Chiffrement, sécurité et libertés

Positionnement de l'Observatoire des libertés et du Numérique, janvier 2017

Résumé du positionnement

Les capacités (techniques et légales) de surveillance des États à l'ère numérique sont aujourd'hui telles que le droit fondamental à la vie privée, garant de la liberté d'expression, d'opinion, d'information, dans une société démocratique, a été profondément remis en cause ces dernières années, en France et dans le monde.

Dans ces conditions, la capacité de chiffrer ses communications numériques et ses données informatiques est une condition indispensable à la préservation des droits et libertés fondamentales, et l'un des derniers remparts, individuels et collectifs, aux intrusions arbitraires et illégales de nombreux acteurs, étatiques, privés, ou criminels.

Le chiffrement va bien au-delà d'une question de droits de l'Homme : alors que le numérique a investi l'ensemble des champs d'activité humains, l'affaiblir, quelle que soit la technique utilisée, reviendrait à fragiliser considérablement l'économie, mais aussi la sécurité collective.

Répétons-le, il n'existe pas de technique d'affaiblissement systémique du chiffrement qui ne permettrait de viser que les activités criminelles : l'ensemble des citoyens seraient alors aussi potentiellement visés. Il n'existe pas non plus de technique d'affaiblissement du chiffrement qui ne profiterait qu'à des acteurs « bien intentionnés ». Si une faille est créée pour un État (police, justice, service de renseignements…), elle sera alors disponible pour tous les autres acteurs (Autres États, organisations criminelles, hackers…) moins bien intentionnés.

Le chiffrement est-il utilisé par des personnes se livrant à des activités criminelles ? Oui, puisque par nature celles-ci tentent de dissimuler leurs actes. Mais il est surtout utilisé chaque jour par chaque citoyen, dans chacune ou presque de ses activités numériques. Des criminels peuvent fomenter leurs activités dans une voiture fermée. Il ne viendrait à personne l'idée de supprimer les voitures, ou de les doter systématiquement d'un système d'écoutes intégré directement accessible aux services de l'État.

Pourtant, c'est cette logique que défendent les partisans d'une criminalisation ou d'un affaiblissement du chiffrement. De la même manière qu'il existe des possibilités techniques de mettre sur écoute un espace (comme une voiture) où se dérouleraient des activités criminelles, qui doivent être encadrées par le droit, il existe un large éventail de possibilités légales et de techniques d'enquête permettant aux services de l'État de collecter des éléments de preuve à l'encontre d'organisations suspectées d'activités criminelles. Cet arsenal légal, comme les outils d'interception et de décryptage, a été largement renforcé ces dernières années.

Le bénéfice d'un affaiblissement supplémentaire du chiffrement dans la lutte contre la criminalité semble très faible, pour ne pas dire incertain. Ce qui est certain par contre, c'est que les conséquences seraient dévastatrices pour les droits et libertés de chacun, l'économie et la sécurité du pays, et pour la vie en société de manière générale.

1. Le chiffrement : un outil de protection des libertés

La protection de la vie privée est à la fois une responsabilité collective et individuelle. Loin de l'éternel argument du « rien à cacher » qui individualise les citoyens pour faire disparaître leurs relations avec les autres, la vie privée se réfère avant tout une notion de confiance nécessaire pour la vie en société. Sans cette confiance de base, le simple concept de société perd de son sens. Sans confiance dans la sécurité de nos communications, nous ne pouvons pas nous exprimer ni nous informer véritablement librement. La protection de nos pratiques sur Internet a donc aussi une importance fondamentale sur la liberté d'expression, d'information et la liberté d'opinion.
Il n'y a pas à choisir entre liberté et sécurité comme deux concepts opposés, mais à admettre que la liberté comprend la sécurité et vice-versa.

Oui nous avons tous quelque chose à cacher, nos communications, nos navigations et nos données ! Elles doivent être protégées.

