ASSEMBLÉE NATIONALE

17e LÉGISLATURE

Compte rendu

Commission spéciale chargée d'examiner le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité

Mercredi 9 juillet 2025
Séance de 15 heures 30

Compte rendu n° 14

SESSION EXTRAORDINAIRE DE 2024 - 2025

Présidence de M. Philippe Latombe, *Président*

ASSEMBLÉE NATIONALE

La séance est ouverte à 15 heures 45.

Présidence de M. Philippe Latombe, président.

La commission spéciale a auditionné sous la forme d'une table ronde, ouverte à la presse, MM. Thomas Baignères et Matthieu Finiasz, docteurs en cryptographie, co-fondateurs de la société Olvid et M. Benjamin Beurdouche, chercheur en ingénierie de sécurité et de confidentialité chez Mozilla.

M. le président Philippe Latombe. Nos auditions sur le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité concernent aujourd'hui la question du chiffrement.

Cette audition est entièrement consacrée à l'examen de l'article 16 *bis* du projet de loi, de ses implications concrètes et de son insertion dans le corpus législatif. La commission spéciale n'avait pas encore abordé ce sujet lors de ses auditions.

Si la question du chiffrement est importante, il n'était pas évident qu'elle trouve sa place dans le débat sur ce projet de loi au regard des dispositions de l'article 45 de la Constitution et du contrôle qu'en effectue le Conseil constitutionnel. En tout état de cause, cet article est désormais dans la navette et il nous revient de l'examiner avec toute l'attention qu'il mérite.

M. Benjamin Beurdouche, chercheur en ingénierie de sécurité et de confidentialité chez Mozilla. Je remercie la commission pour son invitation à discuter d'un sujet aussi complexe et important que celui de la résilience de la nation et en particulier de l'impact de la cryptographie dans cet écosystème.

Je suis chercheur en cryptographie chez Mozilla, titulaire d'un doctorat de cryptographie et méthodes formelles de l'École normale supérieure (ENS) et spécialiste de la conception, de l'analyse et de l'implémentation des protocoles cryptographiques.

Je suis l'un des co-auteurs de TLS (*Transport layer security*), principal protocole utilisé pour sécuriser internet et le *web*, et de l'un des nouveaux protocoles qui vont être utilisés pour protéger les communications audio-vidéo et pour la téléphonie mobile.

Je vais centrer mon propos sur les aspects relatifs à la cryptographie, mais suis à votre disposition pour échanger sur les questions plus larges de cybersécurité.

La menace qui pèse sur nos sociétés dans le monde numérique est multiforme. La connectivité et la numérisation permettent de grands progrès technologiques et sociétaux, mais rapprochent aussi chaque jour la menace des attaquants au plus proche de nos infrastructures critiques et des populations française et européenne. Il faudra donc être de plus en plus vigilant.

Dans ce contexte, la transposition des directives REC (Résilience des entités critiques), NIS 2 (*Network and Information Security*) et la réglementation Dora (Digital Operational Resilience Act) sont extrêmement importantes. Il est nécessaire que la loi prévoie

un cadre minimal rigoureux pour l'ensemble des acteurs, mais définisse aussi une ligne directrice permettant aux acteurs les plus proactifs de mener l'effort efficacement sans se trouver confrontés à des incertitudes juridiques. De nombreux efforts ont déjà été effectués et sont en cours pour protéger les utilisateurs des services numériques des entreprises de la BITC (base industrielle et technologique de cybersécurité), dont je considère que Mozilla fait partie. Il faut toutefois que cette démarche soit poursuivie par l'ensemble de l'écosystème économique et pas uniquement par le secteur numérique.

Ces directives visent à rehausser le niveau de sécurité des entités les plus critiques. Les sénateurs ont jugé opportun d'ajouter au titre II un article 16 *bis* afin de sanctuariser les outils les plus fondamentaux de cette sécurité, c'est-à-dire la cryptographie.

La cryptographie est l'outil principal qui nous permet de créer de la confiance dans l'intégrité, la confidentialité et l'authentification de nos données, peu importe le moyen, qu'elles soient en transit au sein de communications ou stockées sur des systèmes pour emploi futur. Il est extrêmement important de se rendre compte que cette pierre angulaire protège nos transactions financières, les communications du gouvernement, des institutions, des services d'urgence, de la sécurité opérationnelle de nos forces armées, de nos journalistes et est utilisée pour la diplomatie. Elle est donc absolument critique.

