L'analyse côté client : case du Royaume-Uni

Décembre 2023

Résumé et recommandations

Dans le cadre de l'examen actuel du projet de loi sur la sécurité en ligne par la Chambre des Lords, certains débats se sont concentrés sur le cryptage de bout en bout (E2EE) et l'utilisation de technologies d'analyse côté client. L'Internet Society cherche à contribuer à ce débat pour trois raisons : premièrement, l'analyse côté client sape la confiance promise par le cryptage de bout en bout, en affaiblissant le niveau de sécurité et de confidentialité des individus au Royaume-Uni et ailleurs ; deuxièmement, le débat met en avant des arguments fallacieux, qui ont persisté tout au long des étapes précédentes du projet de loi et ne constituent pas une base fiable sur laquelle évaluer la législation ; troisièmement, l'analyse côté client n'empêchera pas les individus motivés de partager des contenus illégaux sans être détectés.

Recommandations

L'Internet Society soumet respectueusement les recommandations suivantes aux membres de la chambre des Lords examinant le projet de loi :

1. Soutenir l'amendement visant à exclure les services de messagerie privée du champ d'application du projet de loi. [Amendements 203 et 204]
2. Remédier aux carences dans les garanties prévues dans le projet de loi en soutenant, par exemple, les amendements qui demandent :
    a. Une interdiction explicite de la surveillance générale, y compris l'utilisation de l'analyse côté client ; [Amendement 285]
    b. L'exigence que les requêtes technologiques nécessitent une approbation judiciaire ; [Amendements 207 et 246]
    c. L'exigence que les interventions de l'Ofcom soient soumises à un test d'intérêt public transparent et responsable ; [Amendement 208]
    d. Une obligation explicite pour l'Ofcom de se conformer à la législation relative aux droits de l'homme ; [Amendement 214]
    e. Une obligation explicite pour l'Ofcom de protéger la vie privée de l'individu. [Amendements 209 et 210]

Concernant le point 2(a), le projet de loi sur la sécurité en ligne devrait exclure le *déploiement* massif de technologies permettant une surveillance généralisée, même si son intention déclarée est qu'une telle technologie ne soit *activée* que de manière sélective. Un tel déploiement représenterait toujours une faiblesse systémique pour les technologies grand public, et donc une menace importante pour la cybersécurité et la vie privée.

L'analyse côté client nuit à la confidentialité

Le gouvernement continue d'affirmer que les obligations du projet de loi de détecter et de prévenir les contenus illégaux « n'interdisent et n'affaiblissent pas le cryptage ». Cette affirmation est trompeuse, *si* cette détection repose sur ce que l'on appelle une porte dérobée de cryptage.[1] Si, comme le gouvernement semble l'envisager, la détection est basée sur une « analyse côté client », cette analyse a lieu avant le début du processus de cryptage. Bien que cela puisse donner à l'affirmation du gouvernement une vraisemblance sémantique, la confidentialité est alors perdue. La réalité est que l'analyse annule l'objectif du cryptage, crée de nouveaux risques de sécurité et prive les citoyens des moyens de communiquer en toute confiance.

Même les professionnels de la sécurité nationale du Royaume-Uni considèrent cette proposition comme dangereuse :

> « L'analyse côté client, quoi qu'en disent ses partisans, semble impliquer une certaine sorte de niveau d'accès, une certaine capacité à trier et analyser, et il n'y a donc aucun moyen de limiter cela à un bon usage par des autorités légales crédibles et des démocraties libérales ».
> — Ciaran Martin, ancien directeur général du Centre national de cybersécurité du Royaume-Uni.

Il est légitime de remettre en question la fiabilité des garanties que prétend mettre en place le projet de loi et de se demander pourquoi le gouvernement a jusqu'à présent ignoré les conseils de professionnels informés sur la sécurité nationale.

[1] « A Backdoor is a Backdoor is a Backdoor. » Internet Society, 24 mars 2020, https://www.internetsociety.org/blog/2020/03/a-backdoor-is-a-backdoor-is-a-backdoor/

Quels sont les risques liés à l'analyse côté client ?

L'analyse côté client ou CSS (de l'anglais Client-Side Scanning) fait généralement référence aux systèmes intégrés au téléphone ou à un autre appareil d'un utilisateur, qui analysent le contenu du message (p. ex. texte, images, fichiers) en cherchant des correspondances ou des similitudes avec une base de données de contenus répréhensibles avant l'envoi du message.

Plus nos vies et nos économies dépendent des services en ligne et de la communication numérique, plus il est vital pour les individus, les familles, les entreprises et les gouvernements de communiquer en toute sécurité et avec la certitude que les conversations et transactions sont confidentielles. Les fournisseurs de services de communication en ligne mettent de plus en plus en œuvre le cryptage de bout en bout pour leurs utilisateurs, afin d'améliorer la sécurité, la confidentialité et la confiance, même lorsque la communication passe inévitablement par un ou plusieurs intermédiaires. Dans le même temps, les gouvernements et les forces de l'ordre continuent de chercher à accéder aux communications afin de détecter et de prévenir la criminalité.

