RENAISSANCE numerique

FÉVRIER 2022

Chiffrement : quel équilibre entre vie privée et sécurité nationale ?

SYNTHÈSE DU DÉBAT DU 28 OCTOBRE 2021, ORGANISÉ PAR RENAISSANCE NUMÉRIQUE ET KASPERSKY

Avec l'avènement des systèmes d'information et leur mise en réseau, les utilisateurs d'internet et d'outils informatiques ont vu leurs données devenir d'autant plus vulnérables à mesure qu'ils ont eu accès à de nouveaux services. Le chiffrement, outil de sécurisation des systèmes d'information et protecteur des droits et libertés fondamentaux, notamment de la liberté d'expression et du droit à la vie privée, est alors devenu essentiel pour les économies et les sociétés.

Toutefois, les besoins d'enquête croissants sur le cyberespace des pouvoirs judiciaires et policiers pour lutter contre les organisations criminelles conduisent des autorités à travers le monde à appeler à l'affaiblissement du chiffrement. Si tous les usages de chiffrement ne posent pas la même nature de problème aux autorités publiques lorsqu'il s'agit d'appréhender des activités criminelles, il en est une qui est une problématique pour tous les pays du monde : le chiffrement de bout-en-bout. En effet, le chiffrement de bout-en-bout, en ce qu'il constitue l'obscurcissement d'une information de manière à ce que celle-ci ne soit disponible que pour l'émetteur et les destinataires légitimes du mes-

sage, afin de garantir la confidentialité des échanges, offre de nouvelles opportunités aux organisations criminelles de se prémunir contre les enquêtes policières et judiciaires[1].

Fin avril 2021, Gérald Darmanin, ministre de l'Intérieur français, a déclaré qu'il était nécessaire de laisser le gouvernement *« rentrer et faire des failles de sécurité »* au sein des messageries cryptées pour mener des enquêtes[2]. Une déclaration qui fait écho à celle des ministères américain, australien et britannique de la Justice, qui dans une prise de parole conjointe ont souligné les *« défis importants à la sécurité publique »* que pose le chiffrement moderne, et exhorté les acteurs de la *tech* à mettre en œuvre des *« solutions raisonnables et techniquement réalisables »* pour permettre aux autorités d'accéder à des portes dérobées (*backdoors*) lorsque cela est nécessaire[3]. Tout juste formé, le gouvernement allemand d'Olaf Scholz, a quant à lui, à travers la parole de l'expert en numérique du SPD, Jens Zimmermann, affirmé vouloir faire de la défense du chiffrement de bout-en-bout une priorité afin de garantir la protection de la vie privée des citoyens.[4]

Le chiffrement bout-en-bout est donc au cœur de l'actualité et un objet de tension. Derrière ce débat, est interrogé l'équilibre entre d'une part, la sécurité des données et la protection de la vie privée des citoyens et, d'autre part, les enjeux de sécurité nationale comme la lutte contre la cybercriminalité ou le terrorisme. Cette problématique a fait l'objet d'une table ronde organisée par le think tank Renaissance Numérique et l'entreprise Kaspersky, le 28 octobre 2021, au cours de laquelle des experts juridiques, de la gendarmerie et en cybersécurité ont pu échanger. À l'occasion de cette discussion, ces derniers ont dressé un état des lieux des technologies de chiffrement et de leurs perspectives d'avenir, et sont revenus sur les risques de leur affaiblissement, le cadre juridique qui les entoure et les enjeux de coopération au niveau international qu'ils revêtent. Cette synthèse retrace ces échanges.

---

1 Dans le cadre du chiffrement de bout-en-bout, l'opérateur d'un service de communication dont les flux de communication électronique sont chiffrés de bout-en-bout entre deux utilisateurs ne dispose pas des conventions de chiffrement entre les deux utilisateurs. L'opérateur peut donc se retrouver aveugle des dispositifs de chiffrement et de déchiffrement des services qu'il propose.