Il faut également être conscient que la moindre vulnérabilité dans un système cryptographique est dans une certaine mesure démultipliée par rapport à une faiblesse que l'on introduirait dans un système de sécurité informatique classique, car elle est systémique. La cryptographie étant une pierre angulaire, chaque atteinte qui lui est portée affaiblit le dispositif de sécurité de manière très systématique. Il est donc extrêmement important de veiller à prévenir les fragilités susceptibles d'intervenir silencieusement comme dans n'importe quel système d'information et d'être utilisées contre des journalistes, des opposants politiques, des forces de l'ordre, voire dans des situations plus courantes de violences conjugales ou domestiques.

D'un point de vue technique, je pense que l'article 16 *bis* est une bonne chose puisqu'il renforce la sécurité. Nous pourrions toutefois discuter la terminologie utilisée, notamment l'emploi du mot « chiffrement » en lieu et place du terme « cryptographie ». En effet, le chiffrement renvoie uniquement à la confidentialité, tandis que la cryptographie concerne également l'intégrité et l'authentification.

J'ai noté par ailleurs au chapitre IV, titre II, article 38 une révision des articles 30 et 35 du titre III de la loi pour la confiance dans l'économie numérique (LCEN) sur l'importation et l'exportation des moyens cryptologiques, qui a été introduite par le Sénat. Cela va dans le bon sens, mais doit sans doute être encore discuté.

Je souhaiterais clarifier un point qui ne me semble pas toujours suffisamment visible dans la position des chercheurs notamment. Nous n'avons pas de position idéologique sur le chiffrement, seulement une vision technique. Je comprends tout à fait les problématiques de sécurité défense, qui me sont assez familières, et les besoins opérationnels exprimés auparavant. Toutefois, je ne pense pas qu'il y ait de problématique particulière, si ce n'est la capacité d'accéder aux outils existants. Nous disposons en effet déjà d'outils ciblés qui nous permettent par exemple de faire du renseignement, des techniques d'enquête spéciales et tout ce dont nous avons besoin.

En revanche, il existe peut-être un problème de réorganisation des moyens de l'État pour définir qui y a accès, pour quels besoins, etc. Sans doute vaudrait-il mieux, au lieu de systématiser l'affaiblissement du chiffrement, aller vers l'emploi de ces outils ciblés en replaçant les moyens situés par exemple au ministère des armées vers de l'interministériel, ce qui permettrait au ministère de l'intérieur d'avoir également accès à ce type d'outils dans le cadre de sa lutte contre la criminalité du haut du spectre. On pourrait ainsi imaginer une discussion entre le président de la République chef des armées et le premier ministre sur la désignation de la priorité stratégique à donner à chaque typologie de cible et les moyens à y consacrer, sans affecter la pierre angulaire que constitue le chiffrement. Selon moi, moins on touche au chiffrement, mieux on se porte.

En conclusion, je suis favorable à l'article 16 *bis*. Une cryptographie solide est bien évidemment nécessaire, mais reste insuffisante. Il convient d'envisager également l'ensemble des problématiques de sécurité des systèmes d'information qui s'y rattachent, dont NIS 2, Dora et REC essaient de faire monter le niveau.

M. Thomas Baignères, cofondateur de la société Olvid. Matthieu Finiasz et moi représentons la société Olvid, qui développe la messagerie éponyme. Nous en sommes respectivement CTO (*Chief Technology Officer*) et CEO (*Chief Executive Officer*). Nous faisions partie de l'équipe qui a développé le projet et sommes tous deux docteurs en cryptographie, la science du secret.

Notre objectif avec Olvid était de permettre à tous d'avoir accès à un moyen de communication sur internet. Nous sommes évidemment très directement touchés par le projet de loi et en particulier par l'article 16 *bis*. Nous souhaitons avant tout partager ici notre avis d'experts en cryptographie. Il ne s'agit pas simplement de défendre les intérêts de notre société. Le sujet est bien trop important pour se contenter de défendre son pré carré.

Sur le fond, l'article 16 *bis* nous semble, tel que nous le comprenons, très positif : c'est une excellente chose que d'écrire noir sur blanc que la France refuse de se voir imposer des *backdoors* dans des systèmes de chiffrement et d'affirmer que la cybersécurité en France ne sera pas intrinsèquement plus faible que celle d'autres pays. On peut effectuer un parallèle avec le RGPD (règlement général sur la protection des données), qui avait permis aux utilisateurs européens de voir leurs données mieux protégées, faisant de l'Europe une exception par rapport au reste du monde. Il serait dommage qu'une directive européenne imposant un affaiblissement du chiffrement vienne à nouveau faire de l'Europe une exception, mais dans l'autre sens.

