Résoudre les crimes sans compromettre le chiffrement

Pourquoi un chiffrement fort et la sécurité publique vont de pair

Juin 2026

Synthèse

Dans un monde de plus en plus dominé par le numérique, les forces de l'ordre sont confrontées à des défis croissants lorsqu'elles tentent de déterminer comment trouver des preuves d'investigation et y accéder. Pour leur part, les décideurs peinent à réglementer cet accès afin de protéger la sécurité et la confidentialité des communications en ligne. Le chiffrement étant un outil fondamental de la sécurité et de la fiabilité de l'Internet, les propositions imposant un accès légal intégré dès la conception affecteraient intrinsèquement la sécurité de l'Internet pour tous.

Bien que le chiffrement limite l'accès au contenu de certaines communications, les forces de l'ordre n'ont jamais eu accès à autant de données qu'aujourd'hui, notamment aux historiques de localisation, aux métadonnées et aux journaux de transactions. Dans cet article, nous présentons certains outils qui permettent de mener des enquêtes efficaces sans compromettre le chiffrement. Le problème n'est souvent pas un manque d'informations, mais la capacité à extraire de manière légale, efficace et proportionnée des renseignements exploitables à partir des vastes volumes de données déjà disponibles. L'accent doit donc être mis sur le renforcement des capacités d'enquête, l'amélioration de la coopération transfrontalière, le perfectionnement des investigations numériques, le soutien à l'analyse ciblée des métadonnées et la promotion d'une coopération volontaire et transparente avec les fournisseurs de services. Son objectif ne doit pas être d'augmenter la masse des preuves en introduisant des failles systémiques de sécurité.

Le chiffrement est une technologie fondamentale qui protège la confidentialité et l'intégrité des données, des communications, des appareils et des services. Il est essentiel pour la sécurité et la fiabilité de l'Internet, car il protège les individus, les enfants, les entreprises, les gouvernements, les services publics, les infrastructures critiques, les journalistes, les défenseurs des droits humains et les communautés vulnérables. Les propositions imposant une analyse côté client, des portes dérobées de

chiffrement ou d'autres formes d'accès exceptionnel affaibliraient ce fondement et nuiraient globalement à la sécurité intrinsèque de l'Internet pour tout le monde.

Les tentatives de création de portes dérobées ou d'introduction d'une analyse côté client, qu'il s'agisse sur les appareils, ou dans les systèmes de chiffrement, sont techniquement irréalisables et contestables sur le plan juridique. L'affaiblissement intentionnel des communications chiffrées ne peut pas être limité à des cibles spécifiques. Ces approches créent des risques systémiques, ne satisfont pas aux critères de nécessité et de proportionnalité et menacent l'Internet ouvert, mondialement connecté, sûr et digne de confiance.

Les décideurs ont donc intérêt à mettre en œuvre trois mesures prioritaires. Premièrement, les lois et politiques relatives aux enquêtes pénales doivent protéger un chiffrement fort et rejeter les mesures qui l'affaiblissent. Deuxièmement, les gouvernements doivent investir dans les capacités et la formation des forces de l'ordre afin que les enquêteurs puissent utiliser efficacement des outils légaux, ciblés et proportionnés, qui préservent la sécurité, la sûreté et la confidentialité des autres utilisateurs. Troisièmement, les cadres réglementaires doivent permettre une coopération volontaire et transparente avec les fournisseurs de services dans les enquêtes sur les crimes graves, étayée par des procédures régulières, la redevabilité et les droits humains.

La protection d'un chiffrement fort n'est pas un obstacle à la sécurité publique, à la protection des enfants ou à la prévention de la criminalité. Elle constitue une condition préalable aux trois et une incontournable pour un Internet sûr et digne de confiance.

Le chiffrement est la base de la sécurité, de la confiance et de la sécurité publique

Le chiffrement est une technologie fondamentale pour la société moderne. Il protège les communications en ligne, permet le développement du commerce électronique et des services publics numériques, sécurise les infrastructures critiques et renforce la confiance dans les systèmes numériques utilisés par les particuliers, les entreprises et les gouvernements. Sans un chiffrement fort, il n'y aurait ni services bancaires en ligne sécurisés, ni services de santé ou publics confidentiels, ni véritable protection contre la cybercriminalité, les violations de données, l'usurpation d'identité ou l'espionnage.