2 « Gérald Darmanin : face au terrorisme, "il ne faut être ni résigné ni outrancier" », *France Inter*, 28 avril 2001 : https://www.franceinter.fr/emissions/l-invite-de-8h20-le-grand-entretien/l-invite-de-8h20-le-grand-entretien-28-avril-2021

3 United States Department of Justice, "International statement : end-to-end encryption and public safety", 11 octobre 2020 : https://www.justice.gov/opa/pr/international-statement-end-end-encryption-and-public-safety

4 « Le nouveau gouvernement allemand défendra fermement le chiffrement de bout en bout », *NextInpact*, 8 décembre 2021 : https://www.nextinpact.com/lebrief/49118/le-nouveau-gouvernement-allemand-defendra-fermement-chiffrement-bout-en-bout

Les défis contemporains du chiffrement

Le chiffrement se heurte de prime abord à un triple défi : technique, du fait du rythme des évolutions technologiques, criminel, du fait de l'essor de nouvelles manières d'organiser le crime impliquant de repenser les enquêtes policières et judiciaires, et légal, du fait de la disparité des cadres juridiques entre les États.

L'informatique fait régulièrement des bonds technologiques conséquents. L'un des grands défis technologiques qui s'annonce pour le chiffrement est l'émergence de l'informatique quantique, qui obéit à un paradigme totalement différent de celui des ordinateurs utilisés aujourd'hui, et permet d'effectuer des opérations face auxquelles les algorithmes actuels ne sont pas « résistants ». En d'autres termes, l'informatique quantique pourrait permettre de « casser » des systèmes de chiffrement très rapidement. En effet, le chiffrement consiste à transformer des données afin de les rendre illisibles grâce à un algorithme de chiffrement et une clé de chiffrement. La clé de chiffrement est utilisée par l'algorithme pour chiffrer et déchiffrer les données en question. Elle est constituée d'une suite de *bits*[5], une série de zéros et de uns, et s'apparente à un mot de passe. L'algorithme de chiffrement, de son côté, renvoie à une méthode de chiffrement, une façon de rendre inintelligibles les données. La clé et l'algorithme de chiffrement sont tous deux nécessaires au déchiffrement des données chiffrées. Or, plus l'algorithme de chiffrement est fort (« irréductibilité » mathématique), plus le déchiffrement des données – sans posséder la clé – sera long, voire impossible. Grâce à une capacité de calcul fondamentalement différente, l'informatique quantique pourrait rebattre les cartes. **Renaud Lifchitz**, directeur scientifique d'Holiseum, affirme que *« pour maintenir à niveau la sécurité et donc la confiance dans les échanges, il faut régulièrement augmenter les tailles de clés, de manière à ce que la puissance de calcul ne vienne pas menacer ces clés, puisqu'il est possible avec des ordinateurs de faire des attaques par force brute et de tester la plupart des clés, voire toutes les clés de manière à casser le chiffrement d'un message »*. Toutefois, il ajoute que ce n'est plus tant la taille des clés qui importe, mais plutôt la nature des algorithmes utilisés[6].

5 Dans la théorie de l'information, un *bit* est la quantité minimale d'information transmise par un message, et constitue à ce titre l'unité de mesure de base de l'information en informatique.

6 À cet égard, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) évoque dans un récent avis que cette transition prendra du temps, dans la mesure où *« [s]i des prototypes de petits ordinateurs quantiques existent déjà, la construction d'ordinateurs reprogrammables à grande échelle en est encore à un stade de recherche très amont »* (citation traduite de l'anglais). "ANSSI views on the post-quantum cryptography transition", 4 janvier 2022 : https://www.ssi.gouv.fr/publication/anssi-views-on-the-post-quantum-cryptography-transition/

