



Décision de télécom CRTC 2022-238

Version PDF

Ottawa, le 6 septembre 2022

Dossier public : 8665-P8-202005769

Centre pour la défense de l'intérêt public – Demande de définition des exigences en matière de protection de la vie privée pour les fournisseurs de services de télécommunication dans le contexte de toute application technologique numérique de recherche des contacts

Sommaire

L'un des objectifs de la politique canadienne de télécommunication est de contribuer à la protection de la vie privée des personnes, comme le prévoit l'alinéa 7i) de la *Loi sur les télécommunications* (*Loi*). Pour atteindre cet objectif, le Conseil a pris certaines mesures réglementaires dans la présente décision afin de mieux protéger les renseignements confidentiels sur les clients canadiens.

Le Centre pour la défense de l'intérêt public (CDIP) a déposé une demande dans laquelle il a demandé au Conseil de définir les exigences en matière de protection de la vie privée pour les fournisseurs de services de télécommunication (FST) dans le contexte de toute application technologique numérique de recherche des contacts. Le CDIP a également demandé au Conseil de concevoir un critère réglementaire relatif à l'utilisation de technologies numériques de recherche des contacts à des fins de santé publique qui déterminerait si les renseignements confidentiels sur les clients peuvent être communiqués ou non.

Bien que le Conseil ait fait remarquer que certains aspects de la demande ne relèvent pas de sa compétence réglementaire en vertu de la *Loi*, il a reconnu que la demande du CDIP soulevait certaines préoccupations politiques, relatives au rôle des FST en ce qui concerne la protection de la vie privée des clients, qui méritent un examen plus approfondi. Par conséquent, dans la présente décision, le Conseil clarifie ses règles relatives aux renseignements confidentiels sur les clients. En particulier, le Conseil confirme que les renseignements confidentiels sur les clients comprennent les adresses de protocole Internet et les numéros de téléphone sans fil mobile et que, en l'absence d'une exception, le consentement exprès à la communication des renseignements confidentiels sur les clients doit être explicite, et donc clair et informé, pour être valable. Le Conseil précise également que l'utilisation de données accessibles au public pour confirmer les renseignements confidentiels sur les clients n'est pas autorisée.

En outre, si le Conseil est convaincu que les règles en matière de renseignements confidentiels sur les clients s'appliquent clairement à la plupart des FST, il reconnaît qu'il existe une lacune en ce qui concerne les services de données sans fil mobiles. Pour y remédier, le Conseil étend les règles relatives aux renseignements confidentiels sur les clients à tous les fournisseurs de services Internet et de services sans fil et exige qu'ils se conforment aux dispositions suivantes :

- À moins que le client ne donne son consentement exprès ou que la communication ne soit faite en vertu d'un pouvoir légal, tous les renseignements conservés par l'entreprise de services de télécommunication concernant le client, autres que le nom, l'adresse et le numéro de téléphone inscrit du client, sont confidentiels et ne peuvent être communiqués par l'entreprise à quiconque, sous réserve des exceptions indiquées dans l'annexe de la présente décision et de toute autre exception applicable que le Conseil pourrait avoir approuvée.
- Aux fins de cette exigence, les formes de consentement exprès acceptables sont celles définies dans la décision de télécom 2005-15.
- Tous les fournisseurs de services doivent également se conformer aux dispositions supplémentaires relatives à la protection de la vie privée énoncées dans les politiques réglementaires de télécom 2009-657 et 2017-11, selon lesquelles les renseignements personnels recueillis aux fins de la gestion du trafic Internet ne doivent pas être utilisés à d'autres fins et ne doivent pas être communiqués.

Toutefois, le Conseil détermine qu'il n'est ni nécessaire ni approprié d'adopter des mesures supplémentaires au-delà des règles relatives aux renseignements confidentiels sur les clients en ce qui concerne le traitement des renseignements relatifs aux clients par les FST. Par conséquent, le Conseil **refuse** la demande du CDIP de concevoir un critère réglementaire relatif au traitement des renseignements sur les clients dans le contexte des technologies numériques de recherche des contacts qui déterminerait si les renseignements confidentiels sur les clients peuvent ou non être communiqués à des fins de santé publique en l'absence de consentement exprès. Si un FST ou une autre entité estime qu'on devrait prévoir offrir plus de latitude afin de permettre à un FST de communiquer des renseignements confidentiels sur les clients à une autorité publique sans consentement exprès, il peut en faire la demande au Conseil, qui pourra alors examiner la question.

Contexte réglementaire

1. Les exigences du Conseil relatives à l'utilisation des renseignements confidentiels sur les clients par les fournisseurs de services de télécommunication (FST) [règles relatives aux renseignements confidentiels sur les clients] sont ancrées dans la décision de télécom 86-7. Dans cette décision, le Conseil a établi les modalités de service pour les entreprises de services de télécommunication qui relevaient alors de sa compétence. Les règles relatives aux renseignements confidentiels sur les clients prévoient que tous les renseignements sur un client, à l'exception de son nom, de son

adresse et de son numéro de téléphone inscrit, sont confidentiels et ne peuvent être communiqués sans le consentement exprès du client, à quelques exceptions près.

2. Les règles relatives aux renseignements confidentiels sur les clients ont été imposées comme modalités de service en vertu de l'article 24 et, plus récemment, de l'article 24.1 de la *Loi sur les télécommunications (Loi)*. Dans certains cas, ces modalités de service ont également été intégrées aux tarifs, mais dans d'autres cas, ce sont des modalités de service autonomes imposées au fil des ans et énoncées dans diverses décisions du Conseil.
3. Dans la décision de télécom 2003-33, le Conseil a déclaré que les clauses de confidentialité énoncées initialement dans la décision de télécom 86-7 s'appliquent également à toutes les entreprises de services de télécommunication canadiennes en ce qui concerne leur prestation de services, sauf dans le cas des services sans fil qui ne sont pas des services publics commutés. Dans cette décision, le Conseil a également conclu qu'il y avait lieu de permettre d'autres formes de consentement exprès en remplacement du consentement écrit.
4. Les règles relatives aux renseignements confidentiels sur les clients ont également été clarifiées et raffinées dans des décisions ultérieures. En particulier, le Conseil a davantage élargi les formes de consentement exprès exigées par les entreprises de services de télécommunication à l'égard de la communication de renseignements confidentiels sur les clients¹ et a modifié les exceptions à l'obligation d'obtenir un consentement exprès préalable, différentes exceptions ayant été adoptées au fil des ans².
5. En plus des règles relatives aux renseignements confidentiels sur les clients, le Conseil a complété ses clauses existantes concernant la protection des renseignements personnels dans la politique réglementaire de télécom 2009-657. Le Conseil a fait remarquer que certaines technologies utilisées dans le cadre des pratiques de gestion du trafic Internet ont la capacité de recueillir et d'utiliser des renseignements personnels et que l'information obtenue de cette manière est tirée du flux du trafic du réseau, sans que le consommateur en ait connaissance ou y donne son consentement, une capacité qui a suscité des préoccupations en matière de protection de la vie privée. À ce titre, le Conseil a ordonné à tous les principaux fournisseurs de services Internet (FSI), en tant que condition de la fourniture de services Internet de détail, de ne pas utiliser à d'autres fins les renseignements personnels recueillis dans le but de gérer le trafic ni de les communiquer.
6. Dans la politique réglementaire de télécom 2017-11, le Conseil a ordonné aux entreprises autres que les entreprises de services de télécommunication, également appelées revendeurs, de se conformer à certaines conditions pour offrir et fournir tout service de télécommunication. Ces revendeurs doivent se conformer i) à toutes les obligations existantes applicables relatives aux garanties offertes aux consommateurs,

¹ Voir, par exemple, la décision de télécom 2005-15.

² Voir, par exemple, la décision de télécom 2007-13 et la politique réglementaire de télécom 2009-723.

notamment les règles relatives aux renseignements confidentiels sur les clients; et ii) à certaines exigences énoncées dans la politique réglementaire de télécom 2009-657, y compris celles liées à l'utilisation et à la communication des renseignements personnels recueillis aux fins de la gestion du trafic.