Les propositions visant à imposer l'accès aux communications chiffrées par des mécanismes tels que l'analyse côté client ou des portes dérobées de chiffrement reposent sur une incompréhension fondamentale du fonctionnement du chiffrement et des enjeux concernés. **Tout affaiblissement intentionnel du chiffrement, quelle qu'en soit la finalité, crée inévitablement des vulnérabilités systémiques qui ne peuvent être limitées à des cibles, des enquêtes ou des juridictions spécifiques. Une fois introduites, ces failles peuvent être découvertes, reproduites ou exploitées par des criminels, des États hostiles et d'autres acteurs malveillants.**

Bien que le chiffrement puisse limiter l'accès au contenu de certaines communications, il ne prive pas les forces de l'ordre de moyens d'action. Au contraire, les enquêteurs n'ont jamais disposé d'autant de données sur les comportements, les déplacements et les interactions des individus qu'aujourd'hui. La question centrale pour les politiques publiques n'est donc pas de savoir si les enquêtes sont possibles dans un monde reposant sur un chiffrement fort. Elle consiste plutôt à trouver les solutions permettant aux forces de l'ordre d'utiliser de manière efficace, légale et proportionnée l'arsenal des outils d'enquête et les nombreuses données déjà disponibles, et ce sans compromettre la sécurité de l'ensemble des utilisateurs.

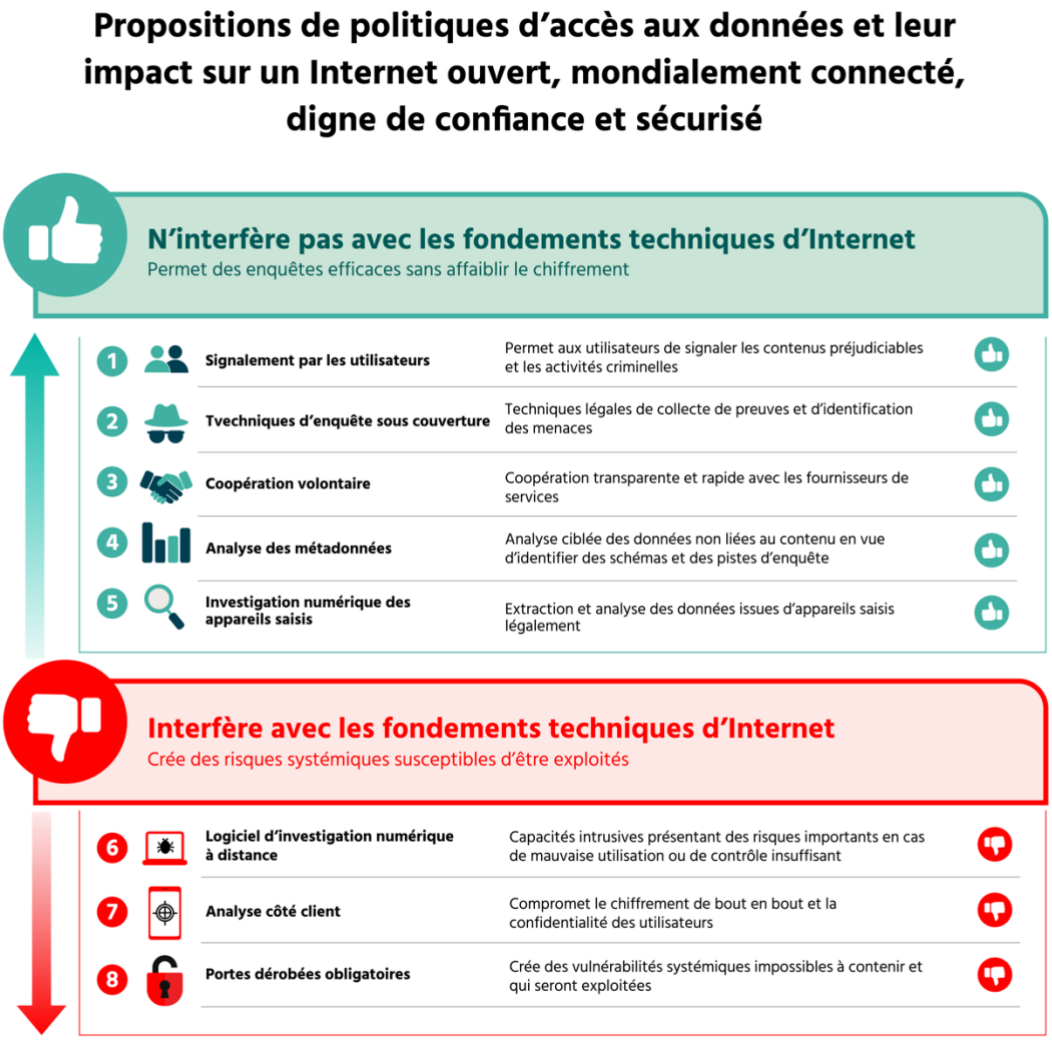
Les fournisseurs de services jouent un rôle central dans cet enjeu de politique publique. Ils conçoivent et mettent en œuvre de nombreux services de communication, plateformes, systèmes de signalement et processus de traitement des données dont les utilisateurs dépendent au quotidien. Ils jouent également un rôle important pour répondre aux demandes légales concernant des données non liées au contenu, ainsi que pour préserver des dispositifs de sécurité robustes et promouvoir les mécanismes de signalement par les utilisateurs. Une politique efficace doit donc favoriser une coopération claire, transparente et respectueuse des droits entre les forces de l'ordre et les fournisseurs de services, tout en préservant un chiffrement fort et en évitant toute obligation susceptible d'introduire des vulnérabilités systémiques.

