Les intermédiaires et le chiffrement

Mettre la pression sur les intermédiaires pour affaiblir la sécurité n'est pas la solution à la circulation de données nocives sur Internet

Internet est un outil puissant, qui relie les peuples du monde entier, les informe et les aide dans leurs activités. Il ouvre un nombre presque infini de portes, en permettant aux individus d'innover, d'améliorer leur qualité de vie, de célébrer et d'apprendre de la diversité et de résoudre les défis les plus complexes auxquels est confrontée la planète. Malheureusement, il est parfois utilisé par des acteurs malveillants, pour commettre des crimes et diffuser en ligne des discours haineux. Dans des cas rares, mais extrêmes, il a servi à diffuser ou à inciter à des actes qui ont engendré des violences physiques.

Certains gouvernements ont suggéré qu'il était possible d'empêcher ce type de comportements néfastes en rendant les intermédiaires d'Internet responsables de ce que publient ou partagent leurs utilisateurs en ligne.[1] Certains gouvernements ont déjà indiqué que les intermédiaires, notamment les plateformes de médias sociaux et les services de messagerie à chiffrement de bout en bout, pourraient être tenus pour responsables[2] s'ils ne parvenaient pas à « tracer » (c'est-à-dire à identifier l'origine) des données partagées sur leurs plateformes. De telles propositions ont peu de chances d'aboutir à l'objectif annoncé, et affaibliront les outils de sécurité que nous utilisons au quotidien pour protéger les individus, les entreprises, les économies et les nations.

Risques et difficultés techniques

Affaiblir le chiffrement affaiblit la confiance et la sécurité : comme indiqué ci-dessus, certains gouvernements sont favorables à la « traçabilité », même pour les messages à chiffrement de bout en bout entre des parties qui souhaitent communiquer de manière confidentielle. Les gouvernements souhaitent pouvoir définir si un message spécifique présente un caractère offensant ou illégal, et savoir de quel utilisateur il provient. Pour ce faire, les intermédiaires devraient avoir accès à au moins l'un des éléments suivants :

- Le message non chiffré, sur l'appareil de l'expéditeur.
- Le message déchiffré, sur l'appareil du destinataire.
- Le message chiffré, avec la possibilité de le déchiffrer.

---

1 Il s'agit par exemple des modifications de la Réglementation indienne sur les technologies de l'information (directives pour les intermédiaires) par la Législation sur les Technologies de l'information.

2 La base légale pour la responsabilité (ou la non responsabilité) peut varier en fonction des juridictions. Ainsi, en Inde, cela est couvert par la section 79 de la Législation sur les Technologies de l'information de 2000 : https://cis-india.org/internet-governance/resources/section-79-information-technology-act
tandis que, pour les intermédiaires aux États-Unis, cela est réglementé par la section 230 de la Communications Decency Act de 1996 : https://en.wikipedia.org/wiki/Section_230_of_the_Communications_Decency_Act

Cela signifierait qu'ils devraient contourner ou outrepasser le chiffrement du message, et donc sa confidentialité.

> **Impact :** la traçabilité romprait avec le principe de communication confidentielle et nuirait à la confiance de l'utilisateur dans les plateformes et prestataires de services qui auraient recours à ces méthodes pour accéder aux données. En définitive, le chiffrement serait affaibli dans sa conception elle-même, et les utilisateurs ne pourraient plus avoir confiance dans la confidentialité et l'intégrité de leurs communications en ligne. Cela détruirait une fonction fondamentale, que nous utilisons au quotidien pour sécuriser des appareils, des données et des transactions, et donc pour protéger les individus, les économies, les infrastructures et les environnements de travail.

Il est inutile de légiférer sur ce qui est impossible : certains gouvernements cherchent à rendre leurs dangereuses propositions plus consensuelles, en ne présentant que l'*objectif* recherché, et non les mesures qu'ils souhaitent prendre pour y parvenir. Ils exigent par exemple que les intermédiaires assurent la sécurité des enfants sur Internet, sans indiquer comment ils souhaitent que cela soit fait.

Cependant, en présentant le problème sous l'angle de l'inaccessibilité des informations pour les forces de l'ordre, ils sous-entendent que le problème vient du chiffrement, et que la solution est de le contourner ou de l'outrepasser. Au moins l'une des propositions actuelles déclare qu'une solution de ce type pourrait être mise en œuvre, sans nuire à la sécurité ou à la confiance des services et utilisateurs légitimes. L'Internet Society considère que cela est tout simplement impossible, c'est pourquoi, en mai 2019, elle était l'un des plus de 50 signataires d'une lettre ouverte présentant les risques et les défauts d'une telle approche.[3]

> **Impact :** Même si elle est animée des meilleures intentions, une loi qui affaiblit les mécanismes de sécurité augmente les risques d'activité malveillante, et met les utilisateurs et services légitimes en danger.
>
> Quelle que soit la façon de présenter l'objectif et de le définir en termes légaux, la réponse de la communauté technique a été claire et cohérente : il est impossible de concevoir un mode de contournement du chiffrement que « seuls les gentils peuvent utiliser ».[4] Il ne s'agit pas d'une réflexion dogmatique de la part des experts techniques : ceux-ci se basent sur les raisons fondamentales, mathématiques, qui rendent efficaces les systèmes de chiffrement. Il ne peut exister de système de chiffrement fiable qui soit à la fois robuste face aux attaquants et faible pour d'autres acteurs. Un système de chiffrement ne peut pas être robuste sauf quand vous désirez qu'il soit faible.

