Résoudre les crimes sans compromettre le chiffrement

Synthèse en trois pages

Juin 2026

Introduction : le faux dilemme

Les décideurs sont souvent confrontés à un dilemme préoccupant : soit affaiblir le chiffrement pour lutter contre la criminalité, soit accepter le phénomène du « going dark » de l'Internet, c'est-à-dire la perte de visibilité de la part des forces de l'ordre. Il s'agit d'un faux dilemme.

Les forces de l'ordre n'ont pas besoin de compromettre la sécurité numérique de milliards d'utilisateurs pour mener des enquêtes efficaces. Nous vivons à l'âge d'or des preuves numériques. Les autorités n'ont jamais disposé d'autant de données qu'aujourd'hui : historiques de géolocalisation, métadonnées et journaux de transactions.

L'affaiblissement du chiffrement, à l'aide de portes dérobées, de l'analyse côté client ou de mécanismes d'accès imposés ne satisfait pas aux critères juridiques de nécessité et de proportionnalité. Il introduit des vulnérabilités systémiques que des criminels et des États hostiles exploiteront, compromettant la sécurité de tous.

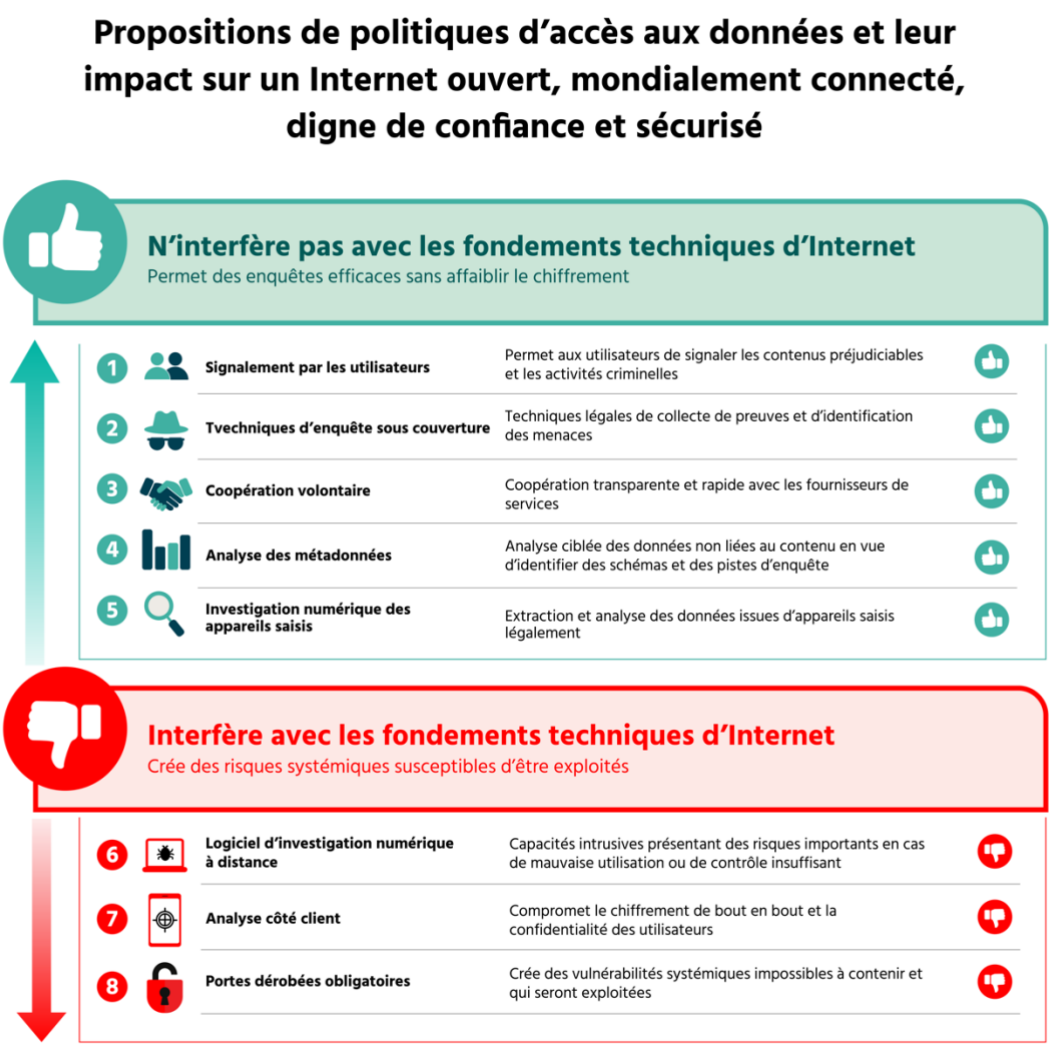
La solution : des outils efficaces (à encourager)