Demande

7. Le Conseil a reçu une demande du Centre pour la défense de l'intérêt public (CDIP), datée du 9 septembre 2020, dans laquelle le CDIP sollicitait l'intervention du Conseil au sujet des règles relatives aux renseignements confidentiels sur les clients, en particulier au sujet de l'utilisation d'applications technologiques numériques de recherche des contacts. Le CDIP s'est concentré spécifiquement sur l'utilisation des applications Alerte COVID³ et ABTraceTogether⁴. Le CDIP était préoccupé par le fait que les entités gouvernementales, en possession d'adresses de protocole Internet (IP) ou de numéros de téléphone sans fil mobile obtenus au moyen des applications concernées, puissent obtenir des renseignements associés sur les clients au moyen de simples demandes auprès des FST.
8. Le CDIP a demandé que le Conseil, dans le cadre de l'utilisation de toute application technologique numérique de recherche des contacts, impose aux FST des modalités de service destinées à contribuer à la protection de la vie privée des personnes. Plus précisément, le CDIP a demandé au Conseil i) de définir les exigences en matière de protection de la vie privée que les FST doivent respecter et de confirmer qu'elles sont les mêmes que les exigences en matière de protection de la vie privée pour les renseignements confidentiels sur les clients élaborées dans le cadre des décisions relatives à la téléphonie; ii) d'établir un régime dans lequel les FST, en l'absence de consentement explicite, ne seraient autorisés à communiquer des renseignements sur les abonnés dans le cadre d'une application technologique numérique de recherche des contacts que si la communication répondait à un critère précisé par le Conseil; et iii) de préciser les exigences de fond, de transparence et de responsabilité dans le critère susmentionné afin d'encourager le respect des règles de protection de la vie privée déterminées par le Conseil.
9. Le CDIP a également indiqué que le Conseil pourrait souhaiter ouvrir une enquête plus large sur les activités des FST liées aux applications de recherche des contacts ou à la facilitation, au niveau du réseau, de la localisation des clients individuels ou d'autres détails personnels ou de communication.

³ L'[application Alerte COVID](#) était administrée par Santé Canada. Elle a été lancée en Ontario le 31 juillet 2020 et était disponible dans presque toutes les provinces canadiennes en octobre 2020. Elle a été mise hors service le 17 juin 2022. Santé Canada était responsable de l'administration de l'application et des processus de recherche des contacts liés à son utilisation. Santé Canada avait fourni une vidéo sur le fonctionnement de l'application, mais elle n'est plus disponible.

⁴ L'application ABTraceTogether est administrée par Alberta Health, le ministère de la santé de l'Alberta. Elle a été lancée en Alberta le 1^{er} mai 2020. Alberta Health est responsable de l'administration des applications et des processus de recherche des contacts liés à leur utilisation. Alberta Health avait fourni [de l'information \(en anglais seulement\)](#) sur le fonctionnement de l'application, mais la page Web en hyperlien ne contient plus aucune information relative à l'application.

10. En guise de réponse initiale, le Conseil a publié une [lettre](#), datée du 28 octobre 2020, dans laquelle il reconnaissait que la demande du CDIP soulevait certaines préoccupations en matière de politique, relatives au rôle des FST en ce qui concerne la vie privée des clients, qui méritent un examen plus approfondi. Cependant, le Conseil s'est dit préoccupé par le fait que certains aspects de la demande semblent aller au-delà des questions directement liées aux actions des FST pour soulever des questions qui ne relèvent pas de la compétence réglementaire du Conseil en vertu de la *Loi*.
11. En conséquence, le Conseil a indiqué qu'il examinerait uniquement les questions assujetties à la *Loi*, en particulier,
- 1) les questions qui se rapportent au rôle des FST dans le traitement des renseignements confidentiels sur les clients;
 - 2) les questions relatives aux renseignements qui devraient être considérés comme des renseignements confidentiels sur les clients;
 - 3) toute mesure résultante qui devrait s'appliquer à la collecte, à l'utilisation et à la communication de ces renseignements par les FST.
12. Le Conseil a reçu, au sujet de la demande, des interventions d'Urs Hengartner et de Marc Nanni, ainsi que de l'Association canadienne des télécommunications sans fil (ACTS), Beanfield Technologies Inc. (Beanfield), Bell Canada (Bell), la Clinique d'intérêt public et de politique d'Internet du Canada Samuelson-Glushko (CIPPIC), le Commissariat à la protection de la vie privée du Canada (CPVPC), Iristel Inc. (Iristel), Rogers Communications Canada Inc. (RCCI), Saskatchewan Telecommunications (SaskTel), TBayTel, TekSavvy Solutions Inc. (TekSavvy), TELUS Communications Inc. (TCI) et Vaxination Informatique (Vaxination).

Questions

13. Le Conseil a déterminé qu'il devait examiner les questions suivantes dans la présente décision :
- Y a-t-il une lacune dans les règles relatives aux renseignements confidentiels sur les clients, notamment en ce qui concerne la fourniture de services d'accès Internet ou de services de données sans fil mobiles?
 - L'intervention supplémentaire du Conseil est-elle justifiée afin de protéger correctement les intérêts des utilisateurs de services de télécommunication en matière de protection de la vie privée et, dans l'affirmative, quelles mesures le Conseil devrait-il adopter?

Y a-t-il une lacune dans les règles relatives aux renseignements confidentiels sur les clients, notamment en ce qui concerne la fourniture de services d'accès Internet ou de services de données sans fil mobiles?

Positions des parties

Position générale du CDIP

14. Le CDIP a reconnu le défi sans précédent et mortel que représente le virus de la COVID-19 et la nécessité de prendre des mesures de santé publique importantes pour y faire face, notamment la recherche des contacts. Cependant, il a estimé que toute application ou système technologique numérique de recherche des contacts, y compris les deux applications qu'il a nommées, peut potentiellement contribuer au détriment de la confidentialité et de la vie privée des citoyens et doit être utilisé de la manière la plus juste, ouverte et transparente possible, sans coercition, sans discrimination et uniquement aux fins prévues.
15. Le CDIP a indiqué être préoccupé par la possibilité qu'une autorité gouvernementale, en possession d'une adresse IP ou d'un numéro de téléphone sans fil mobile obtenu au moyen d'une application technologique numérique de recherche des contacts, puisse, à terme, utiliser ces renseignements pour obtenir des renseignements sur l'abonné auprès d'un FST sans le consentement exprès de l'abonné. Le CDIP a argué que l'utilisateur de l'application, ayant été invité à donner son consentement explicite pour télécharger des clés de diagnostic lors de l'installation de l'application, a raisonnablement consenti à toute utilisation de ce statut par le gouvernement. Toutefois, le CDIP a ajouté que le consentement donné dans le cadre des processus d'inscription aux applications Alerte COVID et ABTraceTogether ne constitue pas un consentement valide et explicite du client en vertu des règles actuelles du Conseil en matière de protection de la vie privée pour la communication par les FST des renseignements qu'ils possèdent sur les abonnés.

Position du CDIP concernant les règles relatives aux renseignements confidentiels sur les clients existantes du Conseil

16. Le CDIP a reconnu que le Conseil a imposé des règles pour protéger les renseignements confidentiels sur les clients et que ces exigences s'appliquent aux services réglementés des entreprises de services de télécommunication. Toutefois, le CDIP a argué que, puisque le Conseil n'a pas mis à jour les règles relatives aux renseignements confidentiels sur les clients pour qu'elles s'appliquent aux services Internet et aux services sans fil mobiles, il est nécessaire d'appliquer explicitement des règles similaires à ces services comme modalité de service, conformément à l'autorité du Conseil en vertu des articles 24 et 24.1 de la *Loi*.
17. Le CDIP a affirmé qu'il considère les adresses IP et les numéros de téléphone sans fil mobiles comme des renseignements personnels, ajoutant que les adresses IP ont été systématiquement jugées par les tribunaux et acceptées par le Conseil comme pouvant être liées à des renseignements privés. Le CDIP a spécifiquement fait remarquer les efforts déployés par le Conseil dans le cadre de la politique réglementaire de télécom 2009-657 pour veiller à ce que les adresses IP des clients ne

soient pas utilisées pour le traçage, l'identification ou la surveillance individuelle, ajoutant que cette décision équivaut à une déclaration effective du Conseil selon laquelle les adresses IP sont des renseignements privés.

