CHIFFREMENT

UNE QUESTION DE DROITS HUMAINS

AMNESTY INTERNATIONAL

SOMMAIRE

SYNTHESE

Aujourd'hui, plus de trois milliards de personnes dans le monde ont accès à Internet. Les entreprises, les hôpitaux et les agences gouvernementales conservent nos informations personnelles dans des bases de données et des ordinateurs connectés à Internet. Les appareils que nous utilisons au quotidien, les smartphones et les ordinateurs, mais également de plus en plus les voitures, les montres et les télévisions, conservent et transmettent nos informations personnelles.

Cette gigantesque quantité de données personnelles, de nos messages et courriels à notre historique de navigation, de nos informations bancaires à nos dossiers médicaux, peut être exposée aux vols et à l'espionnage, que ce soit par des criminels cherchant à voler ou extorquer de l'argent, ou par des gouvernements qui espionnent leur population.

Le chiffrement est un outil essentiel pour protéger nos données personnelles. S'il existe différents types de chiffrement, leur but est toujours le même : s'assurer que les informations ne puissent être accessibles qu'à leur propriétaire ou leur destinataire prévu. Par exemple, dans le cas des courriels, le chiffrement garantit que seuls l'expéditeur et le destinataire peuvent lire le courriel ; si une personne interceptait votre connexion internet, elle ne verrait que des informations cryptées.

Au titre du droit international, les États sont tenus de respecter, garantir et mettre en œuvre le droit à la vie privée de leur population. À l'ère du numérique, cela signifie que les États sont tenus d'assurer la sécurité des communications en ligne, notamment en menant des actions de sensibilisation à la sécurité sur Internet, en encourageant l'identification et la réparation des failles de sécurité sur les réseaux et systèmes informatiques, et en facilitant l'usage d'outils et de services de chiffrement.

Les menaces contre nos données privées sont réelles, et elles augmentent tous les jours. Des millions de personnes à travers le monde se font dérober leurs données personnelles à cause du vol ou de la perte de leurs smartphones et ordinateurs, et à cause d'importantes violations de données d'entreprises ou d'agences gouvernementales. Ces vols de données sont une menace à la fois pour la sécurité et pour la vie privée.

Dans le même temps, on assiste à une augmentation des menaces et des violations de notre droit à la vie privée de la part des gouvernements, par le biais d'une surveillance non justifiée. Depuis 2013, nous avons découvert toute l'étendue des programmes de surveillance de masse menés par les services de renseignements aux États-Unis et au Royaume-Uni. Pendant des années, ces programmes ont opéré dans l'ombre et espionné les communications Internet et téléphoniques de centaines de millions de personnes dans le monde entier.

En plus de cela, la technologie permettant une surveillance électronique ciblée est devenue très répandue et accessible. Ces dernières années, des preuves ont émergé de l'utilisation de technologies de surveillance contre des défenseurs des droits humains dans des pays tels que le Bahreïn ou l'Éthiopie. En 2015, plusieurs pays dont le Pakistan, la France, la Pologne, la Suisse et le Royaume-Uni ont promulgué des lois ou déposé des projets de loi dans le but d'augmenter le périmètre de la surveillance électronique et d'octroyer au gouvernement des pouvoirs intrusifs pour espionner les communications électroniques.

À l'ère du numérique, l'accès au chiffrement et son utilisation favorisent le plein exercice du droit à la vie privée. En protégeant les communications des tentatives d'espionnage, le chiffrement peut aider les individus à partager leur opinion avec d'autres personnes sans risques de représailles, à accéder aux informations sur Internet et à s'organiser à plusieurs pour lutter contre l'injustice. Le chiffrement favorise donc le plein exercice du droit à la liberté d'expression, d'information et d'opinion, et il a également un impact sur le droit à la liberté de réunion pacifique et d'association ainsi que sur d'autres droits humains. Le chiffrement est un outil particulièrement indispensable pour les défenseurs des droits humains, les militants et les journalistes, qui y ont de plus en plus recours pour assurer leur sécurité et celle des autres contre la surveillance illégale.

Cependant, de nombreux gouvernements critiquent le chiffrement et ont mis en place des mesures visant à empêcher ou à restreindre la possibilité pour des individus de chiffrer des données. Des pays comme le Pakistan, l'Inde et Cuba interdisent le chiffrement, limitent la complexité du chiffrement légal ou exigent des utilisateurs une autorisation pour pouvoir utiliser des méthodes de chiffrement. Dans des pays comme la France, le Royaume-Uni et les États-Unis, des représentants du gouvernement ont critiqué le chiffrement en avançant la crainte de « plonger dans le noir » les services de renseignement, c'est à dire que certains pans des communications en ligne ne puissent plus être accessibles aux agences chargées de l'application des lois ou aux services de renseignement.

Il est incontestable qu'un chiffrement complexe peut entraîner des difficultés pour accéder à des informations dans le cadre de l'application légitime des lois. Les gouvernements sont tenus de protéger leurs populations contre les crimes, y compris le terrorisme, et la surveillance électronique peut être employée de manière légitime dans ce but, si elle est mise en œuvre dans les limites fixées par le droit international.

Cependant, en essayant de surmonter la barrière du chiffrement, les autorités ne doivent pas violer le droit à la vie privée et à la liberté d'expression, ni aucun autre droit pour lequel la sécurité des données et des communications électroniques est essentielle.

Étant donné le rôle joué par le chiffrement des données dans la jouissance de ces droits, Amnesty International estime que les restrictions à l'accès et à l'usage du chiffrement peuvent être considérées comme une ingérence dans la jouissance des droits humains. Ainsi, afin de ne pas bafouer leurs obligations en matière de droits humains, les États doivent s'assurer que toutes les restrictions au chiffrement sont inscrites dans la législation de manière précise et transparente, qu'elles ne sont employées qu'en cas de nécessité pour atteindre un objectif légitime et qu'elles n'instaurent pas de discrimination à l'égard de groupes ou d'individus spécifiques.

Toute ingérence dans le chiffrement des données doit être proportionnée à l'objectif légitime qui a motivé son imposition, et les avantages retirés doivent l'emporter sur les dommages causés, notamment aux individus et à la sécurité et à l'infrastructure des réseaux.

Dans des pays comme la France et les États-Unis, deux types de technologies de chiffrement inquiètent les représentants du gouvernement : le chiffrement de bout en bout et le chiffrement complet des données d'un disque dur ou d'un appareil. Le chiffrement de bout en bout est une technologie qui limite l'accès au contenu de communications (courriels, messages, appels vocaux et vidéo) aux seules parties intéressées ; même le fournisseur de service ne peut pas déchiffrer la communication. En pratique, cela signifie que si une agence gouvernementale demande au

fournisseur de service de lui remettre le contenu de la communication, celui-ci ne peut pas donner suite à cette demande.

Le chiffrement des données d'un appareil est au cœur du litige qui oppose actuellement Apple et le FBI. Ce type de chiffrement, installé par défaut sur certains smartphones récents, se caractérise par le fait que toutes les données de l'appareil sont chiffrées et illisibles sans le mot de passe ou le code PIN requis. Même si les autorités mettent la main sur un téléphone chiffré, elles ne peuvent pas accéder de manière intelligible aux informations qu'il contient si elles ne disposent pas des bons codes.

Dans l'affaire Apple c. FBI, si l'entreprise venait à être contrainte de modifier son logiciel pour débloquer le téléphone en question, cela créerait un précédent qui permettrait au gouvernement américain, et éventuellement à d'autres gouvernements, de contraindre les entreprises technologiques à changer leurs produits pour en affaiblir ou contourner le chiffrement en créant une « porte dérobée » pour les services de renseignements et autres agences de sécurité.

Le fait de contraindre les entreprises à créer des « portes dérobées » au chiffrement intégré sur leurs produits et services (affectant potentiellement tous les utilisateurs) constitue une ingérence considérable dans le droit des utilisateurs à la vie privée et à la liberté d'expression. Étant donné que ces mesures affectent de manière indiscriminée la vie privée en ligne de tous les utilisateurs en affaiblissant la sécurité de leurs communications électroniques et de leurs données personnelles, Amnesty International considère qu'elles sont fondamentalement disproportionnées, et donc inacceptables au regard du droit international relatif aux droits humains

Le chiffrement favorise le plein exercice des droits humains. Selon les mots du rapporteur spécial de l'ONU sur la liberté d'expression, il offre aux « individus et aux groupes une zone de confidentialité en ligne pour exprimer leurs opinions et exercer leur liberté d'expression sans faire l'objet d'attaques ou d'immixtions arbitraires et illégales ».

Alors que de plus en plus de nos informations personnelles sont enregistrées sur des appareils connectés à internet et transmises à travers les réseaux, dans de nombreux pays les gouvernements portent atteinte à notre droit à la vie privée en pratiquant une surveillance non justifiée. Le chiffrement est une technologie qui nous permet de nous protéger, aussi bien des violations de notre droit à la vie privée commises par les gouvernements, que des criminels qui tentent de voler notre identité. De fait, les gouvernements qui interdisent l'utilisation du chiffrement ou qui essaient d'affaiblir les technologies de chiffrement, empêchent les populations d'utiliser la meilleure technologie disponible pour protéger leurs données et communications. Ces mesures sont fondamentalement disproportionnées.

Amnesty International demande aux gouvernements de garantir que toute ingérence dans le chiffrement soit nécessaire, proportionnée et n'aie pas pour conséquence un affaiblissement généralisé de la sécurité des communications et des données électroniques. L'organisation demande également aux entreprises d'intégrer un niveau adéquat de chiffrement à leurs produits et services.

1. QU'EST-CE QUE LE CHIFFREMENT ?

Le chiffrement est un terme technique qui désigne la méthode par laquelle les communications (SMS, courriels, appels téléphoniques et vidéo) sont sécurisées afin d'empêcher toute personne autre que le destinataire prévu d'y accéder. Le chiffrement est la manipulation mathématique des informations dans le but de les rendre lisibles uniquement par le ou les destinataires prévus. Le chiffrement est apparu bien avant Internet : l'une des premières méthodes de chiffrement, le Chiffre de César, a en effet été mise au point par l'empereur romain pour sécuriser les notes écrites transmises par ses messagers. Cependant, avec l'avènement des technologies numériques, le chiffrement ne relève plus du seul ressort des experts en cryptologie, mais de celui de chaque internaute.

Nous utilisons quotidiennement l'une des trois méthodes de chiffrement dès que nous utilisons des services connectés :

- **Le chiffrement complet des données d'un disque dur ou d'un appareil** est le procédé par lequel toutes les données stockées sur un ordinateur ou un smartphone sont chiffrées lorsqu'elles se trouvent sur l'appareil. Si vous utilisez certains smartphones ou ordinateurs récents fonctionnant sous la dernière version disponible et mise à jour du système d'exploitation, le chiffrement des données de l'appareil sera activé par défaut,[1] ce qui signifie que vous utilisez peut être cette technologie sans même le savoir. Sur d'autres appareils, il peut être nécessaire de suivre une procédure spécifique pour activer le chiffrement des données de l'appareil. Avec le chiffrement des données d'un appareil, les données stockées sur l'appareil ne seront généralement pas lisibles par une personne qui ne possède pas votre code d'identification personnel (PIN) ou votre mot de passe.

- **Le chiffrement de bout en bout** garantit que les communications transmises entre l'expéditeur et le destinataire ne peuvent pas être déchiffrées ou lues par une tierce personne ou par un fournisseur de services. Lorsque le chiffrement de bout en bout est utilisé, tout appareil ou fournisseur de service intermédiaire ayant accès aux communications électroniques ou toute personne voulant intercepter ces communications est incapable de lire leur contenu. Aujourd'hui, par exemple, toute personne qui intercepte des messages Signal[2] et iMessage notamment, qui sont chiffrés de bout-en-bout, n'est pas en mesure de les lire. WhatsApp compte également parmi les services de messagerie répandus qui utilisent le chiffrement de bout en bout, mais seulement dans

[1] Reportez-vous par exemple à l'article Android 6.0 re-implements mandatory storage encryption for new devices, Ars Technica, disponible en ligne en anglais sur :

http://arstechnica.com/gadgets/2015/10/android-6-0-re-implements-mandatory-device-encryption-for-new-devices/ et How to: Encrypt your iPhone, l'Electronic Frontier Foundation, disponible en ligne en anglais sur : https://ssd.eff.org/en/module/how-encrypt-your-iphone

[2] Signal Private Messenger est une application libre et gratuite utilisant le chiffrement de bout en bout pour les terminaux Android et les iPhones.

certains cas.[3] En plus d'être disponible pour les utilisateurs de ces applications de messagerie sécurisées, le chiffrement de bout en bout peut également être utilisé pour sécuriser les courriels, principalement via une technologie de chiffrement appelée PGP.[4] PGP, iMessage et Signal déploient un type de chiffrement appelé cryptographie à clé publique. Ce système utilise une paire de clés (des valeurs mathématiques utilisant des algorithmes pour chiffrer ou déchiffrer les données) pour le chiffrement : une clé publique, qui chiffre les données, et la clé privée correspondante nécessaire au déchiffrement. La clé publique d'un utilisateur est accessible à n'importe qui, tandis que sa clé privée est gardée secrète sur son appareil. Toute personne disposant de la clé publique d'un utilisateur peut alors chiffrer des informations que seul le destinataire sera en mesure de lire.

- **Le chiffrement du transport ou chiffrement de la couche transport (dont l'implémentation la plus courante est le HTTPS[5] avec le protocole TLS ou SSL[6])** est le moyen par lequel les communications entre les sites Internet que vous consultez (par exemple le moteur de recherche Google, les boutiques en ligne telles qu'Amazon.com, vos services de banque en ligne, ou encore les messageries comme Outlook) et votre navigateur sont chiffrées. Ainsi, lorsque vous saisissez un nom d'utilisateur et un mot de passe sur une page de connexion, ou lorsque vous tapez une requête dans un moteur de recherche, ces informations doivent être transmises aux serveurs de l'entreprise, qui sont souvent situés physiquement dans un autre pays voire un autre continent. Les sites Internet qui utilisent le HTTPS garantissent une meilleure protection : même si les données sont interceptées par une tierce partie quand elles transitent sur Internet, elles auront moins de chances d'être lues que si elles sont transmises par une connexion non chiffrée (en HTTP simple). Néanmoins, lorsque ces données arrivent à destination et sont remises à l'exploitant du site Internet, elles sont déchiffrées et stockées dans un format non chiffré.

