Interception légale des communications par les organismes de la sécurité et du renseignement : Les défis politiques et juridiques posés par la messagerie en temps réel sur les plateformes en ligne

Michael Geist
Chaire de recherche du Canada en droit de l'Internet et du commerce électronique
Université d'Ottawa, Faculté de droit

Mai 2024

Sommaire

La politique publique canadienne en matière d'accès légal vise depuis longtemps à garantir que les organismes d'application de la loi et de renseignement disposent d'un accès approprié aux informations à des fins d'enquête, tout en veillant à ce que la vie privée et l'application régulière de la loi soient pleinement respectées. Le débat juridique et politique a largement envisagé des communications qui placent les entreprises de communication canadiennes – fournisseurs de services de télécommunications, de services sans fil et d'accès à Internet – au centre de la chaîne de communication. La jurisprudence de la Cour suprême en matière de protection de la vie privée a progressivement érodé les justifications politiques de l'accès sans mandat aux informations des internautes recueillies et conservées par ces entreprises. Cela a augmenté la charge de travail des forces de l'ordre, qui doivent désormais obtenir une ordonnance d'un tribunal pour avoir accès aux informations souhaitées. Cependant, parallèlement à l'évolution de la législation sur les attentes raisonnables en matière de vie privée, une autre évolution a transformé l'importance relative de la politique concernant l'accès légal : l'émergence de services de messagerie basés sur Internet qui rendent l'accès des autorités policières encore plus difficile.

La gamme de services de messagerie et de médias sociaux sur Internet est en constante évolution, de nouveaux services attirant des centaines de millions d'utilisateurs et faisant compétition aux services établis les plus populaires. Le présent rapport vise les services les plus importants, dont certains comptent des milliards d'utilisateurs dans le monde. La recherche pour chaque entreprise a comporté plusieurs éléments. Premièrement, un examen complet de toutes les politiques accessibles au public, y compris les informations relatives à la collecte et à la conservation des données, au chiffrement, aux réponses aux demandes des forces de l'ordre, aux lois applicables et aux normes en matière de preuve. Deuxièmement, une analyse des rapports de transparence accessibles au public pour chaque entreprise, le cas échéant. Troisièmement, un examen de la jurisprudence et des sources secondaires a été effectué afin de déterminer les cas pertinents ou d'autres informations accessibles au public.

Parmi ces services, le rapport passe d'abord en revue quatre grands services de messagerie : WhatsApp, Signal, Telegram et Viber. Ce qu'il faut retenir à propos de ces services, c'est que la plupart des contenus ne sont pas stockés sur les serveurs de l'entreprise et que l'utilisation du chiffrement limite encore l'accès potentiel au contenu des messages des utilisateurs. Les entreprises peuvent être en mesure de fournir des informations non liées au contenu concernant les abonnés, sous réserve d'une procédure de communication des informations supervisée par un tribunal.

Trois services de médias sociaux dotés d'une fonction de messagerie sont ensuite abordés : X (anciennement Twitter), TikTok et Snap. La différence entre un service de médias sociaux avec messagerie et un service de messagerie devient immédiatement évidente. Contrairement aux services de messagerie qui ne conservent pas le contenu ou ne déploient pas de chiffrement limitant l'accès, ces services de médias sociaux conservent généralement beaucoup plus d'informations sur le contenu, y compris dans le cadre de leur fonctionnalité de messagerie. Les entreprises doivent donc faire face à un nombre beaucoup plus important de demandes d'informations sur les clients de la part des forces de l'ordre, appliquer des politiques plus

strictes et traiter des questions telles que la conservation des données et le respect de la législation sur la protection de la vie privée.

Enfin, le rapport passe également en revue les trois plus importants géants de la technologie qui offrent également des fonctionnalités de messagerie ou de courriel : Google, Apple, et Microsoft. La principale différence entre les géants de la technologie et les services de médias sociaux dotés d'une fonction de messagerie est l'ampleur des données recueillies par les géants.

Le rapport décrit six questions clés qui devraient être au cœur de l'analyse opérationnelle ou de l'élaboration des politiques futures, compte tenu du rôle essentiel joué par les services de messagerie. Il s'agit notamment des défis posés par les applications servant uniquement à la messagerie, des limites de la communication obligatoire des informations, des problèmes de compétence, des politiques incohérentes, du chiffrement, ainsi que de l'incertitude et de la transparence.

Introduction

La politique publique canadienne en matière d'accès légal vise depuis longtemps à garantir que les organismes d'application de la loi et de renseignement disposent d'un accès approprié aux informations à des fins d'enquête, tout en veillant à ce que la vie privée et l'application régulière de la loi soient pleinement respectées. Le débat juridique et politique a largement envisagé des communications qui placent les entreprises de communication canadiennes – fournisseurs de services de télécommunications, de services sans fil et d'accès à Internet – au centre de la chaîne de communication. Avant la décision de la Cour suprême du Canada dans l'arrêt *Spencer*, les politiques adoptées par ces fournisseurs régissaient généralement le processus de communication des informations, notamment les circonstances dans lesquelles les données seraient fournies, les conditions sous lesquelles elles le seraient et les délais à respecter.

Ces dernières années, la chaîne de communication s'est considérablement élargie, les fournisseurs de services de télécommunications continuant à fournir les moyens d'accès au réseau, mais jouant un rôle moindre dans le contenu des communications elles-mêmes. Cela signifie souvent que les fournisseurs peuvent être en mesure de confirmer les détails relatifs à l'accès, mais avoir peu d'informations sur bien d'autres aspects. Ce sont plutôt les plateformes en ligne et les services de communication en temps réel qui jouent un rôle essentiel en facilitant les communications réseaucentriques grâce à des services qui incluent le clavardage et la messagerie synchrones et asynchrones. Ces entreprises sont rarement basées au Canada, appliquent divers degrés de chiffrement, peuvent établir des normes différentes en matière de communication des informations aux organismes d'application de la loi et publient fréquemment des rapports de transparence détaillés.

Le présent rapport de recherche servira de point de départ à l'élaboration d'une politique relative à ces services. Il est divisé en trois parties. La première partie présente le contexte historique de l'accès légal et du débat politique qui a fait rage au Canada pendant près de vingt ans. La deuxième partie identifie les principaux services de messagerie, répartis en trois groupes : les services de messagerie, les services de médias sociaux dotés d'une fonctionnalité de messagerie et les géants de la technologie. La troisième partie présente des recommandations pour la réforme des politiques et la mobilisation sur la base de l'analyse précédente. Le rapport

comprend également une annexe contenant des données précises sur chaque entreprise pour de nombreux indicateurs, notamment les demandes des gouvernements et des forces de l'ordre, les processus de demande, les types de demande, les données sur les clients, les politiques de conservation et les pratiques de chiffrement.

I. Contexte historique

1. Propositions législatives sur l'accès légal

Le mouvement en faveur de nouvelles capacités de surveillance d'Internet remonte à 1999, lorsque des représentants du gouvernement ont commencé à élaborer des propositions visant à mettre en place de nouvelles technologies de surveillance au sein des réseaux canadiens, ainsi que des pouvoirs supplémentaires conférés par la loi permettant d'avoir accès aux informations relatives à la surveillance et aux abonnés.

Un projet de loi présenté en 2010 contenait une approche à trois volets axée sur la communication d'informations, les technologies de surveillance obligatoires et de nouveaux pouvoirs pour les services de police. Aux fins du présent rapport, c'est le premier volet, qui imposait la communication d'informations sur les clients des fournisseurs d'accès à Internet sans la supervision du tribunal, qui est le plus pertinent. En vertu de la législation sur la protection de la vie privée en vigueur à l'époque, les fournisseurs pouvaient volontairement communiquer des informations sur leurs clients, mais n'étaient pas tenus de le faire. Le nouveau système aurait exigé la communication du nom, de l'adresse, du numéro de téléphone, de l'adresse courriel, de l'adresse de protocole Internet (adresse IP) et d'une série de numéros d'identification de l'appareil du client.