Le chiffrement permet de protéger des données et échanges pour les soustraire aux regards indiscrets, qu'ils soient ceux d'individus malveillants, de régimes autoritaires, etc.
C'est pourquoi le chiffrement est un outil nécessaire et indispensable pour toute la population. Depuis la protection des sources des journalistes, des dossiers médicaux ou des avocats, de la sécurité des transactions bancaires et commerciales (et donc de la « confiance dans l'économie numérique »[1]), jusqu'à la protection de la vie privée des citoyens, le chiffrement des communications et des données est incontournable.
Comme une carte postale sans enveloppe peut être lue par toutes les personnes manipulant cette carte postale, une communication sur Internet en clair (donc non chiffrée) peut être lue par n'importe qui. Le chiffrement des communications est indispensable pour rendre ses échanges lisibles uniquement des personnes à qui le message est adressé. Ainsi, dans notre utilisation quotidienne d'Internet, c'est parce que la connexion est en « HTTPS », donc chiffrée, que des paiements par carte bancaire peuvent être effectués de manière sécurisée sans que quiconque connecté au réseau puisse s'emparer de vos identifiants et données bancaires.

Un cadre international

Dans cette optique, le droit international souligne le devoir de protection contre toute immixtion arbitraire ou illégale dans la vie privée des personnes[2]. Le fait que ces moyens de communication soient numériques n'a pas remis en question ce droit fondamental. Bien au contraire, l'assemblée générale des Nations Unies s'est saisie de la question en demandant en 2014 à tous les états de « *respecter et de protéger le droit à la vie privée, y compris dans le contexte de la communication numérique* »[3].
Le rapporteur spécial des Nations unies sur la liberté d'expression a rappelé en 2015 que toute restriction au chiffrement constitue une atteinte à l'exercice du droit à la vie privée et à la liberté d'expression. Elle doit donc être justifiée selon les principes impératifs de légalité, nécessité, proportionnalité et légitimité des objectifs.
Les États « *doivent faire preuve de transparence quant à la nature et la portée de leurs mesures de pénétration de l'Internet, la méthodologie appliquée et sa justification* », souligne le Rapporteur spécial sur la promotion et la protection des droits de l'Homme et des libertés fondamentales dans la lutte antiterroriste[4].

[1] Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.
[2] Art. 17 du Pacte international relatif aux droits civils et politiques (PIDCP).
[3] Résolution de l'Assemblée générale des Nations Unies du 18 décembre 2013 n°68/167 « The right to privacy in the digital age ».
[4] 4ème rapport annuel du Rapporteur spécial sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste.

Qu'est-ce que le chiffrement ? Comment ça marche ?

Le chiffrement est un procédé qui permet de transformer un message en clair, lisible par tous, en un message codé uniquement compréhensible par qui dispose du code[1]. Les techniques de chiffrement (de cryptologie) sont nombreuses, ont des fonctions différentes et sont utilisées par différents types de services. Pour bien comprendre, il faut différencier :

Le chiffrement en ligne : données « en mouvement / en transit » (*data in motion*)

— **Chiffrement de flux de données** : circulant sur Internet (discussions instantanées chiffrées, TLS, HTTPS[2]…). Il existe pour cela deux types de techniques :

- **Le chiffrement point à point** : Il est utilisé pour chiffrer des données dans leur transit, c'est-à-dire quand elles sont transportées sur le réseau. Ces données sont sous une forme intelligible à différents endroits du réseau (les serveurs) étant donné que les clés ou certificats s'y trouvent. Dans ce cas une personne qui aurait un accès (autorisé ou non) au serveur pourra lire le message.
- **Le chiffrement bout en bout** : Cette technique permet de chiffrer les données avant qu'elles soient envoyées sur le réseau et ne les déchiffre qu'à leur point d'arrivée. À aucun moment, il n'est possible de déchiffrer les données en transit. On ne peut y accéder qu'en ayant accès à l'appareil (ordinateur, téléphone, etc.) des personnes qui communiquent.

— **Chiffrement de bloc** : discussion aux messages asynchrone (GPG - PGP pour des emails, Whatsapp, Signal...)

- Ici le chiffrement point à point n'est pas possible, car il s'agit de chiffrer pour un ou des destinataires, il est de ce fait nécessairement bout en bout.

