Traçabilité et cybersécurité

Série d'ateliers d'experts sur le chiffrement en Inde

Novembre 2020

La traçabilité ou la capacité de retrouver le créateur d'un contenu ou d'un message particulier est au centre du débat en Inde à propos des règles pour les plates-formes en ligne et les prestataires de communications. À la fin 2018, le ministère indien de l'électronique et de l'informatique (MeiTy) a proposé des amendements aux règles pour l'informatique (directives intermédiaires) dans le cadre de la loi sur l'informatique (Information Technology Act).[1] Parmi les changements envisagés figure une demande de traçabilité, décrite comme étant « la possibilité de retrouver le créateur [2] des informations sur sa plate-forme ». L'amendement rendrait la plate-forme en ligne ou le fournisseur responsable des contenus publiés par leurs utilisateurs, si une traçabilité n'était pas fournie. Le MeiTY a sollicité des commentaires du public à propos du projet d'amendement début 2019[3] et, en outre, presque 30 experts en cybersécurité et cryptographie ont, début 2020, envoyé une lettre ouverte au MeiTY exprimant leurs préoccupations concernant les amendements envisagés.[4] La traçabilité fait également l'objet d'un litige devant le tribunal de grande instance de Madras, opposant plusieurs plates-formes en ligne aux pouvoirs publics, concernant plus particulièrement l'accès des forces de l'ordre aux contenus générés par les utilisateurs.[5]

Les aspects suivants sont au cœur du débat actuel :

- la concrétisation de la traçabilité dans les communications chiffrées de bout en bout ;[6]
- les méthodes disponibles pour activer la traçabilité ;
- les ramifications associées à chaque méthode.

L'utilisation **de signatures numériques** et **le recours** à des métadonnées, sont deux méthodes envisagées pour permettre la traçabilité des communications de bout en bout telles que celles des applications de messagerie (par ex. WhatsApp). Cependant, pour respecter les exigences de traçabilité, les plates-formes risquent d'être forcées d'autoriser l'accès aux contenus des communications de leurs utilisateurs, **en**

1 Règles sur l'informatique [Directives intermédiaires (Amendement)] .

2 Selon la loi indienne sur les technologies de l'information, un créateur est défini comme la personne qui envoie, génère, stocke ou transmet tout message électronique ou qui fait en sorte qu'un message électronique soit envoyé, généré, stocké ou transmis à toute autre personne, à l'exception de tout intermédiaire ».

3 https://www.meity.gov.in/writereaddata/files/public_comments_draft_intermediary_guidelines_rules_2018.pdf

4 https://www.internetsociety.org/open-letters/india-intermediary-guidelines/

5 https://www.medianama.com/2019/09/223-sc-adjourns-hearing-on-facebook-transfer-petition-till-september-24/

6 Le chiffrement de bout en bout (en anglais, end-to-end ou E2E) — dans le cadre duquel les clés nécessaires au déchiffrage d'une communication chiffrée sont uniquement stockées sur les appareils qui communiquent — assure le meilleur niveau de sécurité et de fiabilité, car sa conception ne permet qu'au destinataire visé de détenir la clé permettant de déchiffrer le message.

supprimant le chiffrement de bout en bout et en affaiblissant considérablement la sécurité et la confidentialité de leur produit, afin de permettre la traçabilité.

Au cours d'une série de discussions basées sur la règle de Chatham House et organisées par l'Internet Society en partenariat avec Medianama, un groupe international d'experts en cybersécurité et en politiques publiques ont examiné le problème de la traçabilité des messages dans un contexte indien. Les experts ont exprimé de fortes inquiétudes à propos des deux techniques souvent proposées pour activer la traçabilité : l'utilisation des signatures numériques et le recours aux métadonnées. Non seulement ces méthodes sont considérées comme des menaces sur la confidentialité et la sécurité des utilisateurs, elles ne constituent pas forcément une preuve irréfutable à propos de l'origine d'un message. La création d'un accès tiers aux communications des utilisateurs pour permettre la traçabilité engendre d'autres inquiétudes à propos de la sécurité et de la confidentialité.