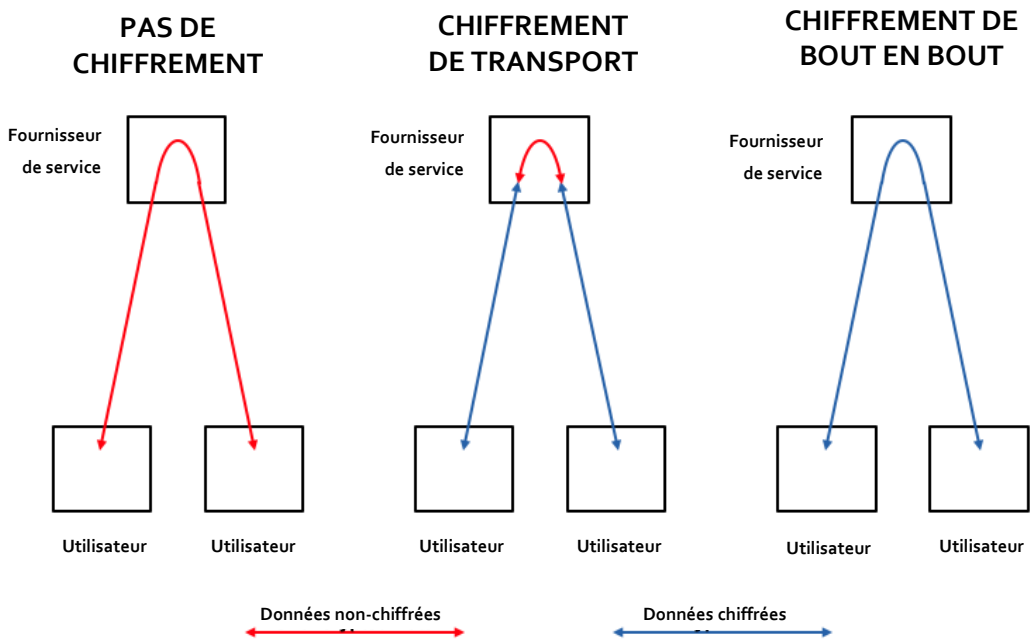
---

[3] Open Whisper Systems, qui développe Signal, a signé un partenariat avec WhatsApp dans le but de déployer le chiffrement de bout en bout pour WhatsApp. Le chiffrement n'est cependant disponible que pour certains types de messages. Voir https://whispersystems.org/blog/whatsapp/

[4] Pour plus d'informations sur PGP, consultez la page https://fr.wikipedia.org/wiki/Pretty_Good_Privacy ainsi que le site Internet de Phil Zimmermann, le créateur de PGP, à l'adresse https://www.philzimmermann.com/EN/essays/index.html

[5] « Hyper Text Transfer Protocol Secure (HTTPS) est la version sécurisée du protocole HTTP, utilisé pour transmettre les données entre votre navigateur et le site Internet auquel vous êtes connecté. Le "S" de HTTPS signifie "Secure" (sécurisé). Cela signifie que toutes les communications entre votre navigateur et le site Internet sont chiffrées. » Source : https://www.instantssl.com/ssl-certificate-products/https.html

[6] TLS signifie Transport Layer Security et SSL signifie Secure Sockets Layer. Voir https://www.instantssl.com/ssl-certificate-products/https.html



En bref, le chiffrement garantit que seul le destinataire prévu est en mesure de lire, d'écouter ou de regarder les communications qui lui ont été transmises. Le chiffrement garantit ainsi le respect de la vie privée et la sécurité du contenu des communications transmises par l'intermédiaire des outils et services utilisant cette technologie.

Il est important de faire la distinction entre la confidentialité et la sécurité qu'offre le chiffrement, et la notion, complémentaire mais distincte, d'anonymat, qui désigne le fait de parvenir à dissimuler sa propre identité. Les communications chiffrées ne sont pas anonymes ; et parvenir à communiquer de façon anonyme requiert un savant mélange de technologie et de savoir-faire. Même lorsque des personnes font en sorte de masquer les informations permettant de les identifier, par exemple leur nom et leur adresse IP (Internet Protocol),[7] en utilisant notamment des pseudonymes ou en ayant recours à des logiciels d'anonymisation tels que Tor,[8] les métadonnées qu'ils génèrent par la simple utilisation des technologies numériques (telles que les données de localisation recueillies et transmises par les téléphones mobiles), peuvent révéler leur identité réelle.

AUTRES DEFINITIONS PERTINENTES

Portes dérobées ou « backdooring » : terme informel utilisé pour désigner des mesures techniques visant à affaiblir ou à altérer des outils, appareils et services de chiffrement afin de faciliter l'accès aux informations et aux communications par des personnes autres que le fournisseur de service et

[7] Une adresse IP est le code numérique affecté à chaque dispositif connecté à Internet. Pour plus d'informations, voir https://fr.wikipedia.org/wiki/Adresse_IP

[8] Pour plus d'informations sur Tor, voir https://www.torproject.org/

les parties aux informations et aux communications.

Piratage : utilisation de vulnérabilités (failles logicielles),[9] de *malware* (logiciels malveillants tels que des virus, des vers et des logiciels espions)[10] et de méthodes d'ingénierie sociale[11] en vue d'accéder à un appareil, un système ou un réseau ; le piratage est souvent utilisé pour contourner le chiffrement et permettre à une tierce partie non autorisée d'accéder aux données stockées sur un ordinateur ou un téléphone sous forme non chiffrée.

Métadonnées ; toute information générée par l'utilisation de technologies de communication autre que le contenu même de la communication. Bien que cette information ne contienne pas nécessairement de détails personnels ou sur le contenu, elle apporte des renseignements sur les appareils utilisés, leurs utilisateurs et la façon dont ils sont utilisés (également appelée « données de communication » ou « données à propos des données », tels que les destinataires des courriels, les heures d'appel, les données de localisation, et dans le cas des téléphones portables, les antennes-relais utilisées). Si elle est associée à d'autres sources de données, une analyse des métadonnées peut apporter une idée précise des liens qu'entretiennent les participants d'une communication ainsi que de leurs habitudes.

---

[9] Pour plus d'informations sur les vulnérabilités, voir https://fr.wikipedia.org/wiki/Vuln%C3%A9rabilit%C3%A9_(informatique)

[10] Pour plus d'informations sur les logiciels malveillants, voir https://fr.wikipedia.org/wiki/Logiciel_malveillant

[11] L'ingénierie sociale, dans le cadre de la sécurité de l'information, peut être définie comme la manipulation psychologique d'individus pour les amener à effectuer certaines actions ou à divulguer des informations confidentielles ; voir https://fr.wikipedia.org/wiki/Ing%C3%A9nierie_sociale_(s%C3%A9curit%C3%A9_de_l%27information)

2. CHIFFREMENT ET DROITS HUMAINS

« Les outils de chiffrement sont largement utilisés partout dans le monde, notamment par les défenseurs des droits humains, la société civile, les journalistes, les lanceurs d'alerte et les dissidents politiques qui risquent persécutions et harcèlement… Le chiffrement et l'anonymat sont nécessaires ; ils favorisent la liberté d'expression et d'opinion ainsi que le droit à la vie privée. Il n'y a rien de fantaisiste ni d'exagéré dans le fait de dire que, sans outil de chiffrement, des vies pourraient être mises en danger. Dans le pire des cas, la capacité d'un gouvernement à s'introduire dans les téléphones de ses citoyens pourrait conduire à des poursuites contre des personnes qui ne font qu'exercer leurs droits fondamentaux. »
Zeid Raad Al Hussein, Haut-Commissaire des Nations unies aux droits de l'homme[12]

Le chiffrement est le garant de la sécurité de nos données et de nos communications en ligne. Lorsque le chiffrement est utilisé, nous pouvons utiliser Internet en toute sécurité pour communiquer sur nos pensées les plus intimes, nos questions médicales, nos informations bancaires, notre sexualité et nos croyances religieuses. Le chiffrement sur Internet est toujours plus omniprésent. Cette évolution est liée aux violations de données, piratages de sites Internet et vols d'informations personnelles et de numéros de cartes de crédit répétés, qui ont toujours conduit à des mesures visant à diffuser et à renforcer le chiffrement des données. Cette évolution s'est accélérée ces dernières années car il est devenu évident que la sécurité et la confidentialité des communications est menacée, non seulement par les cybercriminels et les usurpateurs d'identité, mais également par les États.

Aux États-Unis, on estime que 17,6 millions de personnes ont été victimes de vol d'informations personnelles en 2014.[13] Selon les données de la police britannique, plus de 100 000 téléphones mobiles ont été volés dans la seule ville de Londres en 2013, et parmi les centaines de milliers de téléphones volés dans la capitale anglaise entre 2012 et 2014, la majorité était des smartphones.[14] Il

[12]Bureau du Haut-Commissaire des Nations unies aux droits de l'homme, L'affaire Apple-FBI pourrait avoir de graves conséquences sur les droits de l'homme: Zeid, 4 mars 2016, disponible en ligne sur : http://www.unog.ch/unog/website/news_media.nsf/%28httpNewsByYear_fr%29/C8C51806F21D271EC1257F6C00399C14?OpenDocument&cntxt=AD9F9&cookielang=fr

[13] Département de la Justice des États-Unis, Victims of Identity Theft, 2014, disponible en ligne en anglais sur : http://www.bjs.gov/content/pub/pdf/vit14.pdf

[14] Ministère de l'Intérieur du Royaume-Uni, Reducing Mobile Phone Theft and Improving Security, septembre 2014, disponible en ligne en anglais sur : https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/390901/HO_Mobile_theft_paper_Dec_14_WEB.PDF

est important de noter qu'un vol de smartphone, en plus de son impact financier, implique le vol des communications et des informations personnelles de son propriétaire ; celles-ci peuvent notamment inclure des informations d'ordre médical, financier et professionnel.

Si l'avènement des communications numériques a révolutionné le travail, l'éducation, la politique, les relations, la culture et le langage partout dans le monde, il a également grandement réduit les obstacles à la surveillance par les États, et leur a apporté de nouvelles opportunités. Des activités qui étaient auparavant complexes, coûteuses et nécessitaient beaucoup de temps, telles que l'interception de communications écrites, la mise sur écoute de conversations téléphoniques, ou encore le suivi des habitudes de lecture des dissidents présumés, sont désormais faciles à mettre en œuvre par les États. Il leur suffit pour cela de déployer des technologies de surveillance peu coûteuses, dotées de capacités d'analyse beaucoup plus puissantes que celles des services traditionnels de renseignement et d'application des lois en termes de vitesse et de volume.

LES REVELATIONS D'EDWARD SNOWDEN

Le 5 juin 2013, le journal britannique *The Guardian* a rendu publiques les premières révélations sur la surveillance de masse non ciblée exercée par l'Agence nationale de sécurité américaine (NSA) et le service du renseignement électronique du gouvernement britannique (GCHQ). Edward Snowden, lanceur d'alerte et ancien collaborateur de la NSA, a fourni des preuves qui attestent de l'existence de programmes de surveillance des communications mondiales. Ces programmes surveillent l'activité Internet et téléphonique de plusieurs centaines de millions de personnes à travers le monde. Parmi les informations révélées au grand jour par les médias, à partir de fichiers transmis par Edward Snowden, figurent les points suivants :

- Des entreprises, dont Facebook, Google et Microsoft, ont été contraintes par la loi de transmettre à la NSA les données de leurs clients, en réponse à des ordonnances secrètes prises dans le cadre du programme Prism de la NSA ;

- Un programme de la NSA mis en place en 2009 a permis à l'agence d'enregistrer, de stocker et d'analyser les métadonnées de tous les appels téléphoniques et SMS émis dans plusieurs pays, notamment au Kenya, au Mexique et aux Philippines ;

- Le GCHQ et la NSA ont fait appel aux services des plus grands opérateurs de télécommunications au monde pour mettre sur écoute les câbles sous-marins transatlantiques et intercepter les communications privées qui y transitent, dans le cadre respectivement de leurs programmes TEMPORA et Upstream ;

- En 2010-2011, le GCHQ et la NSA ont piraté le réseau informatique interne de Gemalto, plus grand fabricant mondial de cartes SIM, et auraient dérobé plusieurs milliards de clés de chiffrement servant à protéger la confidentialité des communications mobiles dans le monde entier.

Sans le chiffrement, les États pourraient disposer d'un accès total aux échanges sur Internet. Même avec le chiffrement, les États sont toujours en mesure d'intercepter les communications *de manière massive*.

Outre la surveillance de masse pratiquée par des pays tels que le Royaume-Uni ou les États-Unis, la surveillance ciblée de militants et de journaliste est malheureusement monnaie courante dans de nombreux pays du monde. Au Royaume-Uni, la police a placé des journalistes de la presse écrite

sous surveillance afin d'identifier leurs sources[15]. Au Bahreïn, des militants en exil à l'étranger ont quant à eux été suivis par leur gouvernement à l'aide de logiciels espions[16]. Enfin, des journalistes de radio colombiens ont fait l'objet d'une surveillance électronique par la police nationale.[17] Le gouvernement éthiopien utilise la surveillance électronique pour espionner des militants de l'opposition non seulement en Éthiopie, mais également à l'étranger.[18]

Seule la sécurisation des communications contre toute ingérence extérieure pourra permettre aux internautes, aux défenseurs des droits humains, aux représentants politiques de l'opposition, aux militants politiques et aux journalistes d'investigation de se prémunir contre la cybercriminalité et contre la surveillance orchestrée par les gouvernements du monde entier.

Cependant, les gouvernements de différents pays ont déjà promulgué des lois visant à restreindre considérablement l'accès aux outils et aux services de chiffrement ainsi que leur utilisation. Des pays comme le Pakistan, l'Inde et Cuba interdisent le chiffrement,[19] limitent la complexité du chiffrement légal à un niveau défini par le gouvernement,[20] ou exigent des utilisateurs une autorisation pour pouvoir utiliser des méthodes de chiffrement.[21] La Turquie exige des fournisseurs de services de chiffrement qu'ils remettent des copies des clés de chiffrement à une autorité de régulation gouvernementale avant de proposer les outils à leurs clients. Le Royaume-Uni, la France et l'Espagne peuvent exiger des entreprises qu'elles divulguent les clés de chiffrement et

[15] Dominic Ponsford, « Surveillance court says Met grabs of Sun reports' call records 'not compatible' with human rights law », 17 décembre 2015, disponible en anglais sur : http://www.pressgazette.co.uk/surveillance-court-says-met-was-right-grab-sun-journalists-call-records-hunt-plebgate-sources.

[16] Amar Toor et Russell Brandom, A spy in the machine: How a brutal government used cutting-edge spyware to hijack one activist's life, disponible en ligne en anglais sur : http://www.theverge.com/2015/1/21/7861645/finfisher-spyware-let-bahrain-government-hack-political-activist

[17]Comité pour la protection des journalistes, Claims police spied on two journalists revive surveillance fears of Colombia's press, disponible en ligne en anglais sur : https://www.cpj.org/blog/2016/02/claims-police-spied-on-two-journalists-revive-surv.php et Comité pour la protection des journalistes, In the Americas, Big Brother is watching reporters, disponible en ligne en anglais sur : https://www.cpj.org/2010/02/in-the-americas-big-brother.php

[18] Human Rights Watch, *Éthiopie : La surveillance des télécommunications fragilise les droits humains*, 25 mars 2014, disponible en ligne sur : https://www.hrw.org/fr/news/2014/03/25/ethiopie-la-surveillance-des-telecommunications-fragilise-les-droits-humains

[19] Bytes for All, « Pakistan: Ban on Internet encryption a violation of freedom of expression », 9 février 2011, disponible en anglais sur : https://content.bytesforall.pk/node/40.