La protection d'un chiffrement fort n'est pas un obstacle à la sécurité publique, à la protection des enfants ou à la prévention de la criminalité. Elle est une condition préalable aux trois. Le chiffrement est la garantie d'un Internet sûr et digne de confiance. Il réduit les opportunités de cybercriminalité, protège les victimes et les communautés vulnérables et soutient l'État de droit en veillant à ce que les mesures d'enquête restent ciblées, nécessaires, proportionnées et assorties de garanties de responsabilité.

La boîte à outils d'enquête : propositions de politiques d'accès aux données

Les forces de l'ordre disposent déjà d'une boîte à outils d'enquête vaste et diversifiée qui ne nécessite ni d'affaiblir le chiffrement, ni de compromettre les fondements techniques de l'Internet. Ces mesures varient considérablement quant à leur impact sur la sécurité, la confidentialité et l'intégrité des systèmes numériques.

Le tableau des propositions de politiques d'accès aux données ci-après illustre cette gamme d'options, classées selon leur impact sur les fondements techniques d'Internet. Les mesures indiquées en vert s'inscrivent dans le cadre actuel d'un Internet mondialement connecté, sûr et digne de confiance. Elles préservent le chiffrement tout en permettant des enquêtes efficaces. Les mesures indiquées en rouge nécessitent d'affaiblir le chiffrement ou de compromettre les appareils. Elles introduisent des vulnérabilités systémiques qui ne peuvent être limitées à des suspects ou à des juridictions spécifiques.



Cette comparaison visuelle met en évidence un choix politique essentiel : les gouvernements peuvent soit renforcer les capacités d'enquête tout en préservant la sécurité d'Internet, soit recourir à des mesures intrusives qui affaiblissent l'infrastructure même dont dépendent la sécurité publique, la stabilité économique et les institutions démocratiques.

Les risques des mesures intrusives

Certaines techniques d'enquête présentent des risques bien plus importants que d'autres pour la cybersécurité, les droits humains et la confiance du public. Les risques que posent ces mesures intrusives dépassent largement leurs avantages hypothétiques pour les enquêtes. Il est nécessaire de se confronter directement à de tels risques.

Logiciels d'investigation numérique à distance et exploitation de vulnérabilités zero-day. Les outils d'investigation numérique à distance, souvent appelés logiciels espions, permettent un accès à distance approfondi et continu au contenu et aux fonctionnalités d'un appareil. Leur utilisation repose généralement sur des vulnérabilités logicielles non divulguées (exploits « zero-day »), ce qui crée des incitations à retarder la divulgation des failles et laisse l'ensemble des utilisateurs exposés à ces risques. Ces outils ont été à plusieurs reprises associés à des abus, notamment la surveillance de journalistes, de défenseurs des droits humains et d'opposants politiques. Même lorsqu'ils sont utilisés de façon autorisée, les atteintes systémiques à la cybersécurité sont considérables.

Analyse côté client et portes dérobées de chiffrement. L'analyse côté client et les portes dérobées de chiffrement modifient radicalement le modèle de sécurité des systèmes chiffrés. Ces mécanismes introduisent une surveillance continue, compromettent la confidentialité et créent de nouvelles surfaces d'attaque. Une fois des portes dérobées mises en place, ces failles peuvent être découvertes, reproduites ou exploitées par des criminels, des États hostiles et d'autres acteurs malveillants. Ces mesures sont incompatibles avec un Internet sûr et digne de confiance et ne peuvent être limitées à un usage légal. Leurs effets néfastes sont intrinsèques et inévitables.