Les évolutions technologiques dans le champ de l'informatique impliquent pour les forces de l'ordre de s'adapter en permanence et de se former aux nouveaux usages numériques afin de suivre le rythme des réseaux criminels, qui font évoluer leurs propres modes d'action au fil des innovations techniques. **Pierre-Yves Caniotti**, directeur de la Stratégie, de la Prospective et des Partenariats du Commandement de la Gendarmerie dans le Cyberespace[7], explique : *« nos enquêteurs sont en permanence sur la brèche, composant avec l'évolution des technologies numériques et des modes opératoires des délinquants, nécessitant un travail prospectif permanent pour adapter notre dispositif »*. Il insiste à ce titre sur le besoin de monter en compétences : *« Les forces de l'ordre composent aujourd'hui avec un volume toujours plus important de données à analyser et ont besoin d'enquêteurs avec des compétences assez abouties en termes de* data analyst. *»* Ces compétences sont d'autant plus nécessaires face à la généralisation de l'usage des crypto-monnaies au sein des réseaux de trafiquants, qui implique de réussir à tracer ces actifs sur internet et qui requiert donc le développement de nouveaux outils pour ne pas être dépassé.

Face à la métamorphose de la criminalité en ligne, le besoin d'enquête en ligne se fait plus prégnant. Pour **Pierre-Yves Caniotti**, *« si le chiffrement constitue pour les forces de l'ordre un défi à relever, c'est pour permettre de protéger la population et de lutter contre les organisations criminelles qui utilisent ces technologies pour dissimuler leur activité (proxénétisme en bande organisée, prostitution sur internet, atteintes aux systèmes de traitement automatisés de données par des rançongiciels, etc.) »*. Pour faire face à cette criminalité qui s'affranchit des frontières physiques, les pouvoirs policiers et judiciaires tentent de mettre en place des modes d'actions innovants, ainsi que des outils de coopération.

Dans ce contexte, la disparité des cadres juridiques entre les États est un défi majeur à relever. La juxtaposition de législations qui peuvent être radicalement différentes contraint les forces de l'ordre et les institutions juridiques dans leur capacité d'enquête, crée des incertitudes pour les opérateurs numériques et induit le risque d'affaiblir la protection des citoyens. Selon **Rayna Stamboliyska**, experte en cybersécurité, *« cette disparité est complexe à gérer pour tout le monde, car il faut s'assurer, par exemple, dans le cas où des citoyens européens peuvent être amenés à vivre ailleurs, que leurs droits fondamentaux soient respectés tout*

7 Pour en savoir plus sur le Commandement de la Gendarmerie dans le Cyberespace, voir l'encadré p. 8.

en respectant la législation souveraine du pays où ils résident. » À ce titre, **Étienne Drouard**, avocat associé chez Hogan Lovells, met en exergue une problématique de « *conflit de lois* » qui réside dans le fait qu'« *il ne s'agit pas simplement d'avoir un cadre juridique français, mais de savoir comment il peut être appliqué à l'égard d'opérateurs sur lesquels nous n'avons pas de levier pour faire appliquer la loi française* ».

Les risques induits par les portes dérobées et le chiffrement faible

Certaines autorités justifient la nécessité d'affaiblir le chiffrement par le besoin de facilitation des processus d'enquête, qui sont mis à mal par les défis mentionnés ci-dessus. Toutefois, cette fragilisation du chiffrement risque de détériorer la confiance dans les services et terminaux numériques et d'accentuer le développement du marché des vulnérabilités informatiques.

Selon certains intervenants, affaiblir le chiffrement et laisser les gouvernements instaurer des failles de sécurité serait une atteinte grave à la « confiance numérique », dans la mesure où cela offrirait les moyens techniques d'un accès exceptionnel qui rend les citoyens vulnérables à toute tentative d'intrusion dans un système de chiffrement. À partir du moment où il existe des failles accessibles, n'importe quelle personne mal intentionnée peut s'en servir afin d'espionner, de voler des données sensibles, voire d'exercer une pression pour obtenir une rançon. **Pierre-Yves Caniotti** le constate : « *le fait d'introduire nativement des portes dérobées dans un système d'information est contraire aux règles élémentaires de cybersécurité et est de nature à nuire à la confiance numérique. Cela revient à lancer ouvertement un défi aux cybercriminels pour exploiter cette vulnérabilité* ».

Renaud Lifchitz ajoute que la confiance numérique est fondamentale pour le développement et la démocratisation des nouvelles technologies au sein de la société. Selon l'expert, « *toutes les relations de société et toutes les relations économiques reposent sur la confiance. Si on fragilise cette confiance, on éclate toutes les relations de société et on éclate toutes les relations de commerce électronique, de confiance électronique* ».