Bien que certaines de ces informations aient pu sembler relativement inoffensives, on craignait que la possibilité de les relier à d'autres données n'ouvre souvent la porte à un profil détaillé d'une personne identifiable. Compte tenu de son caractère potentiellement sensible, la décision d'exiger la communication sans aucun contrôle a suscité des inquiétudes au sein de la communauté canadienne de la protection de la vie privée.

Ce projet de loi n'a pas abouti, mais en février 2012, Vic Toews, alors ministre de la Sécurité publique, a présenté un projet de loi sur la surveillance d'Internet qui a une fois de plus suscité de nombreuses critiques de la part de l'ensemble de la communauté de la politique. L'énorme publicité négative a poussé le gouvernement à faire rapidement marche arrière en mettant le projet en attente. En 2013, le ministre de la Justice de l'époque, Rob Nicholson, a annoncé l'abandon du projet de loi, confirmant que « nous ne poursuivrons pas l'étude du projet de loi C-30, et les mesures contenues dans ce projet de loi seront exclues de toute tentative à venir de modernisation du *Code criminel*[1]. »

L'engagement de Nicholson a duré moins d'un an. En 2014, Peter MacKay, alors nouveau ministre fédéral de la Justice, a dévoilé le projet de loi C-13, présenté comme un effort pour lutter contre la cyberintimidation. Pourtant, la grande majorité du projet de loi reprend de nombreuses dispositions relatives à l'accès légal qui figuraient dans le projet précédent (mais pas

[1] https://www.cbc.ca/news/politics/government-killing-online-surveillance-bill-1.1336384 [en anglais seulement]

toutes). Par exemple, le projet de loi encourage les entreprises de télécommunications et les fournisseurs d'accès à Internet à révéler des informations sur leurs clients aux forces de l'ordre sans ordonnance d'un tribunal, en leur accordant une immunité de responsabilité criminelle ou civile pour de telles divulgations.

2. Spencer

Alors que le gouvernement présentait des projets de loi successifs en matière d'accès légal, la Cour suprême du Canada érodait progressivement les fondements de la politique en renforçant les protections de la vie privée. Par exemple, malgré les affirmations selon lesquelles les métadonnées ne présentent que peu d'intérêt en matière de vie privée, la Cour a statué dans l'arrêt *R. c. Vu* que « dans le contexte d'une enquête criminelle, toutefois, ils peuvent également permettre aux enquêteurs d'avoir accès à des détails intimes concernant les intérêts, les habitudes et l'identité de l'utilisateur, à partir d'un dossier que ce dernier a créé sans le savoir[2] ».

Plus important encore, en 2014, la Cour a rendu son arrêt *R. c. Spencer*[3], qui a largement mis fin au débat sur la question de savoir s'il existe une attente raisonnable en matière de vie privée pour les informations de base relatives aux abonnés. Tout d'abord, la Cour a reconnu l'existence d'un intérêt en matière de vie privée pour les informations relatives aux abonnés. Bien que le gouvernement ait toujours cherché à minimiser cet intérêt, la Cour a estimé que les informations étaient bien plus qu'un simple nom et une adresse, en particulier dans le contexte d'Internet. Comme l'indique la Cour :

Internet a augmenté de façon exponentielle la qualité et la quantité des renseignements stockés concernant les internautes. L'historique de navigation, par exemple, permet d'obtenir des renseignements détaillés sur les intérêts des utilisateurs. Les moteurs de recherche peuvent recueillir des renseignements sur les termes recherchés par les utilisateurs. Les annonceurs peuvent suivre leurs utilisateurs à travers les réseaux de sites Web et obtenir un aperçu de leurs intérêts et de leurs préoccupations. Les fichiers témoins peuvent être utilisés pour suivre les habitudes de consommation et peuvent fournir des renseignements sur les options sélectionnées dans un site Web, sur les pages Web consultées avant et après avoir visité le site d'accueil et tout autre renseignement personnel fourni. L'utilisateur n'est pas en mesure d'exercer un contrôle total à l'égard de la personne qui peut observer le profil de ses activités en ligne et il n'est pas toujours informé de l'identité de celle-ci. Or, sous le couvert de l'anonymat – en protégeant le lien entre l'information et l'identité de la personne qu'elle concerne –, l'utilisateur peut en grande partie être assuré que ses activités demeurent confidentielles[4].

Compte tenu de toutes ces informations, l'intérêt en matière de vie privée va bien au-delà du simple nom et de l'adresse.

Deuxièmement, la Cour a élargi les aspects informationnels de la vie privée, en concluant qu'il existe trois facettes conceptuellement distinctes : le secret, le contrôle et l'anonymat. C'est l'anonymat qui est particulièrement remarquable, car la Cour a reconnu son importance dans le contexte de l'utilisation d'Internet. Compte tenu de l'importance des informations et de la

[2] 2013 CSC 60.
[3] 2014 CSC 43.
[4] *Ibid*., par. 46.

possibilité d'établir un lien entre des activités anonymes sur Internet et une personne identifiable, un niveau élevé de protection de la vie privée est en jeu.

Troisièmement, non seulement existe-t-il un intérêt important en matière de vie privée, mais la Cour a conclu qu'il existe également une attente raisonnable en matière de vie privée de la part de l'utilisateur. Le tribunal examine à la fois la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) et les conditions d'utilisation de Shaw (le fournisseur d'accès à Internet en l'espèce) et conclut que la LPRPDE doit être comprise dans le contexte de la protection de la vie privée et que l'accord du fournisseur d'accès à Internet est pour le moins confus et peut soutenir l'attente de protection de la vie privée. C'est dans cette optique qu'elle a déclaré :

compte tenu de l'ensemble des circonstances de la présente affaire, il existe une attente raisonnable en matière de vie privée à l'égard des renseignements relatifs à l'abonnée. La communication de ces renseignements permettra souvent d'identifier l'utilisateur qui mène des activités intimes ou confidentielles en ligne en tenant normalement pour acquis que ces activités demeurent anonymes. La demande faite par un policier visant la communication volontaire par le FSI de renseignements de cette nature constitue donc une fouille[5].

Quatrièmement, ayant conclu que l'obtention d'informations sur les abonnés constituait une fouille ou une perquisition dans le cadre d'une attente raisonnable en matière de vie privée, les informations ont été obtenues de manière inconstitutionnelle, ce qui a mené à la conclusion qu'il s'agissait d'une fouille ou d'une perquisition illégale. En ce qui concerne l'incidence de la clause de divulgation volontaire de la LPRPDE, qui était couramment utilisée par les fournisseurs d'accès à Internet à l'époque, la Cour a noté :

Puisque, en l'espèce, les policiers n'avaient pas le pouvoir d'effectuer une fouille ou une perquisition pour obtenir des renseignements relatifs à l'abonnée en l'absence de circonstances contraignantes ou d'une loi qui n'a rien d'abusif, je ne vois pas comment ils pourraient obtenir un nouveau pouvoir en matière de fouille ou de perquisition par l'effet combiné d'une disposition déclaratoire et d'une disposition adoptée afin de favoriser la protection des renseignements personnels[6].

Cette décision a entraîné une réforme importante de l'approche des fournisseurs d'accès à Internet en ce qui concerne la communication des informations relatives aux abonnés. En effet, la Cour suprême a examiné les conditions d'utilisation des services de Shaw et a constaté qu'elles « prêt [aient] à confusion quant à la manière de Shaw de répondre à une demande de renseignements relatifs à un abonné adressée par la police ». Bien que les fournisseurs aient régulièrement communiqué ces informations des centaines de milliers de fois, la Cour a statué :

Puisque la LPRPDE a pour objet de fixer des règles régissant, entre autres, la communication de « renseignements personnels d'une manière qui tient compte du droit des individus à la vie privée à l'égard des renseignements personnels qui les concernent » (art. 3), il serait raisonnable que l'internaute s'attende à ce qu'une simple demande faite par la police n'entraîne pas l'obligation de communiquer les renseignements personnels en question ou qu'elle n'écarte

[5] *Ibid*., par. 66.
[6] *Ibid*., par. 73.

pas l'interdiction générale prévue par la LPRPDE quant à la communication de renseignements personnels sans le consentement de l'intéressé[7].