[20] Les FAI indiens doivent restreindre le niveau de chiffrement pour les individus, les groupes ou les organisations à une longueur de clé de seulement 40 bits pour les algorithmes de chiffrement symétriques ou équivalents. Voir « Digital Encryption in India », *Indian Case laws,* 10 février 2015, disponible en anglais sur : https://indiancaselaws.wordpress.com/2015/02/10/digital-encryption-laws-in-india/

[21] 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, § 41, disponible en ligne sur : http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/29/32

déchiffrent des données.[22] La Chine a voté en décembre 2015 une loi antiterroriste qui prévoit que les fournisseurs de services de télécommunications « apportent un support technique et assistent les enquêteurs du gouvernement en vue, notamment, de fournir un accès aux interfaces techniques et aux clés de déchiffrement aux autorités chargées de l'application des lois et de la sécurité nationale pour contribuer à la prévention des actes terroristes et aux activités d'investigation » (article 18), et qu'ils « mettent en œuvre des services de sécurisation des réseaux, de surveillance des contenus et des mesures conçues pour limiter la diffusion de contenus ayant trait au terrorisme et à l'extrémisme, qu'ils détruisent ces informations et qu'ils en fassent immédiatement état à la police chinoise » (article 19).[23]

PROTECTION DES DROITS A LA VIE PRIVEE ET A LA LIBERTE D'EXPRESSION A L'ERE DU NUMERIQUE

Les deux droits humains les plus fréquemment associés à l'accès et à l'utilisation du chiffrement sont le droit à la vie privée[24] et le droit à la liberté d'expression.[25] L'accès au chiffrement, ou son absence, peut avoir des conséquences sur d'autres droits, tels que le droit de réunion pacifique et d'association. Les droits à la vie privée et à la liberté d'expression sont souvent considérés comme des droits se renforçant mutuellement. Lorsque des personnes disposent d'un lieu sécurisé pour rechercher des informations, étoffer leurs connaissances, former des opinions et exprimer des idées, le droit à la vie privée favorise l'exercice du droit à la liberté d'expression. La confiance dont nous disposons pour communiquer nos idées et nos opinions, qu'elles soient controversées ou non, repose sur le fait que nous savons que ces communications sont protégées contre toute ingérence illégale.

---

[22] Royaume-Uni, Regulation of Investigatory Powers Act http://www.legislation.gov.uk/ukpga/2000/23/pdfs/ukpga_20000023_en.pdf (divulgation de clés obligatoire) ; France, Loi n° 2001-1062 (divulgation des clés de chiffrement sur autorisation d'un juge) ; Espagne, Loi sur les télécommunications 25/2007 (divulgation des clés de chiffrement).

[23] « China enacts broad counter-terrorism law » *Global Policy Watch – Covington,* 5 janvier 2016, disponible en anglais sur : https://www.globalpolicywatch.com/2016/01/china-enacts-broad-counter-terrorism-law/.

[24] Le droit à la vie privée, inscrit dans l'article 12 de la Déclaration universelle des droits de l'homme et dans l'article 17 du Pacte international relatif aux droits civils et politiques (PIDCP), comprend le droit à ne pas faire l'objet d'immixtions arbitraires ou illégales dans sa vie privée, sa famille, son domicile ou ses correspondances, ni d'atteintes illégales à son honneur et à sa réputation, ainsi que le droit à la protection de la loi contre de telles immixtions ou de telles atteintes. Le droit à la vie privée est également inscrit dans la Convention relative aux droits de l'enfant (article 16) et dans la Convention internationale sur la protection des droits de tous les travailleurs migrants et des membres de leur famille (article 14). Au niveau régional, le droit à la vie privée est protégé par la Convention européenne relative aux droits de l'homme (article 8), la Charte des droits fondamentaux de l'Union européenne (article 7) et la Convention américaine relative aux droits de l'homme (article 11). La notion de vie privée a évolué pour aujourd'hui comprendre le droit à la protection des données personnelles, droit spécifiquement reconnu dans l'article 8 de la Charte de l'Union européenne et dans l'article 21 de la Déclaration des droits humains de l'ANASE.

[25] Le droit à la liberté d'expression est protégé par l'article 19 de la Déclaration universelle des droits de l'homme ; l'article 19 du PIDCP ; l'article 10 de la CEDH ; l'article 11 de la Charte des droits fondamentaux de l'Union européenne, et l'article 13 de la Convention américaine relative aux droits de l'homme de 1969.

Le concept de vie privée et les protections offertes par l'article 17 (relatif au droit à la vie privée) du Pacte international relatif aux droits civils et politiques (PIDCP) portent sur des notions qui dépassent largement le cadre des communications et d'Internet. Néanmoins, avec les avancées réalisées dans le domaine des nouvelles technologies, les droits relatifs à la vie privée ont pris une autre dimension chez les individus, et une nouvelle signification pour les États. Ils ont reçu plus d'attention de la part des tribunaux et des législateurs ces dix dernières années que lors des cinquante années précédentes.[26] L'avènement d'Internet s'est accompagné de nouveaux canaux d'expression, mais également de nouvelles ingérences dans la vie privée des citoyens.

Si les technologies numériques ont créé de nouvelles opportunités en termes de communication et d'expression, elles ont également permis la production, la dissémination et le stockage de quantités toujours plus importantes de données privées. Ces données portent, entre autres, sur les déplacements, les croyances, les préférences politiques, l'orientation sexuelle, la santé et les transactions financières des citoyens.

En 2012, la rapporteuse spéciale des Nations unies (ONU) sur la situation des défenseurs des droits de l'homme a publié un rapport sur la liberté d'expression sur Internet, qui indique :

« Au cours des dix dernières années, l'Internet est devenu un outil indispensable aux fins des activités de nombreux défenseurs des droits de l'homme, notamment afin de transmettre ses opinions, partager des informations sur les droits de l'homme et leurs violations et se tenir en rapport avec d'autres défenseurs des droits de l'homme. [...] La Rapporteuse spéciale s'inquiète [...] du fait que les informations personnelles sur les défenseurs des droits de l'homme transmises via les réseaux sociaux ou d'autres sites Internet sont susceptibles de compromettre leur sécurité, en particulier à la lumière des nouvelles mesures législatives autorisant les gouvernements à renforcer le contrôle qu'ils exercent sur les sites Internet dans plusieurs pays. »[27]

En 2013, le rapporteur spécial sur la liberté d'expression a publié un rapport sur la surveillance des communications par les États et sur la vie privée. Dans ce rapport, le rapporteur spécial conclut que la sécurité des communications est une composante essentielle du droit à la vie privée, droit ébranlé par les lois restreignant l'utilisation d'outils permettant le plein exercice du droit à la vie privée, tels que le chiffrement.[28]

Suite aux révélations d'Edward Snowden, l'ONU a publié une série de rapports, de résolutions et de décisions relatifs à la surveillance des communications « à l'ère du numérique » par les États. Ils comprennent un rapport du Haut-Commissaire aux droits de l'homme sur *le droit à la vie privée à*

---

[26] Pour consulter des exemples de déclarations récentes relatives au droit à la vie privée, reportez-vous au document publié par Amnesty International et Privacy International, Deux ans après Snowden : protéger les droits humains à l'ère de la surveillance de masse, juin 2015, pp 8-9, disponible en ligne sur : https://www.amnesty.org/en/documents/act30/1795/2015/fr/

[27] Assemblée générale des Nations unies, Situation des défenseurs de droits de l'homme, 10 août 2012, § 61-62, disponible en ligne sur : https://documents-dds-ny.un.org/doc/UNDOC/GEN/N12/459/43/pdf/N1245943.pdf?OpenElement

[28] 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, Frank La Rue*, 17 avril 2013, A/HRC/23/40, § 71, Disponible en ligne sur : https://documents-dds-ny.un.org/doc/UNDOC/GEN/G13/133/04/PDF/G1313304.pdf?OpenElement

l'ère du numérique, deux résolutions de l'Assemblée générale, une résolution du Conseil des droits de l'homme établissant un nouveau mandat de procédures spéciales relatif au droit à la vie privée, ainsi que des observations finales du Comité des droits de l'homme suite aux évaluations des États-Unis,[29] du Royaume-Uni,[30] et de la France[31] traitant de l'utilisation de techniques de surveillance numériques spéciales. Plus récemment, l'actuel rapporteur spécial sur la liberté d'expression a publié un rapport en 2015 portant sur les liens entre le chiffrement et l'anonymat d'une part, et les droits à la vie privée et à la liberté d'expression d'autre part.[32] Le rapporteur spécial sur les défenseurs des droits humains a également abordé la question de la surveillance en ligne dans son rapport de 2015, en déclarant :

« Internet, et plus généralement les nouvelles technologies, qui avaient représenté jusqu'à présent un formidable outil d'expression, d'accès à l'information et de mise en réseaux des individus et des organisations, sont aujourd'hui utilisés par des États pour contrôler et limiter l'action des défenseurs. Cela est d'autant plus préoccupant que nombre de défenseurs utilisent quotidiennement Internet pour promouvoir et protéger les droits de l'homme, s'exposant de ce fait à de multiples menaces. [...] Les courriels sont également interceptés et les communications téléphoniques surveillées. »[33]

Parallèlement aux travaux de l'ONU, plusieurs affaires judicaires relatives aux droits humains en Europe et aux États-Unis ont contribué à la création d'une jurisprudence sur la vie privée dans le contexte d'Internet et des technologies numériques. Outre les affaires marquantes portées devant la Cour européenne des droits de l'homme, il convient de citer la récente décision de la Cour de justice européenne dans l'affaire *Maximillian Schrems c. Data Protection Commissioner of Ireland*. La Cour a conclu que, dans le contexte de l'interception de masse des communications numériques, « une réglementation permettant aux autorités publiques d'accéder de manière généralisée au contenu des communications électroniques doit être considérée comme portant atteinte au

---

[29] Comité des droits de l'homme, *Observations finales concernant le quatrième rapport périodique des États-Unis d'Amérique*, 23 avril 2014, disponible en ligne sur : http://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=CCPR%2fC%2fUSA%2fCO%2f4&Lang=fr

[30] Comité des droits de l'homme, *Concluding observations on the seventh periodic report of the United Kingdom of Great Britain and Northern Ireland*, 17 août 2015, disponible en ligne en anglais sur : http://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=CCPR/C/GBR/CO/7&Lang=En

[31] Comité des droits de l'homme, *Observations finales concernant le cinquième rapport périodique de la France*, 17 août 2015, disponible en ligne sur : http://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=CCPR/C/FRA/CO/5&Lang=fr

[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*, A/HRC/29/32, 22 mai 2015, disponible en ligne sur : http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/29/32

[33] Assemblée générale des Nations unies, Situation des défenseurs de droits de l'homme, A/70/217, 22 mai 2015, § 46, disponible en ligne sur : http://www.un.org/en/ga/search/view_doc.asp?symbol=A/70/217

contenu essentiel du droit fondamental au respect de la vie privée [...]. »[34]

Il existe désormais un fondement juridique important pour soutenir l'idée que la surveillance de masse constitue une menace sérieuse pour le droit à la vie privée. Amnesty International estime que le chiffrement est un outil décisif pour l'exercice du droit à la vie privée et à la liberté d'expression sur Internet, offrant « aux personnes et aux groupes un espace de confidentialité en ligne qui leur permet d'exercer leur liberté d'opinion et d'expression et les protège contre toute immixtion arbitraire ou illégale et contre toute attaque ».[35]

Les restrictions du chiffrement constituent une atteinte à l'exercice du droit à la vie privée et à la liberté d'expression, et doivent être justifiées selon les conditions prévues par le droit relatif aux droits humains. Le cadre juridique applicable pour déterminer si une restriction du chiffrement est acceptable a été formulé par le rapporteur spécial des Nations unies sur la liberté d'expression dans son rapport de 2015 comme suit :

> « Premièrement, pour qu'une mesure de restriction au chiffrement ou à l'anonymat soit "prévue par la loi", **elle doit être précise, publique et transparente,** et ne doit pas conférer aux autorités publiques un pouvoir illimité quant à son application (voir Observation générale no 34 (2011) du Comité des droits de l'homme). Les propositions de restriction au chiffrement ou à l'anonymat devraient être soumises au débat public et uniquement adoptées, le cas échéant, par les voies législatives ordinaires. **De solides garanties procédurales et judiciaires devraient aussi être établies** pour garantir une procédure régulière à toute personne dont l'utilisation du chiffrement ou de l'anonymat aurait été restreinte. **En particulier, la mise en œuvre de la restriction doit être supervisée par une cour, un tribunal ou un autre organe juridictionnel indépendant.**
>
> Deuxièmement, les **limitations ne sont justifiées que si elles visent à protéger des intérêts précis** : droits ou réputation d'autrui, sécurité nationale, ordre public, santé publique ou morale publique. [...] De plus, comme des objectifs légitimes sont souvent invoqués pour commettre des actes illégitimes, les restrictions elles-mêmes doivent être appliquées de manière restrictive.
>
> Troisièmement, **l'État doit montrer que la restriction au chiffrement ou à l'anonymat est "nécessaire" pour atteindre l'objectif légitime visé**. La Cour européenne des droits de l'homme a conclu de façon pertinente que l'adjectif "nécessaire" dans l'article 10 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales signifiait que la restriction devait être plus qu'"utile", "raisonnable" ou "souhaitable". Une fois l'objectif légitime atteint, la restriction doit être levée. Compte tenu des droits fondamentaux qui sont en jeu, les limitations doivent être soumises à une autorité judiciaire indépendante et

---

[34] Cour de justice de l'Union européenne (UE), 6 octobre 2015, § 94, disponible en ligne sur : http://curia.europa.eu/juris/document/document.jsf?%20text=&docid=169195&pageIndex=0&doclang=FR&mode=req&dir=&occ=first&part=1&cid=116845

[35] 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, § 16, disponible en ligne sur : http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Pages/ListReports.aspx

impartiale, en vue notamment de garantir le droit à une procédure régulière.