Par ailleurs, affaiblir le chiffrement contribuerait au développement d'un marché des vulnérabilités informatiques. **Étienne Drouard** insiste ainsi sur le fait que *« si on laisse un marché des vulnérabilités informatiques se développer, on crée une économie accessible au plus offrant et non à ceux qui ont raison. Nous ne sommes pas sûrs d'avoir les moyens financiers ou géopolitiques d'attirer les offres de vulnérabilités vers nous ou de les utiliser de manière vertueuse au service de l'État et de la protection des concitoyens ».* Cette situation serait d'autant plus complexe, selon lui, qu'il existe un flou juridique autour de la détention de vulnérabilités d'un système d'information. En effet, l'article 323 du code pénal dispose que le fait de détenir le moyen de transformer une information dans un système d'information, à savoir donc de pouvoir le déchiffrer, est une infraction pénale.[8] Cependant, l'article ne précise pas le caractère licite ou non de la détention d'une telle faille, ce qui fait peser sur les services de l'État un risque de responsabilité concernant la détention et l'utilisation de vulnérabilités informatiques.

Dès lors, pour ne pas avoir à tomber dans les travers dans lesquels pourraient mener l'instauration de *backdoors* et l'affaiblissement du chiffrement, il convient d'étudier d'autres pistes qui permettraient de subvenir aux besoins d'enquête tout en respectant les droits et les libertés fondamentales des citoyens.

Le cadre juridique existant suffit-il à garantir l'équilibre entre protection de la vie privée et sécurité nationale ?

De nombreux moyens permettent de contourner le chiffrement sans avoir à l'affaiblir dans le cadre d'enquêtes[9]. La France est à ce titre dotée d'un cadre juridique particulièrement fourni. Le principal enjeu se situe donc plutôt au niveau de la coopération internationale sur un sujet qui a trait à la souveraineté des États.

---

8 Code Pénal, article 323-1 : https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000030939438/

9 Par exemple, la possibilité (légale) pour la police d'utiliser des *malwares* pour infecter les ordinateurs des suspects.

10 Notons ici qu'il est possible que cette source se tarisse également, à terme. À cet égard, les travaux menés par Signal visant à réduire ou chiffrer les métadonnées elles-mêmes, sont intéressants. Il est possible que les autres messageries soient contraintes de s'aligner. Pour en savoir plus sur les travaux de Signal, voir : https://signal.org/blog/sealed-sender/

D'un point de vue technique, **Renaud Lifchitz** souligne que *« l'analyse des métadonnées est intéressante. Même sans connaître la nature des messages qui sont échangés entre un groupe de personnes, connaître la fréquence de ces échanges, la constitution d'un réseau de personnes peut être très intéressante. »* [10] L'expert met aussi en exergue la question de l'*« auditabilité* a posteriori ». En effet, il explique qu'*« il existe des systèmes auditables* a posteriori, *dit de « rechiffrement » dans lesquels, lors d'une enquête qui porte sur les échanges électroniques, il est possible de dévoiler* a posteriori *l'historique des échanges »*. Pour rendre cela possible, il suffirait d'*« imposer des standards aux fournisseurs de communications électroniques »*. Sur ces points, **Pierre-Yves Caniotti** a souligné que la gendarmerie travaille *« dans des cas spécifiquement encadrés par la loi et dans des cadres visant spécifiquement la criminalité organisée, sur la mise en œuvre de moyens de déchiffrement avancés et de techniques particulières telle que la captation de données informatiques prévue par le code de procédure pénale »*.

À ce titre, le cadre législatif français concernant le chiffrement est assez développé. Selon **Étienne Drouard**, *« la problématique de sécurité et de liberté autour du chiffrement est bien encadrée en droit français. Lorsqu'on envisage de rendre illégale la non-communication des modes de chiffrement, cette interdiction existe dans le droit français depuis 2015 dans l'article L-871 du code de la sécurité intérieure*[11]*. Celui qui ne fournit pas les clés permettant au service public d'accomplir ses missions est passible de prison »*. **Pierre-Yves Caniotti** constate également que la technologie évolue à un tel rythme, que le défi consiste à composer avec ces évolutions techniques, plutôt qu'avec des dispositions juridiques.

