Position du VGT sur le chiffrement de bout en bout

Le Virtual Global Taskforce (VGT), une alliance internationale d'organismes d'application de la loi, constitue un Conseil de direction (CD) chargé de l'application de la loi. Le CD du VGT travaille avec les principaux organismes non gouvernementaux (ONG) et partenaires de l'industrie. Son mandat consiste à protéger les enfants contre l'exploitation sexuelle sur Internet et d'autres infractions sexuelles transnationales commises contre des enfants. L'un de ses objectifs stratégiques est d'aider le secteur privé à améliorer sa sécurité préventive en communiquant du renseignement sur la menace pour les enfants que posent l'exploitation et les sévices sexuels en ligne. Par conséquent, nous avons suivi avec intérêt les faits nouveaux concernant le chiffrement de bout en bout (E2EE), l'utilisation des technologies de chiffrement et leur incidence sur la capacité de détecter le matériel d'exploitation sexuelle des enfants (ESE) et les comportements de conditionnement sur les médias sociaux et les plateformes de messagerie.

La priorité des organismes d'application de la loi du monde entier, y compris des membres du VGT, est accordée aux victimes d'exploitation sexuelle des enfants sur Internet. Les victimes souffrent non seulement des effets physiques réels des sévices sexuels, mais également d'une victimisation continue par la production et la distribution de matériel d'ESE. De nombreuses victimes ont déclaré que la circulation continue de leurs sévices sexuels a des conséquences négatives pour elles, souvent tout au long de leur vie adulte. Le fait de trouver les victimes pour les secourir et la capacité d'empêcher la remise en circulation de matériel d'ESE sont des moyens positifs par lesquels les fournisseurs de service peuvent contribuer à prévenir la revictimisation à divers niveaux. Les efforts déployés par l'industrie pour empêcher les enfants de devenir des victimes par la détection des structures linguistiques qui indiquent un conditionnement ou d'une sollicitation pour le partage de matériel d'ESE sont également soutenus. Ces efforts peuvent également prévenir les agressions sexuelles à proprement dire.

Le VGT est conscient de l'effet négatif de l'E2EE sur la capacité des entreprises et des organismes d'application de la loi de lutter contre le crime que constitue l'exploitation sexuelle des enfants sur Internet. En 2020, le CyberTipline du National Centre for Missing and Exploited Children (NCMEC) des États-Unis a reçu plus de 21,4 millions de signalements de la part de fournisseurs de services électroniques, dont la plupart concernaient : du matériel d'ESE manifeste; la séduction en ligne, y compris l'extorsion sexuelle; la traite d'enfants à des fins sexuelles et l'atteinte à la pudeur dans l'enfance, 20,3 millions de ces signalements ont été reçus par Facebook. En 2018, Facebook Messenger était responsable de 12 millions des 18,4 millions de signalements de matériel d'ESE au NCMEC. L'Alliance mondiale WePROTECT a évalué en 2019 que ces signalements risquent de disparaître si l'E2EE est mis en œuvre, car les outils actuels utilisés pour détecter l'exploitation sexuelle des enfants sur Internet ne fonctionnent pas dans les environnements chiffrés de bout en bout. Au cours de la même année, le NCMEC a également publié une déclaration indiquant que « si le chiffrement de bout en bout est mis en œuvre sans qu'un plan ou une solution soit en place pour protéger les enfants, le NCMEC estime que plus de la moitié de ses signalements CyberTipline disparaîtront ».

Pour plus de clarté, la transmission de renseignements par l'industrie aux organismes d'application de la loi est basée sur les résultats des signalements des victimes, l'intelligence

artificielle (IA) et les modérateurs humains. Les membres de l'industrie veillent à protéger la vie privée de leurs utilisateurs, et ils utilisent presque tous l'AI pour signaler les comportements préoccupants qui peuvent être détectés sans consulter le contenu créé par les utilisateurs. En général, on a seulement recours aux modérateurs humains dans les espaces publics des plateformes de médias sociaux une fois qu'un utilisateur signale être victime ou témoin de sévices sexuels contre les enfants ou lorsque les indicateurs de l'AI atteignent un seuil élevé et nécessitent l'intervention de modérateurs humains.