Le critère de nécessité suppose également une évaluation du caractère proportionné des mesures limitant l'utilisation des outils de sécurité en ligne et l'accès à ces outils. Une telle évaluation devrait garantir que la restriction "constitue le moyen le moins perturbateur parmi ceux qui pourraient permettre d'obtenir le résultat recherché". **La limitation doit être appliquée dans un objectif précis et ne saurait porter atteinte aux autres droits de la personne visée ; de plus, tout empiétement sur les droits de tierces parties doit être limité et justifié à la lumière de l'intérêt que cette mesure de limitation vise à défendre.** La restriction doit aussi être "proportionnée à l'intérêt à protéger". Un risque important d'atteinte à un intérêt essentiel et légitime de l'État peut justifier une restriction limitée de la liberté d'expression. Inversement, lorsqu'une mesure de restriction a de nombreuses conséquences pour des individus qui ne menacent pas les intérêts légitimes du gouvernement, l'État sera tenu de prouver point par point le bien-fondé de cette mesure. **En outre, dans le cadre de l'évaluation de la proportionnalité, il doit être tenu compte du fait que les restrictions du chiffrement et de l'anonymat seront très probablement exploitées par les réseaux criminels et terroristes que les mesures de restriction visent précisément à dissuader d'agir.** Dans tous les cas, "une justification publique, complète et fondée sur des preuves" est cruciale pour qu'il puisse y avoir un débat public et transparent sur les restrictions qui concernent la liberté d'expression et risquent de la compromettre (voir A/69/397, § 12) » (*citations omises - mise en gras ajoutée).*

Dans le cas de l'application de ce cadre juridique à des restrictions particulières à l'accès et à l'utilisation du chiffrement, le rapporteur spécial conclut ce qui suit :

- **Les interdictions générales du chiffrement**, ou les mesures qui peuvent s'y apparenter (y compris l'obligation d'obtenir une autorisation auprès du gouvernement pour utiliser le chiffrement ou l'obligation d'utiliser uniquement un chiffrement faible) contreviennent aux exigences de proportionnalité d'une restriction autorisée, « car elle[s] prive[nt] les utilisateurs qui relèvent de la compétence de l'autorité concernée du droit de disposer, en ligne, d'un espace privé où formuler leurs opinions et s'exprimer, sans qu'aucune allégation d'utilisation de ces technologies ne soit à des fins illicites invoquée pour la justifier. »[36]

- **Exiger des entreprises qu'elles affaiblissent le chiffrement, offrent des portes dérobées ou adoptent des systèmes de dépôt de clés** [voir chapitre 4 du document] « ne répondrai[t] [très probablement] pas au critère de proportionnalité » si ces exigences sont mises en œuvre de telle sorte qu'elles pourraient être appliquées massivement sans une évaluation préalable au cas par cas.[37]

---

[36] 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, § 40, disponible en ligne sur : http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/29/32

[37] 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, § 43, disponible en ligne sur : http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/29/32

■ **Les ordonnances de déchiffrement ciblé** [voir chapitre 4 du document] ont une portée plus limitée et sont moins susceptibles de poser problème en ce qui concerne le critère de proportionnalité que les **ordonnances de divulgation de clés obligatoire**. Dans les deux cas, il faut toutefois « que de telles ordonnances reposent sur des lois qui peuvent être consultées publiquement, dont la portée est clairement limitée et ciblée, qui sont appliquées par une autorité judiciaire indépendante et impartiale, notamment pour préserver les droits des personnes visées à une procédure équitable, et qui sont adoptées uniquement en cas de nécessité, faute d'autres moyens d'enquête moins intrusifs. De telles mesures ne pourront se justifier que lorsqu'elles visent un utilisateur ou un groupe d'utilisateurs spécifiques et qu'elles font l'objet d'un contrôle juridictionnel. »[38]

[38] 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, § 45, disponible en ligne sur : http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/29/32

3. PEUR DE « PLONGER DANS LE NOIR » : TENTATIVES DES GOUVERNEMENTS POUR AFFAIBLIR LE CHIFFREMENT

« Le chiffrement risque de nous plonger tous dans le noir le plus complet. »

James Comey, directeur du FBI, en octobre 2014, réclamant l'ouverture d'un débat visant à imposer aux entreprises l'obligation de fournir un accès à leurs services chiffrés.[39]

Ces dernières années, des hauts fonctionnaires de nombreux pays ont commencé à s'élever ouvertement contre les techniques de chiffrement complexes en brandissant la peur de « plonger dans le noir ». À l'origine, ce concept était employé par les forces de l'ordre américaines (puis repris par d'autres) pour décrire la capacité de plus en plus restreinte des agences d'application des lois à accéder au contenu des communications à cause de l'usage croissant du chiffrement dans les technologies et les services de communication courants.

En réalité, si le chiffrement peut effectivement empêcher de lire le contenu des communications, les autorités sont toujours capables d'intercepter des communications chiffrées et d'accéder à certaines informations relatives à celles-ci, telles que la date, l'heure, les expéditeurs, la taille, etc. qui sont désignées sous le nom de métadonnées.

La controverse qui entoure le chiffrement tire son origine d'un aspect pratique de la sécurité informatique : en protégeant les communications contre les ingérences illégales des criminels, le chiffrement protège également les communications des ingérences des autorités, qu'elles soient illégitimes ou *légitimes*.

Il est généralement accepté dans le droit international qu'une surveillance ciblée des communications, si elle remplit certains critères, est un moyen acceptable et efficace d'atteindre des objectifs légitimes, tels que la prévention et l'élucidation d'infractions, et la protection de la

[39] James B. Comey, 16 octobre 2014, disponible en ligne en anglais sur : https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course

sécurité nationale.[40] La prévention, l'élucidation, l'investigation et la poursuite de ces infractions peuvent requérir des capacités exceptionnelles pour accéder au contenu des courriels et des SMS, suivre la trace d'achats en ligne, et surveiller des mouvements financiers, en interceptant des communications numériques et des flux de données.

Cependant, le chiffrement doit être impossible à décrypter par qui que ce soit, même les personnes dont les intentions sont légitimes, afin qu'il puisse être efficace contre les personnes dont les intentions ne le sont pas.[41] C'est pour cela que son déploiement, sa promotion et son utilisation sont désormais au cœur du débat politique et font l'objet de mesures législatives.

Le chiffrement est de plus en plus critiqué par les gouvernements, dans un contexte de peur généralisée (alimentée par les agences de sécurité)[42] qu'Internet soit devenu un environnement propice aux activités terroristes et aux cybercriminels. Plusieurs personnalités importantes ont condamné le chiffrement (et ceux qui le fournissent) car il favorise l'apparition d'« espaces sûrs »[43] pour les activités criminelles. En janvier 2015, le Premier ministre britannique David Cameron a déclaré que « nous ne pouvons pas permettre aux nouvelles formes de communication de s'affranchir de la possibilité… d'être écoutées ».[44] En août 2015, trois hauts magistrats et un officier supérieur de police, respectivement français, espagnol, américain et britannique, ont critiqué le chiffrement complet des données :

---

[40] Voir le rapport du Haut-Commissariat des Nations unies aux droits de l'homme *« Le droit à la vie privée à l'ère du numérique »*, A/HRC/27/37, § 15, disponible en ligne à l'adresse : http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A-HRC-27-37_fr.doc.

[41] Bruce Schneier, *iPhone Encryption and the Return of the Crypto Wars*, 6 octobre 2014, disponible en ligneen anglais sur : www.schneier.com/blog/archives/2014/10/iphone_encrypti_1.html

[42] Voir par exemple l'article de Robert Hannigan, chef du GCHQ, les services britanniques de renseignements électroniques, « The web is a terrorist's command and control centre of choice », *The Financial Times,* 3 novembre 2014, disponible en anglais sur : http://www.ft.com/cms/s/2/c89b6c58-6342-11e4-8a63-00144feabdco.html#axzz42y5fToAo. Voir également le rapport d'Europol *Changes in Modus Operandi of Islamic State Terror Attacks*, qui souligne qu'« Internet et les réseaux sociaux sont utilisés pour communiquer et pour acheter des biens (armes, faux papiers) et des services, de façon relativement sécurisée pour les terroristes grâce à des outils sûrs et entièrement chiffrés tels que WhatsApp, Skype et Viber ». Disponible en anglais sur : https://www.europol.europa.eu/content/changes-modus-operandi-islamic-state-terrorist-attacks

[43] Cameron: surveillance powers will deny terrorists 'safe space,' *BBC*, 2 novembre 2015, disponible en anglais sur : http://www.bbc.co.uk/news/uk-politics-34697535.

[44] *UK's Cameron won't "allow" strong encryption of communications*, BBC, 12 janvier 2015, disponible en ligne en anglais sur : https://gigaom.com/2015/01/12/uks-cameron-wont-allow-strong-encryption-of-communications/

« Le chiffrement complet des données limite considérablement notre capacité à enquêter sur ces infractions et réduit sérieusement notre efficacité dans la lutte contre le terrorisme. Pourquoi devrions-nous permettre à des activités criminelles de prospérer sur une plateforme hors de portée des forces de l'ordre ? Enquêter sur ces affaires sans avoir accès aux données contenues sur les smartphones revient à travailler avec une main attachée derrière le dos. »[45]

Cependant, certains gouvernements ont pris une direction diamétralement opposée. En janvier 2016, le gouvernement français a rejeté une proposition de loi qui aurait obligé les fabricants de matériel à prendre en compte les besoins des forces de l'ordre et des services de renseignement dans la conception de leurs technologies, en ajoutant des portes dérobées à leurs appareils.[46] Dans une lettre publiée en janvier 2016, le ministre de la Sécurité et de la Justice néerlandais a déclaré que toute décision visant à affaiblir le chiffrement ou à y intégrer des portes dérobées « aurait des conséquences indésirables pour la sécurité des informations stockées et partagées et pour l'intégrité des technologies de l'information et de la communication, dont l'importance est de plus en plus cruciale pour le bon fonctionnement de nos sociétés ».[47]

Pourtant, le débat fait rage, alimenté par l'introduction en novembre 2015 d'un projet de loi au Royaume-Uni sur les pouvoirs d'enquête, une loi très exhaustive sur la surveillance qui, si elle était adoptée, ferait peser sur les épaules des fournisseurs de services de communication de nombreuses obligations pour faciliter les interceptions. Une première version de ce projet de loi habilitait le ministre de l'Intérieur à exiger des entreprises qu'elles suppriment les « protections électroniques » des communications,[48] laissant entrevoir la possibilité que le gouvernement britannique puisse obliger les entreprises à les laisser accéder aux données chiffrées via des portes dérobées.[49] Après une levée de boucliers des personnes, organisations et entreprises qui avaient participé à la consultation publique sur le projet de loi, et suite aux critiques émises par la commission parlementaire mixte qui menait la consultation, le gouvernement a modifié le projet de loi avant de le présenter au Parlement en mars 2015, en précisant qu'il ne serait demandé aux entreprises que de supprimer le chiffrement qu'elles auraient elles-mêmes installé, et uniquement dans la mesure du possible.

---

[45] Cyrus R. Vance Jr. et al, *When Phone Encryption Blocks Justice*, New York Times, 11 août 2015, disponible en ligne en anglais sur : http://www.nytimes.com/2015/08/12/opinion/apple-google-when-phone-encryption-blocks-justice.html

[46] Jeff John Roberts, « France Rejects 'Backdoors' Law to Defeat Encryption », *Fortune*, 13 janvier 2016, disponible en anglais sur : http://fortune.com/2016/01/13/france-encryption/.

[47] Dutch government says no to 'encryption backdoors', *BBC News*, 7 janvier 2016, disponible en anglais sur : http://www.bbc.co.uk/news/technology-35251429.

[48] Partie 189, projet de loi sur les pouvoirs d'enquête.

[49] *Snooper's Charter: Tech companies will have to give police 'back-door' access to customers' data*, the Independent, 14 mars 2016, disponible en ligne en anglais sur : http://www.independent.co.uk/news/uk/politics/investigatory-powers-bill-tech-companies-will-have-to-give-police-back-door-access-to-private-data-a6928581.html

L'AFFAIRE APPLE C. FBI

Depuis un an, Apple et le FBI sont engagés dans une bataille publique sur la question du chiffrement, en raison de l'utilisation de plus en plus fréquente de systèmes de chiffrement complexes dans les produits Apple. La situation a atteint un point critique lorsque le FBI a cherché à débloquer un iPhone 5C utilisé par l'un des tireurs de l'attaque de San Bernardino, Californie, au cours de laquelle 14 personnes ont été tuées en décembre 2015.

Le 16 février 2016, suite à une demande du ministère de la Justice américain, une juge fédérale a ordonné à Apple de créer une version spéciale de son système d'exploitation iOS qui permettrait aux enquêteurs de contourner les protections du téléphone. Tim Cook, le directeur général d'Apple, a répondu dans une lettre ouverte, dans laquelle il a qualifié les demandes du gouvernement de « violation de la vie privée » aux conséquences « inquiétantes ». M. Cook a déclaré :

« Lorsque le FBI a exigé des données qui étaient en notre possession, nous les leur avons fournies. Apple se conforme aux assignations à comparaître et aux mandats de perquisition valides. Nous l'avons fait lors de l'affaire de San Bernardino. Nous avons également mis des ingénieurs d'Apple à la disposition du FBI pour les conseiller, et nous avons apporté nos meilleures idées sur de nombreuses pistes d'enquête possibles... Mais là, le gouvernement américain nous a demandé quelque chose dont nous ne disposons tout simplement pas, et dont la conception nous semble trop dangereuse. Ils nous ont demandé de concevoir une porte dérobée sur l'iPhone. »[50]

Apple a fait appel de cette décision et une audience devant un tribunal fédéral était prévue le 22 mars 2016.[51] De nombreux experts indépendants du domaine des technologies, professeurs de droit, entreprises technologiques et organisations de défense des droits humains ont soutenu la position d'Apple dans cette affaire.[52] Un grand nombre de personnes qui s'opposent à la demande du FBI, parmi lesquelles Amnesty International, estime que si l'entreprise venait à être contrainte de modifier son logiciel pour débloquer le téléphone en question, cela créerait un précédent qui permettrait au gouvernement américain, et éventuellement à d'autres gouvernements, de contraindre les entreprises technologiques à changer leurs produits pour en affaiblir ou contourner le chiffrement, en créant une « porte dérobée » pour les services de renseignements et autres agences de sécurité.

En réponse à cette affaire, le Haut-Commissaire des Nations unies aux droits de l'homme a déclaré : « Un succès dans l'affaire contre Apple aux Etats-Unis établirait un précédent qui pourrait rendre impossible pour Apple ou toute autre société informatique internationale majeure de protéger la vie privée de ses clients partout dans le monde... Cela pourrait être un cadeau fait aux régimes autoritaires et aux pirates informatiques. Les autorités d'autres Etats ont déjà déployé des efforts concertés pour forcer des sociétés

[50] Tim Cook, A Message to Our Customers, 16 février 2016, disponible en ligne en anglais sur : http://www.apple.com/customer-letter/

[51] Apple, FBI to head to court March 22, USA Today, 20 février 2016, disponible en ligne en anglais sur : http://www.usatoday.com/story/tech/news/2016/02/19/apple-fbi--court-march-22-riverside-march-22/80635402/

[52] Une liste de mémoires destinés à éclairer le tribunal pour soutenir Apple le 22 mars 2016 est disponible ici : http://www.apple.com/pr/library/2016/03/03Amicus-Briefs-in-Support-of-Apple.html

du secteur de l'informatique et des communications, comme Google et Blackberry, afin qu'elles exposent leurs clients à de la surveillance de masse. »[53]

COMMENT LE CHIFFREMENT RESTREINT L'ACCES AUX DONNEES PAR LE GOUVERNEMENT

Tandis que les États se retranchent derrière l'inquiétude généralisée de « plonger dans le noir », les trois formes de chiffrement principales représentent des obstacles différents à la surveillance électronique par les agences gouvernementales. Cette section présente un aperçu des protections apportées par les trois principaux types de chiffrement des données et de leur effet sur la capacité des États à accéder aux informations.