Nous sommes, chez Olvid, favorables à l'idée défendue par l'article 16 *bis*. Toutefois, cela ne nous empêche pas d'être à l'écoute de l'ensemble des parties prenantes et en particulier des forces de l'ordre. Notre objectif est aussi de comprendre leurs problématiques. Leur travail est évidemment fondamental et il est de notre devoir de prendre en compte leur point de vue dans notre réflexion. Notre conviction est que seul un dialogue dépassionné, scientifique et précis permettra d'apporter une solution mesurée à ces problématiques de fond. C'est la raison pour laquelle nous nous tenons à votre disposition, ainsi qu'à celle de toutes les parties prenantes, pour répondre de façon aussi transparente que possible à l'ensemble des questions soulevées par ce sujet si sensible.

M. Éric Bothorel, rapporteur général. Vous succédez à d'autres organisations qui n'ont pas tenu exactement le même discours que vous sur l'article 16 *bis*, dont je pense qu'il

n’est pas forcément écrit comme il devrait l’être et qu’il peut être compromettant pour l’avenir. Nous aurons l’occasion d’y revenir.

Concernant les recommandations d’usage de la messagerie Olvid, savez-vous si la circulaire du 22 novembre 2023 est respectée ? Pensez-vous qu’il faille l’étendre à d’autres organismes publics ? Vous aviez alors bénéficié d’une belle exposition grâce à l’exécutif. Quels sont selon vous les obstacles au développement de messageries instantanées chiffrées dites souveraines ? Comment réduire la dépendance aux applications les plus connues du grand public et, de manière plus générale, aux grands éditeurs de logiciels américains ?

A-t-on vraiment d’autres choix, lorsque les plateformes refusent de coopérer avec les autorités françaises, que d’imaginer des dispositifs venant compromettre le chiffrement ? Cet enjeu, majeur, est au cœur de nos débats. Force est de constater que certains acteurs ne veulent pas coopérer. Or cette coopération semble indispensable pour recueillir des informations et pouvoir mener des actions allant parfois jusqu’à l’interpellation. Comment procéder lorsque les plateformes refusent de coopérer ?

M. Matthieu Finiasz, cofondateur de la société Olvid. Intégrer dans la loi des règles imposant une *backdoor* pour permettre de déchiffrer des communications ne changera pas forcément grand-chose, car si les plateformes refusent de coopérer, elles ne le feront pas davantage pour la *backdoor*.

Cela soulève un premier problème de fond : comment s’assurer que les plateformes partagent avec les autorités, c’est-à-dire au moins avec la police et la gendarmerie, les données auxquelles elles ont déjà accès ? Il s’agit d’un problème de coopération. Une société qui propose une messagerie instantanée va-t-elle par exemple donner accès à tous ses logs, à toutes les données qu’elle a collectées grâce aux différents moyens à sa disposition dans cette opération ? Apparemment, certaines messageries coopèrent très bien, d’autres pas du tout. L’arrestation de Pavel Dourov était, me semble-t-il, liée à cela.

Un second problème, très différent, se pose ensuite : veut-on obliger les plateformes à fournir plus que les données auxquelles elles ont accès pour créer leur service ? Cela va à l’encontre du RGPD et de tous les dispositifs visant, en Europe, à protéger la vie privée. Cette collecte doit-elle par ailleurs être systématique pour tout le monde ou ciblée sur certains individus ? Les forces de l’ordre souhaitent évidemment qu’elle soit ciblée. La question est de savoir s’il est techniquement possible d’effectuer une collecte de données ciblée, sur demande, sans que cela n’implique une collecte généralisée des informations de l’ensemble des usagers. Mon point de vue est qu’une collecte ciblée n’est pas forcément possible techniquement. Cela signifie en effet que le système doit affaiblir le chiffrement, la cryptographie et la sécurité en général pour tout le monde, afin de pouvoir de temps en temps piocher dans un nouveau pool de données que l’on aura forcé des opérateurs à collecter afin d’en extraire quelques informations. Cela conduit à affecter le niveau de sécurité de l’ensemble d’une solution.

Lorsque nous avons conçu la messagerie, l’un des objectifs de base d’Olvid était, par opposition à toutes les autres messageries, de rendre impossible toute attaque de masse sur notre solution. La cryptographie d’Olvid a été conçue pour qu’il n’y ait jamais de tiers de confiance obligatoire pour tous les utilisateurs. Cela signifie que si l’on veut récupérer des données d’un utilisateur, il faut s’attaquer spécifiquement à lui, à son téléphone, à son ordinateur. Il n’est pas possible de les collecter en un seul point commun à tous les utilisateurs, comme un serveur de distribution de messages ou autres dispositifs de ce type.

Cela fait partie des fondements qui ont présidé à la création d'Olvid. Toute tentative de mise en place de mesures permettant de collecter les données de tout le monde en un point unique irait à l'encontre de cette démarche et viendrait abaisser le niveau de sécurité.