Les méthodes de prévention proactives adoptées par les membres de l'industrie comprennent l'utilisation de logiciels et de listes de hachage pour repérer le matériel d'ESE connu afin d'empêcher les délinquants de télécharger du matériel qui a déjà été désigné comme étant criminel. Ils peuvent effectuer ce travail sans voir le contenu des communications des utilisateurs de la même manière que les logiciels antivirus sont utilisés. De plus, certaines entreprises utilisent des listes de blocage d'URL afin d'empêcher les utilisateurs de consulter intentionnellement ou accidentellement du matériel d'ESE et elles travaillent en étroite collaboration avec les lignes d'assistance internationales pour aider les entreprises à supprimer ce contenu illicite de leurs domaines et de leur infrastructure. Dans l'ensemble, les mesures prises par l'industrie sont soigneusement équilibrées avec la nécessité de protéger la vie privée des utilisateurs tout en accordant la priorité à la protection des enfants.

Certains fournisseurs de services Internet, développeurs d'applications et fabricants de dispositifs élaborent et lancent des produits et des services avec E2EE. Cela a pour effet d'empêcher les entreprises de détecter l'exploitation des enfants qui se produit sur leurs plateformes et de transmettre les cas détectés aux organismes d'application de la loi aux fins d'enquête, notamment en exécutant des mandats légaux en vue d'identifier les délinquants et les victimes. L'E2EE vise à empêcher les partenaires de l'industrie et d'autres d'accéder au contenu des utilisateurs en les obligeant à s'appuyer sur l'IA pour détecter les indicateurs de comportement au moyen de métadonnées. Il est possible de déduire beaucoup de renseignements à partir de métadonnées, mais celles-ci ne sont habituellement pas suffisantes pour atteindre le seuil requis afin d'obtenir un mandat de perquisition. Par ailleurs, les entreprises elles-mêmes avisent que, souvent, les personnes identifiées grâce à ces méthodes atteignent uniquement le seuil de la politique concernant la réception d'avertissements ou l'exclusion de certaines fonctions de la plateforme et ne déclenchent pas un signalement aux organismes d'application de la loi. En fin de compte, en raison de l'E2EE, les entreprises risquent de ne pas être en mesure de protéger adéquatement les enfants qui utilisent leurs services, car elles ne disposent pas de suffisamment de renseignements sur les comportements en ligne pour justifier la transmission de renseignements concernant des sévices possibles aux organismes d'application de la loi. En outre, il est beaucoup plus difficile de protéger les victimes dont les sévices ont déjà été enregistrés et pourraient être diffusés au moyen de services qui utilisent l'E2EE.

Le VGT exhorte toutes les parties concernées à prendre sérieusement en considération le droit à la vie privée des victimes directement touchées par ce crime tout en tenant compte des conséquences pour la société de réduire considérablement la capacité des organismes d'application de la loi d'enquêter sur les atteintes à ces droits et de secourir les enfants. Nous appuyons également la déclaration du Groupe des cinq et encourageons les entreprises

spécialisées dans la technologie à travailler avec les gouvernements pour prendre les mesures suivantes, axées sur des solutions raisonnables et techniquement réalisables :

- intégrer la sécurité du public dans la conception des systèmes, permettant ainsi aux entreprises d'agir efficacement contre le contenu et les activités illicites sans réduire la sécurité, et facilitant les enquêtes et les poursuites des infractions et la protection des personnes vulnérables;
- permettre aux organismes d'application de la loi d'accéder au contenu dans un format lisible et utilisable lorsqu'une autorisation est légalement délivrée, nécessaire et proportionnée et soumise à de solides garanties et à un contrôle strict;
- tenir des consultations avec les gouvernements et les autres intervenants pour faciliter l'accès légal d'une manière qui soit substantielle et qui influence réellement les décisions de conception.

Je vous remercie de votre attention.

Surintendante principale Marie-Claude Arsenault, Gendarmerie royale du Canada
Présidente du VGT