18. En outre, le CDIP a suggéré que le Conseil définisse des règles qui régiraient la communication possible par les FST de renseignements sur les abonnés ou d'autres données sur les abonnés associés à des adresses IP ou à des numéros de téléphone qui pourraient avoir été glanés grâce à une application technologique numérique de recherche des contacts.
19. Le CDIP a fait remarquer que les règles relatives aux renseignements confidentiels sur les clients permettent la communication de renseignements confidentiels sur les clients dans certaines circonstances, notamment i) lorsque le FST dispose du consentement préalable, vérifiable et explicite du client; ou ii) en l'absence de consentement ou de pouvoir légal, pour des raisons d'ordre public.
20. Le CDIP a spécifiquement cité les exceptions d'ordre public suivantes du Tarif général de Bell Canada qui indiquent que l'entreprise peut communiquer des renseignements confidentiels sur les clients, en l'absence de consentement ou de pouvoir légal, à :
 - a) une autorité publique ou son mandataire, si, de l'avis raisonnable de la Compagnie, il pourrait exister un danger imminent pour la vie ou la propriété qui pourrait être évité ou réduit par la communication des renseignements;
 - b) une autorité publique ou le mandataire d'une autorité publique, aux fins des alertes publiques d'urgence, si l'autorité publique a conclu être en présence d'un danger imminent ou sur le point de se produire mettant en danger la vie, la santé ou la sécurité de tout particulier et que le danger pourrait être évité ou minimisé par la communication de l'information.
21. En ce qui concerne les préjudices potentiels particuliers mentionnés ci-dessus, le CDIP était d'avis que les règles relatives aux renseignements confidentiels sur les clients, et en particulier les exceptions d'ordre public mentionnées ci-dessus, ne permettent pas à un FST de communiquer des renseignements sur les abonnés en relation avec les renseignements de l'application technologique numérique de recherche des contacts.

Intervenants

22. Le CPVPC a déclaré que son intervention avait été éclairée par son examen des applications Alerte COVID et par la [déclaration](#) commune publiée par les commissaires fédéral, provinciaux et territoriaux à la protection de la vie privée, *Appuyer la santé publique et bâtir la confiance des Canadiens : principes de protection de la vie privée et des renseignements personnels pour les applications de traçage des contacts et autres applications similaires*. L'ACTS et certains FST (Bell, RCCI, TBayTel et TCI) ont fait remarquer que les applications ont fait l'objet d'un

examen approfondi et ont été approuvées par les commissaires à la protection de la vie privée fédéral et provinciaux.

23. L'ACTS, ainsi que RCCI, TBayTel et TCI, ont formulé des observations sur le rôle des FST dans les applications de recherche des contacts relatifs à la COVID-19, faisant remarquer que les FST n'étaient pas impliqués dans leur conception, leur mise en œuvre ou leur fonctionnement. L'ACTS et certains FST (RCCI, Sasktel et TCI) ont fait valoir que les FST ne recueillent ni n'enregistrent aucun renseignement provenant des applications et qu'ils ne participent pas non plus à la mise en correspondance ou à la notification de tout diagnostic positif à la COVID-19 résultant de leur utilisation. Ils ont ajouté que le rôle des FST se limite à la transmission des données des applications sur leurs réseaux.
24. En ce qui concerne les renseignements sur les clients, le CPVPC a fait valoir que la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) offre des protections importantes pour le traitement des renseignements personnels par les FST. Plus précisément, en vertu de la LPRPDE, les FST sont tenus d'obtenir le consentement des personnes en ce qui concerne la collecte, l'utilisation et la communication de leurs renseignements personnels, sous réserve d'exceptions précises.
25. Le CPVPC a également fait valoir que compte tenu du droit actuel, en l'absence de circonstances urgentes ou d'une loi raisonnable, les responsables de l'application de la loi doivent obtenir une autorisation judiciaire préalable pour obtenir des renseignements sur les abonnés auprès des entreprises de services de télécommunication et que les sanctions prévues par le *Code criminel*, ainsi que les exigences de la loi sur la protection de la vie privée, ont fixé des limites strictes à l'action du gouvernement ou aux pratiques du secteur privé en matière d'accès aux renseignements privés.
26. Le CPVPC est d'avis que les règles relatives aux renseignements confidentiels sur les clients constituent un élément supplémentaire important pour la protection de la vie privée des consommateurs dans le secteur des télécommunications. Le CPVPC a fait remarquer que les règles relatives aux renseignements confidentiels sur les clients interdisent aux FST de communiquer des renseignements confidentiels sur les clients sans consentement explicite, sauf dans des circonstances précises. En outre, et en se référant à certaines prises de position antérieures du Conseil, le CPVPC a déclaré qu'il comprenait que les règles du Conseil sur les renseignements confidentiels sur les clients s'appliquent à tous les fournisseurs de services, y compris les fournisseurs de services sans fil (FSSF), sauf en ce qui concerne la fourniture de services sans fil mobiles qui ne sont pas commutés⁵, et que la définition actuelle des renseignements confidentiels sur les clients du Conseil englobe les adresses IP et les numéros de téléphone sans fil mobile. Le CPVPC a toutefois fait valoir qu'en cas de doute ou d'ambiguïté sur la question de savoir si les adresses IP et les numéros de téléphone sans fil mobile répondent à la définition actuelle des

⁵ Comme, par exemple, les services de radiomessagerie.

renseignements confidentiels sur les clients du Conseil, ou si les règles existantes s'appliquent aux FSSF, il exhortait le Conseil à étendre les règles au besoin.

27. L'ACTS, Bell, RCCI, Sasktel, TBayTel, TCI et TekSavvy ont argué qu'il n'est pas nécessaire que le Conseil intervienne, car il existe déjà un solide cadre de protection de la vie privée, qui comprend les règles relatives aux renseignements confidentiels sur les clients et la LPRPDE, régissant la collecte, l'utilisation et la communication des renseignements sur les abonnés.
28. En général, les points de vue de l'ACTS et des FST étaient les suivants :
 - Les règles relatives aux renseignements confidentiels sur les clients s'appliquent à tous les FST, y compris les FSI, les FSSF et les revendeurs, et les adresses IP et les numéros de téléphone sans fil mobile sont protégés en vertu des règles en matière de protection de la vie privée applicables;
 - Le cadre actuel du Conseil en matière de protection de la vie privée interdit aux FST de communiquer des renseignements confidentiels sur les clients sans le consentement exprès du client, sauf dans certaines circonstances précises;
 - Les politiques de confidentialité et les contrats de service respectifs des FST sont conformes à la législation canadienne sur la protection de la vie privée et au cadre de protection de la vie privée du Conseil, et ne se limitent pas au téléphone filaire, mais s'appliquent plus largement aux services de télécommunication que les FST fournissent.
29. RCCI a suggéré que le Conseil traite la demande du CDIP en rappelant simplement à tous les FST que les règles du Conseil concernant la protection des renseignements sur les clients s'appliquent déjà aux renseignements sur les clients liés aux numéros de téléphone sans fil mobile et aux adresses Internet, et que les FST doivent mettre à jour leurs modalités de service et leurs politiques de confidentialité pour s'assurer que c'est effectivement le cas.
30. Marc Nanni, l'ACTS et Bell ont déclaré que les renseignements confidentiels sur les clients sont définis de façon générale dans les règles relatives aux renseignements confidentiels sur les clients pour inclure tous les renseignements sur les abonnés détenus par les FST et concernant le client, autres que le nom, l'adresse et le numéro de téléphone inscrit du client, et qu'ils incluent donc déjà les renseignements sur les adresses IP.
31. Urs Hengartner et Marc Nanni ont soutenu les propositions du CDIP, notamment en ce qui concerne son opinion selon laquelle les adresses IP devraient être considérées comme des renseignements confidentiels sur les clients et que des conditions devraient être mises en place pour protéger le flux d'informations sur les abonnés, y compris les adresses IP, depuis les FST vers le gouvernement ou vers d'autres intérêts non explicitement pris en compte dans les règles relatives aux renseignements confidentiels sur les clients. Marc Nanni a ajouté que les numéros de téléphone sans fil mobile devraient également être inclus dans ces protections.