Plutôt que d'exiger des solutions miracles, les gouvernements devraient financer et encadrer légalement les méthodes d'enquête efficaces suivantes :

- **Signalement par les utilisateurs** : des éléments de preuve importants peuvent souvent être obtenus directement auprès des témoins, des victimes ou de personnes impliquées dans une activité criminelle et acceptant de coopérer. Il convient de mettre en place des mécanismes simples permettant ces signalements d'infractions et la collecte de preuves numériques sur les appareils.
- **Opérations sous couverture pour les crimes clandestins et graves tels que les contenus pédopornographiques (CSAM)** : les méthodes d'enquête traditionnelles adaptées à l'ère

numérique, telles que l'infiltration de groupes et l'utilisation de comptes leurres, restent une référence pour identifier les malfaisants.

- Coopération volontaire : des canaux rapides et fiables permettant aux plateformes de partager des données non liées au contenu (historique de connexion, activité du compte) résolvent davantage d'affaires que des obligations imposant des vulnérabilités techniques.
- Analyse des métadonnées : le chiffrement protège le contenu, mais pas les comportements. Les enquêteurs peuvent reconstituer des chronologies, cartographier des réseaux criminels et identifier des suspects à partir de données non liées au contenu (qui, quand, où), sans déchiffrer les messages. Cette mesure n'implique pas une collecte et une conservation systématiques de ces données pour chaque utilisateur.
- Investigation numérique des appareils saisis : l'accès aux données stockées physiquement sur un appareil saisi chez un suspect constitue une alternative ciblée à la surveillance de masse. Cela permet d'accéder aux preuves au niveau du terminal, tout en laissant intact le canal sécurisé pour le reste du monde.



La zone rouge : propositions dangereuses (à rejeter)

- **Portes dérobées obligatoires** : introduction intentionnelle de failles dans les logiciels.
- **Analyse côté client** : transformation des appareils des utilisateurs en outils de surveillance.
- « **Accès légal dès la conception** » : terme marketing désignant des vulnérabilités systémiques.

Conclusion : la protection d'un chiffrement fort n'est pas un obstacle à la sécurité publique, mais une condition préalable à cette dernière. Les décideurs doivent cesser de rechercher une porte dérobée technique et commencer à investir dans les capacités humaines et les outils criminalistiques permettant de résoudre les crimes.

Recommandations

Les réponses politiques aux crimes graves dans l'environnement numérique doivent s'appuyer sur les principes suivants :

- **Préserver un chiffrement fort** : le chiffrement est essentiel pour garantir la confidentialité, l'intégrité et l'authenticité des données et des communications. Il constitue le fondement d'un Internet sûr et digne de confiance et protège les individus, les entreprises et les gouvernements, ainsi que les infrastructures critiques. Les politiques publiques doivent renforcer le chiffrement, et non l'affaiblir.
- **Garantir la nécessité et la proportionnalité** : les mesures d'enquête doivent être ciblées, légales et limitées à ce qui est strictement nécessaire. Elles doivent aussi être proportionnées à la gravité de l'infraction. Les mesures qui compromettent la sécurité de l'ensemble des utilisateurs pour enquêter sur un nombre limité de cas ne satisfont pas à ce critère et ne doivent pas être mises en œuvre.
- **Promouvoir un Internet sûr et digne de confiance** : les approches politiques et opérationnelles doivent s'aligner sur l'objectif d'un Internet résilient qui protège la confidentialité, l'intégrité et la disponibilité des données. La préservation d'une cybersécurité forte à l'échelle de l'écosystème numérique est essentielle pour la sécurité publique, la stabilité économique et la confiance dans les services numériques.