Juillet 2025

LE CHIFFREMENT

au centre *de la sécurité et de la confiance numériques*

numeum
Engager le numérique

Résumé exécutif

Le chiffrement constitue aujourd'hui l'un des fondements techniques les plus importants de la sécurité numérique. Utilisé dans de nombreux secteurs — communications, finance, santé, industrie, gouvernance — il garantit que seules les personnes autorisées peuvent accéder à des données, documents, ainsi qu'aux contenus d'un échange, excluant même les fournisseurs de services (fournisseurs cloud ou messageries). **Sa remise en cause, notamment au travers des mécanismes d'accès volontaire (backdoors, utilisateur fantôme), pose de graves risques en matière de cybersécurité, de respect de la vie privée, et de compétitivité économique.**

Alors que le recours à des techniques de chiffrement devient essentiel pour la confidentialité des communications électroniques et la protection des données sensibles et du secret des affaires, **leur affaiblissement aurait des effets systémiques graves : vulnérabilité accrue aux cyberattaques, perte de confiance des usagers, fragmentation technologique, ou encore décrochage industriel.**

Les débats relatifs au chiffrement ont été régulièrement relancés lorsque la sécurité nationale était en jeu, notamment à la suite d'attentats ou de menaces transnationales. En 2016 déjà, la CNIL, le Conseil national du Numérique[1] et l'ANSSI[2] avaient averti des conséquences d'un encadrement trop large ou imprécis du chiffrement.

Dans le cadre de la proposition de loi « *Sortir la France du piège du narcotrafic* », le projet d'article 8 ter (non-retenu en commission mixte paritaire) introduisait une rupture d'équilibre en ouvrant la possibilité d'accès à des données chiffrées dans des affaires de criminalité organisée, **sans garanties suffisantes.** Cette proposition a fait courir un risque de précédents réglementaires affectant les technologies sécurisées françaises et européennes.

---

1 « En s'attaquant au chiffrement contre le terrorisme, on se trompe de cible », Le Monde, 22 août 2016
2 « Contrôler le chiffrement : un calcul difficile pour le gouvernent », Libération, 2 août 2016

Le chiffrement et ses applications pour la sécurité numérique

Le chiffrement est un procédé de cryptographie permettant d'encoder des données dans un format qui ne peut être déchiffré que par un utilisateur disposant de la clé de déchiffrement. Historiquement, les premières techniques de cryptographie remontent à l'Antiquité (« chiffre de César ») et le chiffrement moderne a connu son essor au XXème siècle pour des besoins militaires et diplomatiques. Si les technologies de cryptographie ont longtemps été réservées à une communauté très restreinte, son usage s'est largement démocratisé ces dernières décennies avec **l'augmentation des cybermenaces et le développement croissant des communications et des usages numériques.** Le chiffrement est aujourd'hui omniprésent dans la vie quotidienne des citoyens mais et est aussi utilisé par l'intégralité des acteurs économiques. Il est déployé par de nombreuses messageries instantanées (Signal, WhatsApp, Olvid), mais aussi pour sécuriser les transactions bancaires, le stockage des données sensibles, ou encore les communications des entreprises, des systèmes de santé et des services publics. Tout projet stratégique ne peut être valablement mené aujourd'hui sans une protection par chiffrement.

Le **chiffrement de bout-en-bout** (*end-to-end encryption*, E2EE) est plus spécifiquement un protocole de sécurité des communications qui garantit que **seuls l'émetteur et le destinataire d'un message peuvent accéder à son contenu.** Aucun intermédiaire — y compris le fournisseur de service — ne peut accéder aux données en clair. Les messageries instantanées, tant professionnelles que grand public, reposent sur cette technique de chiffrement. Dans ces situations, il est impossible de déchiffrer des données sauf à ménager des portes dérobées (« backdoors ») qui sont autant de failles de sécurité utilisables par des cybercriminels. Le chiffrement de bout-en-bout repose sur des principes mathématiques robustes (notamment la cryptographie asymétrique) et des normes recommandées par les acteurs de la cybersécurité. Le chiffrement de bout-en-bout est devenu un standard dans la sécurisation des données sensibles, dans le cloud comme sur les terminaux.