Chiffrement hors-ligne : données au repos (*data at rest*)

Chiffrement de tout ou partie de la mémoire de stockage d'un téléphone, d'une tablette, d'un ordinateur ou simplement d'un disque dur : il est utilisé pour rendre inintelligibles les informations présentes sur un appareil à toute personne qui ne dispose pas de la clé de déchiffrement.
La technique utilisée est celle d'un chiffrement symétrique (par phrase de passe) pour des données qui ne sont plus dans un processus de communication, mais auxquelles des individus pourraient accéder en cas de perte ou vol d'ordinateurs, ordiphones, tablettes, etc.

---

[1] Entrée « cryptage » sur le Larousse.fr.
[2] Le protocole HTTPS : il est la combinaison du HTTP (HyperText Transfer Protocol) avec une couche de chiffrement SSL (Secure Socket Layer). Cela permet également à l'internaute de vérifier l'identité du site web auquel il accède, grâce à un certificat d'authentification émis par une autorité tierce, réputée fiable.

2. De l'importance d'un chiffrement sûr et complet

2.1 Une remise en question croissante par les États

Malgré les prises de position répétées de nombreux acteurs et institutions en faveur du chiffrement (ONU – Haut-commissariat aux droits de l'Homme, rapporteurs spéciaux, Assemblée générale, Conseil des droits de l'Homme, Comité des droits de l'Homme –, Conseil de l'Europe[5], ENISA[6], de nombreuses institutions bancaires, et en France CNIL[7], CNNum[8], ANSSI[9], etc.) de nombreux États envisagent de promulguer des lois (ou l'ont déjà fait) visant à restreindre l'utilisation et l'accès au chiffrement. Ces mesures sont le plus souvent présentées au nom de la lutte contre le terrorisme. Ces affaiblissements remettent pourtant en question notre sécurité.

Cela a pu être constaté lorsque les problèmes d'accès aux données de l'iPhone d'un des présumés tueurs de San Bernardino ont servi de prétexte au FBI pour tenter de forcer Apple à développer une porte dérobée pour accéder aux contenus de l'ensemble des téléphones similaires. On peut penser que derrière cette affaire, le FBI avait également l'espoir d'une jurisprudence favorable qui aurait permis de contraindre l'ensemble des développeurs de logiciels à fournir des méthodes d'accès équivalentes. Ce conflit, bien que botté en touche, a ouvert la voie à des volontés similaires d'affaiblissement légal du droit au chiffrement. En témoignent les déclarations récentes du Procureur de la République de Paris et de trois de ses homologues (anglais, américain et espagnol)[10]. Le ministre de l'Intérieur français s'est également prononcé en faveur[11] d'une initiative européenne remettant en cause le droit au chiffrement.

Les techniques possibles pour affaiblir le chiffrement

À ce jour, une interdiction générale des techniques de chiffrement semble peu envisageable. Néanmoins de nombreuses méthodes ont pu être utilisées, et le sont encore aujourd'hui, pour affaiblir ou limiter le chiffrement. Un chiffrement limité revient à affaiblir la sécurité des systèmes d'information et de communication, tout en ayant – selon le Conseil national du numérique – « une efficacité limitée ».

[5] « Filtrage, blocage et suppression de contenus illégaux sur l'internet ».
[6] ENISA, « On the free use of cryptographic tools for (self) protection of EU citizens », 20 janv. 2016, et ENISA et Europol, "On lawful criminal investigation that respects 21st Century data protection. Europol and ENISA Joint Statement.", 20 mai 2016 ; ENISA et Europol, « On lawful criminal investigation that respects 21st Century data protection. Europol and ENISA Joint Statement. », 20 mai 2016.
[7] CNIL "Les enjeux de 2016 (3) : quelle position de la CNIL en matière de chiffrement ?", 8 avril 2016.
[8] Tribune du CNNum « Chiffrement et lutte contre le terrorisme : attention à ne pas se tromper de cible ».
[9] G. Pépin, « L'ANSSI défend le chiffrement de bout-en-bout, sans portes portées », NextInpact, 3 août 2016.
[10] Leppard, Cyrus R. Vance Jr, François Molins, Adrian, et Javier Zaragoza. « When Phone Encryption Blocks Justice », The New York Times, 11 août 2015.
[11] « Bernard Cazeneuve veut « une initiative européenne» contre le chiffrement ». Le Monde.fr avec Reuters, 12 août 2016, sect. Pixels.