Toutefois, la dimension internationale de la problématique pose des limites à l'application du cadre existant. Une vision commune sur les questions de chiffrement est complexe à mettre en œuvre. Pour illustrer cette difficulté, **Rayna Stamboliyska** prend l'exemple du débat autour du règlement e-Privacy[12] au sein de l'Union européenne (UE). Alors que ce texte, censé remplacer la directive e-Privacy de 2002, aurait dû être adopté en même temps que le Règlement général sur la protection des données (RGPD), soit en 2016, les discussions sont bloquées.

---

11 Code de la sécurité intérieure, article L871-1 : https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000030937647/

12 Proposition de règlement du Parlement européen et du Conseil concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE (règlement « vie privée et communications électroniques »), COM/2017/010 final - 2017/03 (COD) : https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A52017PC0010

Selon l'experte, cette incapacité des États membres de l'UE à s'entendre sur certains points fait que, en matière de chiffrement comme en matière de protection des données personnelles, on reste, à certains égards, *« dans le flou »*. L'avènement d'un cadre légal plus homogène en matière de chiffrement au niveau européen se heurte ainsi *« aux divergences concernant les pratiques des différents gouvernements »*.

La question est d'autant plus complexe qu'elle ne relève pas seulement du judiciaire et du policier mais aussi du renseignement, ce sur quoi insiste **Étienne Drouard** en expliquant que *« comme tous les États, nous n'avons pas de relation d'amitié, mais des relations d'intérêt. Ce qui structure l'Union européenne, ce sont des objectifs communs. Sur le renseignement, aucun État ne se dit qu'il va confier des pans de son renseignement. Ce serait contraire au principe de souveraineté. Il n'y a pas de fédéralisme du renseignement »*.

La question de la recherche d'un équilibre entre la sécurité nationale et le droit à la vie privée à travers le chiffrement se heurte ainsi à la complexité de la géopolitique. Toutefois, le cadre existant, bien que perfectible, permet de ne pas céder à la tentation de l'affaiblissement du chiffrement et de préserver la « confiance numérique ». Selon **Rayna Stamboliyska**, le débat que l'on a sur l'affaiblissement du chiffrement depuis plusieurs années est dépassé et la discussion remet *« au centre l'objectif de punir les coupables et de protéger les victimes »*.

LE COMMANDEMENT DE LA GENDARMERIE DANS LE CYBERESPACE

Créé officiellement le 25 février 2021[13], le Commandement de la Gendarmerie dans le Cyberespace (ComCyberGend) a pour vocation de rassembler les actions menées par la gendarmerie afin de lutter contre les cybermenaces et la criminalité dans le cyberespace. Il intègre notamment le Centre de lutte contre les criminalités numériques (C3N) et le département informatique-électronique de l'Institut de recherche criminelle de la Gendarmerie nationale, dans l'objectif de rassembler ses forces cyber et d'accroître ainsi son efficacité en termes d'enquête et de prévention.

Source : COMCyberGEND[14]

13 Arrêté du 25 février 2021 portant sur la création du commandement de la gendarmerie dans le cyberespace : https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000043261338

14 « COMCyberGEND : la gendarmerie monte en puissance face à la menace cyber », *GENDinfo*, 9 août 2021 : https://www.gendinfo.fr/actualites/2021/comcybergend-la-gendarmerie-monte-en-puissance-face-a-la-menace-cyber

—

Rédaction

Arthur Druel-Hodak, Chargé de mission, Renaissance Numérique

—

Relecture

Jennyfer Chrétien, Déléguée générale, Renaissance Numérique

Arnaud Dechoux, Responsable des affaires publiques Europe, Kaspersky

Jessica Galissaire, Responsable des études, Renaissance Numérique

Noémie Minster, Responsable communication, Kaspersky

Renaissance Numérique et Kaspersky remercient chaleureusement les intervenants et participants à ce débat qui s'est tenu dans le cadre du mois européen de la cybersécurité.