32. Vaxination a fait valoir que la demande du CDIP donne au Conseil l'occasion de renforcer les règles afin d'empêcher tout FST de profiter de sa position privilégiée pour examiner les flux de télécommunications. La demande du CDIP donne également au Conseil l'occasion de favoriser la confiance dans la vie privée des utilisateurs du système de télécommunications du Canada.
33. En ce qui concerne le consentement recueilli par les applications de recherche des contacts COVID-19, la plupart des intervenants, à l'exception du CPVPC et de TBayTel, n'ont pas donné d'avis sur la question de savoir si le processus d'inscription à ces applications pouvait être utilisé pour donner le consentement des FST à communiquer des renseignements confidentiels sur les clients. Cependant, le CPVPC a souligné qu'il est interdit aux FST de communiquer des renseignements confidentiels sur les clients sans consentement explicite, sauf dans des circonstances précises. TBayTel a explicitement fait remarquer que les abonnés qui ont installé des applications de recherche des contacts relatifs à la COVID-19 n'ont pas donné leur consentement pour que les FST communiquent des renseignements confidentiels sur les clients en relation avec ces applications.

Analyse du Conseil

34. L'objectif des règles relatives aux renseignements confidentiels sur les clients est de protéger la vie privée des consommateurs et de leur fournir un contrôle approprié concernant l'utilisation et la communication de leurs renseignements personnels par les FST.
35. Comme indiqué ci-dessus, les règles relatives aux renseignements confidentiels sur les clients ne résultent pas d'une décision unique applicable à tous les services et fournisseurs de services. Elles ont plutôt évolué au cours de nombreuses années et ont été imposées, au fil du temps, à différents services et fournisseurs de services.
36. La plupart des FST et des autres parties ont adopté la position selon laquelle les règles relatives aux renseignements confidentiels sur les clients et les mesures associées qui ont été adoptées pour les services téléphoniques locaux s'appliquaient également à la fourniture de services d'accès Internet sur tous les réseaux, y compris les réseaux de données sans fil mobiles. En outre, les FST semblent avoir mis en œuvre des politiques de protection de la vie privée qui paraissent généralement conformes au cadre des renseignements confidentiels sur les clients du Conseil.
37. Bien que le Conseil soit convaincu que les règles relatives aux renseignements confidentiels sur les clients s'appliquent clairement à la plupart des FST, il reconnaît qu'il existe une lacune du côté des services sans fil mobiles et que les intervenants ne sont pas certains de l'existence éventuelle d'autres lacunes.
38. Dans la décision de télécom 96-14, le Conseil a fait la distinction entre les services vocaux sans fil mobiles commutés et les autres services sans fil mobiles (qui

comprennent les services de données sans fil mobiles)⁶. Un régime d'abstention différent a été établi pour chacune de ces deux catégories de services. Le Conseil s'est inconditionnellement abstenu de réglementer les services de données sans fil mobiles, notamment en ce qui concerne ses pouvoirs d'imposer des modalités de service en vertu de l'article 24 de la *Loi*. Par conséquent, toute règle relative aux renseignements confidentiels sur les clients qui aurait pu être en place en ce qui concerne la fourniture de services de données sans fil mobiles par les entreprises de services sans fil aurait été éliminée à ce moment-là. Le Conseil n'a réaffirmé ses pouvoirs en vertu de l'article 24 relativement à ces services que dans la décision de télécom 2010-445, lorsqu'il a imposé aux fournisseurs de données sans fil mobiles les exigences relatives à la confidentialité énoncées dans la politique réglementaire de télécom 2009-657. Toutefois, ces exigences ne concernent que les renseignements recueillis aux fins de la gestion du trafic, et non les renseignements confidentiels sur les clients de manière plus générale.

39. En ce qui concerne la fourniture de services d'accès Internet par des entreprises autres que les entreprises de services locaux titulaires (y compris les petites entreprises de services locaux titulaires) et les entreprises de services sans fil mobiles, le Conseil est d'avis qu'il convient de clarifier davantage l'applicabilité des règles relatives aux renseignements confidentiels sur les clients à ces entreprises, car le Conseil n'a pas appliqué sans ambiguïté les règles relatives aux renseignements confidentiels sur les clients à toutes les entreprises lorsqu'il a traité des dispositions relatives à la confidentialité dans ses décisions précédentes.
40. D'autre part, il ne semble pas y avoir d'ambiguïté en ce qui concerne l'application des règles relatives aux renseignements confidentiels sur les clients pour les entreprises autres que les FST, car dans la politique réglementaire de télécom 2017-11, le Conseil a étendu sans ambiguïté les exigences existantes en matière de renseignements confidentiels sur les clients à toutes les entreprises autres que les FST, ainsi que les exigences pertinentes énoncées pour la première fois dans la politique réglementaire de télécom 2009-657. Afin de mieux garantir la protection de la vie privée de la population canadienne, quel que soit le service ou le fournisseur de services qu'ils utilisent, le Conseil reconnaît l'importance d'appliquer de manière symétrique les règles relatives aux renseignements confidentiels sur les clients à tous les fournisseurs de services en ce qui concerne la fourniture de services de télécommunication⁷.
41. En ce qui concerne la question de savoir si les renseignements confidentiels sur les clients comprennent l'adresse IP et le numéro de téléphone sans fil mobile d'un client, le Conseil fait remarquer qu'il n'a jamais établi de liste détaillée des renseignements qu'il estime être des renseignements confidentiels sur les clients aux

⁶ Dans des décisions ultérieures, par exemple les décisions de télécom 98-18 et 98-19 et l'ordonnance de télécom 99-991, le Conseil a étendu les conclusions de la décision de télécom 96-14 à d'autres FSSF.

⁷ Les « services de télécommunication », comme discutés ici, ne comprennent pas les services sans fil mobiles qui ne sont pas des services publics commutés.

fins de ses mesures réglementaires. Au contraire, lorsque le Conseil a imposé pour la première fois des obligations concernant les renseignements confidentiels sur les clients dans la décision de télécom 86-7, il a indiqué les renseignements qui n'étaient pas estimés être des renseignements confidentiels sur les clients, à savoir le nom, l'adresse et le numéro de téléphone inscrit du client. Tous les autres renseignements conservés par l'entreprise concernant un client étaient estimés comme confidentiels.

42. Le Conseil reconnaît qu'une adresse IP ou un numéro de téléphone sans fil mobile ne peuvent, à eux seuls, être utilisés pour identifier un individu. Toutefois, lorsqu'ils sont associés à d'autres renseignements, ils peuvent être utilisés à cette fin. Par conséquent, toute adresse IP ou tout numéro de téléphone sans fil mobile non inscrit associé à un client doit être estimé comme renseignement confidentiel sur le client. Le Conseil fait toutefois remarquer que la communication des adresses IP sur le réseau est nécessaire au fonctionnement d'Internet (p. ex. un ordinateur qui cherche à interagir avec un autre ordinateur doit s'identifier à cet autre ordinateur au moyen d'une adresse IP) et précise que cette communication n'est pas contraire à sa réglementation.
43. Le Conseil confirme que les règles relatives aux renseignements confidentiels sur les clients interdisent à un FST de communiquer tout renseignement au sujet d'un client dans le cadre d'une demande de communication, y compris le nom, l'adresse ou le numéro de téléphone inscrit du client, lorsque le renseignement pourrait être utilisé conjointement avec tout renseignement confidentiel sur le client pour identifier individuellement un client, sauf si l'une des exceptions à la communication s'applique. Bien que les renseignements officiellement communiqués dans un tel cas puissent ne pas être estimés comme confidentiels en vertu des règles relatives aux renseignements confidentiels sur les clients, si un fournisseur de services, en réponse à une demande d'un tiers, communique le nom d'un utilisateur final associé à une adresse IP ou à un numéro de téléphone sans fil mobile déjà connu du demandeur, il révélera plus qu'un simple nom. Parce qu'il communiquerait l'identité d'une personne utilisant une adresse IP particulière, il révélerait également un lien entre l'abonné et les renseignements confidentiels sur les clients, ce qui pourrait mener à des renseignements très sensibles qui ne pourraient pas être glanés à partir du seul nom ou du seul numéro de téléphone inscrit.
44. Le Conseil est d'accord avec l'affirmation du CDIP selon laquelle les processus d'inscription aux applications de recherche de contacts relatifs à la COVID-19 mentionnées dans sa demande ne semblent pas fournir un consentement adéquat pour que les FST communiquent les renseignements au sujet des abonnés associés aux adresses IP ou aux numéros de téléphone sans fil mobile. En outre, le Conseil fait remarquer que rien dans le dossier de la présente instance n'indique qu'il ait été demandé aux FST de communiquer des renseignements au sujet des abonnés associés à une adresse IP ou à un numéro de téléphone sans fil mobile obtenus au moyen d'applications technologiques numériques de recherche des contacts.
45. En outre, si le Conseil a défini le consentement exprès en relation avec la communication des renseignements confidentiels sur les clients, il précise qu'en vertu des règles relatives aux renseignements confidentiels sur les clients, en