- **Les points clairs** : dans un chiffrement de point à point, il s'agit pour l'opérateur de laisser un accès aux autorités à certains « points » du réseau, où les certificats et clés de déchiffrement sont détenus, en leur permettant d'accéder par ce biais aux contenus des échanges.

- **Les portes dérobées** : sont des « passages secrets », des failles de sécurité, que les concepteurs de produits et de services seraient obligés d'intégrer ou de laisser discrètement dans leurs appareils et services afin de permettre aux autorités l'accès à des données chiffrées en profitant de cette faille. À l'image de l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information), tous les professionnels et institutions spécialisées s'accordent pour dire que de tels affaiblissements « *sont susceptibles d'être exploités par des attaquants aux profils variés* »[1].

- **Une certification obligatoire pour les fournisseurs de services** : ce système avait été utilisé au début des « Crypto Wars »[2] aux États-Unis. Il consiste à obliger toute entreprise qui fournit une solution de chiffrement à obtenir une autorisation de l'État, voire à lui confier les clés de déchiffrement, afin que cette solution soit utilisable et légale dans le pays en question. Cela permet à l'État de rendre illégaux les services qu'il estime ne pas être en mesure de contrôler ou simplement trop puissants. De plus, ces licences peuvent également être coûteuses à obtenir. Une telle méthode peut *de facto* empêcher tout système de cryptographie basé sur du logiciel libre et un développement communautaire.

- **Une limitation de la longueur des clés** : la sécurité d'un chiffrement repose en grande partie sur la clé de chiffrement. Plus la clé est longue, plus le temps nécessaire pour casser le code sera long et donc plus le chiffrement sera sécurisé. Limiter la taille des clés de chiffrement pour n'autoriser que des clés susceptibles d'être cassées par les autorités revient à affaiblir fortement la sécurité et la confidentialité des communications. Lorsque cela avait été mis en place aux États-Unis dans les années 1990, de nombreuses entreprises avaient déploré une perte de confiance des utilisateurs en leurs services.

- **Une législation à double vitesse entre les entreprises et les individus** : il est indispensable de ne jamais perdre de vue que le chiffrement est autant lié aux questions de cyber sécurité que de vie privée. Une législation autorisant un chiffrement robuste pour certaines personnes morales qui accepteraient de remettre leurs clés de déchiffrement, comme les banques, mais le refusant aux simples personnes physiques n'est pas à exclure. Elle ne saurait être tolérée : elle nierait l'importance du chiffrement pour tout un chacun de protéger sa vie privée.

---

[1] Note de l'ANSSI « Évolution des mesures législatives relatives à la cryptographie », 24 mars 2016, le risque est évidemment que les portes dérobées soient détournées de leurs usages « légitimes » et/ou découvertes et exploitées par d'autres personnes mal intentionnées.
[2] Entrée « Crypto Wars » sur Wikipédia.fr, dernière édition du 30 nov. 2016.

2.2 L'affaiblissement du chiffrement : ni indispensable en matière judiciaire, ni opportun pour la sécurité informatique

Un droit au chiffrement sûr, sans portes dérobées et accessible à toutes et tous de façon égale apparaît indispensable, non seulement pour conserver la confiance que les utilisateurs accordent aux services et outils numériques, mais également pour assurer le respect de la vie privée et la protection des données personnelles : deux libertés fondamentales consacrées par la DUDH, le PIDCP et les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne[12].

2.2.1 Le chiffrement dans les procédures judiciaires

La poursuite, par l'institution judiciaire, des infractions pénales les plus graves peut justifier qu'il soit porté atteinte à des libertés individuelles et collectives, dans des conditions d'encadrement strict et sous réserve du respect des principes de proportionnalité, de nécessité et de non-excessivité. Les techniques visant à s'attaquer au chiffrement, comme toute technique policière intrusive, doivent être examinées avec soin. Il importe ainsi de déterminer dans quelle mesure et sous quelles conditions des techniques peuvent être utilisées pour contrer le chiffrement des communications. Pour ce faire, l'appréciation de la proportionnalité de la mesure doit se faire selon une appréhension globale de ses conséquences : le développement et la légalisation d'un certain nombre de techniques comportent-ils des effets induits qui dépassent le cadre judiciaire ?