La Cour a remarqué que les fournisseurs d'accès à Internet n'étaient pas tenus de communiquer ces informations et a conclu qu'ils n'étaient pas non plus autorisés à le faire en l'absence d'un mandat.

3. Bykovets

L'arrêt Spencer portait sur l'attente raisonnable en matière de vie privée associée aux informations de base sur les abonnés. La Cour suprême a élargi son analyse en 2024 en examinant les attentes en matière de vie privée pour les adresses IP dans l'arrêt *R. c. Bykovets*[8]. Les adresses IP, qui sont une chaîne de nombres reliée à un emplacement précis dans Internet, étaient auparavant considérées comme présentant un intérêt encore plus faible en matière de vie privée que les informations relatives aux abonnés. Toutefois, la Cour a jugé qu'il existait également une attente raisonnable en matière de vie privée, soulignant la manière dont l'adresse IP peut être utilisée pour établir un lien avec d'autres informations personnelles :

Considérer l'objet de la présente fouille comme une chaîne abstraite de chiffres utilisée uniquement pour obtenir un mandat de type Spencer va à l'encontre de ces précédents. Les adresses IP ne sont pas simplement des numéros dénués de sens. En tant que lien qui relie une activité Internet à un endroit donné, les adresses IP sont plutôt susceptibles de révéler des renseignements très personnels – y compris l'identité de l'utilisateur de l'appareil – sans jamais faire naître l'obligation d'un mandat. L'activité en ligne précise associée à la fouille effectuée par l'État peut elle-même tendre à révéler des renseignements très privés. Lorsqu'elle est mise en corrélation avec d'autres renseignements en ligne qui y sont associés, comme ceux que fournissent de leur plein gré des sociétés privées ou que recueille autrement l'État, une adresse IP peut révéler un éventail d'activités en ligne très personnelles. De plus, lorsqu'elle est associée aux profils créés et conservés par des tiers du secteur privé, les risques en matière de vie privée liés aux adresses IP augmentent de façon exponentielle. L'information que recueillent, agrègent et analysent ces tiers leur permet de répertorier nos renseignements biographiques les plus intimes. Considérée de manière normative et dans son contexte, une adresse IP est le premier fragment numérique qui peut mener l'État sur la trace de l'activité Internet d'une personne. Elle est susceptible de révéler des renseignements personnels bien avant qu'un mandat de type Spencer ne soit sollicité[9].

À la lumière de cette analyse, la Cour a conclu qu'un mandat était également nécessaire dans ce cas :

En tant qu'élément inhérent crucial dans la structure d'Internet, une adresse IP est la clé susceptible de guider l'État dans le labyrinthe de l'activité Internet d'un utilisateur ainsi que le lien par lequel des intermédiaires peuvent fournir de leur plein gré à l'État des renseignements relatifs à cet utilisateur. Par conséquent, l'art. 8 devrait protéger les adresses IP. Cela aurait pour effet de préserver le premier « fragment numérique » et d'obscurcir la trace du parcours

[7] *Ibid*., par. 62.
[8] 2024 CSC 6.
[9] *Ibid*., par. 9.

d'un internaute dans le cyberespace; cela aurait également pour effet de favoriser la réalisation de l'objectif de l'art. 8 consistant à empêcher les possibles atteintes à la vie privée plutôt que de circonscrire sa portée suivant les intentions déclarées de l'État quant à la manière dont il utilisera cette clé[10].

Bien que les effets de l'arrêt *Bykovets* ne se soient pas encore fait pleinement sentir, il semble probable que cet arrêt limitera davantage l'accès sans mandat aux informations Internet pouvant être communiquées par les entreprises de télécommunications et d'Internet.

La jurisprudence de la Cour suprême en matière de protection de la vie privée a progressivement érodé les justifications politiques de l'accès sans mandat aux informations des utilisateurs d'Internet recueillies et conservées par les entreprises d'Internet et de télécommunications. Cela a augmenté la charge de travail des forces de l'ordre, qui doivent désormais généralement obtenir une ordonnance d'un tribunal pour avoir accès aux informations souhaitées. Cependant, parallèlement à l'évolution de la législation sur l'attente raisonnable en matière de vie privée, une autre évolution a transformé l'importance relative de la politique d'accès légal : l'émergence de services de messagerie basés sur Internet qui peuvent rendre l'accès des forces de l'ordre encore plus difficile.

II. Politiques sur les services de messagerie et de médias sociaux

Les services de messagerie et de médias sociaux fournis sur Internet sont en constante évolution. De nouveaux services attirent des centaines de millions d'utilisateurs et constituent un défi pour les chefs de file établis. Cette étude couvre les services les plus importants, dont certains comptent des milliards d'utilisateurs dans le monde entier. Alors que la proposition initiale de cette étude se limitait en grande partie à des services tels que Twitter (aujourd'hui X), Snap, WhatsApp, Signal et Viber, des recherches plus approfondies ont montré que ce groupe de services ne permettait pas de saisir toute l'étendue du marché et les défis auxquels les autorités policières et gouvernementales sont confrontées lorsqu'elles présentent une demande d'accès aux renseignements issus des communications comme elles présentent une demande d'accès légal auprès des entreprises de communication nationales. La recherche a donc été considérablement élargie en supprimant un service (Slack, qui ne correspondait pas exactement au paradigme de service de messagerie et de médias sociaux en tant que service de messagerie interne) et en incluant un éventail beaucoup plus large de services, dont Telegram, Snap, TikTok, Google, Apple et Microsoft.

La recherche menée pour chaque entreprise comportait plusieurs éléments. D'abord, un examen complet de toutes les politiques accessibles au public, y compris les informations relatives à la collecte et à la conservation des données, au chiffrement, aux réponses aux demandes des autorités policières, aux lois applicables et aux normes en matière de preuve. Ensuite, une analyse des rapports de transparence accessibles au public pour chaque entreprise lorsqu'ils sont disponibles. Ces rapports fournissent des renseignements supplémentaires sur la manière dont les politiques sont mises en œuvre ainsi que des données agrégées sur les demandes et les réponses. Dans certains cas, les données sont propres au Canada. Enfin, un examen de la jurisprudence et

[10] *Ibid*., par. 13.

des sources secondaires a été effectué afin de déterminer les cas pertinents ou d'autres renseignements accessibles au public. Cet examen a permis de relever certains cas et rapports médiatiques pertinents, notamment une décision québécoise concernant Snap qui traite tout spécialement des questions pertinentes à la présente étude. Toutes les données sont à jour par rapport aux données publiées en janvier 2024, bien que les données réelles puissent référer à des pratiques remontant à 2021-2022.

Les résultats de cette recherche sont présentés ci-dessous, entreprise par entreprise, et regroupés en trois catégories : les services de messagerie, les services de médias sociaux dotés d'une fonctionnalité de messagerie et les géants du Web, c'est-à-dire Apple, Google et Microsoft, qui proposent tous des services de messagerie dans le cadre d'une gamme beaucoup plus large de produits et de services. Une annexe à ce rapport présente les données brutes compilées au cours de la phase de recherche.

i. Services de messagerie

Cette section passe en revue quatre grands services de messagerie : WhatsApp, Signal, Telegram et Viber. Ces services comptent, collectivement, des milliards d'utilisateurs. Ce qu'il faut retenir de ces services, c'est que la plupart des contenus ne sont pas stockés sur les serveurs de l'entreprise et que l'utilisation du chiffrement limite encore l'accès potentiel au contenu des messages des utilisateurs. Les entreprises peuvent être en mesure de fournir des informations non liées au contenu concernant les abonnés, sous réserve d'une procédure de communication sous la surveillance du tribunal.

1. WhatsApp[11]

WhatsApp est le service de messagerie le plus populaire au monde. Racheté par Meta (alors Facebook) en 2014, le service compte actuellement quelque trois milliards d'utilisateurs. WhatsApp ne peut pas produire et ne produit pas le contenu des messages de ses utilisateurs pour répondre aux demandes gouvernementales. Le contenu de tous les messages envoyés à l'aide de WhatsApp est protégé par un protocole de chiffrement qui sécurise les messages avant qu'ils ne quittent l'appareil de l'utilisateur, garantissant ainsi que seuls l'utilisateur et le destinataire peuvent écouter ou lire le message. Il n'y a donc aucun intermédiaire, pas même WhatsApp.