l'absence d'une exception, le consentement exprès doit être explicite, et donc clair et informé, pour être valable. Le Conseil fait également remarquer que la LPRPDE et la *Loi sur la protection des renseignements personnels* exigent toutes deux que les personnes soient informées des utilisations possibles des données lorsqu'elles consentent à ce que leurs données soient collectées et stockées.

46. Compte tenu de ce qui précède, le Conseil :

- a) reconnaît l'existence d'une lacune dans l'application des règles relatives aux renseignements confidentiels sur les clients en ce qui concerne la fourniture de services de données sans fil mobiles par les entreprises de services sans fil mobiles, et qu'il peut y avoir un manque de clarté quant à savoir à qui les règles relatives aux renseignements confidentiels sur les clients s'appliquent et à la fourniture de quels services;
- b) reconnaît l'importance d'appliquer de manière symétrique les règles relatives aux renseignements confidentiels sur les clients à tous les FSSF et FSI en ce qui concerne la fourniture de services sans fil mobiles et d'accès Internet, conformément aux Instructions de 2006⁸;
- c) exige donc, conformément aux articles 24 (concernant les entreprises de services de télécommunication) et 24.1 (dans le cas des entreprises autres que les entreprises de services de télécommunication) de la *Loi* que, comme condition pour offrir ou fournir des services de télécommunication, tous les FST sont tenus, en ce qui concerne la fourniture de services d'accès Internet, et tous les FSI sont tenus, en ce qui concerne la fourniture de services sans fil mobiles, à l'exception des services sans fil mobiles qui ne sont pas des services publics commutés, de se conformer aux dispositions suivantes :
 - À moins que le client ne donne son consentement exprès ou que la communication ne soit faite en vertu d'un pouvoir légal, tous les renseignements conservés par l'entreprise concernant le client, autres que le nom, l'adresse et le numéro de téléphone inscrit du client, sont confidentiels et ne peuvent être communiqués par l'entreprise à quiconque, sous réserve des exceptions indiquées dans l'annexe de la présente décision et de toute autre exception applicable que le Conseil pourrait avoir approuvée⁹.

⁸ Décret donnant au CRTC des instructions relativement à la mise en œuvre de la politique canadienne de télécommunication, DORS/2006-355, 14 décembre 2006

⁹ Par souci de clarté, toute exception supplémentaire propre à un FST, telle que celle figurant dans le tarif d'un FST qui a été approuvé par le Conseil, continue de s'appliquer, le cas échéant.

- Aux fins de l'exigence susmentionnée, les formes de consentement exprès acceptables sont celles qui figurent à l'annexe de la présente décision.
- Tous les fournisseurs de services doivent également se conformer aux dispositions supplémentaires relatives à la protection de la vie privée, énoncées dans les politiques réglementaire de télécom 2009-657 et 2017-11, selon lesquelles les FST ne doivent pas utiliser les renseignements personnels recueillis aux fins de la gestion du trafic Internet à d'autres fins et ne doivent pas communiquer ces renseignements.

47. En outre, afin d'éliminer toute incertitude, le Conseil :

- a) confirme que toute adresse IP ou tout numéro de téléphone sans fil mobile non inscrit associé à un client doit être estimé comme renseignement confidentiel sur le client;
- b) précise que les règles relatives aux renseignements confidentiels sur les clients interdisent à un FST de communiquer le nom, l'adresse ou le numéro de téléphone inscrit d'un client si, dans le cadre d'une demande de communication, il reçoit tout renseignement confidentiel sur le client, y compris, mais sans s'y limiter, l'adresse IP ou le numéro de téléphone sans fil mobile du client, et qu'il lui est demandé de fournir des informations relatives à la personne associée à cette adresse IP ou à ce numéro de téléphone, sauf si l'une des exceptions à la communication est appliquée;
- c) confirme que, selon les règles relatives aux renseignements confidentiels sur les clients, le consentement exprès doit être explicite, et donc clair et informé, pour être valable.

L'intervention supplémentaire du Conseil est-elle justifiée afin de protéger correctement les intérêts des utilisateurs de services de télécommunication en matière de protection de la vie privée et, dans l'affirmative, quelles mesures le Conseil devrait-il adopter?

Positions des parties

48. Le CDIP a fait valoir que, s'il était manifestement et absolument nécessaire de mettre en œuvre efficacement la recherche des contacts dirigée par la santé publique, la recherche des contacts à l'aide des renseignements confidentiels sur les clients générée par les FST pourrait et devrait possiblement être autorisée sans le consentement exprès du client, mais sous réserve de certaines exigences, notamment la notification aux clients concernés.
49. Pour aider le Conseil dans le cas où il jugerait qu'il convenait de créer une telle exception aux règles relatives aux renseignements confidentiels sur les clients, le CDIP a proposé un critère juridique et réglementaire précis (critère de la demande de

communication pour application COVID), qui, selon le CDIP, protégerait au maximum la vie privée des consommateurs. Selon le régime proposé par le CDIP, un FST devrait d'abord demander au Conseil l'autorisation de communiquer les renseignements confidentiels sur les clients d'un client. Ces demandes seraient alors résolues au moyen d'un critère comme celui proposé par le CDIP.

50. Marc Nanni était d'avis qu'un critère préalable à la communication des renseignements confidentiels sur les clients permettrait d'éviter tout abus potentiel des renseignements confidentiels sur les clients.
51. En revanche, l'ACTS, Bell, le CPVPC et RCCI étaient d'avis que le CDIP n'a pas démontré que des mesures supplémentaires, comme le critère proposé, sont nécessaires. L'ACTS, Beanfield, Bell, Iristel, RCCI, SaskTel, TBayTel, TCI et TekSavvy ont fait valoir qu'aucune nouvelle exception n'est nécessaire, étant donné qu'elles (ou, dans le cas de l'ACTS, ses FST membres) ont déjà mis en place des politiques et des procédures d'accès légal complètes conformément à la LPRPDE et aux décisions du Conseil concernant les renseignements confidentiels sur les clients, et que les politiques d'accès légal existantes s'appliqueraient à une demande de communication provenant du gouvernement fédéral ou d'un gouvernement provincial en rapport avec les applications de recherche des contacts relatifs à la COVID-19. Elles ont soutenu qu'en vertu de ces règles et politiques, un FST ne pourrait pas simplement communiquer, sur demande, des renseignements sur les clients liés à une adresse IP précise ou à un numéro de téléphone sans fil mobile.
52. Comme indiqué ci-dessus, le CPVPC a fait valoir qu'il existe des limites strictes à l'action du gouvernement ou aux pratiques du secteur privé en ce qui concerne l'accès aux renseignements privés.
53. Le CPVPC a fait valoir qu'en l'absence de tout besoin identifié en matière de santé publique pour obtenir, sans consentement, des renseignements sur les abonnés des utilisateurs d'une application technologique numérique de recherche des contacts auprès d'un FST, il n'y avait aucune raison légitime de créer une nouvelle exception aux importantes protections offertes par les règles existantes du Conseil sur les renseignements confidentiels sur les clients. Il a ajouté que la création d'une telle exception irait directement à l'encontre des attentes des utilisateurs et des engagements qui ont été pris envers eux par les autorités gouvernementales en ce qui concerne l'application Alerte COVID, et que s'il existe un besoin de santé publique d'accéder à l'identité des utilisateurs pour la recherche des contacts ou autre, cela devrait être pris en compte dans la conception de l'application, en tenant compte des principes de confidentialité pour la recherche des contacts et des applications similaires.
54. L'ACTS et RCCI ont argué que le critère de la demande de communication pour application COVID imposerait, s'il était adopté, un niveau supplémentaire de réglementation de la vie privée tout à fait inutile et intrusif. RCCI a fait remarquer que le critère proposé par le CDIP et le processus connexe nécessiteraient i) une demande au Conseil par le FST, un avis à la personne (ou aux personnes) dont le FST propose de communiquer les renseignements, la participation de cette personne