Au préalable, il convient de rappeler l'état de la législation existante relative à la cryptologie dans les procédures pénales (en France). La préoccupation pour les communications chiffrées, si elle est relativement récente, n'est pas entièrement neuve. Elle provient d'un constat réel : des techniques de chiffrement (par le biais de messageries chiffrées) sont parfois utilisées par des personnes dans le cadre d'activités illégales, qui ne se limitent d'ailleurs pas aux infractions terroristes. C'est le propre de ces actes que de s'organiser de manière occulte : le recours à des messageries chiffrées n'est qu'une forme supplémentaire de ces dissimulations (utilisation de diverses puces téléphoniques, conversations « codées », utilisation de pseudonymes...). Malgré cela, il semble que le criminel « reste un internaute comme les autres » et que l'usage des méthodes de chiffrement semble loin d'être unanimement adopté. Ainsi la très décriée messagerie « Telegram », semble plus utilisée y compris dans des cadres djihadistes pour ses aspects de « réseaux sociaux » (discussion de groupe) que dans le cadre d'une messagerie chiffrée. Les possibilités d'enquête ou de renseignement restent ainsi importantes[13].

2.2.2 Des possibilités déjà étendues de mise au clair judiciaire des données

Des moyens d'expertise larges…

Face à ces pratiques, non majoritaires, mais réelles, le code de procédure pénale a confié aux autorités policières et judiciaires des prérogatives déjà très larges permettant la « mise au clair des données chiffrées ».

Lors d'une perquisition, l'article 57-1 du code de procédure pénale donne ainsi le pouvoir aux officiers de police judiciaire, quelle que soit la peine encourue, de requérir « *toute personne susceptible soit d'avoir connaissance des mesures appliquées pour protéger les données auxquelles il est permis d'accéder dans le cadre de la perquisition, soit de leur remettre les informations permettant d'accéder à ces données* ». Le défaut de réponse à cette réquisition est puni d'une amende.

[12] Charte des droits fondamentaux de l'Union européenne, 200/C 364/01, 18 déc. 2000.
[13] C. Adaoust, « Cinq moyens d'enquêter sur Telegram, la messagerie des jihadistes ». Franceinfo, 11 août 2016 et E. Leclère « Telegram : les messages postés sur le réseau social utilisé par les djihadistes ne sont ni chiffrés ni protégés ». France Inter, 16 août 2016.

Le code de procédure pénale comporte en outre un chapitre intitulé « *De la mise au clair des données chiffrées nécessaires à la manifestation de la vérité* », récemment modifié par la loi du 13 novembre 2014 et la loi du 3 juin 2016. Le procureur de la République comme le juge d'instruction peut ainsi, lorsque les « *données saisies ou obtenues* […] *ont fait l'objet d'opérations de transformation empêchant d'accéder aux informations en clair qu'elles contiennent ou de les comprendre, ou que ces données sont protégées par un mécanisme d'authentification* », requérir une personne physique ou morale pour effectuer « *les opérations techniques permettant d'obtenir l'accès à ces informations, leur version en clair, ainsi que, dans le cas où un moyen de cryptologie a été utilisé, la convention secrète de déchiffrement, si cela apparaît nécessaire* ».

Les moyens de l'État soumis au secret de la Défense nationale peuvent même être utilisés pour toutes les enquêtes concernant des infractions pénales punies d'au moins deux ans d'emprisonnement. Les possibilités en termes d'enquête sont ainsi colossales en permettant le recours au centre technique d'assistance (CTA) de la Direction générale de la sécurité intérieure[14]. Couvertes par le secret de la défense nationale, ces opérations seront, sauf rares exceptions, mises en œuvre de manière aveugle pour les autorités judiciaires (ainsi que les avocats de la défense) : seul le résultat de la technique, les données déchiffrées, sera produit au dossier judiciaire, sans moyen de contester les techniques utilisées.

… fondés sur le recueil préalable de données …

Les techniques de déchiffrement ou de décryptement alors utilisées peuvent notamment se nourrir des informations tenues à la disposition du Premier ministre par les fournisseurs d'un moyen de cryptologie (pour les moyens fournis par des entreprises s'y étant conformées), en application de la loi n° 2004-575 du 21 juin 2004 (LCEN) : les caractéristiques techniques et le code source des logiciels utilisés. Aux termes du décret n° 2007-663 du 2 mai 2007, le Premier ministre peut notamment exiger la communication, des caractéristiques techniques et du code source du moyen de cryptologie qui a fait l'objet de la déclaration, ainsi que la mise à disposition de l'Agence nationale de la sécurité des systèmes d'information de deux exemplaires du moyen de cryptologie pour une durée qui ne peut excéder six mois.