Bien que le contenu ne puisse pas être communiqué, WhatsApp communique des renseignements de base sur les abonnés, tels que le nom, la date de début du service, la date de la dernière consultation, l'adresse IP, le type d'appareil et l'adresse courriel. En outre, les renseignements relatifs au compte, comme les renseignements « à propos de » l'utilisateur, les photos de profil, les renseignements sur les groupes et la liste des contacts, sont conservés par l'entreprise et susceptibles d'être communiqués. Afin de se conformer aux demandes d'accès légal, WhatsApp enregistre, après approbation, les messages et les journaux d'appels d'un utilisateur particulier, en indiquant le nom de la personne à qui la communication était destinée ou de qui elle provenait, l'heure à laquelle elle a été transmise et à partir de quelle adresse IP, ainsi que le type de communication (texte ou appel, par exemple).

[11] https://faq.whatsapp.com/808280033839222

WhatsApp publie les demandes et les réponses deux fois par an dans le rapport sur les demandes de données présentées par le gouvernement de Meta. Il s'agit d'un rapport global. Au cours des six premiers mois de 2022, les autorités canadiennes ont envoyé 1 149 demandes d'accès légal à WhatsApp ainsi que 1 710 demandes de communication d'urgence supplémentaires. Ces demandes concernaient 4 150 comptes d'utilisateurs et 83,70 % d'entre elles ont donné lieu à la production de données[12].

WhatsApp dispose d'une équipe de réponse aux autorités policières (Law Enforcement Response Team [LERT]) dédiée et formée qui examine et évalue chaque demande de données de l'utilisateur présentée par le gouvernement, que la demande ait été présentée dans le cadre d'une situation d'urgence ou d'un processus judiciaire intenté par les autorités policières ou gouvernementales. Pour prendre une décision sur les demandes de communication, WhatsApp examine le droit applicable, les normes reconnues à l'échelle internationale, telles que les normes relatives aux droits de la personne, l'application régulière de la loi et la règle de droit. Une demande relative à un traité d'entraide juridique ou des commissions rogatoires peuvent être nécessaires pour les demandes internationales. Si des données sont communiquées, les utilisateurs en sont avisés, sauf dans les cas d'exploitation d'enfants et de danger de mort. WhatsApp peut préserver les données sur les clients en réponse à une demande de préservation valable, mais elle n'a pas communiqué publiquement le délai de préservation.

2. *Signal*[13]

Signal est un service de messagerie chiffrée. Créé en 2010, Signal est aujourd'hui géré par la Signal Foundation, soutenue par Brian Acton, cofondateur de WhatsApp. En 2022, le nombre d'utilisateurs de Signal était estimé à 40 millions dans le monde entier.

Signal utilise un modèle de chiffrement de bout en bout par défaut, ce qui signifie que les messages ne sont pas stockés. Signal est donc incapable d'accéder à pratiquement tous les détails concernant ses utilisateurs, y compris les messages, les listes de clavardage, les groupes, les contacts ou même les noms de profil. Signal ne rend pas compte des demandes d'accès légal, maintenant son incapacité à répondre à ces demandes.

Bien que Signal ne fournisse pas de données liées au contenu, le service de messagerie fournit des données non liées au contenu, comme la date d'inscription et la date de la dernière connexion à ses serveurs, à la réception d'une ordonnance valide d'un tribunal.

3. *Telegram*[14]

Telegram a été lancé en 2013 par deux frères russes qui avaient auparavant fondé VK, un service de médias sociaux russe. L'entreprise est désormais enregistrée aux îles Vierges britanniques et à Dubaï à titre de société à responsabilité limitée. Le service compte 900 millions d'utilisateurs et envisage de devenir une société ouverte[15].

---

[12] https://transparency.fb.com/data/government-data-requests/country/CA/
[13] https://signal.org/legal/
[14] https://telegram.org/privacy?setln=it
[15] https://www.ft.com/content/8d6ceb0d-4cdb-4165-bdfa-4b95b3e07b2a

Telegram propose deux principaux types de messages, qui sont tous deux chiffrés, mais diffèrent en ce qui concerne l'accès possible de l'entreprise. Tout d'abord, les clavardages en nuage sont stockés sur les serveurs de Telegram. Telegram conserve les clés de chiffrement dans un lieu physique et un pays différents de ceux où le message chiffré est stocké. Ensuite, les clavardages secrets sont chiffrés à l'aide d'une clé connue uniquement de l'expéditeur et du destinataire. Les clavardages secrets ne sont pas stockés sur les serveurs de Telegram.

Telegram peut accéder aux données de l'utilisateur suivantes :

- le numéro de téléphone;
- le nom de profil (qui n'a pas à être le vrai nom);
- la photo de profil;
- les renseignements sur le profil figurant sous « À propos de »;
- l'adresse courriel, si elle est utilisée pour l'authentification à deux facteurs;
- les données de localisation, si elles sont communiquées dans un clavardage en nuage.

Telegram maintient qu'elle ne communiquera les informations de l'utilisateur que si un tribunal le soupçonne de terrorisme. Bien que la société soutienne n'avoir jamais communiqué les données de ses clients, un rapport du magazine *Der Spiegel* datant de 2022 affirme que Telegram a partagé des données avec la police allemande dans des cas de violence envers les enfants et de terrorisme[16].

4. Viber[17]

Viber est un service de messagerie instantanée et vocale fondé à l'origine en Israël et détenu depuis 2014 par Rakuten, une entreprise japonaise. Le service compte environ 1,3 milliard d'utilisateurs et il est particulièrement populaire dans les pays d'Europe de l'Est.

L'accès qu'a l'entreprise aux données liées au contenu se limite aux messages non délivrés. Dans les autres cas, les données liées au contenu sont chiffrées de bout en bout et ne peuvent pas être déchiffrées par Viber. Les données liées au contenu sont déchiffrées uniquement par l'expéditeur et le destinataire. Viber peut communiquer les données sur les clients aux autorités policières en réponse à des demandes relatives à des activités susceptibles de comporter un risque de responsabilité légale pour Viber ou le client. L'entreprise communique des renseignements aux autorités policières, aux organismes gouvernementaux ou à des tiers autorisés en réponse à une demande vérifiée concernant des actes terroristes, des enquêtes criminelles, des activités illégales présumées ou toute autre activité. Les données non liées au contenu que détient l'entreprise sont les suivantes :

- le numéro de téléphone cellulaire;

[16] https://www.spiegel.de/netzwelt/apps/telegram-gibt-nutzerdaten-an-das-bundeskriminalamt-a-0e4d3fcb-8081-4b87-b062-db412bbc294b
[17] https://www.viber.com/fr/terms/viber-public-content-policy/

- le nom;
- l'adresse courriel;
- la liste des contacts;
- l'adresse IP;
- les identifiants des appareils.

Dans sa politique, Viber indique qu'elle avise les utilisateurs de la soumission d'une demande des autorités policières avant de communiquer tout enregistrement de compte, sauf dans les cas suivants : i) la transmission d'un avis est interdite en vertu de la réglementation applicable, d'une ordonnance d'un tribunal, d'une assignation à témoigner ou de tout autre processus judiciaire; ii) une situation d'urgence se produit et la transmission d'un avis pourrait entraîner un risque important (p. ex. des blessures ou la mort) pour une personne ou un groupe de personnes; ou iii) une situation d'urgence pourrait causer un préjudice à des personnes mineures. Viber honorera les demandes de préservation pendant une période de 90 jours, et elle acceptera les demandes de prolongation pour une période supplémentaire de 90 jours.

ii. Services de médias sociaux dotés d'une fonctionnalité de messagerie

Trois services de médias sociaux offrant une fonctionnalité de messagerie sont abordés dans cette partie : X (anciennement Twitter), TikTok et Snap. Ces services extrêmement populaires ne sont pas axés sur la messagerie de personne à personne, mais chacun d'entre eux la propose. La différence entre un service de médias sociaux avec messagerie et un service de messagerie ressort immédiatement à l'examen des données. À la différence des services de messagerie qui ne conservent pas le contenu ou ne déploient pas de chiffrement limitant l'accès, ces services de médias sociaux conservent généralement beaucoup plus d'informations basées sur le contenu, y compris dans le cadre de leur fonctionnalité de messagerie. Les entreprises reçoivent donc un nombre beaucoup plus important de demandes de renseignements sur les clients de la part des autorités policières, appliquent des politiques plus rigoureuses et traitent de questions telles que la conservation des données et la conformité aux exigences relatives au respect de la vie privée.