si elle souhaite prendre part et une décision du Conseil; et ii) qu'on donne à la personne concernée un avis de cette décision, ainsi que la possibilité de contester le résultat, lorsqu'un avis ne peut être donné. L'ACTS et RCCI étaient d'avis que le critère proposé serait difficile à appliquer, car le Conseil ne dispose pas de l'expertise nécessaire pour évaluer de telles demandes liées à la santé publique.

55. L'ACTS et certains FST ont donné des précisions sur la façon dont les FST traitent les demandes de renseignements sur les abonnés émanant du gouvernement ou d'autorités chargées de l'application de la loi, en soulignant l'existence d'un cadre juridique très élaboré établi dans les lois applicables d'application générale, notamment la LPRPDE, le *Code criminel* et la *Loi sur le Service canadien du renseignement de sécurité*. L'ACTS a déclaré que les FST ne communiqueront des renseignements sur des abonnés à un gouvernement ou à une autorité chargée de l'application de la loi que sur présentation d'un ordre valable émanant d'un tribunal, d'une personne ou d'un organisme ayant la compétence pour exiger ces renseignements (p. ex. une ordonnance de communication ou un mandat) ou lorsque l'autorité a déterminé son pouvoir légal d'obtenir ces renseignements. L'ACTS a ajouté que les FST examinent la validité de chaque demande et vérifient les demandes pour s'assurer qu'elles relèvent de la compétence appropriée et qu'elles ne comportent pas d'erreurs ou d'omissions, et qu'ils tiennent compte de l'étendue et de la portée de la demande. En outre, l'ACTS a indiqué que les FST demandent régulièrement aux autorités des renseignements et des justifications supplémentaires concernant ces demandes, repoussent les demandes incomplètes, incorrectes ou trop larges et exigent que toute erreur soit corrigée avant de répondre à une demande. L'ACTS a fait remarquer que, dans certains cas, les demandes sont refusées.
56. Toutefois, certains intervenants étaient d'avis que des mesures supplémentaires étaient justifiées. Plus précisément, Beanfield a proposé que le Conseil amorce une instance visant à moderniser les règles du Conseil sur la vie privée et sur les renseignements confidentiels sur les clients. La CIPPIC a également soutenu une consultation plus large.

Analyse du Conseil

57. Les FST disposent actuellement de procédures solides pour traiter les demandes de renseignements au sujet des abonnés émanant des autorités gouvernementales ou des autorités chargées de faire respecter la loi. Les règles relatives aux renseignements confidentiels sur les clients du Conseil autorisent la communication sans consentement exprès préalable dans des circonstances très précises, lesquelles n'incluent pas les demandes génériques des agences gouvernementales. En l'absence de consentement exprès, la communication ne peut se faire qu'en vertu d'un pouvoir légal ou lorsque des exceptions particulières s'appliquent. En ce qui concerne l'exception générale qui permet la communication des renseignements confidentiels sur les clients sans consentement exprès, en vertu d'un pouvoir légal, et la préoccupation du CDIP selon laquelle cela pourrait permettre une telle communication en l'absence d'un mandat ou d'un autre acte judiciaire, le Conseil est d'avis que le dossier de la présente instance ne fournit pas d'éléments de preuves convaincants de la raison pour laquelle le respect d'une loi constitutionnelle soulève

des préoccupations qui doivent être traitées par le Conseil. Il ne serait pas approprié que le Conseil adopte des mesures qui auraient pour effet d'empêcher une entité de se conformer à la législation dûment promulguée par le corps législatif compétent en vue de la réalisation d'objectifs d'intérêt public ou aux textes réglementaires adoptés en vertu de cette législation.

58. En outre, et plus particulièrement en ce qui concerne la question de la conformité constitutionnelle, lorsqu'un acteur gouvernemental tente d'obtenir des renseignements sur un abonné dans le but d'appliquer un régime légal ou réglementaire, les protections de l'article 8 de la *Charte canadienne des droits et libertés* (*Charte*) contre les fouilles, perquisitions et saisies abusives seront engagées¹⁰. La décision de la Cour suprême du Canada (CSC) dans l'affaire *R. c. Spencer*¹¹, à laquelle un certain nombre de parties à la présente instance ont fait référence, est instructive à cet égard, car elle concerne une demande faite par la police à Shaw Communications Inc. en vue de communiquer des renseignements sur les abonnés concernant une adresse IP en sa possession. Dans cette décision, la CSC a estimé qu'il existait une attente raisonnable en matière de protection de la vie privée pour les renseignements relatifs aux abonnés associés à une adresse IP, étant donné que la communication de ces renseignements révèle souvent des détails intimes sur une personne¹². La CSC a donc statué que de telles demandes par une entité chargée de l'application de la loi constituent une fouille aux fins de l'article 8 de la *Charte*. Selon le Conseil, ce raisonnement peut être appliqué aux renseignements relatifs aux abonnés de tout appareil connecté à des réseaux accessibles au public.
59. Lorsque l'article 8 de la *Charte* est invoqué, une perquisition effectuée en l'absence d'un mandat ou d'une ordonnance de communication est estimée déraisonnable, sauf s'il peut être démontré que la perquisition a été effectuée en raison de circonstances pressantes, comme lorsque les renseignements sont nécessaires pour prévenir un préjudice imminent à une personne, ou qu'elle a été autorisée par une loi raisonnable¹³.
60. L'évaluation du caractère raisonnable d'une perquisition sans mandat sera nécessairement contextuelle. Lorsqu'une perquisition se fonde sur un pouvoir de perquisition légal, l'évaluation dépendra dans une large mesure des objectifs poursuivis par la loi pertinente, de la nature des intérêts de la vie privée en jeu (dans le cas de renseignements relatifs à un abonné associés à une adresse IP ou à un appareil mobile connecté à un réseau de télécommunication accessible au public,

¹⁰ L'article 8 de la *Charte* indique que « [c]hacun a droit à la protection contre les fouilles, les perquisitions ou les saisies abusives. »

¹¹ *R. c. Spencer* [2014] 2 CSC 212

¹² Voir *Spencer*, *supra* note 11, au para. 66.

¹³ Voir *Spencer*, *supra* note 11, au para. 71.

ceux-ci seront généralement substantiels) et du degré d'intrusion dans ces intérêts de la vie privée que la loi autorise¹⁴.