Préservation du chiffrement : des options pour les forces de l'ordre

Analyse des métadonnées. Même lorsque le contenu des communications est chiffré, les métadonnées associées (horodatages, identifiants de l'expéditeur et du destinataire, données de géolocalisation et de l'appareil, journaux de transactions et schémas d'utilisation) restent souvent accessibles via des procédures légales. Grâce aux outils d'analyse modernes, les métadonnées peuvent être utilisées pour reconstituer des chronologies, identifier des réseaux, détecter des tendances et localiser des suspects. Lorsqu'elle est correctement ciblée et encadrée par le respect des procédures régulières, l'analyse des métadonnées peut constituer un outil d'enquête puissant et proportionné. Elle doit être une condition préalable à l'examen de toute mesure plus intrusive.

Investigation numérique des appareils saisis. Lorsqu'ils sont légalement saisis, les enquêteurs peuvent analyser les appareils à l'aide de techniques d'investigation numérique telles que l'extraction de mémoire, la récupération de mots de passe ou la reconstruction de données. Des investissements dans

la formation et les capacités en criminalistique peuvent améliorer significativement l'accès aux preuves sans affaiblir les systèmes de chiffrement eux-mêmes. Ces méthodes doivent rester strictement encadrées, ciblées et soumises à une autorisation judiciaire.

Techniques d'enquête sous couverture et secrètes. Les méthodes d'enquête traditionnelles, telles que les opérations sous couverture et le renseignement humain, restent efficaces dans les environnements numériques. Les forces de l'ordre ont adapté avec succès ces techniques aux enquêtes en ligne, y compris pour des crimes graves tels que la diffusion de contenus pédopornographiques (CSAM), en recourant à des comptes leurres et à des interactions dissimulées. Ces approches sont intrinsèquement ciblées et permettent d'éviter les risques systémiques pour la sécurité numérique.

Coopération, signalement et preuves numériques directes

Coopération volontaire avec les fournisseurs de services. De nombreux fournisseurs donnent déjà un accès légal à des données non liées au contenu, telles que les informations de compte, l'historique de connexion et les schémas d'utilisation. Une coopération volontaire fondée sur la confiance, distincte des obligations d'accès imposées, peut améliorer les résultats des enquêtes tout en respectant la confidentialité des utilisateurs et les procédures régulières. La transparence, la responsabilité et le contrôle sont essentiels pour garantir que cette coopération reste conforme aux droits humains et à l'État de droit.

Mécanismes de signalement par les utilisateurs. Des outils de signalement efficaces permettent aux utilisateurs de signaler directement aux plateformes des activités illégales ou préjudiciables. Des consignes claires, un suivi réactif et des processus transparents renforcent la confiance et améliorent la qualité des pistes d'enquête. Des systèmes de signalement robustes sont particulièrement importants pour la protection des enfants et les signalements liés aux abus.

Preuves numériques directes fournies par les victimes et les témoins. Les preuves peuvent souvent être obtenues directement auprès des personnes impliquées dans une activité criminelle ou qui en sont victimes. La simplification des procédures de transmission des preuves numériques et l'accompagnement des victimes dans cette démarche peuvent renforcer significativement les enquêtes, sans introduire de nouveaux risques pour la sécurité.

Mettre fin aux mythes tenaces

- **Mythe : « L'*accès légal dès la conception* » est techniquement réalisable.** Aucun système ne peut offrir un accès exceptionnel sans affaiblir la sécurité de tous. Les mécanismes d'accès techniques ne peuvent pas faire la distinction entre un usage légitime et un usage malveillant.

- **Mythe : Le phénomène du « *going dark* » empêche aux forces de l'ordre de mettre fin aux crimes.** Bien que certains contenus soient chiffrés, les données relatives aux comportements, aux réseaux et aux localisations sont plus abondantes que jamais. Les forces de l'ordre ne sont pas privées d'accès aux données : elles opèrent dans une ère où la disponibilité des données est sans précédent.
- **Mythe : Une porte dérobée sécurisée peut être créée uniquement pour les forces de l'ordre.** Par nature, de tels mécanismes sont indifférenciés et entraînent d'importants dommages sociétaux pour répondre aux agissements d'une minorité criminelle.