1. X (anciennement Twitter)[18]

X, anciennement connu sous le nom de Twitter, est un service de médias sociaux de microblogage très populaire. Actuellement détenu par Elon Musk, le service a connu des transformations spectaculaires avec les changements de propriétaire, de sorte que certaines politiques de l'entreprise ne reflètent peut-être plus pleinement ses pratiques. Le service compte actuellement plus de 500 millions d'utilisateurs actifs. Twitter publie deux fois par année des rapports sur toutes les demandes d'accès légal qu'il reçoit[19].

Les données non liées au contenu que détient l'entreprise sont les suivantes :

- le nom affiché;
- le nom d'utilisateur;

[18] https://help.x.com/fr/rules-and-policies/x-law-enforcement-support
[19] https://transparency.x.com/fr.html

- le courriel;
- le numéro de téléphone;
- les modes de paiement;
- l'adresse IP.

Les données liées au contenu comprennent :

- les gazouillis;
- les images;
- les messages directs.

X applique les pratiques exemplaires de l'industrie en matière de chiffrement des données inactives et en cours de transfert. Les applications de X doivent utiliser le chiffrement pour se connecter à l'API X.

X examine les demandes d'accès légal relatives aux données sur les clients lorsque ces demandes sont fondées en droit. X examine les demandes d'accès d'urgence dans les situations où elle croit que la communication des données est nécessaire pour empêcher qu'une personne ne meure ou pour éviter un préjudice physique grave. X honorera les demandes de préservation pendant une période de 90 jours, et peut, à sa discrétion, honorer les demandes de prolongation de la période de préservation.

L'entreprise gère les comptes d'utilisateurs à partir de deux emplacements. En raison du Groupe des représentants permanents suppléants sur la mise en lecture publique de documents OTAN (GDPR), les comptes européens sont gérés depuis Dublin, en Irlande, tandis que tous les autres renseignements personnels sont gérés depuis San Francisco, en Californie. Indépendamment du lieu, il faut un mandat de perquisition pour les messages directs, les photos et les gazouillis. En règle générale, X avise le titulaire du compte lorsque son compte fait l'objet d'un mandat de perquisition. Toutefois, à l'instar d'autres plateformes, il existe des exceptions lorsque la loi l'interdit ou lorsque la sécurité est en jeu. X facilite également les demandes de communication d'urgence, qui sont évaluées au cas par cas et doivent atteindre le seuil de « situation d'urgence comportant un danger de mort ou de préjudice physique grave pour une personne ».

Les politiques de conservation des données de X reflètent les pratiques du GDPR. X affirme ne conserver que les données des comptes désactivés pendant une très courte période, après quoi le contenu n'est plus disponible. En outre, le contenu supprimé par le titulaire d'un compte (p. ex. un gazouillis supprimé) n'est pas disponible.

2. *TikTok*[20]

TikTok est un service de médias sociaux populaire axé sur les vidéos de courte durée. La messagerie entre utilisateurs est une fonctionnalité du service. TikTok provient de la Chine, où le service exerce toujours ses activités sous le nom de Douyin. La version non chinoise du service est gérée depuis Singapour et Los Angeles, en Californie, bien que le rôle du gouvernement

[20] https://www.tiktok.com/legal/page/global/law-enforcement/fr

chinois fasse l'objet d'un débat sérieux et ait donné lieu à une interdiction de l'application dans certains endroits. Les versions chinoise et non chinoise sont actuellement détenues par ByteDance. Le gouvernement canadien interdit l'utilisation du service sur les appareils qui sont délivrés par le gouvernement.

Les données non liées au contenu que détient l'entreprise peuvent comprendre :

- le nom d'utilisateur;
- l'adresse courriel;
- le numéro de téléphone;
- la date de création du compte;
- les registres des adresses IP;
- les date et heure de création des vidéos.

Voici quelques exemples de données liées au contenu :

- le contenu vidéo;
- les commentaires;
- les messages directs.

Les données inactives et en cours de transfert sont chiffrées. Les clés de chiffrement sont gérées par l'équipe de sécurité de TikTok basée aux États-Unis.

TikTok a trois types de demandes : les demandes d'accès légal, les demandes d'accès d'urgence et les demandes de préservation. Toutes les demandes présentées par les autorités policières canadiennes doivent être adressées à TikTok PTE Limited, l'entité juridique singapourienne. L'entreprise indique qu'il peut être nécessaire pour les organismes d'application de la loi situés en dehors de Singapour de s'appuyer sur des traités d'entraide juridique plutôt que d'adresser une demande directement à TikTok.

Les demandes d'accès légal nécessitent des renseignements sur l'organisme d'application de la loi, le fondement juridique de la demande et les données précises de l'utilisateur qui sont demandées. Des demandes d'accès d'urgence peuvent être présentées dans les cas qui concernent la sécurité d'un enfant, la disparition d'une personne ou une menace imminente de violence. TikTok a pour politique d'aviser le titulaire du compte lorsque ses données sont communiquées aux autorités policières, sauf si l'entité requérante fournit une raison valable de ne pas aviser l'utilisateur, par exemple si la communication risque d'entraver l'enquête ou de soulever des problèmes de sécurité. TikTok honorera les demandes de préservation pendant 90 jours. TikTok renouvellera la demande pour une période supplémentaire de 90 jours; cependant, elle peut ou pas honorer d'autres demandes de prolongation.

Les statistiques de 2022 sur les demandes des autorités policières canadiennes provenant de TikTok sont les suivantes :

- 57 demandes d'accès légal ont été présentées par le Canada en 2022, dont 64,9 % ont donné lieu à la communication de certaines données de l'utilisateur, à tout le moins, aux autorités policières;

- 184 demandes d'accès d'urgence ont été faites par le Canada en 2022, dont 82 % ont donné lieu à la communication de certaines données de l'utilisateur, à tout le moins, aux autorités policières;
- 73 demandes de préservation ont été présentées par le Canada en 2022. TikTok a pour politique d'honorer les demandes de préservation valables pendant 90 jours, bien qu'il se réserve le droit de ne pas les renouveler pour des périodes supplémentaires de 90 jours.

3. Snap[21]

Snap, anciennement Snapchat, est un service de messagerie multimédia qui permet de joindre des photos à des messages. Basé en Californie, le service compte plus de 400 millions d'utilisateurs actifs quotidiens et 750 millions d'utilisateurs actifs mensuels dans le monde entier. Snap a de courtes périodes de conservation, ce qui fait qu'une grande partie du contenu des utilisateurs est supprimée dans un délai de 24 heures à un mois après la publication ou le partage du contenu. Par exemple, les messages sont supprimés des serveurs Snap 24 heures après avoir été consultés par le destinataire, tandis que les photos sont supprimées immédiatement après avoir été consultées par le destinataire.

Étant donné que Snapchat est conçu pour supprimer les images et les messages après leur ouverture, les données liées au contenu qu'il stocke se limitent donc :

- aux photos (images) non ouvertes;
- aux clavardages non ouverts;
- aux histoires (images qui restent affichées pendant 24 heures);
- aux photos ou histoires sauvegardées par l'utilisateur.

Les données non liées au contenu que détient l'entreprise comprennent les renseignements sur l'utilisateur tels que :

- le nom;
- le nom d'utilisateur;
- le mot de passe;
- l'adresse courriel;
- le numéro de téléphone;
- la date de naissance.