L'arrêté du 29 janvier 2015 définit largement les données à communiquer à l'autorité administrative, à savoir une description des fonctionnalités cryptographiques du moyen, les protocoles sécurisés utilisés (IPsec, SSH, SSL/TLS, Protocoles liés à la VoIP de type SIP/RTP), les algorithmes cryptographiques utilisés et leurs longueurs maximales de clés.

… et une incitation à l'auto incrimination : la circonstance aggravante liée au chiffrement.

Les possibilités policières de s'attaquer au chiffrement se doublent de l'aggravation des peines encourues, jusqu'au double, et ce quel que soit le délit : une circonstance aggravante est constituée « *lorsqu'un moyen de cryptologie au sens de l'article 29 de la loi n° 2004-575 du 21 juin 2004 (LCEN) a été utilisé pour préparer ou commettre un crime ou un délit, ou pour en faciliter la préparation ou la commission* ». L'article 132-79 du code pénal, qui prévoit cette répression accrue, incite les personnes mises en cause à remettre aux autorités judiciaires (mais aussi administratives) la version en clair des messages chiffrés et les conventions secrètes nécessaires au déchiffrement, afin d'échapper à l'aggravation de la peine. Cette disposition, qui s'accommode mal du droit de ne pas s'auto-incriminer, vient ainsi compléter un régime permettant soit d'attaquer le chiffrement, soit d'obtenir le déchiffrement de la personne mise en cause elle-même.

L'approfondissement des dispositions existantes, qui tendraient soit à interdire purement et simplement le chiffrement, soit à introduire des portes dérobées permettant un accès aux données non chiffrées constituerait une mesure dangereuse au regard des éléments rappelés précédemment.

Une pratique judiciaire peu quantifiable (hors mise en œuvre du CTA)

L'ampleur des techniques mises en œuvre n'est pas connue. Toutefois, l'étude d'impact de la loi du 13 novembre 2014 mentionnait les éléments suivants : « *Le volume actuel des opérations de déchiffrement a pu être déterminé*

[14] Créé par le décret n°2002-1073 du 7 août 2002.

seulement pour celles mises en œuvre par le CTA. Ainsi, pour l'année 2013, les saisines du CTA s'élevaient à 31 (8 dans le cadre d'affaires de terrorisme, 4 pour des homicides, 5 pour du vol et recel de vol, 3 pour de la pédopornographie, 2 pour escroqueries, 3 pour du trafic de stupéfiants, 1 pour une affaire de viol et 5 pour des infractions diverses), contre 26 en 2012. Pour la période de janvier à juin 2014, les saisines du CTA s'élèvent à 13 affaires. »

Ces chiffres ne prennent pas en compte les saisines par les magistrats de prestataires privés spécialisés dans le décryptement. Il n'existe pas de recensement des sociétés ou personnes physiques exerçants une telle activité.

Bien que le nombre des saisines du CTA soit stable et relativement faible, les évolutions technologiques constantes accroissent le nombre de matériels exploités dans le cadre d'une même saisine. De la même manière, certaines opérations de déchiffrement qui jusqu'à présent étaient impossibles techniquement, le deviennent grâce aux avancées de ce service (exemple : carte SIM détériorée).

2.2.3 Le décryptement : une technique d'enquête parmi d'autres

Au demeurant, la focalisation sur les communications chiffrées occulte le fait que les autorités policières et judiciaires disposent de nombreuses techniques d'enquête susceptibles de permettre le recueil d'éléments de preuve. Ainsi, les techniques de dissimulation ne sont pas nouvelles en matière de criminalité organisée ou de terrorisme, qu'elles se fassent par le recours aux nouvelles technologies ou non. Si le retard (voir parfois l'impossibilité) du déchiffrement ou du décryptement est une réalité, elle n'empêche pas les services d'enquête d'obtenir un certain nombre d'informations par d'autres moyens.