Signatures numériques

Il a été suggéré que la signature numérique[7] de l'expéditeur soit ajoutée aux messages afin de pouvoir identifier le créateur du message. Par exemple, dans le cadre du litige devant le tribunal de grande instance de Madras, le Dr V. Kamakoti a proposé l'utilisation des signatures numériques pour identifier le créateur d'un message transféré au sein de WhatsApp.[8] Selon cette suggestion, la signature serait soit visible par tous dans la chaîne de message ou serait chiffrée en utilisant une clé publique fournie par WhatsApp. En utilisant la clé privée correspondante, WhatsApp serait en mesure de déchiffrer les informations du créateur, en réponse à une décision de justice éventuelle.

Toutefois, de nombreuses personnes, y compris les experts participant aux discussions de l'Internet Society, ont des inquiétudes à propos de l'utilisation des signatures numériques en tant qu'outil de traçabilité :

- **L'attribution numérique n'est pas absolue et est vulnérable à l'usurpation d'identité :** pour établir la responsabilité pénale, la culpabilité doit être prouvée au-delà du doute raisonnable, un seuil difficile à franchir étant donné que l'usurpation d'identité en ligne est très facile et très répandue. Prouver que la personne A, utilisatrice du portable/de l'ordinateur A, a en réalité envoyé ces messages dans le cadre d'une campagne de désinformation est une tâche très ardue même si les forces de l'ordre possèdent l'identifiant de l'expéditeur. Pour établir si *l'utilisation* de l'appareil d'une personne constitue nécessairement une preuve de *l'utilisation de l'appareil par celle-ci*, il faut disposer d'informations supplémentaires.[9] Plus grave encore est l'implication d'utilisateurs innocents dans des activités illégales entreprises par des cyberdélinquants usurpant l'identité de ces utilisateurs. Cette inquiétude a été soulignée dans la réponse de WhatsApp à la proposition de V. Komakoti selon laquelle des « acteurs malveillants pourraient utiliser des versions modifiées de WhatsApp pour attribuer un numéro de téléphone différent à un message ».[10]

- **Les signatures numériques ajoutent des vulnérabilités.** Les clés privées pour les signatures numériques, en particulier si elles sont détenues par des tiers à la communication, comme le prestataire de services de communication, constitueraient une cible de choix pour les acteurs malveillants. Par exemple, dans la proposition de V. Kamokoti, une tierce partie compromise aurait la possibilité de voir lorsqu'un utilisateur particulier envoie un message, en recevant et en déchiffrant les coordonnées du créateur. Si utilisée à mauvais escient, la méthode de la « signature numérique » représente un risque considérable pour la liberté d'expression des citoyens et risque d'exposer les

7 Une signature numérique est un mécanisme garantissant l'authenticité d'un message ou des informations envoyées. Elle permet à l'expéditeur du message de joindre un code en guise de signature. Comme pour la signature manuscrite d'une personne, la signature est unique pour chaque signataire et est comparable à un sceau inviolable garantissant que les informations n'ont pas été altérées de quelques façons que ce soient depuis leur envoi.

8 https://www.medianama.com/2019/08/223-kamakoti-medianama-whatsapp-traceability-interview/

9 Par exemple, quelqu'un d'autre peut être en train d'utiliser son appareil.

10 https://www.medianama.com/2019/08/223-exclusive-whatsapps-response-kamakotis-submission/

individus (y compris les plus vulnérables et marginalisés) à l'emprunt d'identité, au harcèlement et à la persécution.

- **Une fonctionnalité multiplateforme serait irréalisable.** Étant donné que différents protocoles régissent différents services et plates-formes, les méthodes essayant d'établir la collaboration entre les plates-formes ne fonctionneraient pas. La traçabilité inter plates-formes est également difficile dans les systèmes fédérés comme les messageries électroniques ou l'Internet Relay Chat (IRC). Les méthodes pour fournir la traçabilité à travers les plates-formes, comme l'utilisation de la même signature numérique obligatoire dans le texte de chaque message sur chaque plate-forme, à l'échelle mondiale, seraient difficiles à mettre en œuvre. Un registre central de *chaque* appareil et de *chaque* application client dans le monde serait probablement nécessaire pour authentifier les signatures numériques. Cela aurait pour effet de freiner gravement l'innovation en forçant les développeurs dans le monde entier à coordonner leurs travaux avec les exploitants de la base de données centrale. En outre, une signature numérique obligatoire constituerait un risque accru pour la confidentialité et la sécurité des utilisateurs en établissant un point de défaillance unique ou une vulnérabilité unique que les acteurs malveillants pourraient cibler pour compromettre ou contrôler les activités d'un utilisateur.[11] Il serait également nécessaire de pouvoir révoquer ces signatures numériques ou de les recréer facilement, ce qui soulève le problème de la sécurité des clés privées associées. Si cela dépend des données biométriques des utilisateurs, alors une couche supplémentaire de complexité technique et opérationnelle est ajoutée.