M. Thomas Baignères. Ces mesures imposeraient nécessairement abaisser le niveau de sécurité car on ne sait pas *a priori*, au moment où l'on conçoit la solution, quelles personnes on pourrait être amené à cibler. Cela suppose donc que les moyens à déployer pour cibler une personne six mois après la conception du système soient intégrés d'emblée pour l'intégralité des utilisateurs. Il faut nécessairement mettre en place un dispositif qui touche tout le monde afin de pouvoir l'activer *a posteriori*. Il ne sera pas possible selon nous de réaliser un ciblage réellement fin ; le dispositif concernera nécessairement tout le monde, dès le départ, avec un abaissement général du niveau de sécurité.

La directive de Mme Borne nous a effectivement été très bénéfique. Certaines sociétés en France font l'effort de développer des solutions pas simplement prétendument sûres, mais qui démontrent leur niveau de sécurité, par du code open source et de la documentation technique expliquant le code et permettant aux personnes chargées d'en effectuer l'audit de le faire dans les meilleures conditions. Il est désormais possible, grâce à l'Anssi (Agence nationale de la sécurité des systèmes d'information), de passer en France des CSPN (certifications de sécurité de premier niveau). Nous ne sommes pas les seuls à l'avoir fait. Il nous semblerait naturel de mettre en avant toutes les sociétés qui font cet effort et engagent des fonds pour aller au bout du processus et démontrer leur qualité.

Mme Anne Le Hénanff, rapporteure. Pouvez-vous préciser en quoi le fait d'intégrer un système donnant *a priori* la capacité au service de cibler une personne six mois plus tard le fragilise ?

Quel est par ailleurs le type de données demandé par les services de l'État et dans quelle mesure y répondez-vous ? Certains services de l'État indiquent que des entreprises refusent de transmettre des données auxquelles elles ont pourtant accès tout en acceptant de les fournir aux services américains.

Dans quelle mesure la technique dite de l'utilisateur fantôme, qui permet à un utilisateur invisible de participer à une conversation via une messagerie cryptée, ne constitue-t-elle selon vous ni une vulnérabilité informatique ni un affaiblissement du chiffrement ?

Je souhaiterais enfin vous entendre sur l'enjeu spécifique de la cryptographie post-quantique. On entend dire en effet que le système quantique fera disparaître toute protection de messagerie cryptée. Est-ce un mythe ou une réalité ?

M. Benjamin Beurdouche. La technique de l'utilisateur fantôme est un affaiblissement d'un protocole cryptographique qui sous-entend que l'on ajoute dans les destinataires légitimes d'une communication sécurisée un tiers invisible par les utilisateurs. Cela n'est possible que dans certains cas. Cette technique affaiblit le but de sécurité qui veut qu'une communication chiffrée ait pour destination une cible définie, constituée d'individus bien particuliers. Le recours à l'utilisateur fantôme étend cette cible de manière anormale et rompt les propriétés de sécurité du protocole et du système. Cette rupture des promesses de sécurité peut s'effectuer au niveau du protocole cryptographique ou de l'application, qui peut utiliser le protocole correctement mais être activement malicieuse et contourner le chiffrement. De manière générale, cela n'est possible que dans le cas où le protocole cryptographique ne construit pas la propriété de consensus sur les participants au groupe.

Dans les protocoles modernes, notamment ceux qui vont être déployés dans les téléphones mobiles Android IRC (*Internet Relay Chat*) et iOS (*iPhone Operating System*) pour la prochaine génération de messageries chiffrées, le protocole ne permet pas d'ajouter des participants invisibles. L'application peut toujours tricher, mais le protocole cryptographique en lui-même prend des dispositions en ce sens.

Tout est possible, mais cela revient à réduire la sécurité du système et à donner potentiellement un accès aux données, puisqu'il faut ajouter la personne fantôme : qui l'ajoute ? Comment procéder de manière ciblée ? Autant de questions auxquelles on ne peut pas répondre, puisque lorsque l'on distribue un logiciel de manière générale à toute la population, soit on affaiblit le système d'emblée, avec une réserve qui fait que toute personne en ayant connaissance peut utiliser cette faiblesse, soit on procède de manière active, ciblée, avec des outils offensifs – ce qui est à mon avis beaucoup plus sûr. Mais autant, en réalité, ne pas le faire et attaquer directement le terminal de la personne. Une démarche offensive ciblée est préférable à une vulnérabilisation de l'ensemble des utilisateurs.

