*) ordonnait à Apple d'apporter son aide au FBI afin de déchiffrer un téléphone mobile (iPhone 5) saisi lors d'une perquisition menée dans le cadre de l'enquête sur la tuerie de San Bernardino. La réaction publique d'Apple[25] (refus et contestation devant un juge de la légalité du jugement) a alors lancé un débat parmi les acteurs de la société civile, les entreprises et les plus hautes autorités des Etats, chacun y allant de son commentaire. Si l'enjeu était, dans cette affaire, la création d'un précédent visant à permettre aux autorités américaines de forcer une entreprise à déchiffrer des données chiffrées dans le cadre d'une enquête, le débat de fond pourrait être résumé de la façon suivante : sécurité vs vie privée. Il s'agira donc de revenir sur la « crypto war » des 90 avant de s'intéresser au fond du débat puis de présenter les réactions des Etats face à cette affaire.

L'affaire Apple-FBI : un remake des années 90

Les débats autour du chiffrement ont commencé dès les années 70 avec l'apparition des moyens modernes de cryptologie et la clé de chiffrement publique[26]. Pour la première fois, deux chercheurs démontraient comment les individus et entreprises pouvaient sécuriser leurs données et communications. Face à ces évolutions, d'âpres discussions eurent lieu sur le droit pour les entreprises de vendre des systèmes et logiciels ayant un niveau de chiffrement élevé et du droit pour les universitaires de publier leurs recherches sur le chiffrement. Au sein des institutions gouvernementales, les réticences étaient nombreuses face à l'opportunité que ces découvertes offraient aux individus et entreprises. Les personnes travaillant avec ces technologies avaient tout de suite perçu les défis que la vulgarisation du chiffrement engendrerait pour les forces de l'ordre et les agences de renseignement.

L'accès de plus en plus large par les individus aux ordinateurs, téléphones et autres moyens de communications et l'explosion d'Internet dans les années 90 ont amené le gouvernement américain à adopter une série de mesures visant à lutter contre le développement du chiffrement. En 1993, l'administration Clinton proposa la puce Clipper (*Clipper chip*) dont l'objectif était de pouvoir accéder aux données chiffrées. Le projet de loi visait à autoriser l'installation de puces de sécurité qui brouillerait les communications par un algorithme de chiffrement, *Skipjack*, les rendant ainsi protégées. La description de l'algorithme n'était pas publique puisque celui-ci était l'œuvre de la NSA. Cependant, la mise à disposition de l'algorithme était conditionnée à l'insertion d'une porte dérobée connue sous le nom de « *Law Enforcement Access Field* » visant à permettre aux agents gouvernementaux un accès à la clé de chiffrement. Les réactions de la société civile[27], du monde

[23] Conseil des droits de l'homme, Rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, David KAYE, A/HRC/29/32, 22 mai 2015, p.24
[24] https://assets.documentcloud.org/documents/2714001/SB-Shooter-Order-Compelling-Apple-Asst-iPhone.pdf
[25] https://www.apple.com/customer-letter/
[26] Whitfield Diffie and Martin Hellman, "New Directions in Cryptography," IEEE Transactions on Information Theory, Vol. IT-22, Nov. 6, November 1976. http://www.cs.tau.ac.il/~bchor/diffie-hellman.pdf

[27] Eric Hughes, "Welcome to the Cypherpunks Email," Cyphernomicon, September 10, 1994, available at http://www.cypherpunks.to/faq/cyphernomicron/chapter4.html; "Electronic Petition to Oppose Clipper," Computer Professionals for Social Responsibility, January 24, 1994, available at https://www. epic.org/crypto/clipper/cpsr_electronic_petition.html

universitaire[28] ou encore des industriels[29] furent nombreuses et virulentes et un véritable bras de fer s'engagea alors avec l'administration Clinton. Parmi les arguments avancés, figuraient une baisse de la sécurité des systèmes, l'augmentation de la complexité techniques des systèmes, les difficultés (insurmontables ?) de mise en œuvre à l'échelle mondiale ou encore l'augmentation du coût pour les utilisateurs[30].