Son usage est **promu depuis longtemps par la doctrine française de cybersécurité.** Les autorités recommandent en effet de manière constante d'intégrer des techniques de chiffrement pour développer les solutions numériques les plus sécurisées possibles. Selon l'ANSSI, le chiffrement « *a toujours été et reste un enjeu clé pour se protéger contre la menace, en particulier dans un contexte où les opérateurs de télécommunications sont particulièrement ciblés*[3] ». Ainsi, dans le cadre de la mise en œuvre de la directive « NIS2 », les autorités de cybersécurité recommandent spécifiquement la mise en place d'une politique de chiffrement par les entités assujetties. Par ailleurs, la **filière française de cybersécurité** est reconnue pour ses compétences en la matière, comme en témoigne le succès de la startup Olvid, dont l'utilisation est plébiscitée par les pouvoirs publics.

Son importance est ainsi multiple : **il protège la vie privée, garantit l'intégrité des données, empêche les interceptions illicites, protège contre l'espionnage industriel, sécurise les infrastructures critiques et participe à la confiance numérique. Tout affaiblissement de ce mécanisme introduit une vulnérabilité généralisée dans les écosystèmes numériques.** A l'heure où la France porte des objectifs ambitieux pour développer **une filière européenne forte de numérique de confiance, le chiffrement, en tant que pilier de la sécurité numérique, doit être préservé.**

---

3 « Cybersécurité : 'Rester maître de son destin, c'est aussi avoir la capacité de fixer des règles », Libération, 17 avril 2025

Contexte juridique et international

Le chiffrement se situe à l'intersection de plusieurs régimes juridiques (droit pénal, droit des communications électroniques, droit de la protection des données) et de rapports de force géopolitiques majeurs.

En droit français, son usage est encadré par la loi de 1996, qui libéralise son utilisation sous conditions, mais impose aux prestataires de cryptologie **des obligations de coopération** (remise des clés sous réquisition judiciaire, art. L.871-1 CSI et 434-15-2 CP). Le code pénal et le code de la sécurité intérieure imposent en effet déjà aux prestataires de chiffrement la remise des clés si elles existent, dans des délais contraints. Les autorités disposent de dispositifs d'interception judiciaire et de déchiffrement, via le Service technique national de captation judiciaire (STNCJ), ainsi que de la capacité à obtenir les métadonnées[4] d'une conversation, même si elles sont chiffrées.

Le Conseil constitutionnel et la Cour européenne des droits de l'Homme (CEDH) ont rappelé que **la protection des communications privées via le chiffrement découle du droit au respect de la vie privée et des correspondances** (article 8 CEDH). Toute mesure d'accès aux contenus chiffrés doit être strictement proportionnée, motivée, et encadrée par un contrôle juridictionnel indépendant.

À l'échelle internationale, plusieurs précédents démontrent les limites des politiques de contournement du chiffrement. En Australie, l'Assistance and Access Act (2018) a suscité une opposition forte de l'industrie et n'a pas démontré d'efficacité significative, si bien que l'autorité indépendante australienne de contrôle de la législation en matière de sécurité a recommandé d'y apporter des modifications[5]. Au Royaume-Uni, l'Investigatory Powers Act (2016) a été partiellement invalidé par la CEDH pour disproportionnalité.

Ces précédents montrent que la mise en cause du chiffrement ne résout pas les difficultés opérationnelles rencontrées par les services de sécurité, **tout en créant des vulnérabilités exploitables à grande échelle.**

Par ailleurs, de nombreuses voix, notamment celles de la Global Encryption Coalition et de l'Internet Society, dénoncent un risque de fragmentation du numérique si chaque État décide d'imposer ses propres exigences en matière de déchiffrement, au détriment de l'interopérabilité et de la sécurité globale.

---

4 Heure et date d'envoi d'un message, émetteur et destinataire.

5 « Australia's security monitor recommends changes to controversial 'anti-ecryption' legislation », Lexology, 17 juillet 2020

Risques associés à une remise en cause du chiffrement

La proposition de loi « Narcotrafic » et son article 8 ter (non-retenu dans la version finale adoptée par le Parlement) ont suscité une inquiétude légitime. En prétendant imposer aux fournisseurs de services numériques des « *mesures techniques nécessaires* » pour permettre aux services de renseignement d'accéder aux communications chiffrées, **le texte contourne les principes de la cryptographie moderne et les fondements techniques sur lesquels repose la sécurité numérique.** Les solutions techniques envisagées – création de portes dérobées, ajout d'un participant « *fantôme* », conservation obligatoire de clés de déchiffrement – ne sont pas neutres : en créant ainsi une forme de « *passe-partout* » donnant accès aux conversations chiffrées, **elles affaiblissent structurellement les protocoles de sécurité. Toute ouverture créée pour un acteur légitime est susceptible d'être exploitée par un acteur malveillant.** Cela augmente mécaniquement la surface d'attaque pour les cybercriminels et compromet la confidentialité globale des échanges. Ainsi, fin 2024 aux Etats-Unis, un groupe de hackers, « Salt Typhoon », qui a des liens présumés avec le gouvernement chinois, a ainsi exploité les portes dérobées qu'impose le *Communications Assistance for Law Enforcement Act*[6]. Cette règlementation qui s'applique notamment aux opérateurs de communications électroniques vise à faciliter l'accès des autorités aux données qui transitent ou figurent sur leurs services.

