L'UE mène la lutte contre le chiffrement : les citoyens européens en danger

Sécurité

Posté par : JulieM

Publié le : 16/9/2022 14:00:00

La proposition de la Commission Européenne, visant à lutter contre les matériels relatifs aux abus sexuels commis sur des enfants en ligne, compromet la sécurité et la protection de tous, y compris des plus jeunes.

Partout en Europe, les gouvernements cherchent à élaborer une réponse solide au fléau que constituent les contenus relatifs aux abus sexuels commis sur des enfants en ligne.

Dans cette optique, les responsables de l'action publique de l'Union Européenne (UE) se sont concentrés sur les cibles habituelles de ce type de législation, à savoir les plateformes de messagerie privée telles que Signal, WhatsApp, Snapchat et Facebook.

La proposition de la Commission Européenne obligera les plateformes de messagerie à accéder aux données et aux messages privés dans le but d'identifier les cas d'abus sexuels commis sur des enfants.

En théorie, les utilisateurs continueront à bénéficier de la confidentialité et de la sécurité que permet le chiffrement, tout en empêchant les criminels et les auteurs d'abus pédopornographiques d'exploiter les plateformes en ligne, grâce à des raccourcis techniques.

C'est un vœu pieux. Pour les fournisseurs de services, la seule façon de se conformer au règlement de l'UE consisterait donc à affaiblir le chiffrement de bout en bout (E2EE) pour tous, une décision catastrophique qui nuira à Internet, aura des répercussions économiques et portera atteinte à la sécurité et à la vie privée des internautes en Europe et au-delà, y compris des enfants que la législation entend protéger.

Une fois le chiffrement compromis, il sera en effet impossible de faire machine arrière. La totalité des données et des communications en ligne seront exposées au vu et au su des gouvernements et de tiers qui pourront les consulter et ne s'en priveront pas.

Cette proposition sonnera le glas de la vie privée et de la sécurité en Europe

La Commission soutient que son approche est compatible avec le chiffrement de bout en bout (E2EE). Or, aucune technologie ne permet aux fournisseurs de services d'offrir cet accès tout en garantissant un chiffrement fort.

Pour assurer leur conformité, ils devront soit compromettre le chiffrement, soit en affaiblir les possibilités en utilisant des technologies d'analyse côté client, lesquelles balayent le contenu des téléphones des utilisateurs avant l'envoi d'un message.

Ce débat n'est pas nouveau. Depuis plusieurs années, les forces de l'ordre réclament des « portes dérobées » dans le chiffrement en dépit des avertissements de la communauté des cyber-experts, qui soulignent les risques pour la sécurité. En réponse, les décideurs politiques privilégient de plus en plus des techniques comme l'analyse côté client.

Le chiffrement est indispensable pour prÃ©server la confidentialitÃ© et la sÃ©curitÃ© de nos activitÃ©s en ligne. Il permet de partager en toute confiance les donnÃ©es financiÃ¨res, les dossiers mÃ©dicaux et les informations personnelles, en ayant la certitude que ces donnÃ©es sensibles ne seront pas interceptÃ©es et que les messages privÃ©s le resteront.

En matiÃ¨re de chiffrement fort, le chiffrement de bout en bout E2E reprÃ©sente le nec plus ultra de la sÃ©curitÃ© dans un contexte oÃ¹ nos faits et gestes sont de plus en plus dÃ©matÃ©rialisÃ©s.

Des solutions, telles que lâ€™analyse cÃ¢tÃ© client, savent en profondeur lâ€™objectif du chiffrement E2E en permettant Ã un inconnu dâ€™accÃ©der Ã des informations considÃ©rÃ©es comme privÃ©es.

Les citoyens europÃ©ens seront ainsi exposÃ©s Ã de nouvelles escroqueries et cyberattaques en ligne, tandis que les donnÃ©es et les communications de leurs enfants pourront Ãatre piratÃ©es par les auteurs dâ€™abus que la proposition tente de stopper.