Métadonnées

L'utilisation des métadonnées dans la traçabilité a également été évoquée par plusieurs entités au cours du débat sur le chiffrement. Les métadonnées, qui contiennent des informations sur la communication mais pas sur son contenu, peuvent être utilisées pour déterminer, par exemple, la source, l'heure, la date et la destination d'une communication, et potentiellement l'emplacement du destinataire, ou même être utilisées pour estimer certaines caractéristiques des contenus de la communication.

Certains ont souligné que les métadonnées à propos de la taille du message, en particulier un message multimédia, peuvent potentiellement être utilisées pour vérifier la distribution non contrôlée de messages particuliers. Par exemple, WhatsApp maintient un journal chiffré des messages multimédia envoyés. WhatsApp n'a pas accès au contenu du fichier multimédia qui est affiché comme un groupe de données d'une taille spécifique. Chaque fois que ce message multimédia est transféré, le serveur obtient une estimation du nombre de fois que le groupe de données est transféré et utilise cette information pour lutter contre les courriers indésirables sur sa plate-forme. Il peut être possible d'établir l'historique du message avec l'accès à une copie non chiffrée du fichier multimédia et supprimer par conséquent la confidentialité de la communication.

D'autres pensent que les métadonnées peuvent être analysées pour établir des tendances comme des associations d'interlocuteurs, la fréquence de leurs interactions et leurs dates. Des graphes sociaux de base peuvent être créés par les plates-formes pour établir des réseaux d'interactions. Les structures de répertoire, qui sont fondamentales pour n'importe quelle plate-forme de communication, pourraient être mises à contribution dans le cadre d'enquêtes sans accéder aux contenus. Ces répertoires enregistrent les interactions sans cependant intercepter les contenus proprement dits.

Toutefois, des experts, y compris ceux participant aux discussions de l'Internet Society, ont formulé des inquiétudes à propos de l'utilisation des métadonnées pour la traçabilité :

- **L'attribution numérique n'est pas absolue, notamment par le biais des métadonnées.** Il est encore plus difficile d'établir la responsabilité criminelle sur la base des métadonnées. Des changements mineurs dans les contenus d'un message peuvent altérer ses métadonnées et limiter la capacité de

11 https://www.internetsociety.org/policybriefs/identity

suivre la chaîne de métadonnées similaires vers un créateur. Comme pour les signatures numériques, il est difficile d'associer un utilisateur à un message lorsque l'emprunt d'identité en ligne est si facile et omniprésent. Encore plus inquiétant est le risque que court un utilisateur innocent d'être incriminé de conduite criminelle uniquement sur la base de métadonnées falsifiées.

- **Mise à mal des principes de minimisation des données et de respect de la vie privée lors de la conception.** La dépendance sur les métadonnées pourrait être nuisible aux efforts en faveur de la minimisation des données et la protection intégrée de la vie privée qu'un nombre croissant de politiques de protection des données exigent désormais. Cela engendre des risques encore plus grands pour la confidentialité et la sécurité des personnes en réduisant les normes de sécurité pour tout le monde. Les métadonnées conservées pour être utilisées dans la traçabilité représenteraient une cible de valeur pour les acteurs malveillants. Les criminels et les adversaires étrangers pourraient utiliser les métadonnées stockées pour élaborer des graphes sociaux des utilisateurs ou pour recueillir des informations permettant de monter des attaques comme des extorsions, de l'ingénierie sociale ou du chantage.