CHIFFREMENT COMPLET DES DONNEES D'UN DISQUE DUR OU D'UN APPAREIL

Bien que le chiffrement complet soit une fonctionnalité disponible depuis un certain temps sur de nombreux ordinateurs de bureau et ordinateurs portables, ce n'est que depuis 2014 que les entreprises du secteur technologique telles qu'Apple et Google ont commencé à activer le chiffrement complet des données par défaut sur leurs produits. Les téléphones qui comportent cette fonctionnalité ne peuvent être déchiffrés que par la personne en possession du code PIN ou du mot de passe du téléphone.

Le chiffrement complet des données joue un rôle capital dans la prévention et la dissuasion des vols de smartphones et des autres activités délictueuses qui pourraient découler de l'accès aux informations contenues dans ces appareils.

En 2011, Symantec, une entreprise de sécurité informatique de premier plan, a réalisé une expérience dans plusieurs grandes villes d'Amérique du Nord appelée « The Symantec Smartphone Honey Stick Project », qui impliquait la perte intentionnelle de 50 smartphones, dans lesquels des données personnelles et professionnelles factices avaient été ajoutées. L'entreprise pouvait surveiller à distance ce qui arrivait aux smartphones une fois qu'ils étaient trouvés. Les résultats de l'expérience ont notamment relevé des tentatives pour accéder à :[54]

- Au moins un des divers fichiers ou applications, sur 96 % des appareils ;
- Des données ou applications personnelles sur 89 % des appareils ;
- Une application privée de photos sur 72 % des appareils ;
- Une application de services bancaires sur 43 % des appareils ;
- Des comptes de réseaux sociaux et des courriels personnels sur plus de 60 % des appareils ;

[53]Bureau du Haut-Commissaire des Nations unies aux droits de l'homme, L'affaire Apple-FBI pourrait avoir de graves conséquences sur les droits de l'homme : Zeid, 4 mars 2016, disponible en ligne sur : http://www.unog.ch/unog/website/news_media.nsf/%28httpNewsByYear_fr%29/C8C51806F21D271EC1257F6C00399C14?OpenDocument&cntxt=AD9F9&cookielang=fr

[54] Symantec, *The Symantec Smartphone Honey Stick Project*, disponible en ligne en anglais sur : http://www.symantec.com/content/en/us/about/presskits/b-symantec-smartphone-honey-stick-project.en-us.pdf

- Des données ou applications d'ordre professionnel sur 83 % des appareils.

Le vol massif de données personnelles, qu'elles soient privées ou professionnelles, représente un risque réel pour tout utilisateur d'un ordinateur ou d'un smartphone, et a de graves implications sur la vie privée. Le chiffrement complet des données est un moyen sûr et efficace de protéger la vie privée des individus contre ce risque.

Par ailleurs, le chiffrement complet des données peut rendre le contenu d'un appareil inaccessible sous un format intelligible aux États, même si l'appareil est en leur possession, à moins qu'ils ne puissent obtenir le code PIN ou le mot de passe. Cette question est au cœur de l'affaire qui oppose Apple au FBI, abordée dans la section précédente.

CHIFFREMENT DE BOUT EN BOUT

Au cours des dernières années, plusieurs services de messagerie numérique répandus ont adopté la technologie du chiffrement de bout en bout. Certains d'entre eux, comme iMessage et Signal, utilisent le chiffrement de bout en bout pour tous les utilisateurs du service. D'autres, comme WhatsApp, utilisent le chiffrement de bout en bout entre certains messages (mais pas tous), tandis que d'autres comme Telegram proposent une option distincte qui utilise le chiffrement de bout en bout. Lorsque ce type de chiffrement est utilisé, seuls les utilisateurs, et non les fournisseurs de service, possèdent les clés pour déchiffrer les données.

Bien qu'en pratique, relativement peu de services proposent un chiffrement de bout en bout par défaut, le nombre considérable de personnes ayant accès à ces services (à titre d'exemple, WhatsApp avait un milliard d'utilisateurs en février 2016[55]) a fait de cette question l'une des priorités des forces de l'ordre en matière de chiffrement.

L'existence de services de messagerie dotés du chiffrement de bout en bout présente des avantages indéniables pour la vie privée : cela signifie que même si un message est intercepté, il ne pourra pas être lu dans un format intelligible. Même lorsqu'ils sont stockés ou envoyés par l'intermédiaire des serveurs de l'entreprise, les messages sont sous un format chiffré que la société elle-même est incapable de lire ou d'analyser. Bien qu'il soit toujours possible pour une tierce partie, telle qu'un État, d'intercepter des messages via ces services, celle-ci ne pourra pas lire le contenu des messages.[56]

De toute évidence, proposer le chiffrement de bout en bout suppose un compromis de la part des entreprises technologiques : d'une part, cette technologie leur permet d'attirer des utilisateurs pour qui le respect de la vie privée est important ; d'autre part, elle les prive des revenus issus de la vente de publicité adaptée au contenu des communications de leurs utilisateurs. En termes de réputation cependant, les entreprises sont en meilleure position pour réfuter les accusations selon lesquelles elles prennent part à la surveillance des États si elles proposent un chiffrement de bout en bout.

[55] Blog de WhatsApp, One Billion, 1er février 2016, disponible en ligne sur : https://blog.whatsapp.com/616/Un-milliard?

[56] En revanche, les métadonnées associées aux messages interceptés, qui comprennent l'expéditeur, le destinataire et l'heure à laquelle le message a été envoyé, sont généralement accessibles.

C'est d'ailleurs une priorité croissante pour les entreprises technologiques, dans le sillage des révélations d'Edward Snowden concernant le rôle qu'ont joué les entreprises dans le programme de surveillance américain Prism.

Avec l'adoption du chiffrement de bout en bout par les services de messagerie, les agences gouvernementales ne peuvent plus accéder au contenu de certaines communications qui, jusque récemment, leur était facilement accessible. L'utilisation généralisée de services de messagerie Internet comme iMessage ou WhatsApp au lieu des SMS illustre parfaitement cette tendance. Les messages envoyés par SMS ne sont pas chiffrés de bout en bout, et sont par conséquent potentiellement accessibles aux agences gouvernementales.

Pour autant, l'utilisation de ces services chiffrés de bout en bout n'empêche pas la surveillance ou la recherche d'appareils ciblés, ni l'analyse des métadonnées associées aux messages chiffrés interceptés. En revanche, ces services constituent un frein au déploiement de programmes de surveillance de masse. Ils sont potentiellement à l'origine des politiques visant à endiguer l'expansion du chiffrement de bout en bout.

CHIFFREMENT DE TRANSPORT

Le chiffrement de données en mouvement est le type de chiffrement le plus couramment rencontré par la plupart des gens. De plus en plus de services, sites internet et applications utilisent le chiffrement de transport : les données transférées aux services d'une entreprise sont chiffrées et ne peuvent donc pas être lues par des tierces parties, y compris par les fournisseurs d'accès Internet ou toute personne qui intercepterait le trafic Internet. Cela permet d'empêcher des pirates informatiques d'avoir accès aux informations bancaires d'un individu, ou à ses identifiants et mots de passe lorsqu'ils sont renseignés sur un formulaire en ligne, même s'ils peuvent accéder à sa connexion Internet.

La transition vers le chiffrement de transport, sous la forme de l'HTTPS, a commencé bien avant les révélations d'Edward Snowden, mais elle s'est accélérée depuis. Le déploiement de l'HTTPS par les entreprises garantit aux consommateurs que leurs données ne sont pas exposées aux criminels et aux pirates informatiques, et il est généralement considéré comme indispensable à la sécurité et à la vie privée.[57] Une fois que les données parviennent aux serveurs d'une entreprise, elles sont déchiffrables, autrement dit, elles peuvent être lues par les ordinateurs (et les employés) de l'entreprise. Dans une déclaration, l'Internet Architecture Board, le comité chargé par l'Internet Society de superviser le développement technique et technologique d'Internet,[58] a recommandé que tous « les protocoles nouvellement élaborés [...] privilégient le chiffrement au texte en clair », et a incité « les développeurs à intégrer le chiffrement dans leur versions, et à les rendre chiffrées par défaut. »[59]

---

[57] Voir par exemple Mike Shema, *Web security: why you should always use HTTPS*, 31 mai 2011, disponible en ligne en anglais sur : http://mashable.com/2011/05/31/https-web-security/#su01rbovusqy and Scott Gilbertson, *HTTPS is more secure, so why isn't the web using it?* 20 mars 2011, disponible en ligne en anglais sur http://arstechnica.com/business/2011/03/https-is-more-secure-so-why-isnt-the-web-using-it/

[58] Pour plus d'informations sur l'Internet Architecture Board, visitez : https://www.iab.org/about/

[59] IAB Statement on Internet Confidentiality, 14 novembre 2015 : https://www.iab.org/2014/11/14/iab-

Du point de vue de la surveillance par les États, le déploiement de l'HTTPS diminue la valeur de l'interception des communications lorsqu'elles circulent dans un réseau. Lorsqu'un service utilise l'HTTPS, les communications envoyées via ce service peuvent être interceptées, mais leur contenu chiffré ne peut être lu. Cependant, le chiffrement de transport n'empêche pas complètement les autorités d'accéder aux données.

Les agences gouvernementales peuvent toujours délivrer des mandats, par exemple à une entreprise qui possède un site internet qui utilise l'HTTPS, pour lui ordonner de révéler le contenu déchiffré de ses données et communications. De plus, il est important de souligner que certaines formes de chiffrement de transport peuvent être exposées au déchiffrement par les agences de renseignement les plus avancées en matière de technologies.[60]

---

statement-on-internet-confidentiality/

[60] Voir par exemple John Leyden, *Let's talk about that NSA Diffie-Hellman crack*, 19 octobre 2015, disponible en ligne en anglais sur : http://www.theregister.co.uk/2015/10/19/nsa_crypto_breaking_theory/

4. RESTRICTIONS SUR LE CHIFFREMENT ET LEUR APPLICABILITE TECHNIQUE ET PRATIQUE

Il existe un certain nombre d'approches permettant aux gouvernements de contourner ou de restreindre le chiffrement. Cela va de l'interdiction pure et simple à des restrictions générales, telles qu'une obligation d'affaiblir le chiffrement ou de prévoir une porte dérobée, en passant par des ordonnances de déchiffrement ciblé. Toutes ces approches, et notamment les restrictions les plus générales, posent aux gouvernements et aux entreprises des défis techniques et pratiques. Cette section présente les types de restrictions suivants :

- Mesures générales interdisant ou restreignant le chiffrement ;
- Obligation pour les entreprises de prévoir une porte dérobée aux services de chiffrement ;
- Obligation de divulgation des clés de chiffrement ;
- Ordonnances de déchiffrement ciblé.

MESURES GENERALES INTERDISANT OU RESTREIGNANT LE CHIFFREMENT

L'interdiction généralisée du chiffrement existe déjà dans des pays tels que la Russie, le Maroc, le Kazakhstan, le Pakistan et la Colombie.[61] Dans ces pays comme dans d'autres, les individus doivent généralement disposer d'un permis ou d'une autorisation gouvernementale pour pouvoir utiliser des services chiffrés ou qui dépassent un certain niveau de chiffrement.

Les obstacles techniques et pratiques à l'interdiction du chiffrement sont nombreux et incluent notamment les considérations suivantes :

1. La nature d'Internet est telle que des services interdits dans une certaine juridiction restent souvent techniquement accessibles. L'application de ces restrictions exigerait un investissement technique considérable de la part des fournisseurs d'accès Internet ;

2. Même si les logiciels utilisant un chiffrement complexe sont interdits à la vente ou au téléchargement dans un pays, ils restent téléchargeables par le biais de sites Internet ou de services basés dans d'autres pays ;

[61] Article 1, loi n°1738 de 2014 ; voir http://www.digitalrightslac.net/en/la-peligrosa-ambiguedad-de-las-normas-sobre-cifrado-de-comunicaciones-en-colombia/ – Pour consulter la liste complète des réglementations nationales relatives à la cryptographie, rendez-vous sur http://www.cryptolaw.org/.

3. L'adoption d'une interdiction totale du chiffrement ne constituerait pas seulement une grave menace pour la cybersécurité d'un pays donné, mais dissuaderait également l'industrie technologique d'y faire commerce ou d'y proposer ses services, avec toutes les conséquences économiques potentielles que cela impliquerait pour le pays concerné.

OBLIGATION POUR LES ENTREPRISES DE PREVOIR UNE PORTE DEROBEE AUX SERVICES DE CHIFFREMENT

La position du gouvernement américain sur la question des portes dérobées est d'autant plus importante qu'un grand nombre d'entreprises technologiques majeures sont établies aux États-Unis. Pour cette raison, si le gouvernement américain ordonnait la présence systématique de portes dérobées, cela affecterait les utilisateurs du monde entier. En 2015, l'administration Obama a envisagé quatre types de mesures mais a finalement renoncé à les adopter.[62] Ces mesures représentent bien les types de portes dérobées susceptibles d'être envisagées par d'autres gouvernements.

4. Obligation pour les entreprises de modifier leurs appareils afin d'y inclure un port physique et indépendant chiffré pour lequel le gouvernement disposerait d'un jeu séparé de clés de chiffrement qu'il pourrait utiliser s'il avait physiquement accès à l'appareil. Un tel système ne permettrait d'accéder qu'aux données (potentiellement limitées) stockées sur l'appareil. De plus, ce système pourrait être contourné par les utilisateurs employant d'autres formes de chiffrement sur leurs appareils.

5. Obligation pour les entreprises d'envoyer à un utilisateur de fausses mises à jour de sécurité visant à installer un logiciel malveillant développé par les autorités responsables de l'application des lois et permettant au gouvernement d'accéder à l'appareil à distance. Cette mesure aurait de graves conséquences sur la sécurité des communications, car elle remettrait en question la fiabilité des mises à jour de sécurité, dissuadant ainsi les utilisateurs de les télécharger.

6. Obligation pour les entreprises de créer une sauvegarde forcée et ponctuelle des données à un emplacement distinct accessible, sans obligation d'en informer l'utilisateur. Cette mesure obligerait le fournisseur de service à avoir la capacité technique de sauvegarder des informations initialement stockées sur un appareil chiffré à un emplacement différent, non chiffré, auquel les agences responsables de l'application des lois auraient accès. Cela obligerait donc de nombreux fournisseurs de service à modifier leurs systèmes existants ou à en développer de nouveaux.