Face à l'opposition, le gouvernement modifia son projet et proposa un système de recouvrement des clés de chiffrement qui serait opéré par des acteurs privés et non par une agence gouvernementale. Les réactions négatives furent nombreuses, tant du côté des acteurs privés que de certaines organisations internationales ou régionales. Ainsi, l'Organisation pour la coopération et le développement en Europe adopta une Recommandation relative aux Lignes directrices régissant la politique de cryptographie dans laquelle elle reconnut le rôle primordiale que pouvait jouer la cryptographie dans la protection de la vie privée et pour avoir un *« usage sûr des technologies de l'information en garantissant la confidentialité, l'intégrité et la disponibilité des données »*. Les lignes directrices encourageaient la libre circulation des outils de cryptographie *(« les utilisateurs devraient avoir le droit de choisir toute méthode cryptographique, dans le respect de la législation applicable »*) et reconnaissaient un droit d'accès légal dans le respect d'un certain nombre de principes *(« les politiques nationales à l'égard de la cryptographie peuvent autoriser l'accès légal au texte en clair ou aux clés cryptographiques de données chiffrées. Ces politiques doivent respecter dans toute la mesure du possible les autres principes énoncés dans les lignes directrices »*). La Commission européenne adopte, au même moment, une déclaration allant dans le même sens[31].

Les débats continuèrent et le gouvernement finit par abandonner son projet, se tournant vers la législation en matière d'exportation de matériels de guerre pour limiter l'exportation des technologies de chiffrement. En effet, ces technologies étaient assimilées à des munitions et par conséquent, soumises à ce régime juridique. Plusieurs affaires judiciaires sont venues étayer le débat, fondant le droit à l'exportation sur le respect du 1er amendement et le droit à la vie privée. Entre 1996 et 2000, l'administration Clinton procéda à plusieurs assouplissement de la législation applicable à ces technologies, changeant d'abord leur qualification, puis libéralisant l'exportation pour certains secteurs d'activités (finance, santé) et enfin pour toutes les technologies, quelle que soit leur utilisation finale.

Au-delà des enjeux commerciaux pour les entreprises, c'est un débat sur la protection de la vie privée face à la mission de sécurité publique qui a marqué la « crypto war ».

Chiffrement : sécurité vs vie privée, sécurité informatique et responsabilité des entreprises du web

Les débats autour du chiffrement et l'accès par les autorités aux données cryptées, quel que soit le moyen utilisé (introduction de portes dérobées, système de recouvrement de clés ou recours au *brute force* par exemple), soulèvent trois grandes questions : l'équilibre sécurité vs vie privée, le risque d'atteinte à un haut niveau de sécurité informatique et le rôle et la responsabilité des entreprises.

Un des enjeux autour du chiffrement est l'équilibre, ou le rapport de force, à trouver entre le besoin de sécurité et le respect de la vie privée et de la liberté d'expression. En effet, les technologies de l'information et des

[28] Bruce Schneier (dir.), The risks of key recovery, key escrow, and trusted third party encryption, 27 mai 1997, http://academiccommons.columbia.edu/catalog/ac:127127
[29] "Letter to the President," Computer Professionals for Social Responsibility, January 24, 1994, available at http://cpsr.org/prevsite/program/clipper/cpsr-clipper-letter.html/; Matt Blaze, "Protocol Failure in the Escrowed Encryption Standard," AT&T Bell Laboratories, 1994, http://www.crypto.com/papers/eesproto.pdf; John Marko , "Computer Code Plan Challenged," The New York Times, May 29, 1993, http://www.nytimes.com/1993/05/29/business/ company-news-computer-code-plan-challenged.html
[30] Bruce Schneier (dir.), The risks of key recovery, key escrow, and trusted third party encryption, op.cit, p.3
[31] Towards a European Framework for Digital Signatures and Encryption," European Commission, October 8, 1997, http://groups.csail.mit.edu/mac/classes/6.805/articles/crypto/eu-october-8-97.html