- **Risques de profilage social.** Lorsque les métadonnées sont utilisées pour élaborer des graphes sociaux afin de permettre la traçabilité, ces graphes courent le risque d'être compromis par des criminels ou des adversaires étrangers. Le risque de monétisation des graphes sociaux par les plates-formes est également présent, ce qui peut provoquer la divulgation d'informations sensibles concernant des fonctionnaires, des élus, des journalistes, des activistes, des avocats et des dissidents pour le bénéfice de revendeurs de données et de leurs clients.

- **Des périodes plus longues de conservation des données engendrent des risques de sécurité :** les règles de conservation des métadonnées incluent souvent l'obligation de conserver les données pendant une durée spécifique. Si les pouvoirs publics imposent des périodes de conservation plus longues pour les métadonnées, cela aggrave les risques pour la confidentialité et la sécurité en augmentant la quantité de métadonnées potentiellement compromises en cas de violation des données. Plus la quantité de données conservées est importante, plus l'intérêt des criminels et des adversaires étrangers est élevé.

- **Les plates-formes ne recueillent pas toutes la même quantité de métadonnées :** par exemple, Signal recueille la quantité minimale requise de métadonnées pour permettre les communications sans recueillir de données supplémentaires.[12] Les obligations de conservation de plus grandes quantités de métadonnées pourraient forcer les plates-formes à reconfigurer de façon considérable leurs systèmes, générant des coûts et augmentant les risques d'introduction de nouvelles vulnérabilités.

Interruption du chiffrement de bout en bout

Étant donné que l'utilité des signatures numériques et des métadonnées pour la traçabilité n'est pas claire, les plates-formes peuvent être amenées à utiliser des méthodes permettant à des tierces parties d'accéder aux contenus des communications, ce qui est parfois appelé accès exceptionnel, afin de respecter la conformité avec les exigences de traçabilité. En créant un accès aux contenus des messages des utilisateurs, une plate-forme ou un service administratif pourrait éventuellement examiner les messages envoyés par les utilisateurs, leur permettant ainsi d'identifier des contenus répréhensibles et le compte à l'origine du message.

De nombreuses techniques ont été proposées pour fournir un accès tiers aux communications chiffrées. Ces techniques comprennent :

12 https://signal.org/blog/sealed-sender/

- *Entiercement de clé* - Les clés utilisées pour déchiffrer les messages sont détenues (partiellement ou complètement) par un tiers (comme le fournisseur de la plate-forme) pour permettre l'accès aux contenus des communications chiffrées.
- *Participant fantôme* - Un tiers est silencieusement ajouté à une communication.
- *Analyse côté client* - Les communications ou les codes de hachage[13] créés à partir des communications sont examinés pour établir des correspondances avec une base de données de contenus avant l'envoi du message au destinataire prévu.

Cependant, le consensus parmi les experts, y compris les participants aux discussions de l'Internet Society, est que les méthodes d'accès pour les tierces parties auraient pour effet d'interrompre le chiffrement de bout en bout en permettant aux tierces parties d'accéder aux contenus, et affaibliraient la sécurité et la protection de la confidentialité des utilisateurs.

- **Un accès pour un utilisateur constitue un accès pour tous les utilisateurs.** Lorsqu'on donne à un tiers une méthode d'accès aux communications chiffrées des utilisateurs, de nouvelles vulnérabilités sont en fait introduites dans le système. Une fois identifiées par des acteurs malveillants, les mêmes méthodes utilisées pour fournir un accès aux forces de l'ordre ou aux plates-formes peuvent être utilisées pour des activités malveillantes. Par exemple, si un acteur malveillant obtient l'accès aux clés de déchiffrement entiercées, il est en mesure de déchiffrer toutes les communications envoyées par l'intermédiaire d'un système de communication. Il n'y a aucun moyen de garantir que les vulnérabilités créées par une méthode d'accès exceptionnelle ne tomberont pas entre de mauvaises mains.[14]