7. Développement d'un système de dépôt de clés : cela donnerait lieu à un accord selon lequel les clés nécessaires au déchiffrement des données seraient divisées et réparties entre les différentes parties prenantes, de sorte que, dans certaines circonstances, les clés soient réassemblées pour

[62] *Obama administration explored ways to bypass smartphone encryption*, Washington Post, 24 septembre 2015, disponible en ligne en anglais sur : https://www.washingtonpost.com/world/national-security/obama-administration-ponders-how-to-seek-access-to-encrypted-data/2015/09/23/107a811c-5b22-11e5-b38e-06883aacba64_story.html ; le projet de rapport de l'administration Obama sur les options techniques concernant le chiffrement est disponible à l'adresse suivante : http://apps.washingtonpost.com/g/documents/world/read-the-obama-administrations-draft-paper-on-technical-options-for-the-encryption-debate/1753/

pouvoir accéder aux données. Le gouvernement américain, tout en soutenant la faisabilité technique d'un système de dépôt de clés, admet qu'un tel système « serait difficile à mettre en place et à maintenir, car il nécessiterait un réseau de parties indépendantes chargées de la récupération des clés qui seraient ensuite validées par des tiers de confiance. »[63]

L'administration Obama a conclu qu'elle n'adopterait aucune de ces propositions. Il semble qu'il existe des dissensions au sein de l'administration, certains hauts responsables apportant leur soutien à un chiffrement renforcé.[64]

Les propositions en faveur des portes dérobées ont été sévèrement critiquées par de nombreux experts en sécurité informatique, qui considèrent qu'elles entraîneraient de graves risques en termes de sécurité et mettraient en péril les droits humains. L'un des articles faisant le plus autorité sur ces questions, *Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications,* a été publié en 2015 par quinze des cryptographes et ingénieurs informaticiens les plus réputés au monde. Dans cet article, ils plaident contre les dispositifs d'« accès exceptionnel ». Ils affirment :

> « Cela présente trois grands problèmes. Tout d'abord, l'octroi d'un accès exceptionnel aux communications constituerait un revers pour les bonnes pratiques actuellement déployées pour rendre le réseau Internet plus sûr. Ces pratiques incluent notamment la confidentialité persistante, en vertu de laquelle les clés de déchiffrement sont supprimées immédiatement après utilisation, de sorte que le vol de la clé de chiffrement utilisée par un serveur de communication ne compromette pas la confidentialité des communications passées ou futures [...]
>
> Deuxièmement, l'intégration d'un accès exceptionnel augmenterait sensiblement la complexité des systèmes. Les chercheurs spécialisés dans la sécurité, qu'ils soient employés par le gouvernement ou non, s'accordent à dire que la complexité est l'ennemie de la sécurité. Toute nouvelle fonctionnalité est susceptible d'interagir avec les autres et de créer des vulnérabilités. Afin de permettre un accès exceptionnel généralisé, de nouvelles fonctionnalités devraient être mises au point et testées par des centaines de milliers de développeurs dans le monde entier.
>
> Enfin, un accès exceptionnel créerait des cibles concentrées susceptibles d'attirer des utilisateurs malveillants. Les certificats de sécurité qui déverrouillent les données devraient être conservés par le fournisseur de la plateforme, par les agences responsables de l'application des lois ou par un autre tiers de confiance. Si les clés remises aux forces de

[63] Extrait du projet de rapport de l'administration Obama sur les options techniques concernant le chiffrement, disponible en ligne en anglais sur : http://apps.washingtonpost.com/g/documents/world/read-the-obama-administrations-draft-paper-on-technical-options-for-the-encryption-debate/1753/

[64] Voir par exemple : "Defense secretary favors strong encryption, not 'back doors,'" Associated Press, 2 mars 2016, disponible en ligne en anglais sur : http://bigstory.ap.org/article/01cc8a109f934081b341a573e382a5f3/defense-secretary-favors-strong-encryption-not-back-doors ; "Obama, at South by Southwest, Calls for Law Enforcement Access in Encryption Fight," 11 mars 2016, disponible en ligne en anglais sur : http://www.nytimes.com/2016/03/12/us/politics/obama-heads-to-south-by-southwest-festival-to-talk-about-technology.html

> l'ordre garantissaient l'accès à toutes les données, un pirate informatique ayant obtenu ces clés bénéficierait du même privilège. En outre, la requête des autorités d'avoir un accès rapide aux données rendrait impossible le stockage des clés hors ligne ou leur répartition entre plusieurs tiers, comme le font normalement les ingénieurs de sécurité pour les certificats extrêmement sensibles [...] Si les fournisseurs de service appliquaient mal les normes d'accès exceptionnel, ils mettraient en danger la sécurité de tous leurs usagers. »[65]

L'approche actuellement adoptée par le gouvernement américain repose sur des accords passés avec des fournisseurs de services de communication. D'après la note interne de la Maison-Blanche, qui évoquait les quatre mesures potentielles discutées plus haut, « les tentatives de coopération avec l'industrie [...] constituent l'option la plus adaptée pour avancer sur cette question. »[66] Une telle « coopération » pourrait encourager les entreprises technologiques à affaiblir, réduire ou limiter le déploiement de chiffrement complexe par défaut.

LES « CRYPTO WARS », CES GUERRES DE LA CRYPTOGRAPHIE

L'actuelle polémique relative à la restriction du chiffrement est surnommée la seconde « guerre de la cryptographie » (« Crypto Wars » en anglais),[67] une référence troublante à la fameuse guerre de la cryptographie qui opposa le gouvernement américain à l'industrie technologique dans les années 90. Ses origines remontent aux années 70, lorsque le gouvernement américain a classé les algorithmes de chiffrement sous la catégorie de « munitions » dans le but de contrôler les exportations.[68] Dans les années 90, les États-Unis ont cherché à renforcer les contrôles sur les personnes souhaitant diffuser gratuitement sur le marché de la grande consommation des produits de chiffrement destinés à des applications non militaires, et ont même tenté de poursuivre en justice le développeur du logiciel PGP, Phil Zimmermann.[69] Les spécialistes et les militants ont réagi en imprimant des codes et des clés de chiffrement sur des T-shirts et sur papier lors de leurs voyages à l'étranger, pour manifester leur opposition à l'application de règles de contrôle draconiennes par les États-Unis. [70]

---

[65] Harold Abelson et al, *Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications*, Massachusetts Institute of Technology, 6 juillet 2015, disponible en ligne en anglais sur : http://www.crypto.com/papers/Keys_Under_Doormats_FINAL.pdf

[66] Extrait du projet de rapport de l'administration Obama sur les options techniques concernant le chiffrement, disponible en ligne en anglais sur : http://apps.washingtonpost.com/g/documents/world/read-the-obama-administrations-draft-paper-on-technical-options-for-the-encryption-debate/1753/

[67] Voir par exemple : The Economist, *Spooks v tech firms: Crypto wars 2.0*, 8 novembre 2014, disponible en ligne en anglais sur : http://www.economist.com/news/business/21631055-intelligence-agencies-and-tech-firms-have-little-choice-compromise-crypto-wars-20 et Matthew Prince, The Second Crypto War and the Future of the Internet, Huffington Post, 21 janvier 2015, disponible en ligne en anglais sur : http://www.huffingtonpost.com/matthew-prince/the-second-crypto-war-and_b_6517528.html

[68] Voir par exemple Electronic Frontier Foundation, *EFF sues to overturn cryptography restrictions*, 21 février 1995, disponible en ligne en anglais sur : https://www.eff.org/press/archives/2008/04/21-42

[69] Philip Zimmermann, *Frequently Asked Questions*, disponible en ligne en anglais sur : https://www.philzimmermann.com/EN/faq/index.html

[70] *The latest weapon in encryption war: a t-shirt*, GCN, 5 février 1996, disponible en ligne en anglais sur :

Au même moment, l'administration du président Bill Clinton a tenté de faire adopter par l'industrie technologique un système de porte dérobée appelé la « puce Clipper », un cryptoprocesseur que les opérateurs installeraient sur leurs réseaux et dont le gouvernement possèderait la clé de déchiffrement.[71] Lorsque l'industrie a refusé d'adopter ce plan, les États-Unis ont demandé à ce que d'autres formes de dépôts de clés soient adoptées et ont incité d'autres pays, notamment le Royaume-Uni, à proposer des systèmes similaires. Néanmoins, l'opposition de l'industrie, y compris du secteur bancaire, la colère de la société civile et le changement d'administration après les élections présidentielles de 2000 ont finalement conduit à l'abandon de ces tentatives.

OBLIGATION DE DIVULGATION DES CLES DE CHIFFREMENT

Lorsque les autorités sont en mesure d'intercepter les communications mais pas de les déchiffrer, elles peuvent chercher à pouvoir imposer aux entreprises de dévoiler leurs clés de chiffrement. L'obligation de divulgation des clés de chiffrement est prévue dans la législation d'un certain nombre de pays européens, parmi lesquels le Royaume-Uni, l'Espagne et la France. Elle se distingue de l'obligation de divulgation des données stockées, par exemple sur ordonnance du tribunal ou sur mandat, et de l'obligation de déchiffrer les informations (voir paragraphe ci-après, Ordonnances de déchiffrement ciblé), car elle implique que le fournisseur de services dévoile les clés de chiffrement aux agences gouvernementales, ces dernières disposant ainsi d'un contrôle total sur le type et la quantité de données déchiffrées.

La faisabilité technique de cette mesure est de plus en plus entravée par une fonction qui peut être ajoutée au chiffrement de transport, appelée confidentialité persistante parfaite.[72] La mise en place de protocoles de confidentialité persistante permet, lorsque les clés de chiffrement privées d'un serveur sont compromises, d'empêcher le déchiffrement des communications antérieures.[73] Google et Facebook comptent parmi les acteurs majeurs d'Internet en faveur de la confidentialité persistante parfaite ;[74] il en est de même pour les messageries instantanées qui utilisent le protocole OTR.[75] Les entreprises qui proposent des produits équipés du chiffrement de bout en bout, telles qu'iMessage et Whatsapp,[76] ne détiennent pas les clés de chiffrement des messages

---

https://gcn.com/articles/1996/02/05/the-latest-weapon-in-encryption-war-a-tshirt.aspx

[71] Electronic Privacy Information Center, *The Clipper Chip*, disponible en ligne en anglais sur : https://www.epic.org/crypto/clipper/

[72] Pour en savoir plus, voir https://fr.wikipedia.org/wiki/Confidentialit%C3%A9_persistante

[73] Pour en savoir plus, voir Electronic Frontier Foundation, *Why the web needs perfect forward secrecy more than ever*, 8 avril 2014, disponible en ligne en anglais sur : https://www.eff.org/deeplinks/2014/04/why-web-needs-perfect-forward-secrecy

[74] *Pushing for Perfect Forward Secrecy, an Important Web Privacy Protection*, Electronic Frontier Foundation, 28 août 2013, disponible en ligne en anglais sur :

https://www.eff.org/deeplinks/2013/08/pushing-perfect-forward-secrecy-important-web-privacy-protection

[75] OTR, pour « Off-the-Record Messaging », est un protocole cryptographique qui fournit un chiffrement aux applications de messagerie instantanée. Voir https://en.wikipedia.org/wiki/Off-the-Record_Messaging

[76] Il existe des limites à l'applicabilité du chiffrement de bout en bout, tant pour iMessage que pour WhatsApp. Pour en savoir plus, voir Kurt Wagner, *Is Your Messaging App Encrypted?*, 21 décembre 2015, disponible en ligne en anglais sur : http://recode.net/2015/12/21/is-your-messaging-app-encrypted/

envoyés via leurs plateformes. Cela signifie qu'elles ne sont pas en mesure de se soumettre aux ordonnances de divulgation de clés de chiffrement.

ORDONNANCES DE DECHIFFREMENT CIBLE

Plusieurs juridictions donnent aux forces de l'ordre et/ou aux services de renseignement le droit d'exiger le déchiffrement de données afin de leur permettre de mener des enquêtes criminelles ou d'empêcher des actes criminels, notamment des actes terroristes. Ainsi, la partie III de la Regulation of Investigatory Powers Act (RIPA) (loi britannique portant sur les pouvoirs en matière d'enquête), prévoit que toute personne en possession d'une clé de chiffrement a l'obligation de déchiffrer des informations spécifiques si elle en reçoit l'ordre. 76 autorisations d'ordonnances de déchiffrement ont été accordées par le National Technical Assistance Centre (centre britannique d'assistance technique national) en 2013-2014, dernière période pour laquelle des statistiques sont disponibles.[77] Même dans les cas où la loi ne prévoit pas spécifiquement d'ordonnances de déchiffrement, des dispositions générales réglementant/imposant l'assistance aux perquisitions informatiques peuvent être invoquées pour exiger le déchiffrement.[78]

---

[77] Office of Surveillance Commissioners, *Rapport Annuel 2013-2014*, HC 343 SG/2014/92, disponible en ligne en anglais sur : https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/350857/Annual-Report-of-the-Chief-Surveillance-Commissioner-for-2013-2014-laid-4-September-2014.pdf

[78] Par exemple, d'après l'article 30 du projet de loi zimbabwéen sur la cybercriminalité, toute personne (qui n'est pas suspectée de crime) ayant des connaissance relatives à un système informatique soumis à une enquête peut être contrainte d'apporter son aide en fournissant des informations qui permettent d'obtenir des données intelligibles à partir du système informatique en question, dans un format recevable, pour les besoins d'une procédure judiciaire.

5. AUCUNE PORTE DEROBEE NE DOIT MENACER NOS DROITS

A l'ère du numérique, l'accès au chiffrement et son usage favorisent le plein exercice du droit à la vie privée et à la liberté d'expression, d'information et d'opinion, et ont également un impact sur le droit à la liberté de réunion pacifique et d'association, entre autres droits humains.

Le chiffrement est un outil particulièrement indispensable pour les défenseurs des droits humains, les militants et les journalistes, qui y ont de plus en plus recours pour assurer leur sécurité et celle des autres. Sans le chiffrement, l'omniprésence des technologies de surveillance et leur usage généralisé par les États mettent en danger le travail de ceux qui se battent pour leurs droits et ceux de leur communauté.

Amnesty International estime que les États doivent faciliter l'utilisation du chiffrement et ne doivent pas s'ingérer ou permettre l'ingérence d'autres parties dans ce chiffrement sans raison valable.

Étant donné le rôle critique que joue le chiffrement des données dans la jouissance des droits à la vie privée et à la liberté d'expression notamment, les restrictions concernant son accès et son usage constituent une ingérence dans la jouissance des droits humains. Ainsi, toutes les restrictions relatives au chiffrement doivent être inscrites dans la législation de manière précise et transparente, n'être employées qu'en cas de nécessité pour atteindre un objectif légitime, et ne pas être discriminatoires à l'égard de groupes ou d'individus spécifiques. Il est important de souligner que toute mesure d'ingérence dans le chiffrement des données doit être proportionnée à l'objectif légitime qui a motivé son imposition, et les avantages retirés doivent l'emporter sur les dommages causés, notamment aux individus et à la sécurité et à l'infrastructure des réseaux.

Amnesty International estime que les lois et les politiques qui interdisent l'utilisation de services ou d'outils de chiffrement spécifiques en tant que tels, qui interdisent l'utilisation du chiffrement (en dehors des spécifications approuvées par l'État) ou qui exigent des individus qu'ils obtiennent des autorisations gouvernementales pour pouvoir utiliser le chiffrement, représentent une ingérence disproportionnée dans la jouissance des droits à la vie privée et à la liberté d'expression. De telles mesures ont non seulement pour effet de priver tous les individus d'une juridiction particulière de leur capacité à protéger efficacement leurs communications, mais elles font aussi obstacle à l'accès libre et confidentiel à Internet et aux autres technologies, et peuvent avoir un « effet néfaste » sur la liberté d'expression et sur l'accès à l'information.