Snap examine les demandes d'accès légal relatives aux données sur les clients lorsque ces demandes sont fondées en droit. Snap examine les demandes d'accès d'urgence dans les situations où elle croit que la communication des données est nécessaire pour empêcher qu'une personne ne meure ou pour éviter un préjudice physique grave. Les autorités policières peuvent présenter des demandes de préservation, ce qui peut amener Snap à conserver les données pendant un an. L'entreprise exige généralement l'utilisation d'un traité d'entraide juridique pour les demandes ne provenant pas des États-Unis, bien qu'on sache qu'elle répond à des demandes pour lesquelles une telle procédure est en cours, y compris donner accès aux renseignements de

[21] https://values.snap.com/fr-FR/safety/safety-enforcement

base sur les abonnés. Snap peut, à sa discrétion, préserver les données jusqu'à un an pendant que les traités d'entraide juridique sont en cours pour les demandes d'autorités policières autres que des États-Unis. Cette période de préservation peut être prolongée de six mois.

D'un point de vue canadien, 372 demandes d'accès légal (concernant 617 comptes) ont été présentées au cours de la période comprise entre janvier et juin 2022. De ce nombre, 65,86 % ont donné lieu à la communication de certaines données aux autorités policières. L'entreprise a été partie à 2 022 affaires devant la Cour supérieure du Québec, ce qui l'a obligée à fournir au Service de police de la Ville de Montréal des renseignements de base sur les abonnés, des données de transmission et des données de localisation[22]. Dans sa décision rendue dans l'affaire *Re SPVM*, la Cour a conclu que, malgré les défis sur les plans pratique et juridique que pose l'exécution forcée, pour une société, d'une ordonnance de communication à *l'étranger*, le tribunal était toujours compétent pour rendre et exécuter une ordonnance *au* Canada.

La Cour a notamment conclu qu'il suffit, pour autoriser une ordonnance de communication en vertu du *Code criminel*, que l'entreprise ayant en sa possession ou sous son contrôle les renseignements soit située au Canada ou que la personne visée par l'enquête ou les renseignements visés par l'ordonnance de communication, ainsi que la personne ayant en sa possession ou sous son contrôle les renseignements entretiennent un lien réel et important avec le Canada.

iii. Géants du Web

Cette partie passe en revue les trois principaux géants du Web qui offrent également une fonctionnalité de messagerie ou de courrier électronique : Google, Apple et Microsoft. La principale différence entre les géants du Web et les services de médias sociaux offrant une fonctionnalité de messagerie est l'ampleur des données recueillies par les géants du Web. Compte tenu de leur gamme exceptionnellement large de produits et de services, les entreprises ont accès à un vaste éventail de données – notamment des données financières – qui peuvent ne pas être disponibles sur d'autres services. Chacun de ces services collabore activement avec les autorités policières à un large éventail de demandes et à l'élaboration de politiques. Il existe certaines différences quant aux méthodes de chiffrement, notamment l'utilisation plus généralisée du chiffrement par Apple dans ses produits grand public et les limitations d'accès aux données chiffrées.

1. Google[23]

Google est le plus grand moteur de recherche au monde et le propriétaire d'un vaste éventail de services, notamment le service de messagerie électronique Gmail, le service de diffusion vidéo en continu YouTube et la boutique Google Play qui fournit des services aux appareils Android. Les produits Google les plus couramment visés par les demandes des autorités policières sont Gmail, YouTube, Google Voice et Blogger. Tous ces produits contiennent des « renseignements sur le contenu », tels que des messages, qui sont théoriquement mis à la disposition des autorités

[22] Re SPVM (2022 QCCS 3935)
[23] https://support.google.com/transparencyreport/answer/9713961?hl=FR

policières si leur demande est valable. Toutefois, le rapport de transparence de Google ne fournit pas de données précises sur les catégories de données communiquées.

Les données liées au contenu peuvent concerner :

- le contenu de courriels;
- les messages privés;
- les vidéos privées;
- les messages texte et les messages vocaux;
- les entrées et commentaires de blogue privés.

Les données non liées au contenu que détient Google comprennent :

- les renseignements sur l'inscription des abonnés;
- les adresses IP de connexion et l'horodatage;
- les adresses IP pour téléchargement et l'horodatage;
- les renseignements sur la facturation.

Par défaut, Google chiffre les données inactives sur ses serveurs et gère les clés de chiffrement. Toutes les données en cours de transfert de Google sont chiffrées.

Les demandes de données des autorités policières qui concernent des clients canadiens sont adressées à Google LLC, l'entité américaine. La position de l'entreprise est que les demandes doivent être conformes à la législation américaine, à la législation du pays demandeur, aux normes internationales (en particulier les principes de liberté d'expression et de protection des renseignements personnels de la Global Network Initiative) et aux propres règles de Google, telles que ses conditions d'utilisation, sa politique de confidentialité et sa politique en matière de liberté d'expression. Google avise les utilisateurs avant de communiquer des données, sauf dans des circonstances limitées, telles que celles touchant la sécurité des enfants, ou si la communication est interdite par la loi. Selon son rapport de transparence, 1 164 demandes d'accès légal ont été présentées entre janvier et juin 2022, et 82 % de ces demandes ont donné lieu à la communication de certaines données, à tout le moins.

Google examine les demandes d'accès légal relatives aux données sur les clients lorsque ces demandes sont fondées en droit. Google examine les demandes d'accès d'urgence lorsqu'elle croit raisonnablement pouvoir éviter qu'une personne ne meure ou subisse un préjudice physique grave. Google préservera les données sur les clients pendant que les autorités policières présentent une demande de processus judiciaire approprié afin d'exiger la communication des données. La demande de préservation ne s'applique qu'aux données que détient Google au moment de la présentation de la demande. La période de préservation des données par Google n'est pas rendue publique.

Google exige la délivrance d'une assignation à témoigner pour communiquer des renseignements de base sur ses abonnés. Un mandat de perquisition est nécessaire pour les renseignements sur le contenu, comme les messages, les documents et les photos. Google avise les clients par courriel avant de communiquer leurs renseignements aux autorités gouvernementales, sauf si cela est interdit par la loi ou si le fait d'aviser le client poserait des problèmes de sécurité.

2. *Apple*[24]

Apple est l'une des plus grandes entreprises technologiques au monde, et ses produits phares sont l'iPhone, l'iPad, l'iWatch et la gamme d'ordinateurs personnels Macintosh. L'entreprise propose également une gamme de services de musique, de films et de messagerie en ligne. L'entreprise propose également un service de sauvegarde infonuagique (iCloud) largement utilisé par les consommateurs. Par exemple, on estime à 1,3 milliard le nombre d'utilisateurs de Messages.

Compte tenu de l'immense place qu'elle occupe, Apple détient une grande quantité de données sur ses clients, même si la plupart de ces données ne sont pas liées au contenu. Voici quelques exemples de données non liées au contenu que conserve Apple :

- les renseignements de base sur l'enregistrement des appareils (nom, adresse, courriel, etc.);
- les transactions dans une boutique Apple;
- les journaux courrier (heure et date des courriels envoyés ou reçus, adresses courriel de l'expéditeur et du destinataire);
- les journaux de connexion pour divers produits;
- les journaux d'invitation à un appel FaceTime (n'indiquent pas si un appel a effectivement eu lieu et n'incluent pas le contenu des communications).

Les données liées au contenu se limitent :

- au contenu d'iCloud (messages, images, documents, etc.);
- aux données extraites des iPhones – uniquement pour certains appareils fonctionnant sous iOS 4 à iOS 7 (iOS 7 est sorti en 2013).

Apple chiffre certaines données sur le serveur où elles sont stockées. D'autres données sont chiffrées de bout en bout. Apple conserve les clés de chiffrement des données qu'elle peut déchiffrer dans ses centres de données aux États-Unis. Apple ne reçoit pas et ne conserve pas les clés de chiffrement des données chiffrées de bout en bout des clients.

Ses rapports de transparence fournissent des descriptions détaillées des données qui peuvent être mises à la disposition des autorités policières, sous réserve de garanties appropriées. Apple examine les demandes d'accès légal relatives aux données sur les clients lorsque ces demandes sont fondées en droit. Apple examine les demandes d'accès d'urgence liées à des menaces imminentes pour la sécurité physique ou la vie, à la sécurité nationale et à la sécurité des infrastructures essentielles. Apple conservera pendant 90 jours une extraction unique des données demandées sur les clients. Ceci s'applique aux données que détient Apple au moment de la présentation de la demande. Les données préservées sont automatiquement supprimées après 90 jours, mais la durée de préservation peut être prolongée de 90 jours supplémentaires au renouvellement de la demande par les autorités policières.