61. Il convient de souligner que c'est à l'acteur gouvernemental qui tente d'obtenir des renseignements sur les abonnés d'un FSI ou d'un FSSF dans le but d'appliquer un régime légal ou réglementaire en l'absence d'un mandat ou d'une ordonnance de communication qu'il incombe de démontrer le caractère raisonnable de la perquisition sans mandat.
62. En ce qui concerne l'opinion du CDIP selon laquelle les exceptions d'ordre public énoncées dans le Tarif général de Bell Canada ne sont pas suffisantes pour permettre la communication, sans consentement exprès, de renseignements sur les abonnés à une autorité gouvernementale à des fins de dépistage public, et ce, même dans les situations où il existe un besoin manifeste de mettre en œuvre efficacement la recherche des contacts dirigée par la santé publique à l'aide des renseignements confidentiels sur les clients générés par les FST, le Conseil fait remarquer que ces exceptions n'ont pas été conçues pour ce scénario théorique¹⁵. Entre autres, les

¹⁴ En particulier, pour déterminer si une loi autorisant une perquisition sans mandat est raisonnable, il convient d'évaluer les facteurs suivants : sa nature et son objectif, le degré d'intrusion qu'elle autorise, le mécanisme d'intrusion autorisé, la mesure dans laquelle elle prévoit un contrôle judiciaire et toute autre mesure de responsabilisation ou mécanisme de contrôle qu'elle contient pour limiter l'étendue de l'intrusion de l'État dans la vie privée d'un individu. Voir, à cet égard, [*Goodwin c. British Columbia \(Superintendent of Motor Vehicles\)*, \[2015\] 3 SCR 250](#) aux paras. 57 et 70 à 71.

¹⁵ Le Conseil fait remarquer que les règles relatives aux renseignements confidentiels sur les clients énoncées dans la politique réglementaire de télécom 2017-11 (qui s'appliquent aux revendeurs) et l'exemple de dispositions relatives à la confidentialité des clients des FST figurant à l'annexe de la politique réglementaire de télécom 2009-723 (une décision concernant directement les entreprises de services de télécommunication) ne comprennent pas toutes les exceptions d'ordre public comprises dans le Tarif général de Bell Canada. En particulier, l'exception qui permet la communication à « une autorité publique ou son mandataire, si, de l'avis raisonnable de la Compagnie, il pourrait exister un danger imminent pour la vie ou la propriété qui pourrait être évité ou réduit par la communication des renseignements » n'est pas comprise. Cependant, le Conseil fait également remarquer que dans les politiques réglementaires de télécom 2017-11 et 2009-723, il existe une disposition générale permettant la communication des renseignements confidentiels sur les clients sans consentement « en vertu d'un pouvoir légal ». En ce qui concerne les différences dans les exceptions, dans la politique réglementaire de télécom 2009-723, le Conseil a reconnu que les tarifs approuvés de certaines entreprises de services de télécommunication canadiennes contiennent des circonstances supplémentaires dans lesquelles la communication est autorisée sans le consentement exprès du client. À cet égard, le Conseil, dès la décision de télécom 95-6, a approuvé des modalités de service tarifées qui différaient d'une entreprise à l'autre. Dans cette décision et dans l'avis public qui a donné lieu à cette décision, le Conseil a exprimé l'avis que les modalités de service sont destinées à équilibrer les droits et obligations du client individuel, ceux de l'ensemble des abonnés et ceux de l'entreprise concernée. Toutefois, le Conseil a déterminé qu'il n'était pas nécessaire d'exiger une stricte uniformité dans les modalités de service approuvées afin d'atteindre cet équilibre. La décision de télécom 95-6 a approuvé les modalités de service de trois entreprises de services de télécommunication différentes, à savoir AGT Limited, The New Brunswick Telephone Company Limited et la Newfoundland Telephone Company Limited. Les exceptions particulières à l'obligation d'obtenir le consentement avant de communiquer des renseignements concernant les clients différaient selon les modalités de service approuvées. Plus précisément, l'une des disparités entre les tarifs approuvés dans cette décision portait essentiellement sur cette même exception d'ordre public. Ainsi, le Conseil a été conscient et a accepté qu'il existe des différences dans les exceptions prévues dans les tarifs approuvés existants de certaines entreprises de services de télécommunication canadiennes. Le Conseil fait remarquer

exceptions particulières indiquées par le CDIP intègrent un critère de danger « imminent » ou « imminent ou en cours de réalisation » qui évoque l'existence de circonstances exigeant une action urgente afin d'empêcher la réalisation du danger sous-jacent ou d'en minimiser les conséquences, et où il ne serait pas possible d'obtenir un ordre légal de communication.

63. En ce qui concerne la nouvelle exception à la demande de communication pour application COVID proposée par le CDIP, le dossier ne démontre pas que la capacité d'un acteur gouvernemental à contraindre la communication de renseignements confidentiels sur les clients en utilisant des pouvoirs juridiques appropriés et conformes à la *Charte*, telle qu'une ordonnance de communication, est insuffisante pour répondre aux scénarios hypothétiques présentés dans la demande du CDIP. Le dossier ne démontre pas non plus qu'une nouvelle exception est nécessaire.
64. En outre, alors qu'un tel critère fournirait aux FST une autre façon de communiquer des renseignements confidentiels sur les clients sans le consentement exprès du client, aucun FST n'a demandé l'adoption d'un tel critère.
65. Par conséquent, le Conseil conclut qu'il n'est ni nécessaire ni justifié d'imposer de nouvelles mesures concernant le traitement des renseignements relatifs aux clients par les FST, notamment la création d'une exception particulière qui régirait la communication, à des fins de santé publique, des renseignements relatifs aux abonnés associés à l'adresse IP ou au numéro de téléphone sans fil mobile d'un utilisateur d'une application technologique numérique de recherche des contacts, en l'absence de consentement exprès du client sous-jacent.
66. Compte tenu de ce qui précède, le Conseil **refuse** la demande du CDIP d'élaborer un régime permettant la communication de renseignements sur les abonnés dans le cadre d'efforts de recherche de contacts en matière de santé publique, comme sa demande de communication pour application COVID proposée, et de préciser des exigences de fond, de transparence et de responsabilité dans ce régime.
67. Le Conseil fait remarquer que, si un FST ou une autre entité estime qu'on devrait prévoir offrir plus de latitude afin de permettre à un FST de communiquer des renseignements confidentiels sur les clients à une autorité publique sans consentement exprès, ce FST ou cette autre entité peut en faire la demande au Conseil, qui pourra alors examiner la question. Dans un tel cas, il incombera au demandeur de démontrer que sa proposition protège de manière adéquate les intérêts de la vie privée des abonnés aux services de télécommunication eu égard à l'objectif ou aux objectifs de la demande de latitude supplémentaire.

que les règles relatives aux renseignements confidentiels sur les clients énoncées dans les politiques réglementaires de télécom 2017-11 et 2009-723 autorisent la communication à une autorité publique ou à un agent d'une autorité publique, à des fins d'alerte publique d'urgence, si une autorité publique a déterminé qu'il existe un danger imminent ou en cours.

Conclusion

68. Compte tenu de ce tout qui précède, le Conseil :

- a) reconnaît l'existence d'une lacune dans l'application des règles relatives aux renseignements confidentiels sur les clients en ce qui concerne la fourniture de services de données sans fil mobiles par les entreprises de services sans fil mobiles, et qu'il peut y avoir un manque de clarté quant à savoir à qui les règles relatives aux renseignements confidentiels sur les clients s'appliquent et à la fourniture de quels services;
- b) reconnaît l'importance d'appliquer de manière symétrique les règles relatives aux renseignements confidentiels sur les clients à tous les FSSF et FSI en ce qui concerne la fourniture de services sans fil mobiles et d'accès Internet, conformément aux Instructions de 2006;
- c) exige donc, conformément aux articles 24 (concernant les entreprises de services de télécommunication) et 24.1 (dans le cas des entreprises autres que les entreprises de services de télécommunication) de la *Loi* que, comme condition pour offrir ou fournir des services d'accès Internet ou des services sans fil mobiles publics commutés, tous les FST sont tenus, en ce qui concerne la fourniture de services d'accès Internet, et tous les FSI sont tenus, en ce qui concerne la fourniture de services sans fil mobiles, à l'exception des services sans fil mobiles qui ne sont pas des services publics commutés, de se conformer aux dispositions suivantes :
 - À moins que le client ne donne son consentement exprès ou que la communication ne soit faite en vertu d'un pouvoir légal, tous les renseignements conservés par l'entreprise concernant le client, autres que le nom, l'adresse et le numéro de téléphone inscrit du client, sont confidentiels et ne peuvent être communiqués par l'entreprise à quiconque, sous réserve des exceptions indiquées dans l'annexe de la présente décision et de toute autre exception applicable que le Conseil pourrait avoir approuvée¹⁶.
 - Aux fins de l'exigence susmentionnée, les formes de consentement exprès acceptables sont celles qui figurent à l'annexe de la présente décision.
 - Tous les fournisseurs de services doivent également se conformer aux dispositions supplémentaires relatives à la protection de la vie privée, énoncées dans les politiques réglementaires de télécom 2009-657 et 2017-11, selon lesquelles les FST ne doivent pas utiliser les renseignements personnels recueillis aux fins de la gestion du trafic

¹⁶ Par souci de clarté, toute exception supplémentaire propre à un FST, telle que celle figurant dans le tarif d'un FST qui a été approuvé par le Conseil, continue de s'appliquer, le cas échéant.