L'authentification obligatoire des utilisateurs augmente les coûts et la complexité : afin de pouvoir plus facilement identifier les personnes à l'origine de données illégales, certains pays désirent que les utilisateurs soient obligés de s'authentifier pour pouvoir accéder à un service en ligne.[5] Cela peut sembler simple, mais il est difficile de parvenir à mettre en place une authentification fiable, même lorsque cela est dans le meilleur intérêt de l'utilisateur (par exemple pour les retraits d'espèces dans les distributeurs de billets). Si l'utilisateur a un intérêt à éviter l'identification, cette tâche est encore plus complexe. Les approches basées sur l'authentification des utilisateurs grâce à leurs documents d'identité officiels (permis de conduire, passeport, carte d'identité numérique) sont complexes et coûteuses, et leur fiabilité est à la merci de nombreux facteurs, techniques ou non, notamment la fiabilité de l'émission, la résistance à la fraude, la gestion des identités et des accès, etc. Dans la plupart des cas, l'ajout de moyens biométriques rend le problème encore plus complexe.

Il existe également d'autres propositions d'« accès exceptionnel » qui reposent sur l'affaiblissement des protocoles d'authentification à la base de tout chiffrement fiable[6] : si vous n'êtes pas certain que seul le

3 https://regmedia.co.uk/2019/05/30/letter_to_gchq_ghost_user_cryptobusting_plan.pdf

4 https://mitpress.mit.edu/blog/keys-under-doormats-security-report

5 https://www.chinalawtranslate.com/en/provisions-on-the-management-of-internet-forum-community-services/

6 https://www.internetsociety.org/resources/doc/2020/fact-sheet-ghost-proposals/

destinataire prévu peut détenir la clé pour déchiffrer votre message, vous ne pouvez pas être certain de sa confidentialité.

> **Impact :** Les propositions basées sur l'authentification obligatoire augmentent les coûts et la difficulté d'utilisation sans nécessairement atteindre l'objectif déclaré. Les propositions de politiques dans ce domaine semblent émettre des demandes contradictoires : à la fois une authentification fiable et l'affaiblissement des protocoles fiables.

Le fait de rendre responsables les intermédiaires nuit à la confiance et à la sécurité, sans atteindre l'objectif souhaité

Lutter contre la diffusion sur Internet de données illégales est un objectif très important, et nous devons tous tenter de trouver des solutions. Cependant, les données illégales, de même que les comportements qui en sont à l'origine, existaient bien avant Internet, et sont par essence un problème de société et non un problème technique. Le fait de se concentrer uniquement sur l'affaiblissement du chiffrement pour contrer ce problème nuit à la sécurité : cela nécessite des ressources qui pourraient être consacrées à d'autres solutions, comme l'amélioration des moyens globaux dont disposent les forces de l'ordre pour lutter contre la criminalité utilisant des moyens techniques,[7] que cela concerne ou non le chiffrement. De plus, le fait de recourir uniquement à des solutions technologiques pour répondre à des problèmes de société est rarement efficace sur le long terme.

- Le fait d'empêcher les applications de messagerie confidentielle d'assurer la confidentialité rend ces applications inutiles dans le meilleur des cas, et nocives dans le pire. Ces mesures ne rendent pas Internet plus sûr, et ne lui bénéficient nullement.
- Les politiques contradictoires vis-à-vis de l'authentification engendrent encore plus de confusion et de complexité technique, ce qui nuit à la confiance des utilisateurs de services en ligne et de communications confidentielles.

Même s'il arrive parfois qu'Internet soit utilisé de façon malveillante, nous devons lutter contre les propositions de loi visant à contraindre les prestataires de services à outrepasser la capacité des individus à sécuriser leurs informations et leurs interactions sur Internet. Ces contraintes augmentent les risques, pour les particuliers comme pour les organisations, sans la moindre garantie d'atteindre l'objectif souhaité. Nous invitons les décideurs politiques à soutenir les politiques et pratiques pour un chiffrement robuste ; cela contribuera à la sécurité sur Internet des individus, des infrastructures et des pays, et permettra à Internet de rester un vecteur d'innovation, d'éducation, et de progrès économiques et sociaux.

7 https://eshoo.house.gov/sites/eshoo.house.gov/files/migrated/wp-content/uploads/2019/10/Eshoo-Wyden-Letter-to-AG-Barr-re-encryption.pdf