Recommandations

À l'attention des décideurs :

- Renseignez-vous sur les fondamentaux du chiffrement et découvrez pourquoi il est important. Comprenez le rôle technique fondamental du chiffrement dans la protection de la confidentialité, de l'intégrité et de la sécurité des données, des communications, des appareils et des services des utilisateurs. Ces notions sont essentielles pour garantir que les lois destinées à renforcer la sécurité publique ne compromettent pas involontairement la sécurité de l'ensemble des internautes.
- Les politiques et lois relatives aux enquêtes criminelles doivent protéger un chiffrement fort et non pas l'affaiblir.
- Les forces de l'ordre doivent disposer de capacités et de formations suffisantes pour utiliser une gamme de mesures d'enquête qui ne compromettent pas la sécurité, la sûreté et la confidentialité des autres utilisateurs. Ces mesures doivent être appliquées uniquement lorsque cela est nécessaire et proportionné, et faire l'objet d'un contrôle adéquat.
- Les politiques doivent permettre une coopération volontaire avec les fournisseurs de services dans le cadre d'enquêtes sur des crimes graves, dans le respect des procédures régulières, de la responsabilité et des droits humains.
- Les politiques doivent renforcer le financement de la formation en criminalistique numérique et des autres compétences protégeant le chiffrement.

À l'attention des fournisseurs de services :

- Préservez et déployez un chiffrement fort par défaut. Ne mettez pas en place des portes dérobées ou des vulnérabilités systémiques.
- Répondez de manière efficace et transparente aux demandes légales portant sur des données non liées au contenu, conformément aux procédures régulières.
- Renforcez la coopération volontaire avec les forces de l'ordre grâce à des canaux opérationnels clairs et à des points de contact fiables.
- Investissez dans des mécanismes de signalement efficaces et faciles à utiliser, en particulier pour les questions liées à la protection des enfants et aux comportements abusifs.

- Dialoguez régulièrement avec les décideurs politiques, les forces de l'ordre et la société civile afin d'expliquer les réalités techniques et les impacts sur la sécurité.

Autres parties prenantes (société civile, universités, communauté technique, éducateurs)

- Surveillez et évaluez les impacts des mesures d'enquête sur les droits humains et la sécurité.
- Fournissez une expertise indépendante fondée sur des données probantes afin de contrer les discours erronés sur le chiffrement et le phénomène du « going dark », soit la perte de visibilité de la part des forces de l'ordre.
- Préconisez la littératie numérique et l'éducation à la sécurité en ligne pour les enfants, les parents et les responsables légaux ou les tuteurs.
- Soutenez les initiatives de signalement précoce et de prévention qui atténuent les conséquences néfastes et améliorent les résultats des enquêtes.
- Favorisez un dialogue multipartite afin de garantir que les politiques renforcent la confiance, la sécurité et la protection du public en ligne.

Ressources supplémentaires

Liens vers des ressources complémentaires et des publications de l'Internet Society :

- What is Encryption (Qu'est-ce que le chiffrement ?) : https://www.internetsociety.org/issues/encryption/what-is/
- Protect Encryption, Protect Yourself (Protéger le chiffrement, se protéger soi-même) : https://www.internetsociety.org/issues/encryption/protect-encryption-protect-yourself/
- Encryption Keeps Kids Safe Online (Le chiffrement protège les enfants en ligne) : https://www.internetsociety.org/blog/2023/05/encryption-keeps-kids-safe-online/
- Factsheet: How Encryption can Protect Journalists and the Free Press (Fiche d'information : comment le chiffrement peut protéger les journalistes et la liberté de la presse) : https://www.internetsociety.org/resources/doc/2020/fact-sheet-how-encryption-can-protect-journalists-and-the-free-press/
- The Economic Impact of Laws that Weaken Encryption (L'impact économique des lois qui affaiblissent le chiffrement) : https://www.internetsociety.org/resources/doc/2021/the-economic-impact-of-laws-that-weaken-encryption/
- Keeping Kids Safe Online: Navigating the New Parent's Guide to Encryption: (Protéger les enfants en ligne : guide pour les parents sur le chiffrement) : https://www.internetsociety.org/blog/2024/01/keeping-kids-safe-online-navigating-the-new-parents-guide-to-encryption/
- Cours de formation sur le chiffrement : https://www.internetsociety.org/fr/learning/encryption/