***L'UE mÃ©prise le chiffrement : les citoyens europÃ©ens en danger***
**SÃ©curitÃ©**
PostÃ© par : JulieM
PubliÃ©e le : 16/9/2022 14:00:00

La proposition de la Commission EuropÃ©enne, visant Ã lutter contre les matÃ©riels relatifs aux abus sexuels commis sur des enfants en ligne, compromet la sÃ©curitÃ© et la protection de tous, y compris des plus jeunes.

Partout en Europe, les gouvernements cherchent Ã Ã©laborer une rÃ©ponse solide au flÃ©au que constituent les contenus relatifs aux abus sexuels commis sur des enfants en ligne.Â

Dans cette optique, les responsables de lâ□□action publique de lâ□□Union EuropÃ©enne (UE) se sont concentrÃ©s sur les cibles habituelles de ce type de lÃ©gislation, Ã savoir les plateformes de messagerie privÃ©e telles que Signal, WhatsApp, Snapchat et Facebook.

La proposition de la Commission EuropÃ©enne obligera les plateformes de messagerie Ã accÃ©der aux donnÃ©es et aux messages privÃ©s dans le but dâ□□y dÃ©tecter les cas dâ□□abus sexuels commis sur des enfants.Â

En thÃ©orie, les utilisateurs continueront Ã bÃ©nÃ©ficier de la confidentialitÃ© et de la sÃ©curitÃ© que permet le chiffrement, tout en empÃªchant les criminels et les auteurs dâ□□abus pÃ©dopornographiques dâ□□exploiter les plateformes en ligne, grÃ¢ce Ã des raccourcis techniques.

Câ□□est un vÅ□u pieux. Pour les fournisseurs de services, la seule faÃ§on de se conformer au rÃ¨glement de lâ□□UE consisterait donc Ã affaiblir le chiffrement de bout en bout (E2EE) pour tous, une dÃ©cision catastrophique qui nuira Ã Internet, aura des rÃ©percussions Ã©conomiques et portera atteinte Ã la sÃ©curitÃ© et Ã la vie privÃ©e des internautes en Europe et au-delÃ â□□ y compris des enfants que la lÃ©gislation entend protÃ©ger.

Une fois le chiffrement compromis, il sera en effet impossible de faire machine arriÃ¨re. La totalitÃ© des donnÃ©es et des communications en ligne seront exposÃ©es au vu et au su des gouvernements et de tiers qui pourront les consulter â□□ et ne sâ□□en priveront pas.

**Cette proposition sonnera le glas de la vie privÃ©e et de la sÃ©curitÃ© 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 dâ□□offrir cet accÃ¨s tout en garantissant un chiffrement fort.Â

Pour assurer leur conformitÃ©, ils devront soit compromettre le chiffrement, soit en affaiblir les possibilitÃ©s en utilisant des technologies dâ□□analyse cÃ´tÃ© client, lesquelles balaient le contenu des tÃ©lÃ©phones des utilisateurs avant lâ□□envoi dâ□□un message.

Ce dÃ©bat nâ□□est pas nouveau. Depuis plusieurs annÃ©es, les forces de lâ□□ordre rÃ©clament des Â« portes dÃ©robÃ©es Â» dans le chiffrement en dÃ©pit des avertissements de la communautÃ© des cyber-experts, qui soulignent les risques pour la sÃ©curitÃ©. En rÃ©ponse, les dÃ©cideurs politiques privilÃ©gient de plus en plus des techniques comme lâ□□analyse cÃ´tÃ© 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, sapent 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.Â

Seuls les grands fournisseurs pourront procÃ©der Ã de tels investissements, confortant leur domination sur le marchÃ© et tuant dans lâ□□Å□uf 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.Â

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©.Â

A cet Ã©gard, lâ□□assassinat du journaliste slovaque JÃin Kuciak en fÃ©vrier 2018 et celui de sa consÅ□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

a Ã©tÃ© mise en Ã©vidence dÃ¨s les premiers jours du conflit en Ukraine, lorsque des milliers de personnes ont tÃ©lÃ©chargÃ© des services de messagerie cryptÃ©e de bout en bout pour communiquer avec leurs parents et leurs proches en toute sÃ©curitÃ©.

## La riposte

Heureusement, des signes de mÃ©contentement se font sentir Ã Bruxelles. Le ContrÃ´leur europÃ©en de la protection des donnÃ©es (CEPD) et le ComitÃ© europÃ©en de la protection des donnÃ©es (EDBP) ont publiÃ© un avis conjoint Ã propos de la proposition relative aux abus sexuels commis sur des enfants, qualifiant de Â« disproportionnÃ©s Â» les efforts visant Ã porter atteinte au chiffrement E2E et dÃ©clarant que le chiffrement contribue Â« de maniÃ¨re fondamentale au respect de la vie privÃ©e et Ã la confidentialitÃ© des communications Â».

Plusieurs membres du Parlement europÃ©en se sont Ã©galement exprimÃ©s. Lâ□□eurodÃ©putÃ© allemand Patrik Breyer a qualifiÃ© les mesures proposÃ©es de Â« surveillance de masse Â» et averti que les failles quâ□□elle ne manquerait pas de crÃ©er Â« risquent dâ□□Ãªtre exploitÃ©es par quiconque dispose des moyens techniques nÃ©cessaires, par exemple des criminels ou des services de renseignement Ã©trangers Â».

Ivan BartoÅi, vice-premier ministre chargÃ© du numÃ©rique de la RÃ©publique tchÃ¨que, la Coalition mondiale pour le chiffrement (Global Encryption Coalition) et lâ□□Initiative europÃ©enne pour les droits numÃ©riques (EDRI) lâ□□ont soutenu dans sa dÃ©marche.

Il est impÃ©ratif que chaque citoyen europÃ©en sâ□□Ã©lÃ¨ve contre cette proposition et contre lâ□□idÃ©e destructrice selon laquelle lâ□□Ã©limination de la confidentialitÃ© et de la sÃ©curitÃ© en ligne mettra un terme Ã la criminalitÃ© et aux problÃ¨mes sociÃ©taux.

Si une solution est nÃ©cessaire, la disparition du chiffrement aura des consÃ©quences que nous ne sommes certainement pas prÃªts Ã encaisser. La Commission europÃ©enne doit revoir sa copie. Le chiffrement de bout en bout est notre meilleure dÃ©fense, et il est de notre devoir de le protÃ©ger.