Il existe, en matière de cryptographie post-quantique, une problématique de transition post ordinateurs quantiques. Depuis plusieurs années, nous déployons, lors de la conception des logiciels de sécurité des protocoles de communication, notamment pour internet, des protocoles dits hybrides, qui protègent contre les ordinateurs classiques et quantiques. Cela existe depuis très longtemps pour les sites de très haute valeur ajoutée comme internet, avec le protocole HTTPS (*Hypertext Transfer Protocol Secure* ou protocole de transfert hypertexte sécurisé), les transactions financières, etc. Si vous utilisez par exemple Firefox, il faut savoir que 20 % environ de vos connexions se déroulent dans le cadre d'un protocole protégeant contre l'apparition d'un ordinateur quantique.

L'idée est que les attaquants collectent les messages chiffrés transitant sur internet en essayant par exemple de cibler une ambassade non protégée contre le post-quantique et dont ils savent que le diplomate va, à une heure donnée, passer un appel. Quand un ordinateur quantique suffisamment fort pour casser la cryptographie apparaîtra, il sera capable de déchiffrer les communications collectées jusqu'alors. Si nous sommes actuellement incapables d'estimer quand cet ordinateur apparaîtra, nous sommes en revanche scientifiquement convaincus qu'il arrivera. Nous prenons donc depuis plusieurs années déjà des dispositions visant à protéger tous nos protocoles de première classe en hybridant le système, c'est-à-dire en incluant à la fois de la cryptographie classique et de la cryptographie résistant à un ordinateur quantique, afin de sécuriser rapidement le maximum de cas d'usage.

Cela s'avère toutefois très compliqué, notamment dans les déploiements de matériel qui prennent souvent beaucoup de temps, parfois des décennies. Á titre d'exemple, le dernier gros déploiement cryptographique effectué sur internet remonte à 2018, lors de la conception du protocole précédemment évoqué. Or en 2025, il apparaît que 70 % seulement des personnes cibles utilisent la dernière version du protocole. Cela signifie donc que 30 % des gens utilisent des protocoles vieux de parfois vingt ou trente ans. Dans ce contexte, il est très important que les règlementations NIS 2 ou Dora insistent sur l'effort quantique qu'il convient d'effectuer. Cela s'annonce critique. Il est donc essentiel de commencer le plus tôt possible.

M. Matthieu Finiasz. Il est important de savoir qu'il existe déjà des algorithmes cryptographiques post-quantiques capables de résister aux ordinateurs quantiques ; encore faut-il les intégrer dans les différents logiciels. Olvid dispose d'une certification Anssi et il est question que l'Agence impose à tous les produits certifiés d'avoir une résistance post-

quantique, donc du chiffrement hybride, afin de conserver leur certification. Nous allons progressivement travailler sur ce point. Nous n'avons pas intégré cet élément dès l'origine, car lorsque nous avons conçu la cryptographie d'Olvid, les protocoles en question n'étaient pas complètement standardisés. Des standards existent dorénavant, sur lesquels nous pouvons nous appuyer, considérant que, tout le monde ayant les mêmes standards, le système devrait résister.

Cela ne signifie pas que les ordinateurs quantiques vont arriver demain – bien malin qui pourrait dire quand apparaîtra un ordinateur quantique capable de casser réellement la cryptographie. Nous savons en tout cas nous en protéger en cas de besoin. Il ne restera qu'à effectuer le déploiement et la mise à jour des protocoles, afin d'effectuer la bascule d'un univers cryptographique classique sujet à des attaques d'ordinateurs quantiques vers une cryptographie hybride post-quantique.

Sur des systèmes comme TLS pour du chiffrement de sessions web, c'est assez simple parce qu'il n'y a pas forcément beaucoup de persistance dans le temps. Il s'agit de protocoles qui ont été conçus pour prévoir des évolutions au cours du temps. Dans les cas de systèmes hardware, rien n'est parfois prévu et il faut changer les puces. Dans du logiciel, cela va souvent plus vite.

Olvid a été conçu pour ne jamais avoir un point de faiblesse face à une attaque de masse de tous les utilisateurs en un seul coup. L'utilisateur fantôme, c'est exactement cela. En gros, c'est un moyen applicable à n'importe quel utilisateur, qui va permettre de récupérer le contenu de ses communications parce que ses messages vont partir vers un utilisateur fantôme. Donc dans les cas où on peut mettre en place cet utilisateur fantôme, on peut générer une attaque de masse. Le problème, c'est que ce qui déclenche cette attaque de masse, ce n'est pas de la cryptographie.