communications ouvrent des possibilités immenses pour le développement économique et social. Internet, via le développement de services de messagerie ou de réseaux sociaux, est un outil précieux offrant de nouvelles opportunités en termes de moyens de communication. Il est devenu, selon David KAYE, Rapport spécial des Nations unies sur la promotion et la protection du droit à la liberté d'opinion et d'expression, *« la principale tribune publique mondiale »*[32]. Cependant, les technologies numériques présentent également un risque pour la sécurité dans la mesure où elles permettent à de nombreux acteurs, mal intentionnés, de communiquer et d'échanger. De même, elles donnent aux pouvoirs publics de nouvelles opportunités pour surveiller les citoyens et collecter des données.

Les outils de chiffrement et d'anonymisation permettent de protéger d'une part la confidentialité des contenus, et d'autre part leur intégrité en les prémunissant contre des tentatives d'intrusion ou de manipulation. L'accès relativement facile à ces outils, imposé par défaut par les entreprises ou recherché et utilisé consciemment par les individus, comporte des aspects positifs et négatifs. En effet, elles mettent à disposition des citoyens des moyens pour protéger leurs communications et s'assurer du respect de leur vie privée en empêchant que celles-ci soient lues par des tiers non sollicités. Elles permettent en outre à chacun de pouvoir échanger des idées et de débattre sans risque d'immixtion et d'assurer le droit à la liberté d'expression, les individus n'ayant pas la crainte d'être condamnés pour des propos tenus. A contrario, elles offrent aussi l'opportunité à des criminels de communiquer de façon sécurisée, sans que leurs conversations soient surveillées. En cas de surveillance d'un individu par des forces de l'ordre, ces dernières pourront être confrontées à l'impossibilité d'accéder au contenu des conversations, empêchant peut-être la survenance d'un délit ou d'un crime. De même, dans le cadre d'enquêtes judiciaires postérieures à la commission d'une infraction, certains échanges, pourtant nécessaires à l'avancement de l'enquête, pourront ne pas être lus par les agents gouvernementaux, nuisant ainsi au bon fonctionnement de la justice. C'est ce côté obscur du chiffrement qui est régulièrement dénoncé par les autorités de certains pays. Pour faire face à cette situation, lesdites autorités ont invoqué la nécessité de disposer de moyens leurs permettant d'accéder au contenu des communications, l'un deux étant l'insertion de portes dérobées ou l'établissement de systèmes de recouvrement des clés de chiffrement. Dès lors, il s'agit de trouver un équilibre entre les besoins des forces de l'ordre et des agences de renseignements et la nécessaire protection de la vie privée et de la liberté d'expression des citoyens.

Les droits au respect de la vie privée et à la liberté d'expression *« sont essentiels à la dignité humaine et à la gouvernance démocratique »*[33]. Les conventions internationales en matière de protection des droits de l'homme et la jurisprudence associée reconnaissent la nécessaire existence de limites à ces droits. Cependant, pour être légales, ces limites doivent traditionnellement respecter plusieurs conditions : être prévues par la loi, être appliquées de manière stricte et uniquement dans des circonstances exceptionnelles et être nécessaires et proportionnelles. Les propositions des gouvernements devront donc répondre à ces critères. Les limitations devront répondre à un objectif précis (ordre public, sécurité nationale, etc.). Les Etats devront démontrer que les restrictions apportées au chiffrement sont nécessaires pour atteindre l'objectif affiché, qu'il n'existe pas d'autre moyen d'y parvenir. Enfin, ils devront évaluer le caractère proportionnel de la limite par rapport à l'objectif et à sa non application. Ainsi, la restriction devra *« constituer le moyen le moins perturbateur parmi ceux qui pourraient permettre d'obtenir le résultat recherché »*[34]. C'est sans doute là que le bât blesse lorsque l'on examine les différentes demandes gouvernementales. En effet, l'introduction de portes dérobées ou l'obligation pour les entreprises de divulguer aux autorités étatiques les clés de chiffrement utilisées semble non seulement disproportionné par rapport aux conséquences pour les individus, mais également disproportionné par rapport à l'objectif de création d'une culture mondiale de la cybersécurité[35].