L'efficacité opérationnelle de telles mesures est par ailleurs discutable. Les réseaux criminels disposent souvent de compétences techniques et de ressources suffisantes pour se détourner de services légitimes et recourir à des plateformes moins réglementées, voire à des solutions personnalisées. **L'effet principal de cette législation serait donc de fragiliser la sécurité des messageries utilisées par le plus grand nombre - institutions publiques, citoyens, entreprises - sans impact réel sur les cibles visées.**

Cet épisode législatif s'inscrit dans une séquence historique plus large. Déjà en 2016, une régulation plus contraignante du chiffrement avait été envisagée. A cette occasion, les présidents du Conseil national du numérique (CNNum) et de la CNIL alertaient dans une tribune publiée dans Le Monde le 22 août 2016, contre les « solutions de facilité » que constitueraient l'affaiblissement du chiffrement ou la mise en place de « portes dérobées », en rappelant **leur efficacité très limitée pour les services de renseignement et leurs conséquences disproportionnées pour la sécurité globale du numérique**[7]. L'ANSSI, en tant qu'autorité de référence en matière de cybersécurité, avait à cette époque mis en garde sur l'impossibilité technique de garantir que des portes dérobées ne soient accessibles qu'aux seules autorités habilitées. Elle avait rappelé dans ses référentiels (RGS, bulletins CERT-FR) que les algorithmes robustes et les protocoles certifiés devaient être promus, et que le chiffrement était une composante critique de la sécurité des systèmes d'information.

Plus récemment, le Conseil de l'Europe a proscrit l'utilisation de ces technologies dans une résolution : « *la création de 'trappes' ou toute autre technique visant à fragiliser ou à contourner les mesures de sécurité, ou à exploiter les failles existantes, devrait être rigoureusement interdite* »[8]. Par ailleurs, les agences européennes de cybersécurité (ENISA) et de police criminelle (EUROPOL) ont également pointé dans une déclaration commune que les portes dérobées et dépôts de clés de chiffrement « *offrirai[en]t aux enquêteurs un accès légal en cas de crimes graves ou de menaces terroristes* » mais que « *cela augmenterait également la surface d'attaque pour des abus malveillants, ce qui, par conséquent, aurait des implications bien plus larges pour la société* »[9].

---

6 « Tempête de cybersécurité aux Etats-Unis, pleins feux sur le chiffrement des communications », Next INpact, 6 décembre 2024
7 Précité.
8 Résolution 2045 (2015) de l'Assemblée parlementaire du Conseil de l'Europe, « Les opérations de surveillance massive », avril 2015
9 ENISA et Europol, « On lawful criminal investigation that respects 21st Century data protection. Joint Statement », 20 mai 2016

Ces prises de position convergentes illustrent la constance des recommandations émanant des experts techniques : le chiffrement, s'il peut complexifier certaines enquêtes, reste une garantie fondamentale de sécurité pour l'ensemble de la société.

Vrai / Faux sur le chiffrement

« Il est possible d'insérer un 'participant fantôme' dans une conversation de messagerie instantanée sans affaiblir le chiffrement »

✗ **FAUX.** Cette technique revient à introduire une porte dérobée déguisée, et compromet l'intégrité du chiffrement de bout-en-bout. Ce type de pratique augmenterait le risque de vulnérabilité pouvant ensuite être exploitée par des acteurs malveillants. Comment s'assurer que ce type de dispositif ne serait pas utilisé à l'avenir à des fins autres que la lutte contre la criminalité ? Par ailleurs, quels seraient les risques en cas d'adoption de dispositifs similaires dans d'autres Etats, notamment dans des pays dont la législation est moins respectueuse de la vie privée ?

« Il est possible d'intercepter des conversations sans porter atteinte au chiffrement »

√ **VRAI.** Il est effectivement possible d'intercepter des conversations protégées par chiffrement de bout-en-bout sans affaiblir le chiffrement lui-même. Cela s'effectue principalement en ciblant les appareils des utilisateurs (par exemple via des logiciels espions ou l'accès physique), car le chiffrement protège les messages lors de leur transit, mais pas nécessairement sur les terminaux où ils sont lus ou écrits. Les métadonnées (qui communique avec qui, quand, où) peuvent aussi être collectées sans casser le chiffrement, fournissant des informations précieuses sur les réseaux et les habitudes de communication, même si le contenu reste protégé.