Quand on fait un protocole cryptographique entre plusieurs utilisateurs, on a une preuve scientifique que si les conditions d'application du modèle de sécurité sont respectées, la sécurité va tenir. C'est une preuve scientifique. Dans un système avec utilisateur fantôme, on n'a plus de preuve scientifique et il faut alors se demander comment protéger l'accès avec le déclenchement de l'ajout. On sort complètement du cadre de la cryptographie. Il y a quelque part dans un bureau quelqu'un qui a un bouton lui permettant d'activer l'utilisateur fantôme pour telle personne. Ce n'est plus de la cryptographie, ce n'est plus de la science et il est difficile de mesurer l'impact que cela peut avoir. Ce qui est sûr, c'est que cela a un impact négatif sur la sécurité. Dans le cas où l'application de l'utilisateur fantôme n'est pas sélective, le problème est le même : comment contrôler l'accès au pool de données ? Ce n'est plus de la cryptographie, c'est de la sécurité standard, physique, pour empêcher l'accès aux disques durs sur lesquels se trouvent les données. C'est précisément ce que nous voulons absolument éviter. La sécurité de la cryptographie de notre système est scientifiquement prouvée et nous ne voulons pas retomber dans un dispositif à l'ancienne avec des informations cachées dans un cahier placé au fond d'un coffre-fort. Ce serait dommage de revenir à cela au XXI^{e} siècle.

M. le président Philippe Latombe. Récemment, le gouvernement fédéral américain a demandé aux fonctionnaires fédéraux de ne plus utiliser une certaine application de messagerie chiffrée au bénéfice d'une autre, jugée plus sûre. Ces questions de chiffrement, de déchiffrement et d'affaiblissement du chiffrement traversent-elles selon vous de la même façon toutes les sociétés démocratiques ? Si c'est le cas, les réponses sont-elles les mêmes ?

Les sénateurs, lors de l'examen du projet de loi sur la cybersécurité, ont ajouté un article 16 *bis*, en réaction à un amendement adopté lors des débats sur la loi contre le narcotrafic qui visait à affaiblir le chiffrement. Avez-vous été associés, en tant que spécialistes de la cryptographie, à la réflexion globale menée à l'époque par le ministère de l'intérieur ? Le ministre de l'intérieur nous avait expliqué, lors des débats, que l'utilisateur fantôme ne représentait pas un affaiblissement du chiffrement.

M. Thomas Baignères. La question se pose clairement de manière globale. Elle s'est posée aux États-Unis et une première réponse a été apportée. Selon moi, celle-ci ne sera pas la même partout. Nous verrons la réponse qui sera apportée en France, mais elle sera potentiellement différente de celle des États-Unis. Le RGPD est un dispositif profondément européen. L'état d'esprit ici est différent de celui de pays plus lointains.

Non, nous n'avons pas été consultés préalablement aux réflexions scientifiques, notamment sur l'utilisateur fantôme. Nous avons participé au débat, de manière un peu précipitée, alors que c'était quasiment déjà trop tard, si j'ose dire. Nous avons été pris au dépourvu.

Je reviens sur la question de l'utilisateur fantôme. Certes, nous sommes passionnés par les mathématiques derrière le chiffrement ; elles sont en effet suffisamment belles pour qu'on s'y intéresse. Cela étant, je comprends que la plupart des gens s'intéressent, non pas au chiffrement en lui-même, mais aux garanties de confidentialité, d'authenticité et d'intégrité qu'il apporte. Or avec une solution comme l'utilisateur fantôme, ces garanties ne sont plus nécessairement présentes. Certes, mathématiquement, elle ne touche pas au chiffrement et notamment pas à l'algorithme AES (*Advanced Encryption Standard)*, qui est utilisé majoritairement, mais, en envoyant des messages en clair à une autre source, le chiffrement lui-même est contourné. La question est donc de savoir, non pas si on touche au chiffrement, mais si on continue à garantir la confidentialité, l'authenticité et l'intégrité des communications. Le chiffrement n'est pas une fin en soi : c'est un moyen d'apporter ces garanties. De notre point de vue, une solution telle que l'utilisateur fantôme affaiblit nécessairement les communications de tous ceux qui utilisent des systèmes comme le nôtre.

M. Benjamin Beurdouche. D'un point de vue scientifique, quand on conçoit un système de sécurité informatique, on part des propriétés de sécurité de la session de télécommunication, par exemple la confidentialité, l'authentification et l'intégrité. Si un attaquant est présent dans une session, par exemple en raison d'un malware installé sur le téléphone, on va jouer son jeu au niveau des primitifs cryptographiques, au niveau des protocoles cryptographiques, au niveau des applicatifs, puis vers les infrastructures pour arriver jusqu'à internet. La cryptographie n'est que le moyen d'obtenir les garanties de confiance attendue du système, notamment ces trois propriétés.