---

[32] Conseil des droits de l'homme, Rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, David KAYE, op.cit., p.5
[33] Ibid., p.7
[34] Comité des droits de l'homme sur la liberté de circulation, Observation générale n°27 (1999), para. 14
[35] Assemblée générale des Nations unies, résolution sur la Création d'une culture mondiale de la cybersécurité et protection des infrastructures essentielles de l'information, A/RES/58/199, 30 janvier 2004

C'est en effet le deuxième enjeu derrière le débat sur l'accès demandé par les autorités gouvernementales aux données chiffrées. Il existe un consensus au sein de la communauté internationale, mais également entre les Etats et les acteurs privés (société civile, entreprises) sur la nécessité d'avoir un haut niveau de sécurité. Or, en organisant un système d'accès permanent aux données et communications chiffrées par les forces de l'ordre, est invoqué le risque d'atteinte à cet objectif. De nombreux chercheurs et entreprises ont soulevé le danger que représentaient les demandes gouvernementales pour la sécurité informatique. D'après un rapport[36] publié par des experts en cryptographie courant 2015, cela entraînerait un tournant à 180° dans le recours aux bonnes pratiques instituées pour rendre Internet plus sûr. De même, cela augmenterait significativement la complexité des systèmes. La complexité étant l'ennemi de la sécurité puisque créant plus de risques de vulnérabilités, on s'éloignerait rapidement de l'objectif d'un haut niveau de cybersécurité.

Enfin, les débats autour du chiffrement posent une nouvelle fois la question de la responsabilité des entreprises du web et des plateformes d'intermédiation. Dans un contexte post-Snowden où la coopération des entreprises avec les services de renseignement a été largement montrée du doigt et dénoncée, la question de la responsabilité des entreprises et du niveau de coopération qu'elles doivent entretenir avec les autorités est centrale. Suite aux révélations, elles ont annoncé une augmentation du niveau de sécurité des produits et services offerts et nombre d'entre elles ont adopté un système de chiffrement par défaut. Ce faisant, elles offrent aux utilisateurs une meilleure protection de la confidentialité et de l'intégrité de leurs données et communications. Cependant, elles sont à l'origine des difficultés que peuvent rencontrer les forces de l'ordre et ces dernières vont dès lors se tourner vers elles pour accéder aux contenus souhaités. Elles ont ainsi le pouvoir de faciliter ou d'entraver le chiffrement. Pour les entreprises, l'enjeu est donc d'assurer la confiance des clients tout en aidant, dans la mesure du possible, les autorités gouvernementales à remplir leurs missions.

Bien que n'étant pas des sujets du droit international, celui-ci a peu à peu pris en compte la place grandissante qu'occupent les entreprises. Les Nations unies ont reconnu que les entreprises avaient *« la responsabilité de faire respecter les droits de l'homme dans le cadre de toutes leurs activités mondiales, où que se trouvent leurs utilisateurs, et ce, indépendamment du fait que l'Etat s'acquitte ou non de ses propres obligations en matière de droits de l'homme »*[37]. A partir de ce rappel, il y a donc une profonde réflexion à mener sur le rôle des entreprises et les limites à leur liberté d'action en matière de coopération publique privée.

La question du chiffrement dans le monde

Suite aux attentats contre Charlie Hebdo et du 13 novembre 2015 en France, le débat sur l'accès par les autorités aux données chiffrées et la coopération des entreprises du web a été relancé. Les attaques de San Bernardino début décembre 2015 et le bras de fer entre Apple et le FBI aux mois de février et mars 2016 ont définitivement installé les discussions sur la scène publique. Courant 2015, le Congrès avait débattu, dans le cadre de la révision du *Communications Assistance for Law Enforcement Act*, de l'obligation qui pourrait être imposée aux entreprises du web de mettre en œuvre des processus visant à permettre aux agences gouvernementales d'accéder aux données. Les membres du Congrès n'avaient pas souhaité créer une telle obligation et l'administration Obama avait retiré le projet. Des débats similaires ont eu lieu dans plusieurs pays et enceintes internationales et certains ont fait voter des lois relativement contraignantes pour les entreprises.