« Le chiffrement n'empêche pas d'enquêter »

√ **VRAI.** Des moyens d'investigation existent déjà via la collecte de métadonnées, la captation judiciaire[10], et l'exploitation des failles. De plus, le renseignement humain et les techniques d'infiltration (y compris en ligne) demeurent une voie pertinente et efficace pour mener le travail d'investigation.

« Les messageries chiffrées refusent toute coopération »

✗ **FAUX**. Les principales plateformes coopèrent souvent dès lors que le cadre légal est clair, et transmettent aux autorités judiciaires les métadonnées, le contenu des conversations n'étant pas accessible car chiffré.

« Le chiffrement est un obstacle technique créé par les géants du numérique »

✗ **FAUX.** Il est largement utilisé pour l'ensemble de la chaine de valeur numérique, dans toutes les filières économiques, et constitue une norme promue par l'ensemble des autorités de cybersécurité, notamment européennes.

« Rien n'est prévu dans les messageries pour lutter contre les contenus dangereux »

✗ **FAUX.** Certaines messageries ont mis en place une procédure de signalement pour maintenir la sécurité des utilisateurs. Cette procédure permet d'accéder aux métadonnées et identifier les comportements malveillants sans pour autant déchiffrer le contenu signalé et créer une « backdoor ».

---

10 Articles 706-102-1 et suivants du code de procédure pénal.

Pistes de solutions

- *Renforcer les moyens du Service technique national des captations judiciaires (STNCJ),* avec des ressources humaines et technologiques accrues. Il s'agit de l'autorité compétente en matière d'interception et de déchiffrement des communications dans le cadre des enquêtes judiciaires. Des ressources supplémentaires lui permettraient de développer encore davantage son expertise et ses moyens techniques.

- *Relancer le « groupe de contact permanent » (GCP),* créé en 2015 pour faciliter la coopération entre les opérateurs et l'Etat, comme espace de discussion pour faire émerger des solutions communes à la fois efficaces et respectueuses du chiffrement.

- *Soutenir la recherche sur des techniques d'enquête compatibles avec le chiffrement,* comme l'analyse comportementale ou l'exploitation des métadonnées. L'analyse par algorithme ou le recours aux systèmes d'IA offrent en effet de réelles perspectives dans l'identification de profils criminels à partir de variables statiques et dynamiques.

Conclusion

Le débat sur le chiffrement doit être abordé sous tous ses angles, celui de la lutte contre la criminalité, mais également du respect de la vie privée et de la confidentialité, ainsi que la compétitivité des acteurs économiques en France et en l'Europe.

La robustesse des communications numériques conditionne aujourd'hui notre souveraineté, notre résilience économique, et nos libertés fondamentales. Le chiffrement de bout-en-bout, en tant que standard technologique éprouvé, doit être préservé. **Toute remise en cause du chiffrement risquerait de pénaliser durablement le développement d'une filière de numérique de confiance forte sur le sol français.** Les pistes d'amélioration doivent se concentrer sur le renforcement ciblé des capacités étatiques et sur la coopération avec les opérateurs de messageries, et non sur l'affaiblissement des infrastructures numériques.

À propos de Numeum

Numeum est le syndicat patronal et la première organisation des professionnels du numérique en France. Membre de la fédération Syntec qui constitue la deuxième branche représentative du MEDEF, il représente les entreprises de services du numérique (ESN), les éditeurs de logiciels, les plateformes et les sociétés d'Ingénierie et de Conseil en Technologies (ICT).

Numeum rassemble plus de 2 500 entreprises adhérentes qui réalisent 85% du chiffre d'affaires total du secteur qui lui-même représente 70 milliards d'euros de chiffre d'affaires et 670 000 collaborateurs en France. Présidé par Véronique Torner depuis juin 2023, Numeum met en œuvre un projet d'impact pour faire rayonner la filière et fédérer les écosystèmes des professionnels du Numérique en France et en Europe.

La présidence se fixe trois grandes priorités : les régions, pour accompagner les adhérents partout en France, les compétences, pour répondre aux défis de l'attractivité et de la mixité, et le numérique responsable pour accompagner et soutenir le développement d'un écosystème numérique dans une trajectoire d'impact positif sur le plan économique, social, sociétal et environnemental.

Pour en savoir plus : www.numeum.fr

Crédits : Freepik juicy_fish

Engager
le numérique