Tout le monde doit faire face aux mêmes problématiques. Les recommandations de changement d'outils de sécurité pour les communications viennent du fait que les applicatifs sont maîtrisés par différentes parties. Tout le monde est d'accord pour dire que la cryptographie doit être solide, mais l'effort de sécurité doit être fait pour chaque couche. Olvid est maîtrisé par une entreprise de confiance et son système peut donc être utilisé pour des informations de plus haut niveau de sensibilité. Signal a un très bon protocole, mais l'application est opérée aux États-Unis. Un système *open source* permet de vérifier qu'il se comporte comme il est censé se comporter. Même si le code est fait pas un ensemble hétérogène de personnes de différentes nationalités, il est possible de vérifier, grâce à l'ouverture du code, les propriétés de sécurité de ce dernier. Dans un système de messagerie,

on ne fait pas confiance à l'infrastructure et on fait donc en sorte qu'elle voie le moins de choses possible. Une messagerie souveraine nécessite donc des infrastructures souveraines aux niveaux français et européen.

Personnellement, je ne connais aucun collègue qui aurait été auditionné au préalable sur l'article 8 *ter*, sur les *backdoors*, sur les propriétés de sécurité ou sur les objectifs des forces de sécurité intérieure et du ministère de l'intérieur. Je plaide pour une discussion ouverte avec le ministère de l'intérieur et les services de renseignement au niveau purement technique. Je pense que nous sommes tous à disposition.

Mme Anne Le Hénanff, rapporteure. Considérez-vous, déontologiquement, qu'une demande des services de sécurité intérieure, encadrée par la justice et ciblée, entraînerait nécessairement une vulnérabilité ? Les messageries sont utilisées par des trafiquants notamment. Est-il dès lors possible de hiérarchiser ? Face à l'évolution de la menace, envisagez-vous d'évoluer dans votre approche de la cryptographie ?

M. Thomas Baignères. La menace n'est pas dans la question qui nous serait posée, car nous avons pleine confiance dans notre système démocratique. Nous sommes à la disposition des forces de l'ordre pour discuter de manière générale des propriétés du chiffrement ou sur des cas particuliers. Notre inquiétude porte sur notre capacité à développer un système qui conserve les mêmes propriétés de sécurité que nous sommes aujourd'hui en mesure d'offrir tout en leur permettant d'avoir accès à certaines données d'un système de messagerie comportant l'échange de message avec des métadonnées. Nous sommes aujourd'hui dans l'incapacité scientifique d'ouvrir de manière hypersélective le contenu des communications sans compromettre leur sécurité. Ce n'est pas une position politique ou un parti pris : c'est une question scientifique. Celle-ci n'est d'ailleurs pas nouvelle puisque les cryptologues s'y intéressaient avant qu'elle devienne un sujet sociétal important. Personne n'a apporté de solution à ce problème dans une conférence publique.

Je vais essayer d'expliquer de façon compréhensible pourquoi nous considérons qu'un accès sélectif à certaines conversations affaiblirait le chiffrement de manière massive. Il est déjà relativement complexe de développer un système sans faille. Il peut paraître simple d'envoyer un message d'un point A à un point B. Tel n'est pas le cas, et nous avons beaucoup souffert pour y parvenir. La contrainte supplémentaire que constituerait la possibilité d'ouvrir un message spécifique à un instant T dans le futur rend impossible le maintien du même niveau de sécurité. Elle affaiblirait donc nécessairement la sécurité de l'application.

M. Benjamin Beurdouche. Cette possibilité d'ouvrir un message implique de casser une propriété de sécurité bien particulière appelée *forward secrecy* (confidentialité persistante). Les protocoles modernes protègent les anciens messages. Au fur et à mesure que l'on consomme le déchiffrement des messages reçus, les anciens messages sont protégés et ne sont plus déchiffrables. L'ouverture d'un message de manière sélective casserait la propriété de sécurité empêchant l'ouverture des messages antérieurs. Nous nous trouvons donc dans une impasse technique de base. C'est donc impossible.

En revanche, tout le monde est d'accord pour dire que l'accès légitime, mandaté par la justice, à des téléphones ou à des systèmes d'information pour lutter contre le crime organisé ou favoriser le renseignement, doit être effectif dans une démocratie. Les moyens pour le faire, qui permettent de contourner le chiffrement ou d'attaquer directement les terminaux, existent déjà et sont réglementés par la loi. Ils ne sont peut-être pas assez nombreux ni assez disponibles. Plutôt que de chercher à toucher à la sécurité globale du

chiffrement, qui affaiblirait tout le monde, sans doute est-il donc préférable de favoriser l'utilisation des outils déjà existants, dans lesquels le ministère de l'intérieur a peut-être moins investi que le ministère des armées.