[24] https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf

En règle générale, les entités canadiennes d'Apple sont responsables des données sur les clients canadiens. La détermination de l'entité qui conserve les données dépend du produit ou du service Apple visé. Toutes les demandes sont envoyées à une adresse électronique centralisée et triées par Apple. Apple considère qu'une ordonnance de communication constitue un fondement juridique valable qui permet aux autorités policières canadiennes de demander des données sur les clients. Les demandes doivent être liées à un client particulier d'Apple qui utilise un identifiant client, comme :

- des identifiants d'unité (p. ex. numéro de série ou numéro d'identité internationale d'équipement mobile [IMEI]);
- des identifiants financiers (p. ex. carte de crédit ou carte cadeau);
- des identificateurs de compte (p. ex. identifiant Apple ou adresse électronique).

Apple avise les clients, sauf si l'ordonnance du tribunal l'interdit ou si Apple estime que cela présenterait un risque pour la sécurité. L'entreprise précise que certaines données de l'utilisateur peuvent être chiffrées et inaccessibles, selon ses paramètres. Sauf dans les situations d'urgence, les demandes de données liées au contenu doivent être conformes à la législation canadienne et à la loi des États-Unis intitulée *Electronic Communications Privacy Act* (loi sur la confidentialité des communications électroniques).

3. Microsoft

Microsoft est l'entreprise technologique la plus précieuse au monde en termes de capital boursier. L'entreprise est surtout connue pour son système d'exploitation et sa suite de logiciels et de services informatiques. Cependant, Microsoft est également propriétaire d'une grande société de médias sociaux (LinkedIn), d'un grand service de communication (Skype), et elle gère de nombreux autres services en ligne, notamment Hotmail, un service de messagerie électronique de premier plan, et Microsoft Messenger, une application de messagerie.

La majorité des demandes d'accès légal concerne les services gratuits de Microsoft comme Hotmail. Par défaut, l'entreprise détient les clés de chiffrement des données sur les clients; cependant, ces derniers, en particulier les grandes entreprises, peuvent détenir leurs propres clés de chiffrement. Les pratiques de Microsoft en matière de communication requièrent la délivrance d'une assignation à témoigner ordonnée par un tribunal pour les données non liées au contenu, tandis que les données liées au contenu requièrent un mandat. Il existe des exceptions dans les situations d'urgence telles que la violence et l'automutilation, et Microsoft peut communiquer de manière proactive certaines données sur les clients, par exemple dans les cas présumés d'images montrant l'exploitation d'enfants.

Voici quelques exemples de renseignements de base sur les abonnés :

- l'adresse courriel;
- le nom;
- l'État, le pays, le code postal;
- l'adresse IP au moment de l'inscription.

Voici d'autres exemples de données non liées au contenu :

- l'historique de connexions IP;
- les noms d'utilisateur;
- les renseignements sur les cartes de crédit ou la facturation.

Voici quelques exemples de données liées au contenu :

- le contenu de courriels;
- les fichiers stockés sur OneDrive ou d'autres services infonuagiques.

Microsoft chiffre les données inactives et en cours de transfert. De nombreux produits, mais pas tous, utilisent le chiffrement de bout en bout. Dans la plupart des cas, Microsoft stocke les clés de chiffrement.

Microsoft examine les demandes d'accès légal relatives aux données sur les clients lorsque ces demandes sont fondées en droit. Microsoft examine les demandes d'accès d'urgence lorsqu'elle croit que la communication des données est nécessaire pour empêcher qu'une personne ne meure ou pour éviter un préjudice physique grave.

Microsoft ne fournit aucune information publique sur les demandes de préservation. Les demandes doivent être conformes aux lois du pays demandeur. Microsoft conteste les demandes provenant de pays demandeurs dont la législation est incompatible avec celle du pays dans lequel les données sont hébergées. Microsoft avise les clients avant de communiquer leurs renseignements aux autorités gouvernementales, sauf si cela est interdit par la loi ou si le fait d'aviser le client poserait des problèmes de sécurité.

III. Réforme des politiques/questions clés

Les politiques d'accès légal se sont longtemps concentrées sur le rôle des intermédiaires en matière de communication tels que les fournisseurs d'accès à Internet et les fournisseurs de services sans fil. Cependant, la réalité actuelle est que les communications ne passent généralement plus exclusivement par leur infrastructure. Le niveau de communication est évidemment essentiel – les communications en réseau nécessitent naturellement l'accès à un réseau – mais les informations qui peuvent être glanées uniquement à partir du réseau ne représentent qu'une partie du tout, car des milliards de personnes dépendent des médias sociaux et des applications de messagerie qui posent de nouveaux défis en matière d'accès. En effet, l'étude de leurs politiques et de leurs pratiques révèle des incohérences bien plus importantes que celles qui, parmi les fournisseurs de communications, ont initialement incité à se concentrer sur des règles d'accès légal normalisées. En fait, certains services ne conservent absolument aucune donnée, beaucoup déploient un système de chiffrement sophistiqué et certains ont adopté des structures d'entreprise complexes dont les liens en matière de compétence sont incertains. Même parmi les entreprises les plus connues et les mieux établies, il existe des différences dans les politiques de transparence et de communication des informations, ce qui pose des problèmes considérables aux forces de l'ordre qui travaillent dans des situations où le temps est compté.

Cet examen approfondi des pratiques actuelles et des rapports de transparence permet de déterminer les principales préoccupations en vue de réformes futures. L'accès légal est depuis longtemps confronté à la difficulté de concilier les besoins opérationnels des organismes d'application de la loi avec les garanties de la Charte en matière de vie privée et de fouille ou de perquisition. Ces défis sont accentués par les médias sociaux et les applications de messagerie qui sont invariablement hébergés à l'étranger et qui combinent fréquemment des informations sur le contenu et d'autres qui ne le concernent pas. À la lumière de ces complexités, cette section décrit six questions clés qui devraient être au cœur de l'analyse opérationnelle ou de l'élaboration des politiques futures.

1. Défis posés par les applications servant uniquement à la messagerie

L'émergence d'applications servant uniquement à la messagerie, telles que WhatsApp et Signal, a transformé la messagerie pour des milliards de personnes dans le monde entier, car ces services ont effectivement remplacé un flux de revenus de plusieurs milliards de dollars provenant des textos pour les entreprises de télécommunications. Les implications pour les forces de l'ordre ne sont pas moins transformatrices. Alors que les messages courts étaient autrefois largement dominés par les fournisseurs de réseaux, le passage à des services basés sur Internet qui ne conservent pas le contenu des messages et n'y ont pas accès, et qui utilisent des mesures de chiffrement puissantes, rend l'accès à ce contenu de messagerie exceptionnellement difficile, voire impossible.

Les services de médias sociaux et les messageries des géants de la technologie restent populaires – en particulier en tant qu'ajout à des services déjà populaires – et jouent donc un rôle important à des fins d'enquête. En effet, les rapports de transparence de ces entreprises confirment presque quotidiennement les demandes des gouvernements. Pourtant, les services servant uniquement à la messagerie représentent une lacune importante, car ils offrent un mécanisme facile de communication présentant des obstacles importants à l'accès des tiers (ou même des fournisseurs). Il n'existe pas de solution évidente à ces obstacles en matière de technologie et de compétence. En outre, ces services jouent un rôle important dans certaines sociétés où la population profite des garanties qu'ils offrent en matière de protection de la vie privée. Ce défi restera d'actualité dans un avenir prévisible et nécessitera la recherche d'autres formes d'accès et la reconnaissance du fait que certains fournisseurs peuvent être structurés de manière à contrecarrer l'accès externe au contenu des communications des utilisateurs, même avec la supervision appropriée du tribunal et des garanties en matière de protection de la vie privée.