Les mesures obligeant les entreprises à créer des portes dérobées au chiffrement intégré à leurs produits et services (affectant tous les utilisateurs) constituent une ingérence considérable dans le droit des utilisateurs à la vie privée et à la liberté d'expression. Étant donné que ces mesures affectent de manière indiscriminée la vie privée en ligne de tous les utilisateurs en affaiblissant la sécurité de leurs communications électroniques et de leurs données personnelles, Amnesty International considère qu'elles sont fondamentalement disproportionnées, et donc inacceptables au regard du droit international relatif aux droits humains

Les États ont l'obligation de respecter, de protéger et de faire respecter les droits à la vie privée et à la liberté d'expression. Ils doivent notamment assurer la protection des individus contre les violations commises par des tierces parties, parmi lesquelles les États étrangers, les organisations internationales, les entreprises ou les particuliers. Par conséquent, les États doivent activement promouvoir, faciliter et assurer par tout autre moyen la sécurité des communications en ligne. Ils peuvent par exemple sensibiliser leurs populations à la sécurité sur Internet, encourager l'identification et la réparation des failles de sécurité sur les réseaux et systèmes informatiques, et faciliter l'usage d'outils et de services de chiffrement.

RESPONSABILITE DES ENTREPRISES TECHNOLOGIQUES DE RESPECTER LES DROITS HUMAINS

Il incombe aux entreprises de respecter tous les droits humains, où qu'elles opèrent dans le monde,[79] et ce indépendamment des capacités ou de la détermination des États à remplir leurs propres obligations en matière de droits humains.[80] Au titre de cette responsabilité, les entreprises doivent mettre en place des mesures adéquates pour identifier, empêcher et sanctionner les violations des droits humains dans le cadre de leurs activités internationales (mesures appelées diligence requise en matière de droits humains).[81]

Du fait du rôle crucial que joue le chiffrement dans la jouissance des droits à la vie privée et à la liberté d'expression, les entreprises technologiques et les fournisseurs de services pourraient contribuer aux violations des droits humains commises par les États ou les tierces parties si elles incorporent un faible niveau de chiffrement à leurs produits ou si elles se plient aux demandes des gouvernements visant à restreindre l'accès au chiffrement ou son usage. Pour cette raison, les entreprises technologiques et les fournisseurs de services doivent constamment prendre des mesures proactives efficaces pour évaluer et limiter ces risques dans chaque juridiction dans laquelle ils opèrent ou prévoient d'opérer.

Il est de la responsabilité des entreprises d'intégrer au moins un niveau adéquat de chiffrement lorsque leurs produits et services impliquent le stockage, le traitement ou le transfert de données personnelles. Les entreprises doivent développer le chiffrement de manière efficace et

[79] Principes directeurs de l'ONU relatifs aux entreprises et aux droits de l'homme, approuvés par le Conseil des droits de l'homme des Nations Unies en 2011. Haut-Commissariat des Nations Unies aux droits de l'homme, Principes directeurs de l'ONU relatifs aux entreprises et aux droits de l'homme : Mise en œuvre du cadre de référence « protéger, respecter et réparer » des Nations Unies, 2011, doc. ONU HR/PUB/11/04, disponible sur http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_FR.pdf Ces principes apparaissent également dans le chapitre sur les droits humains des Principes directeurs à l'intention des entreprises multinationales de l'OCDE. Depuis 2011, les Principes directeurs contiennent un chapitre sur les droits humains qui détaille la diligence requise que les entreprises doivent exercer pour garantir la protection des droits humains dans leurs activités à l'étranger. Principes directeurs à l'intention des entreprises multinationales de l'OCDE (2011), disponible sur : http://mneguidelines.oecd.org/text/.

[80] Principes directeurs de l'ONU relatifs aux entreprises et aux droits de l'homme, commentaire du principe 11

[81] Principes directeurs de l'ONU relatifs aux entreprises et aux droits de l'homme, principes 15(b) et 17.

proportionnée aux risques identifiés. Les entreprises doivent aussi clairement et explicitement informer leurs utilisateurs du niveau de sécurité intégré à leur produit ou service. De plus, elles doivent les informer du fait qu'elles peuvent être contraintes, conformément à la législation nationale applicable, de rendre les informations des utilisateurs accessibles aux forces de l'ordre ou aux services de renseignements.

Il se peut que les entreprises soient soumises à une pression juridique ou politique importante les incitant à se conformer aux demandes des gouvernements de fournir des informations sur les utilisateurs ou de restreindre l'accès au chiffrement ou son usage, y compris en affaiblissant le chiffrement ou en intégrant des « portes dérobées » à leurs produits. Si une entreprise reçoit une demande d'un gouvernement qui n'est pas conforme à la législation nationale, ou qui y est conforme mais risque d'enfreindre le droit international relatif aux droits humains, elle devra contester cette demande et faire tout ce qui est en son pouvoir pour respecter au mieux les droits humains dans les circonstances dans lesquelles elle opère. De plus, elle devra être en mesure de prouver ses efforts (c'est-à-dire les mesures de diligence requise mises en place en matière de droits humains) à cet égard. Les entreprises devront avertir les utilisateurs affectés et rendre publiques de telles demandes, ainsi que la façon dont elles ont été traitées.

Le chiffrement constitue aujourd'hui un outil essentiel à l'exercice des droits humains et un élément fondamental à la sécurité individuelle, nationale et internationale. Comme le déclare le Haut-Commissaire des Nations unies aux droits de l'homme : « Le débat sur le chiffrement se focalise trop sur un aspect de la question de la sécurité, à savoir son usage potentiel à des fins criminelles en temps de terrorisme. D'un autre côté, l'affaiblissement des protections par chiffrement pourrait engendrer des menaces bien plus graves pour la sécurité nationale et internationale. »[82] Non seulement le chiffrement doit être protégé contre les ingérences injustifiées des États, qui constitueraient une violation de leurs obligations au regard du droit international, mais les États ont également une obligation positive de faciliter son usage, tandis que les entreprises ont la responsabilité d'intégrer un niveau de chiffrement adéquat à leurs produits et services.

[82] Bureau du Haut-Commissaire des Nations unies aux droits de l'homme, L'affaire *Apple-FBI* pourrait avoir de graves conséquences sur les droits de l'homme : Zeid, 4 mars 2016, disponible en ligne sur : http://www.unog.ch/unog/website/news_media.nsf/%28httpNewsByYear_fr%29/C8C51806F21D271EC1257F6C00399C14?OpenDocument&cntxt=AD9F9&cookielang=fr

ANNEXE : POLITIQUE D'AMNESTY INTERNATIONAL SUR LE CHIFFREMENT

Cette politique reflète la position d'Amnesty International vis-à-vis du droit et des normes internationaux relatifs aux droits humains qui s'appliquent à l'utilisation des outils et services de chiffrement dans les technologies numériques par les détenteurs de droits, et les restrictions possibles de cette utilisation par les États. Par cette politique et la documentation qui y est associée, Amnesty International entend contribuer aux discussions internationales menées autour de cette question. Cette politique fera régulièrement l'objet de relectures et de révisions.

1. Définitions

Chiffrement – procédé mathématique de conversion de messages, d'informations ou de données sous une forme lisible uniquement par le destinataire prévu. Il existe trois types de chiffrement principaux qui sont utilisés couramment sur Internet :

- **Le chiffrement de bout en bout** s'utilise lorsque les clés nécessaires au déchiffrement des communications sont détenues exclusivement par l'expéditeur et le destinataire de la communication. Lorsque le chiffrement de bout en bout est utilisé, tout appareil ou fournisseur de service intermédiaire ayant accès aux communications électroniques ou toute personne voulant intercepter ces communications est incapable de lire leur contenu. Par exemple, au moment de la rédaction de cette politique début 2016, toute personne interceptant des iMessages (messages utilisés sur les appareils Apple) ou des messages Signal chiffrés de bout en bout est dans l'incapacité de les lire.
- **Le chiffrement des données d'un disque dur ou d'un appareil** est le procédé par lequel toutes les données stockées sur un ordinateur ou un smartphone sont chiffrées lorsqu'elles se trouvent sur l'appareil. Certaines formes de chiffrement des données d'un appareil rendent les données stockées sur un appareil illisibles et inaccessibles à toute personne ne possédant pas le code PIN ou le mot de passe de l'appareil, y compris l'entreprise ayant produit l'appareil ou son logiciel d'exploitation.
- **Le chiffrement de transport (transport encryption), ou chiffrement de la couche transport (transport layer encryption) (HTTPS, TLS et SSL sont les plus couramment utilisés),** consiste à chiffrer des informations et des données au fur et à mesure qu'elles traversent un réseau informatique, par exemple lorsque l'on accède à un site internet ou que l'on envoie un courriel. Parmi les différents types de chiffrement de la couche transport, on trouve le Secure Socket Layer (SSL) et le Transport Layer Security (TLS) (. En pratique, ces trois types de chiffrement chiffrent les interactions des individus avec des sites internet spécifiques auxquels ils ont accédé via leur navigateur internet. Lorsque les données sont en possession du fournisseur de service, elles sont sous un format non chiffré. Cela signifie qu'elles peuvent être remises aux forces de l'ordre, ou accessibles d'une autre façon sous une forme intelligible, une fois transmises à l'entreprise ou au site Internet destinataire.

Anonymat – le fait d'éviter toute identification. Le chiffrement ne permet pas l'anonymat : bien

que les outils de chiffrement garantissent que le contenu d'une communication soit uniquement déchiffrable par ceux qui détiennent une clé de déchiffrement, ils ne fournissent aucun anonymat, que ce soit à l'expéditeur ou au destinataire. Avec le chiffrement, l'identité des parties d'une communication reste vérifiable, car les métadonnées associées à la communication ne sont pas chiffrées. Si une personne souhaite rester anonyme, elle devra employer des outils et méthodes d'anonymisation, telle que l'utilisation de pseudonymes ou d'outils d'anonymisation comme le navigateur spécial « Tor ».[83]

Portes dérobées ou « backdooring » – terme informel utilisé pour désigner des mesures techniques visant à affaiblir ou à altérer des outils, appareils et services de chiffrement afin de faciliter l'accès aux informations et aux communications pour des personnes autres que le fournisseur de service et les parties aux informations et aux communications. Les États peuvent prendre certaines mesures pour contraindre les fournisseurs de service à créer des portes dérobées, notamment :

- La génération et la conservation de clés de chiffrement, afin d'anticiper le besoin éventuel du gouvernement d'avoir accès à des informations et des communications ;
- Le dépôt (autrement dit la conservation) de clés de chiffrement auprès d'un tiers de confiance neutre afin que, sous certaines conditions, une tierce partie autorisée (appelée « tiers de séquestre »), en général une autorité gouvernementale, puisse avoir accès à ces clés pour effectuer un déchiffrement ;
- L'affaiblissement du niveau de chiffrement des outils, appareils et services de chiffrement ; ou
- La limitation du chiffrement à des formes autorisées ou à des générateurs de nombres aléatoires spécifiques approuvés par l'État, employés pour générer des clés de chiffrement.

Une autre approche a retenu l'attention début 2016 : un ensemble de mesures pour contraindre les entreprises à concevoir et à installer des mises à jour de logiciel qui surmonteraient les protections de chiffrement d'un appareil, d'un outil ou d'un service spécifique. Bien que le procédé soit considéré comme une porte dérobée, on peut aussi le qualifier de tentative de contournement du chiffrement visant à accéder aux informations et aux communications, que l'on appelle généralement piratage (aussi connu sous le nom de computer network exploitation, exploitation de réseau informatique, ou encore equipment interference, interférence du matériel). Le piratage s'effectue en utilisant des vulnérabilités, des logiciels malveillants et l'ingénierie sociale[84] pour accéder à un appareil, un système ou un réseau, et il est généralement employé pour contourner le chiffrement face auquel les autres méthodes d'interception se révéleraient inefficaces. Néanmoins, pour les besoins de la présente politique, nous considérons que l'utilisation de « mises à jour forcées » constitue un autre outil de « backdooring ».

« Plonger dans le noir » – expression utilisée par les forces de l'ordre américaines (et que d'autres se sont appropriés par la suite) pour décrire la diminution présumée des capacités des agences

[83] Pour plus d'informations sur Tor, consultez : https://www.torproject.org/about/overview.html.en

[84] L'ingénierie sociale, dans le cadre de la sécurité de l'information, peut être définie comme la « manipulation psychologique d'individus pour les amener à effectuer certaines actions ou à divulguer des informations confidentielles ».

d'application des lois à accéder au contenu (mais non aux métadonnées) des communications, en raison de l'augmentation de l'utilisation du chiffrement dans les services et technologies des communications courantes. En réalité, le chiffrement n'empêche généralement pas l'interception des communications, ni l'obtention d'informations utiles à partir de celles-ci ; les services de renseignement peuvent toujours extraire des informations des communications chiffrées interceptées, telles que la date, l'heure, l'expéditeur, la taille, etc. qui sont désignées sous le nom de métadonnées.

Métadonnées ; toute information générée par l'utilisation de technologies de communication autre que le contenu même de la communication. Bien que cette information ne contienne pas nécessairement de détails personnels ou sur le contenu, elle apporte des renseignements sur les appareils utilisés, les utilisateurs, et la façon dont ils sont utilisés (d'où le nom de « données de communication » ou « données à propos des données », tels que les destinataires des courriels, les heures d'appel, les données de localisation, et dans le cas des téléphones portables, les antennes-relais utilisées). Si elle est associée à d'autres sources de données, une analyse des métadonnées peut apporter une idée précise des liens qu'entretiennent les participants d'une communication ainsi que de leurs habitudes. L'inspection, le stockage, l'utilisation et la communication des métadonnées des utilisateurs représente une ingérence considérable dans leur droit à la vie privée et à d'autres droits.

2. Principes généraux

A l'ère du numérique, l'accès au chiffrement et son usage favorisent le plein exercice du droit à la vie privée et à la liberté d'expression, d'information et d'opinion, et ont également un impact sur le droit à la liberté de réunion pacifique et d'association ainsi que sur d'autres droits humains. Le chiffrement est un outil particulièrement indispensable pour les défenseurs des droits humains, les militants et les journalistes, qui y ont de plus en plus recours pour assurer leur sécurité et celle des autres. Amnesty International estime que les États doivent faciliter l'utilisation du chiffrement et ne doivent pas s'ingérer ou permettre l'ingérence d'autres parties sans raison valable.

Étant donné le rôle critique que joue le chiffrement des données dans la jouissance des droits à la vie privée et à la liberté d'expression notamment, les restrictions à son accès et à son usage constituent une ingérence dans la jouissance des droits humains qui doivent être garantis par la loi. Aussi, ces restrictions doivent être nécessaires et proportionnées à l'objectif légitime qui a motivé leur imposition.[85] En particulier :[86]

- Les propositions visant à restreindre l'accès au chiffrement et son usage doivent s'appuyer sur des motifs d'ordre public détaillés et étayés par des preuves ; l'État devra apporter la preuve que toute ingérence est justifiée, c'est à dire ni illégale ni arbitraire, mais

[85]Le Comité des droits de l'homme de l'ONU a confirmé que le caractère non-arbitraire (terme utilisé dans l'article 17 du PIDCP) est indissociable du caractère raisonnable, c'est-à-dire de la nécessité et de la proportionnalité, et a rappelé que l'article 17 prévoit les trois mêmes critères que l'article 19 (dans ses Observations finales sur les États-Unis d'Amérique en 2014).