- **L'accès exceptionnel ne peut pas être ciblé, et affaiblit la sécurité pour tous les utilisateurs.** Lorsqu'un système est modifié pour permettre un accès exceptionnel, tous les utilisateurs sont exposés à un plus grand risque. Il n'est pas possible de fournir un accès exceptionnel à un utilisateur sans créer une vulnérabilité pour tous les utilisateurs. Par exemple, pour créer un participant fantôme, le processus de distribution de clés doit être modifié en distribuant secrètement les clés à des personnes n'appartenant pas à la discussion de groupe, et les prestataires doivent supprimer les notifications signifiant aux utilisateurs que des tiers non autorisés ont accès à leurs communications. En modifiant la distribution des clés et la notification dans un service de communication, la plate-forme introduit de nouvelles vulnérabilités qui pourraient être utilisées sur tous ses utilisateurs.[15]

- **L'analyse côté client introduit des vulnérabilités.** Pour certains, l'analyse côté client est sûre, particulièrement lorsque les communications sont hachées avant d'être comparées à une base de données de contenus répréhensibles. Cependant, cette méthode engendre encore des vulnérabilités qui mettent la sécurité et la vie privée des utilisateurs en danger. Les acteurs malveillants qui accèdent à une base de données de contenus peuvent ajouter de nouveaux contenus pour créer des faux positifs ou pour vérifier à qui, quand et où certains contenus ont été communiqués.[16] Les systèmes d'analyse côté client qui envoient les contenus de message à une tierce partie pour une revue manuelle, suite à une mise en correspondance avec une base de données, sont particulièrement dangereux car ils fournissent aux acteurs malveillants une nouvelle opportunité d'accéder aux communications non chiffrées.

- **Inquiétudes pour la sécurité nationale.** Si des pouvoirs publics ou un organisme de maintien de l'ordre pouvaient accéder aux communications d'un utilisateur, la même capacité serait disponible pour n'importe quel autre pays, y compris les pays adversaires. Les fonctionnaires et les organismes de maintien de l'ordre ne pourraient pas non plus accéder à des canaux de communication sécurisés et pourraient potentiellement devenir des cibles de surveillance pour leurs adversaires. De

13 Un code de hachage est une « empreinte » numérique fonctionnellement unique du contenu de l'utilisateur
14 https://www.schneier.com/academic/paperfiles/paper-keys-under-doormats-CSAIL.pdf
15 https://www.internetsociety.org/resources/doc/2020/fact-sheet-ghost-proposals/
16 https://www.internetsociety.org/resources/doc/2020/fact-sheet-client-side-scanning/

nombreuses administrations, y compris la Commission européenne et[17] les forces armées des États-Unis, [18]ont demandé à leurs employés d'utiliser des services de communication chiffrée de bout en bout de masse, dans le but de protéger leurs communications.

Conclusion

Dans le cadre du débat sur les règles applicables aux plates-formes numériques et aux prestataires de services de communication, la traçabilité va probablement continuer d'être un problème saillant en Inde. Toutefois, il existe des préoccupations crédibles concernant la sécurité, la confidentialité et l'efficacité des deux méthodes les plus souvent proposées pour permettre la traçabilité, à savoir **l'utilisation de signatures numériques** et **l'utilisation de métadonnées.** Pour respecter les exigences de traçabilité, les prestataires de services de communication seraient obligés d'accéder aux contenus des communications des utilisateurs entraînant ainsi une réduction considérable de la sécurité et de la confidentialité du système, pour tous les utilisateurs, et introduisant un risque accru pour la sécurité nationale.

Lorsque les décideurs politiques, les législateurs et les magistrats examinent les actions susceptibles de créer des exigences de traçabilité, ils doivent tenir compte des implications graves de l'exigence de conformité imposée aux fournisseurs de contenus et de services.

Remerciements
Nous sommes reconnaissants pour la participation de plus de 50 experts techniques et en politiques publiques de l'Asie-Pacifique, de l'Afrique, de l'Europe, de l'Amérique Latine et de l'Amérique du Nord, aux discussions des experts techniques mondiaux qui se sont déroulées entre juin et août 2020.

17 https://www.politico.eu/article/eu-commission-to-staff-switch-to-signal-messaging-app/
18 https://www.militarytimes.com/flashpoints/2020/01/23/deployed-82nd-airborne-unit-told-to-use-these-encrypted-messaging-apps-on-government-cellphones/