Au Royaume-Uni, le premier ministre a adopté une position très agressive à l'encontre des entreprises du web, prenant parti pour un large accès par les autorités aux données chiffrées au détriment de la protection du droit à la vie privée et à la liberté d'expression. Ainsi, il a dès janvier 2015 proposé d'interdire le chiffrement

[36] Bruce Schneier (dir.), Key under doormats : mandating insecurity by requiring government access to all data and communications, 7 juillet 2015, 31p.
[37] Human Rights Council, The right to privacy in the digital age, A/HRC/27/37, 30 juin 2014

de bout en bout[38]. Le 1er mars 2016, une nouvelle version du projet de loi sur le renseignement a été présentée. Elle contient une disposition visant à imposer aux entreprises l'obligation de déchiffrer les contenus à la demande des autorités lorsque cela est faisable[39]. Le projet de loi est débattu en ce moment à la Chambre des communes. En 2014, le gouvernement britannique avait déjà essayé de faire adopté un projet de loi semblable, surnommé à l'époque « *Snoopers' Charter* ».

La position allemande est aux antipodes du discours britannique. En effet, le gouvernement allemand encourage l'utilisation par tous ses citoyens de moyens de chiffrement. Dans le Digital Agenda 2014-2017[40] publié par le gouvernement fédéral en août 2014, le rôle du chiffrement dans la protection du droit à la vie privée des citoyens ainsi que dans la robustesse des communications est souligné à plusieurs reprises. Le gouvernement annonce également son soutien à ces techniques : *« Nous supportons une plus grande et meilleure utilisation du chiffrement et aspirons à devenir le leader mondial dans ce domaine. Pour y parvenir, le chiffrement des communications privées doit être adopté comme un standard. Nous étendrons le recours à des technologies de sécurité telles De-Mail[41] »*[42]. Le texte va plus loin en reconnaissant le devoir de l'industrie, de la science et des décideurs politiques dans le développement et la vulgarisation de ces produits, pour le bien de tous[43].

Toujours en Europe, l'ENISA a publié début janvier 2016 un rapport[44] dans lequel elle se prononce contre l'insertion de portes dérobées et en faveur d'une libre et sûre utilisation du chiffrement afin de protéger les citoyens européens. L'organisme explique également en quoi la non protection des communications est une menace et le rôle que joue la confiance des utilisateurs dans le développement du commerce électronique. Le commissaire européen chargé du Marché numérique unique, Andrus ANSIP, s'est prononcé sur ce sujet devant le Parlement européen en mai 2015, affirmant que l'Union européenne ne voulait pas autoriser la création de portes dérobées afin de faciliter l'accès, par les Etats, aux données des citoyens européens. Cette déclaration était venue mettre un terme au flou entourant la position de la Commission, suite à l'intervention[45] du coordinateur de l'Union européenne pour la lutte contre le terrorisme qui invitait l'Union européenne à obliger les entreprises à transmettre aux autorités les clés de chiffrement lorsque celles-ci les demandaient.

L'attitude des autorités brésiliennes face au chiffrement et à la coopération des entreprises privées avec les autorités a pu surprendre, près de trois ans après les déclarations de la présidente suite aux révélations de Snowden sur l'espionnage de son pays par les services de renseignement américains. En effet, début mars 2016, le vice-président de Facebook pour l'Amérique Latine a été arrêté par la police brésilienne suite au refus de l'entreprise de collaborer avec la justice du pays. Il était demandé à WhatsApp (propriété de Facebook), de livrer des informations sur un utilisateur de l'application dans le cadre d'une enquête judiciaire. Quelques mois plus tôt, le réseau social avait été suspendu pour non coopération avec les autorités.