[86]Se référer également au rapport de David Kaye, rapporteur spécial des Nations Unis sur la Liberté d'expression, sur le chiffrement et l'anonymat, publié en 2015 et disponible sur http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/29/32

nécessaire et proportionnée ;

- Les mesures qui entravent l'accès au chiffrement ou à son usage doivent s'inscrire dans le cadre de lois qui soient précises, publiques, transparentes et non-discriminatoires, qui apportent des garanties efficaces contre les abus, et qui ne confèrent pas aux autorités publiques un pouvoir illimité ;
- Les mesures visant à contourner la protection apportée par le chiffrement doivent faire l'objet d'une autorisation judiciaire préalable ;
- Les mesures qui entravent le chiffrement doivent être appliquées de façon restrictive et adoptées uniquement dans la mesure où elles sont nécessaires[87] à la réalisation d'un objectif légitime donné, et appliquées de façon proportionnée à cet objectif légitime ;
- Les mesures qui entravent le chiffrement doivent être les moins intrusives possibles pour atteindre le résultat voulu, et ne doivent pas rendre l'essence du droit qui a été entravé insignifiante ;
- Les mesures qui entravent le chiffrement ne doivent pas être discriminatoires à l'encontre d'individus ou de groupes spécifiques sur la base de leur race, sexe/genre, orientation sexuelle, identité de genre, religion ou croyance, opinion politique ou autre, ethnicité, origine géographique ou sociale, handicap, ou d'un autre statut ;
- Les avantages retirés de l'adoption d'une mesure qui porterait atteinte au chiffrement doivent l'emporter sur les préjudices causés, y compris aux personnes tierces et à la sécurité et à l'infrastructure des réseaux ; et
- Les restrictions à l'accès au chiffrement et à son usage, ainsi que les mesures prises pour entraver l'usage du chiffrement, doivent être supervisées par un organe civil efficace indépendant et impartial.

3. Obligations positives

Les États ont l'obligation de respecter, de protéger et de faire respecter les droits à la vie privée et à la liberté d'expression. Ils doivent notamment assurer la protection des individus contre les violations commises par des tierces parties, parmi lesquelles les États étrangers, les organisations internationales, les entreprises ou les particuliers. Par conséquent, les États doivent activement promouvoir, faciliter et assurer par tout autre moyen la sécurité des communications en ligne. Ils peuvent par exemple sensibiliser leurs populations à la sécurité sur Internet, encourager l'identification et la réparation des failles de sécurité sur les réseaux et systèmes informatiques, et faciliter l'usage d'outils et de services de chiffrement.

4. Le secteur privé

Il incombe aux entreprises de respecter tous les droits humains, où qu'elles opèrent dans le monde,[88] et ce indépendamment des capacités ou de la détermination des États de remplir leurs

[87] Un niveau plus élevé que « utile », « raisonnable » ou « souhaitable ».

[88] Principes directeurs de l'ONU relatifs aux entreprises et aux droits de l'homme, approuvés par le Conseil des droits de l'homme des Nations Unies en 2011. Haut-Commissariat des Nations Unies aux droits de l'homme, Principes directeurs de l'ONU relatifs aux entreprises et aux droits de l'homme : Mise en œuvre du cadre de référence « protéger, respecter et réparer » des Nations Unies, 2011, doc. ONU HR/PUB/11/04, disponible sur http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_FR.pdf. Ces principes apparaissent également dans le chapitre sur les droits humains des Principes directeurs à l'intention des entreprises multinationales de l'OCDE. Depuis 2011, les Principes directeurs contiennent un chapitre sur les droits humains qui détaille la diligence requise que les entreprises doivent exercer pour garantir la protection des droits humains dans leurs activités à l'étranger. Principes directeurs à l'intention des entreprises

propres obligations en matière de droits humains.[89] Pour exercer cette responsabilité, les entreprises doivent constamment prendre des mesures proactives efficaces pour s'assurer qu'elles n'occasionnent ou ne contribuent à aucune violation des droits humains. Cela nécessite la mise en place de mesures adéquates de la part des entreprises pour identifier, empêcher et sanctionner les violations des droits humains dans le cadre de leurs activités à l'étranger (mesures appelées diligence requise en matière de droits humains).[90]

Du fait du rôle crucial que joue le chiffrement dans la jouissance des droits à la vie privée et à la liberté d'expression, les entreprises technologiques et les fournisseurs de services pourraient contribuer aux violations des droits humains commises par les États ou les tierces parties si elles incorporent un faible niveau de chiffrement à leurs produits ou si elles se plient aux demandes des gouvernements visant à restreindre l'accès au chiffrement ou son usage. Pour cette raison, les entreprises technologiques et les fournisseurs de services doivent constamment prendre des mesures proactives efficaces pour évaluer et limiter ces risques dans chaque juridiction dans laquelle ils opèrent ou prévoient d'opérer.

Il est de la responsabilité des entreprises d'intégrer au moins un niveau adéquat de chiffrement lorsque leurs produits et services impliquent le stockage, le traitement ou le transfert de données personnelles. Elles doivent intégrer le chiffrement à un niveau qui soit efficace et suffisant face aux risques identifiés, et ceci pour les formes courantes de chiffrement de la couche transport, pour le chiffrement des données d'un disque/appareil, ou encore pour le chiffrement de bout en bout. Ainsi, lorsqu'il existe un risque élevé ou probable de violation ou de contribution à la violation de droits humains, par exemple, en raison de la situation ou du contexte dans lequel les entreprises opèrent, le plus haut niveau de chiffrement devra être mis en place. Dans tous les cas, les entreprises doivent clairement et explicitement informer leurs utilisateurs du niveau de sécurité intégré à leur produit ou service. De plus, elles doivent les informer du fait qu'elles peuvent être contraintes, conformément à la législation nationale applicable, de rendre les informations des utilisateurs accessibles aux agences chargées de l'application des lois ou aux services de renseignements.

Il se peut que les entreprises soient soumises à une pression juridique ou politique importante les incitant à se conformer aux demandes des gouvernements de fournir des informations sur les utilisateurs ou de restreindre l'accès au chiffrement ou son usage, y compris en affaiblissant le chiffrement ou en intégrant des « portes dérobées » à leurs produits. Si une entreprises est sujette à une demande d'un gouvernement qui n'est pas conforme à la législation nationale, ou qui y est conforme mais risque d'enfreindre le droit international relatif aux droits humains et ses normes, elle devra contester de telles demandes et faire tout ce qui est en son pouvoir pour respecter au mieux les droits humains dans les circonstances dans lesquelles elle opère. De plus, elle devra être en mesure de prouver ses efforts (c'est-à-dire les mesures de diligence requise mises en place en matière de droits humains) à cet égard. Les entreprises devront avertir les utilisateurs affectés et rendre publiques de telles demandes, ainsi que la façon dont elles ont été traitées. Elles devront également dévoiler les mesures prises en matière de diligence requise pour identifier et sanctionner les violations des droits humains dans le cadre de leur activité.

---

multinationales de l'OCDE (2011), disponible sur : http://mneguidelines.oecd.org/text/.

[89] Principes directeurs de l'ONU relatifs aux entreprises et aux droits de l'homme, commentaire du principe 11.

[90] Principes directeurs de l'ONU relatifs aux entreprises et aux droits de l'homme, principes 15(b) et 17.

Ces mesures permettront de réduire le risque que des entreprises technologiques et des fournisseurs de services contribuent à des violations des droits humains par les États mais aussi par d'autres tierces parties. Cependant, une procédure de diligence requise en matière de droits humains, aussi solide et exhaustive soit-elle, peut se traduire par l'impossibilité pour une entreprise d'opérer dans une juridiction si aucun moyen efficace de limiter le risque de violation des droits humains ne peut être identifié.

5. Interdictions générales du chiffrement

Les lois et les politiques qui interdisent l'utilisation de certains services ou outils de chiffrement, l'intégration du chiffrement (en dehors des spécifications approuvées par l'État), ou qui exigent des personnes l'obtention d'autorisations de l'État pour avoir recours au chiffrement, représentent une ingérence disproportionnée dans la jouissance des droits à la vie privée et à la liberté d'expression. De telles mesures ont non seulement pour effet de priver tous les individus d'une juridiction particulière de leur capacité à protéger efficacement leurs communications, mais elles font aussi obstacle à l'accès libre et confidentiel à Internet et aux autres technologies, et peuvent avoir un « effet néfaste » sur la liberté d'expression et sur l'accès à l'information.

6. Tentatives des États de contraindre les entreprises à intégrer des « portes dérobées » au chiffrement

Le fait de contraindre les entreprises à créer des « portes dérobées » au chiffrement intégré sur leurs produits et services (affectant tous les utilisateurs), afin de s'assurer que les communications peuvent être déchiffrées par eux-mêmes ou par les pouvoirs publics sur demande, constitue une ingérence considérable dans le droit des utilisateurs à la vie privée et à la liberté d'expression. Étant donné que ces mesures affectent de manière indiscriminée la vie privée en ligne de tous les utilisateurs en affaiblissant la sécurité de leurs communications électroniques et de leurs données personnelles, Amnesty International considère qu'elles sont fondamentalement disproportionnées, et donc inacceptables au regard du droit international relatif aux droits humains. C'est d'autant plus vrai au vu de la disponibilité d'autres mesures moins intrusives (telles que les ordonnances de déchiffrement ciblé), et des préjudices que peuvent causer de telles mesures, notamment l'effet néfaste sur l'exercice de la liberté d'expression et l'exposition des communications en ligne et des données des individus aux failles de sécurité et aux autres menaces à la sécurité. Même s'il était possible de concevoir une porte dérobée qui puisse permettre à un État d'accéder uniquement aux communications d'un individu spécifique et qui ne menacerait pas la sécurité des autres utilisateurs, cela soulèverait une vague d'inquiétude semblable à celles relatives aux divulgations de clés obligatoires (voir point 8 plus bas).

7. Chiffrement de bout en bout

Le chiffrement de bout en bout offre aux personnes la capacité de protéger efficacement leurs communications contre les ingérences de tierces parties, et constitue donc un moyen important pour assurer la protection et la jouissance de leur droit à la vie privée et à la liberté d'expression. Bien que l'utilisation du chiffrement de bout en bout puisse, dans certaines circonstances, compliquer la mise en place de mesures de surveillance légitimes par les États, cette difficulté ne doit pas constituer un motif suffisant pour justifier des mesures radicales à grande échelle visant à interdire, affaiblir ou incorporer des portes dérobées au chiffrement de bout en bout.

8. Divulgation de clés obligatoire

Des ordonnances judiciaires demandant la divulgation de clés de chiffrement permettraient aux

États d'accéder à l'ensemble des communications d'un individu, et non plus seulement à quelques-unes d'entre elles spécifiquement ciblées.[91] Même si ces ordonnances peuvent constituer un moyen efficace pour atteindre un objectif légitime, elles représentent une grave atteinte au droit à la vie privée et à d'autres droits. Elles permettent à une autorité d'examiner des données privées, susceptibles de dépasser largement le cadre d'une enquête ou d'un objectif légitime spécifiques. De plus, de telles ordonnances obligent souvent les entreprises à conserver les clés de chiffrement afin de faciliter leur divulgation lorsque le gouvernement le requiert, ce qui soulève des inquiétudes vis-à-vis de la question de la proportionnalité mentionnée plus haut.

Par ailleurs, l'existence même de pouvoirs de divulgation de clés obligatoire dans une juridiction donnée pourrait avoir un effet dissuasif sur l'utilisation de certains outils ou services qui favorisent la liberté d'expression et l'accès à l'information, engendrant une ingérence excessive dans les communications privées de la part des États, et conduisant à un « effet néfaste ».

Aussi, Amnesty International estime que les ordonnances de divulgation de clés obligatoire ne sauraient respecter les obligations en matière de droits humains, sauf si elles remplissent certains critères, notamment si :

- Elles sont utilisées de manière individualisée contre des personnes spécifiques sur la base de soupçons raisonnables ;
- Elles ont une portée limitée, autrement dit, elles se restreignent aux communications liées de manière suffisamment directe aux agissements devant être empêchés ou devant faire l'objet d'une enquête, afin d'atteindre un objectif légitime ;
- Elles sont délivrées pour une durée qui ne dépasse pas ce qui est strictement nécessaire pour atteindre l'objectif légitime pour lequel le déchiffrement a été autorisé ;
- Elles ne contraignent pas les entreprises à conserver les clés de chiffrement ;
- Elles ne sont utilisées que lorsque des moyens moins intrusifs, notamment les ordonnances de déchiffrement ciblé, ne sont pas disponibles ;
- Elles ne sont pas discriminatoires à l'encontre d'individus ou de groupes spécifiques en raison de leur race, sexe/genre, orientation sexuelle, identité de genre, religion ou croyance, opinion politique ou autre, ethnicité, origine géographique ou sociale, handicap, ou d'un autre statut ;
- Elles doivent être soumises à autorisation préalable par une autorité judiciaire ; et
- Elles doivent pouvoir faire l'objet d'un recours juridictionnel pendant et après leur utilisation.

La législation doit imposer la suppression dès que possible des communications obtenues au moyen d'ordonnances de divulgation de clés obligatoire, et au plus tard lorsque celles-ci ne sont plus strictement nécessaires à la réalisation de l'objectif légitime pour lequel elles ont été délivrées.

9. Ordonnances de déchiffrement ciblé

[91] Ceci est dû au fait que dans de nombreuses applications de chiffrement, une seule série de clés est utilisée pour chiffrer toutes les communications d'un utilisateur. Si les clés sont dévoilées, toutes les communications passées et futures peuvent être déchiffrées.

Bien qu'elles représentent une ingérence qui doit être justifiée par le droit international relatif aux droits humains et ses normes, les ordonnances de déchiffrement ciblé constituent, a priori, une limitation plus proportionnée des droits à la vie privée et à la liberté d'expression, étant donné qu'elles ne concernent que les communications spécifiquement visées et ne nécessitent pas la divulgation d'une clé de chiffrement. Néanmoins, de telles ordonnances ne doivent être délivrées que dans des circonstances exceptionnelles afin d'atteindre un objectif légitime. Elles doivent s'appuyer sur des lois accessibles au public, avoir une portée explicitement limitée, se focaliser sur une cible précise sur la base de soupçons raisonnables, faire l'objet d'une autorisation de la part d'une autorité judiciaire, et être mises en œuvre par une autorité civile compétente, indépendante et impartiale. Elles ne peuvent être utilisées que lorsque des moyens moins intrusifs ne sont pas disponibles.

AMNESTY INTERNATIONAL

www.amnesty.org