Les partisans des technologies de CSS les présentent comme la solution. Cependant :

> Si briser le cryptage revient à ouvrir une lettre à la vapeur lors de son passage dans un bureau de poste, l'analyse côté client revient à lire la lettre au fur et à mesure qu'elle est écrite. Le résultat est le même : la confidentialité des communications individuelles n'existe plus.

Comme l'explique un récent avis conjoint[2] du Comité européen de la protection des données et du Contrôleur européen de la protection des données, la CSS « peut être facilement contournée en cryptant le contenu à l'aide d'une application distincte ». La CSS ouvre ainsi la porte à des mesures disproportionnées qui mettent les citoyens en danger et ne résoudra pas le problème de la détection de contenus illégaux provenant de criminels, même légèrement déterminés.

Conclusion

La communication confidentielle est essentielle à une société numérique et à une économie axée sur les données, et le cryptage de bout en bout est essentiel à la confidentialité des communications. L'analyse côté client va à l'encontre de l'objectif du cryptage de bout en bout, en violant fondamentalement la confidentialité que les utilisateurs attendent et dont ils ont besoin lorsqu'ils communiquent en ligne. De plus, la CSS doit être omniprésente et généralisée pour être efficace, ce qui

[2] « Avis conjoint 04/2022 de l'EDPB et du CEPD sur la proposition de règlement du Parlement européen et du Conseil établissant des règles en vue de prévenir et de combattre les abus sexuels sur les enfants », 28 juillet 2022, https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-042022-proposal_en

crée un cercle vicieux que le projet de loi sur la sécurité en ligne ne peut pas résoudre : si la CSS est facilement contournée, elle est inutile ; si elle est omniprésente, elle est disproportionnée.

Nous savons déjà que le gouvernement souhaite que toutes les principales plateformes de communication soient soumises à cette exigence. Il est fallacieux de la part du gouvernement de prétendre en même temps que cela ne constitue pas une obligation générale de contrôle.

L'analyse côté client, dans les produits et services de grande consommation :

- **Réduit la confiance dans l'écosystème Internet.** La perte de confiance dans les communications en ligne nuirait à l'économie du Royaume-Uni à une période d'extrême fragilité.
- **Présente un risque sérieux pour les droits fondamentaux,** comme indiqué dans l'avis conjoint de l'EDPB et du CEPD.
- **Impose une sécurité défaillante aux utilisateurs, y compris aux plus exposés,** avec peu de chances d'empêcher les actions de criminels ou de gouvernements hostiles.

Les pouvoirs prévus dans le projet de loi sur la sécurité en ligne incluent l'obligation de détecter les contenus illégaux dans les communications privées. Cette mesure est disproportionnée et son efficacité est mise en doute. Le gouvernement devrait supprimer cette obligation du projet de loi et se concentrer plutôt sur d'autres moyens plus efficaces de lutter contre les réseaux criminels et d'assurer la sécurité des utilisateurs.

Pour plus d'informations :

Les partisans de l'analyse côté client considèrent cette technologie comme une solution pour identifier les contenus répréhensibles dans les environnements E2EE. Dans ce document, nous avons expliqué comment la CSS enfreint l'accord de confiance du cryptage de bout en bout et les dangers qu'elle présente.

Pour plus d'informations sur le fonctionnement de la CSS et ses défauts inhérents, la fiche d'information de l'Internet Society sur l'analyse côté client peut servir de ressource pour des discussions politiques détaillées.[3] Nos autres ressources[4] sur le cryptage, la sécurité et la confidentialité peuvent également être utiles aux décideurs politiques concernés qui maîtrisent mal le sujet.

À propos de l'Internet Society

[3] « Fiche d'information : L'analyse côté client » Internet Society, 26 septembre 2022, https://www.internetsociety.org/fr/resources/doc/2020/lanalyse-cote-client/

[4] « Qu'est-ce que le cryptage ? » Internet Society, 14 juillet 2022, https://www.internetsociety.org/issues/encryption/what-is/

L’Internet Society est une organisation caritative mondiale fondée en 1992 par certains des pionniers d’Internet. Nous pensons qu'Internet est une force bénéfique et nous œuvrons pour un Internet ouvert, connecté à l'échelle mondiale, sécurisé et digne de confiance qui profite à tous. Avec 110 chapitres actifs sur six continents, dont 28 en Europe, et plus de 100 000 utilisateurs individuels soutenant nos activités, l'Internet Society est une partie prenante importante et un interlocuteur fiable et techniquement informé de la société civile pour les questions relatives à la gouvernance de l'Internet.