Enfin, citons le cas de la Chine qui, dans une loi votée en décembre 2015, semble exiger des entreprises souhaitant s'installer sur son territoire qu'elles aient un exemplaire de la clé de chiffrement afin de pouvoir la

---

[38] Rowena Mason, "U.K. spy agencies need more powers, says Cameron," The Guardian, January 12, 2015, http://www.theguardian.com/uk-news/2015/jan/12/uk-spy-agencies-need-more-powers-says-cameron-paris- attacks; Rob Price, "The U.K. government insists it's not going to try and ban encryption," Business Insider, July 14, 2015, http://www.businessinsider.com/uk-government-not-going-to-ban-encryption-2015-7

[39] http://www.publications.parliament.uk/pa/bills/cbill/2015-2016/0143/16143.pdf

[40] Germany, The Federal Governement, Digital Agenda 2014-2017, août 2014, 36p., disponible sur https://www.digitale-agenda.de/Content/DE/_Anlagen/2014/08/2014-08-20-digitale-agenda-engl.pdf?__blob=publicationFile&v=6

[41] « De-Mail est un moyen de communication qui doit permettre l'échange de donnée confidentielles et contractuelles par Internet. De-Mail est un projet du gouvernement allemand en partenariat avec plusieurs fournisseurs de services. Le but est de permettre une réduction des coûts des échanges de documents pour les entreprises. » Source : Wikipedia

[42] Ibid., p.21

[43] Ibid., p.5

[44] ENISA, On the free use of cryptographic tools for (self) protection of EU citizens, janvier 2016, 4p., disponible sur https://www.enisa.europa.eu/media/key-documents/on-the-free-use-of-cryptographic-tools-for-self-protection-of-eu-citizens

[45] http://www.pcworld.com/article/2874012/eu-should-oblige-internet-firms-to-hand-over-encryption-keys-says-antiterrorist-advisor.html

transmettre aux autorités chinoises si celles-ci le demandent. Il faudra attendre de voir comment la loi est interprétée et mise en œuvre pour déterminer la nature de l'obligation.

Face à la multiplication des attaques informatiques et alors que les débats sur les programmes de surveillance de masse continuent de se poursuivre, la question du chiffrement et de la collaboration des entreprises privées avec les autorités gouvernementales constitue un nouveau défi pour les individus. Soumis à une chasse à leurs données, ils vont devoir dessiner les contours du concept de droit à la vie privée sous peine d'être totalement démis de ce pouvoir. Quant aux Etats souhaitant mettre en œuvre des procédés d'affaiblissement du chiffrement, la question de la mise en œuvre extraterritoriale de ceux-ci ainsi que la gestion des demandes par les différentes juridictions devra être particulièrement examinée. Enfin, la légitimité de ces Etats dans la lutte contre la censure et pour un Internet sûr, pacifique et ouvert, sera sans nul doute compromise. Les Etats se trouvent donc à nouveau à un tournant et les décisions prises auront nécessairement un impact sur le futur d'Internet.

La **Direction Générale des Relations Internationales et de la Stratégie (DGRIS)** propose les analyses politiques et stratégiques contribuant à renforcer l'appréciation des situations et l'anticipation. Elle soutient la réflexion stratégique indépendante, en particulier celle menée par les instituts de recherche et organismes académiques français et étrangers. Elle contribue au maintien d'une expertise extérieure de qualité sur les questions internationales et de défense.

A ce titre, la **DGRIS** a confié à **CEIS** la réalisation de cet **Observatoire du Monde Cybernétique**, sous le numéro de marché 1502492543. Les opinions développées dans cette étude n'engagent que leur auteur et ne reflètent pas nécessairement la position du Ministère de la Défense.

Ministère de la Défense et des Anciens combattants
Direction Générale des Relations Internationales et de la Stratégie
14 rue Saint-Dominique - 75700 – Paris SP 07

CEIS
280 Boulevard Saint-Germain - 75007 - Paris
Téléphone : 01 45 55 00 20
E-mail : omc@ceis-strat.com