Une proposition qui pÃ©nalise les entreprises europÃ©ennes

Les entreprises europÃ©ennes devront rÃ©pondre Ã une sÃ©rie dâ€™exigences coÃ¢teuses pour crÃ©er des systÃ¨mes onÃ©reux et techniquement complexes dâ€™analyse et de portes dÃ©robÃ©es de chiffrement.Ã

Seuls les grands fournisseurs pourront procÃ©der Ã de tels investissements, confortant leur domination sur le marchÃ© et tuant dans lâ€™Ã©lan les ambitions de nombreuses startups europÃ©ennes.

La proposition limitera Ã©galement la maniÃ¨re dont les entreprises peuvent utiliser le chiffrement E2E pour de nouvelles technologies et de nouveaux produits, ce qui aura pour effet de freiner lâ€™innovation dans tous les secteurs dâ€™activitÃ© et de laisser lâ€™Europe Ã la merci des gÃ©ants de la Silicon Valley.Ã

En deux mots, cette proposition risque dâ€™anÃ©antir les ambitions affichÃ©es par lâ€™UE pour la dÃ©cennie numÃ©rique.

Une proposition qui ouvrira les vannes de la surveillance gÃ©nÃ©ralisÃ©e

Les internautes pourront Ãatre plus facilement surveillÃ©s par lâ€™Ã©tat et dâ€™autres acteurs. Pour les citoyens dâ€™Europe centrale et de lâ€™Est qui ont vÃ©cu la surveillance analogique et les reprÃ©sailles politiques, une telle proposition constituerait un terrible recul des libertÃ©s chÃ©rement acquises par les gÃ©nÃ©rations prÃ©cÃ©dentes.

Par ailleurs, les membres de la communautÃ© LGBTQI+, les victimes dâ€™abus et dâ€™agressions, les rÃ©fugiÃ©s et les groupes minoritaires qui sont la cible de discriminations ou dâ€™attaques ne pourront plus trouver refuge sur Internet.

Des professions, comme les journalistes qui dÃ©pendent du chiffrement pour garantir leur sÃ©curitÃ© et protÃ©ger leurs sources, se heurteront Ã dâ€™importantes difficultÃ©s pour enquÃªter sur la corruption et la criminalitÃ©.Ã

A cet Ã©gard, lâ€™assassinat du journaliste slovaque JÃ¡n Kuciak en fÃ©vrier 2018 et celui de sa consÃ©ur maltaise Daphne Caruana Galizia en octobre 2017 rappellent les risques quâ€™affrontent les reporters et les journalistes dâ€™investigation.

La valeur du chiffrement fort en tant quâ€™outil de sÃ©curitÃ© et de protection de la vie privÃ©e

À la mise en évidence dès les premiers jours du conflit en Ukraine, lorsque des milliers de personnes ont commencé à utiliser des services de messagerie cryptée de bout en bout pour communiquer avec leurs parents et leurs proches en toute sécurité.

La riposte

Heureusement, des signes de mécontentement se font sentir à Bruxelles. Le Contrôleur européen de la protection des données (CEPD) et le Comité européen de la protection des données (EDBP) ont publié un avis conjoint à propos de la proposition relative aux abus sexuels commis sur des enfants, qualifiant de « disproportionnés » les efforts visant à porter atteinte au chiffrement E2E et déclarant que le chiffrement contribue « de manière fondamentale au respect de la vie privée et à la confidentialité des communications ».

Plusieurs membres du Parlement européen se sont également exprimés. L'eurodéputé allemand Patrik Breyer a qualifié les mesures proposées de « surveillance de masse » et averti que les failles qu'elle ne manquerait pas de créer « risquent d'être exploitées par quiconque dispose des moyens techniques nécessaires, par exemple des criminels ou des services de renseignement étrangers ».

Ivan Bartoň, vice-premier ministre chargé du numérique de la République tchèque, la Coalition mondiale pour le chiffrement (Global Encryption Coalition) et l'Initiative européenne pour les droits numériques (EDRI) ont soutenu dans sa démarche.

Il est impératif que chaque citoyen européen s'élève contre cette proposition et contre l'idee destructrice selon laquelle l'élimination de la confidentialité et de la sécurité en ligne mettra un terme à la criminalité et aux problèmes sociaux.

Si une solution est nécessaire, la disparition du chiffrement aura des conséquences que nous ne sommes certainement pas prêts à encaisser. La Commission européenne doit revoir sa copie. Le chiffrement de bout en bout est notre meilleure défense, et il est de notre devoir de le protéger.