M. le président Philippe Latombe. Une messagerie soumise à un dispositif équivalent à celui que prévoyait l'article 8 *ter* verrait-elle la confiance des utilisateurs et sa capacité à se développer entamées ? Signal avait dit que, en cas d'adoption définitive de l'article, elle ne serait plus disponible en France. Quel risque représente un tel dispositif pour une entreprise comme la vôtre ?

M. Matthieu Finiasz. Si Olvid annonçait la mise en place d'un système permettant d'ouvrir les messages sur demande de la justice, nous perdrions des utilisateurs. Les forces de l'ordre ont besoin à la fois de garantir la protection de leurs communications et de pouvoir accéder à des informations sur des actions criminelles. C'est donc compliqué pour elles, car les outils qu'elles utilisent peuvent être aussi utilisés par des personnes malveillantes. Je pense que les utilisateurs des ministères, auxquels la directive Borne a imposé l'utilisation d'Olvid, s'arrêteraient d'utiliser notre système du jour au lendemain. Nous perdrions également nos certifications Anssi qui ne se sont accordées qu'à des applications protégées par de la bonne cryptographie. Cela aurait donc pour nous un énorme impact, d'autant plus que notre but n'est pas d'aller chercher des marchés hors de France. Notre application peut être utilisée partout dans le monde, mais nous avons créé cette société pour pouvoir protéger les communications des administrations et des entreprises françaises, car il y avait un manque en Europe et en France d'une messagerie avec notre modèle de sécurité.

M. Thomas Baignères. Nous aurions dû mettre la clé cryptographique sous la porte. Nous perdrions en effet notre avantage – une garantie cryptographique mathématique de sécurité – par rapport à celui d'autres solutions, comme Signal ou d'autres, qui repose davantage sur leur infrastructure. Nous ne nous contentons en effet pas de chiffrement de bout en bout puisque nous y ajoutons l'authentification de bout en bout. Notre sécurité ne dépend pas d'un serveur qui distribue des clés. Notre modèle de sécurité a mis la barre plus haut par rapport à de nombreuses autres messageries grand public au niveau mondial. Une solution *backdoor* intégrée à Olvid nous ferait perdre tout avantage concurrentiel.

Je n'aime pas l'approche qui consiste à menacer de quitter la France. D'ailleurs, si d'autres pays décidaient de voter le même genre de loi, la messagerie ne serait plus utilisée par personne. Nous préférons discuter et expliquer les choses, comme nous le faisons aujourd'hui et continuerons à le faire.

M. Benjamin Beurdouche. Ce ne seraient pas seulement les utilisateurs de l'administration qui quitteraient l'application, mais aussi ceux de la criminalité organisée. Il faut prendre en compte l'ensemble de l'écosystème. Même si la criminalité organisée – ou les services de renseignement étrangers – utilise ses propres clients, comme EncroChat, elle a recours également aux messageries grand public.

Mme Anne Le Hénanff, rapporteure. Nous avons la possibilité de supprimer l'article 16 *bis* du projet de loi. Êtes-vous prêts à discuter pour trouver des solutions ou demandez-vous impérativement de le maintenir ?

M. Matthieu Finiasz. Cela fait des années que nous vivons sans une telle disposition et nous arrivons à nous en sortir, mais le maintenir serait une très bonne chose. Il s'agirait, non pas de gêner les forces de l'ordre, mais d'exprimer une position forte de l'Assemblée

nationale en faveur de la protection des données personnelles de la population. Nous pourrons survivre sans, nous n’en avons pas un besoin impérieux, mais il nous rassurerait contre le retour éventuel d’un article 8 *ter*.

M. Benjamin Beurdouche. Je ne suis pas très âgé, mais j’ai déjà vu revenir ce type de discussion plusieurs fois et, à chaque fois, nous devons refaire un effort scientifique d’explication. L’avis de la communauté scientifique n’a pas bougé d’un iota sur ce point depuis des décennies.

Personnellement, je préférerais que cet article soit maintenu, car il apporte un confort de sécurité, sans changer la vie des services de renseignement. Il n’empêche pas non plus la discussion et nous sommes totalement disponibles. Si, un jour, une proposition scientifique validée par la communauté permettait d’ouvrir les messages sans compromettre leur sécurité, il serait alors toujours possible de supprimer cette disposition.

M. le président Philippe Latombe. Je vous remercie.

La séance est levée à 16 heures 40.

Membres présents ou excusés

Commission spéciale chargée d'examiner le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité

Réunion du mercredi 9 juillet 2025 à 15 h 30

Présents. - M. Éric Bothorel, Mme Catherine Hervieu, M. Tristan Lahais, M. Philippe Latombe, Mme Anne Le Hénanff, M. Vincent Thiébaut

Excusé. - Mme Marietta Karamanli, M. Laurent Mazaury

Assistait également à la réunion. - Mme Véronique Riotton