2. Limites de la communication obligatoire des informations

Le concept même de communication obligatoire des données stockées par les médias sociaux et les applications de messagerie doit être reconsidéré. Si certains services conservent des données qui peuvent être communiquées moyennant la supervision appropriée du tribunal ou des garanties administratives, la réalité est que certains services ne conservent absolument aucune donnée. Par exemple, des services populaires tels que Signal conservent peu de données utiles pour les forces de l'ordre, ces données se limitant en grande partie aux informations d'enregistrement. Cela suggère que le fournisseur lui-même n'est tout simplement pas en mesure

de fournir aux autorités les informations pertinentes relatives à ses utilisateurs. De même, les « clavardages secrets » sur Telegram ne sont pas stockés par le service, ce qui l'empêche de répondre aux demandes, même s'il était disposé à les communiquer. En fait, Signal et Telegram insistent publiquement sur le fait qu'ils n'ont jamais divulgué d'informations sur le contenu à des tiers. Étant donné l'impossibilité apparente d'une intervention législative pour résoudre ce problème, certains intermédiaires peuvent être techniquement incapables de récupérer des informations qui étaient auparavant accessibles, à condition que les garanties législatives appropriées soient respectées.

En outre, même si l'entreprise conserve certaines informations sur le contenu, beaucoup appliquent des politiques de suppression qui peuvent rendre le contenu inaccessible. Par exemple, Snap a de courtes périodes de conservation, ce qui fait qu'une grande partie du contenu des utilisateurs est supprimée dans un délai allant de 24 heures à un mois après la publication ou le partage du contenu. Les messages sont supprimés des serveurs de Snap 24 heures après avoir été lus par le destinataire, tandis que les photos sont supprimées instantanément après avoir été vues par le destinataire.

3. Problèmes de compétence

Les problèmes de compétence posés par l'écosystème de la messagerie et des médias sociaux représentent un fardeau énorme pour les forces de l'ordre canadiennes. La domination d'une poignée de fournisseurs de communications canadiens a suscité des inquiétudes en matière de concurrence et de prix à la consommation, mais a simplifié la situation pour les organismes d'application de la loi, étant donné qu'ils peuvent traiter avec un nombre relativement restreint de fournisseurs de très grande taille. Cela a eu pour avantage de favoriser les relations personnelles, d'élaborer des politiques bien comprises et d'assurer la formation préalable du personnel en cas d'incidents pour lesquels le temps est compté. En outre, les lois canadiennes sur les télécommunications ont largement garanti que les fournisseurs sont basés au Canada et soumis à la législation canadienne et au système judiciaire canadien.

L'émergence des services de messagerie et de médias sociaux représente un renversement presque complet de cette dynamique. Aucun des principaux services identifiés dans la présente étude n'est une entreprise canadienne. En outre, à l'exception des grandes entreprises technologiques mondiales telles que Google, Apple, Microsoft et Meta (propriétaire de WhatsApp), aucune n'a de présence physique au Canada. En fait, Apple est particulièrement atypique dans la mesure où ses entités canadiennes sont responsables des données des clients canadiens. Les règles en matière de compétence canadiennes peuvent encore permettre à un tribunal canadien de se déclarer compétent s'il est convaincu de l'existence d'un lien réel et substantiel avec le pays, mais l'exécution de toute ordonnance d'un tribunal (ou de toute nouvelle législation) nécessitera souvent des accords d'entraide juridique ou des démarches juridiques supplémentaires dans d'autres pays. Cela crée une incertitude et des retards importants dans le cadre de toute procédure d'accès à des informations provenant de fournisseurs non canadiens.

En supposant que la question de la compétence puisse être réglée, la loi applicable peut constituer un autre obstacle, certaines entreprises brossant un tableau confus d'exigences mixtes.

Par exemple, les demandes d'application de la loi adressées à Google pour obtenir des données concernant des clients canadiens sont adressées à Google LLC, l'entité des États-Unis. D'après l'entreprise, les demandes doivent être conformes à la législation des États-Unis, à la législation du Canada, aux normes internationales (notamment les principes de liberté d'expression et de protection des renseignements personnels de la Global Network Initiative) et aux règles de Google, telles que les conditions d'utilisation, les règles de protection de la vie privée et les règles relatives à la liberté d'expression. De même, Apple exige que les demandes de données sur le contenu soient conformes à la fois à la législation canadienne et à la loi des États-Unis intitulée Electronic Communications Privacy Act (loi sur la confidentialité des communications électroniques). Alors que ces entreprises annoncent les lois applicables, des services tels que X insistent sur le fait que les demandes de communication d'urgence sont évaluées au cas par cas et qu'elles doivent répondre à un seuil d'« urgence impérieuse impliquant un danger de mort ou de blessure physique grave pour une personne ». En d'autres termes, c'est l'entreprise elle-même qui fixe la norme en matière de communication.

4. Politiques incohérentes

Les différents services de messagerie et de médias sociaux appliquent des règles incohérentes en ce qui concerne leurs procédures d'approbation juridique reconnues. En effet, nombre d'entre eux exigent une ordonnance d'un tribunal de leur propre pays et ne respecteront pas une ordonnance d'un tribunal canadien. Par exemple, TikTok exige que les demandes émanant des organismes canadiens d'application de la loi soient adressées à son entité juridique singapourienne et indique qu'il peut être nécessaire pour les organismes d'application de la loi situés en dehors de Singapour de s'appuyer sur les traités d'entraide juridique plutôt que d'adresser la demande directement à TikTok.

5. Chiffrement

Le chiffrement représente, sans surprise, un autre défi de taille. Si certains services conservent les clés de chiffrement et peuvent donc être en mesure de faciliter l'accès, d'autres n'ont tout simplement pas la capacité technique d'accéder au contenu chiffré par l'utilisateur. Par exemple, Microsoft chiffre les données inactives et en cours de transfert. De nombreux produits, mais pas tous, utilisent le chiffrement de bout en bout. Dans la plupart des cas, Microsoft stocke les clés de chiffrement. En revanche, WhatsApp est incapable de communiquer le contenu des messages de ses utilisateurs en réponse à des demandes gouvernementales. Le contenu de tous les messages envoyés avec WhatsApp est protégé par un protocole de chiffrement qui sécurise les messages avant qu'ils ne quittent l'appareil de l'utilisateur, ce qui garantit que seuls l'utilisateur et le destinataire peuvent écouter ou lire le message. Les intermédiaires, y compris WhatsApp, n'ont donc pas accès à ce contenu. Même les sociétés dont la structure de propriété est bien établie, comme Viber, qui appartient à la société japonaise Rakuten, ont structuré leur produit de manière à ce que les données liées au contenu soient chiffrées de bout en bout, ce qui signifie que seuls l'expéditeur et le destinataire peuvent les déchiffrer.

6. Incertitude et transparence

Malgré l'existence de rapports de transparence, il subsiste une grande incertitude quant aux politiques des services de médias sociaux et de messagerie sur un large éventail de questions. C'est le cas pour les demandes de conservation en particulier. Microsoft ne fournit aucune information publique sur les demandes de conservation, WhatsApp n'a pas divulgué la période de conservation, et la période de conservation des données de Google n'est pas non plus divulguée publiquement.

Il existe d'autres incohérences entre les entreprises sur des questions telles que les circonstances dans lesquelles elles divulgueront les demandes aux utilisateurs concernés. Par exemple, Microsoft informera les clients avant de divulguer leurs informations aux autorités gouvernementales, sauf si la loi l'interdit ou si le fait d'informer un client risque de poser des problèmes de sécurité. Viber propose une politique d'exception plus solide, indiquant qu'elle informe les utilisateurs de la soumission d'une demande d'application de la loi avant la communication de toute information liée à un compte, sauf dans les cas suivants : (i) la notification est interdite en vertu de la réglementation applicable, d'une ordonnance d'un tribunal, d'une citation à comparaître ou de toute autre procédure judiciaire; (ii) un événement d'urgence se produit et la notification pourrait entraîner un risque important (p. ex. des blessures ou la mort) pour une personne ou un groupe de personnes; ou (iii) un événement d'urgence implique un préjudice potentiel pour des mineurs.

IV. Annexe

Voir le document ci-joint