Tout d'abord, les moyens de chiffrement des communications n'occultent pas les métadonnées, dont les services enquêteurs peuvent tirer de nombreuses informations (les « fadettes » restent ainsi accessibles). Des procédés d'interception peuvent en outre être utilisés, afin d'enregistrer des conversations sur des cibles déterminées (sonorisations, mais aussi « IMSI catcher » depuis la loi du 3 juin 2016). La cyber infiltration peut également permettre d'intégrer un groupe de discussion chiffré et d'obtenir des informations sans nécessité de casser le chiffrement. Des pratiques policières moins techniques constituent également des moyens d'obtenir des informations de manière plus classique.

Compte tenu des dispositions déjà en vigueur, mais aussi de la possibilité de recourir à d'autres pratiques et techniques d'enquête, une fragilisation supplémentaire du chiffrement n'est pas souhaitable.

Cela est d'autant plus vrai que, quel que soit le régime juridique encadrant une telle évolution, elle aura vocation à se développer en dehors de ce cadre. Il n'aura échappé à personne, notamment, que les pouvoirs consentis aux autorités judiciaires pour la poursuite d'infractions pénales sont immédiatement convoités, quand ils ne sont pas déjà utilisés (par exemple, bien avant leur « légalisation » par la loi renseignement) par les services de renseignement, non seulement pour la prévention du terrorisme, mais aussi pour surveiller des personnes pouvant porter atteinte aux intérêts économiques ou de politique étrangère de la France (champs d'action élargis par la loi renseignement du 24 juillet 2015, susceptible de viser des organisations militantes plus ou moins radicales). Si l'actuel ministre de l'Intérieur affirme aujourd'hui, assez sélectivement d'ailleurs, ne vouloir casser le chiffrement que pour les affaires judiciaires, nul ne doit être dupe sur les autres bénéficiaires de ce projet : les services de renseignement, hors contrôle judiciaire.

L'efficacité des investigations judiciaires, y compris pour les faits les plus graves, ne saurait ainsi fonder un affaiblissement systémique du chiffrement, susceptible de mettre en péril la sécurité informatique générale et le droit au respect de la vie privée.

« Un chiffrement affaibli permettrait une surveillance généralisée des honnêtes citoyens, dont l'efficacité, la nécessité et la proportionnalité ne sont pas démontrées. »

« Nous comprenons tous que les législateurs ressentent le besoin d'agir en réaction aux événements suscitant une grande inquiétude publique. Ma recommandation est qu'ils prennent au sérieux leurs responsabilités pour les droits fondamentaux, tissu même de nos démocraties, et n'utilisent pas à la légère des restrictions injustifiées aux droits fondamentaux au motif que cela semblerait des mesures faciles et à faible coût. »

Extraits traduits d'une déclaration de Giovanni Buttarelli, contrôleur européen de la protection des données pour le colloque « Chiffrement, sécurité et libertés ».

Propositions de l'Observatoire des libertés et du numérique

Les capacités (techniques et légales) de surveillance à l'ère numérique sont aujourd'hui telles que le droit fondamental à la vie privée, garant de la liberté d'expression, d'opinion, d'information, dans une société démocratique, a été profondément remis en cause ces dernières années, en France et dans le monde. Dans ces conditions, la capacité de chiffrer ses communications numériques et ses données informatiques est une condition indispensable d'une part à la sécurité collective et au bon fonctionnement de l'économie et d'autre part à la préservation des droits et libertés fondamentales, en faisant obstacle aux intrusions arbitraires et illégales de nombreux acteurs, étatiques, privés, ou criminels.

L'Observatoire des libertés et du numérique appelle les acteurs publics et acteurs privés du numérique à :

- **renoncer à toute initiative visant à affaiblir juridiquement ou techniquement les outils de chiffrement ;**
- **consulter les institutions et les acteurs de la société civile pertinents suffisamment en amont de tout projet qui aurait des incidences sur le chiffrement ;**
- **garantir à toute personne l'accès à un chiffrement robuste, outil indispensable au respect du droit à la vie privée dans le domaine numérique ;**
- **promouvoir auprès du public l'importance du chiffrement de ses données et communications numériques et en faciliter l'utilisation et le développement.**