Internet à d'autres fins et ne doivent pas communiquer ces renseignements.

69. Le Conseil confirme que toute adresse IP ou tout numéro de téléphone sans fil mobile non inscrit associé à un client doit être estimé comme renseignement confidentiel sur le client. Le Conseil fait toutefois remarquer que la communication des adresses IP sur le réseau est nécessaire au fonctionnement d'Internet (p. ex. un ordinateur qui cherche à interagir avec un autre ordinateur doit s'identifier à cet autre ordinateur au moyen d'une adresse IP). Par conséquent, le Conseil précise qu'une telle communication n'est pas contraire à sa réglementation.
70. Le Conseil confirme que les règles relatives aux renseignements confidentiels sur les clients interdisent à un FST de communiquer le nom, l'adresse ou le numéro de téléphone inscrit d'un client ou tout autre renseignement sur le client si, dans le cadre d'une demande de communication, on lui communique l'adresse IP ou le numéro de téléphone sans fil mobile du client et qu'on lui demande de fournir des informations relatives à la personne associée à cette adresse IP ou à ce numéro de téléphone sans fil mobile, sauf si l'une des exceptions à la communication est appliquée.
71. Le Conseil confirme que, selon les règles relatives aux renseignements confidentiels sur les clients, le consentement exprès doit être explicite, et donc clair et informé, pour être valable.
72. Le Conseil **refuse** la demande du CDIP d'élaborer un régime permettant la communication de renseignements sur les abonnés dans le cadre d'efforts de recherche de contacts en matière de santé publique, comme sa demande de communication pour application COVID proposée, et de préciser des exigences de fond, de transparence et de responsabilité dans ce régime.
73. Le Conseil fait remarquer que, si un FST ou une autre entité estime qu'on devrait prévoir offrir plus de latitude afin de permettre à un FST de communiquer des renseignements confidentiels sur les clients à une autorité publique sans consentement exprès, ce FST ou cette autre entité peut en faire la demande au Conseil, qui pourra alors examiner la question. Dans un tel cas, il incombera au demandeur de démontrer que sa proposition protège de manière adéquate les intérêts de la vie privée des abonnés aux services de télécommunication eu égard à l'objectif ou aux objectifs de la demande de latitude supplémentaire.

Instructions

74. Les Instructions de 2006 précisent que le Conseil doit, dans l'exercice de ses pouvoirs et de ses fonctions, s'appuyer, entre autres, sur le libre jeu du marché dans toute la mesure du possible, afin d'atteindre les objectifs de la politique canadienne de télécommunication énoncés à l'article 7 de la *Loi*. Par ailleurs, lorsqu'il a recours à la réglementation, le Conseil devrait prendre des mesures qui sont efficaces et proportionnelles aux buts et qui ne font obstacle au libre jeu du marché concurrentiel que dans la mesure minimale nécessaire en vue d'atteindre les objectifs de la politique.

75. Le Conseil estime que l'on ne peut compter sur le seul libre jeu du marché pour atteindre l'objectif de la politique énoncé à l'alinéa 7i) de la *Loi*, à savoir contribuer à la protection de la vie privée des personnes.
76. Dans la décision de télécom 2006-15, le Conseil a conclu que le libre jeu du marché, même renforcé par les dispositions de la LPRPDE, n'était pas susceptible de protéger suffisamment la vie privée des clients. Cette conclusion était fondée sur l'expérience du Conseil en matière de dispositions relatives à la confidentialité des clients, ainsi que sur l'avènement de nouvelles technologies et l'émergence du commerce électronique, qui permet de traiter, de réorganiser et d'échanger plus facilement les renseignements. Rien dans le dossier de la présente instance n'indique que les conclusions antérieures du Conseil concernant la capacité de s'appuyer sur le libre jeu du marché ne sont plus appropriées.
77. En outre, les règles du Conseil exigent que le consentement à la communication, lorsqu'il est requis, soit exprès, alors que la LPRPDE permet que le consentement soit implicite dans certaines circonstances. Le Conseil estime que la norme du consentement exprès est appropriée et qu'elle ne serait pas atteinte en s'appuyant uniquement sur le libre jeu du marché.
78. Enfin, les règles du Conseil sont imposées aux FST en tant que modalités de service et sont soumises aux pouvoirs d'exécution du Conseil, y compris la capacité d'imposer des sanctions administratives pécuniaires en cas de non-conformité. En revanche, et comme le reconnaît la politique réglementaire de télécom 2009-723, la LPRPDE ne fournit pas les mêmes outils d'application à l'organisme d'application pertinent, le CPVPC.
79. Le Conseil estime que la présente décision répond au sous-alinéa 1a)(ii) des Instructions de 2006¹⁷, car elle n'entravera pas de manière importante le fonctionnement des forces concurrentielles du marché. À cet égard, les conclusions du Conseil dans la présente décision servent à formaliser une situation que la plupart des parties croyaient déjà en place, à savoir que les mesures existantes du Conseil en matière de renseignements confidentiels sur les clients s'appliquent à tous les fournisseurs de services en ce qui concerne la fourniture de tous les services, à l'exception des services sans fil mobiles non commutés.
80. En outre, les conclusions du Conseil dans la présente décision servent à favoriser une application symétrique des règles relatives aux renseignements confidentiels sur les

¹⁷ Le sous-alinéa 1a)(ii) des Instructions de 2006 précise que le Conseil devrait, lorsqu'il a recours à la réglementation afin de mettre en œuvre les objectifs de la politique de télécommunication, prendre des mesures qui sont efficaces et proportionnelles aux buts visés et qui ne font obstacle au libre jeu d'un marché concurrentiel que dans la mesure minimale nécessaire pour atteindre les objectifs de la politique.

clients pour tous les FST et sont donc conformes au sous-alinéa 1b)(iii) des Instructions de 2006¹⁸.

81. En ce qui concerne la nouvelle exception proposée par le CDIP et le critère associé, comme le Conseil l'a fait remarquer ci-dessus, le dossier de la présente instance ne démontre pas qu'une telle mesure réglementaire serait nécessaire afin de protéger les intérêts des consommateurs. Pour des raisons semblables, l'adoption de cette proposition serait contraire aux Instructions de 2006, car une nouvelle exception, dans de telles circonstances, ne serait pas une mesure efficace ou proportionnée.
82. Les Instructions de 2019¹⁹ précisent que le Conseil doit, dans l'exercice des pouvoirs et des fonctions que lui confère la *Loi* afin de mettre en œuvre les objectifs de la politique canadienne de télécommunication, tenir compte de la façon dont ses décisions peuvent favoriser la concurrence, l'abordabilité, les intérêts des consommateurs et l'innovation.
83. Le Conseil est d'avis que ses conclusions dans la présente décision répondent aux exigences de l'alinéa 1a) des Instructions de 2019²⁰ car, grâce à la clarification de la portée du cadre de protection de la vie privée du Conseil et l'extension de ce cadre aux services de données commutées sans fil mobiles offerts par les entreprises de services de télécommunication, ses conclusions favorisent les intérêts des consommateurs.
84. De plus, le Conseil est d'avis que ses conclusions dans la présente décision répondent aux exigences du sous-alinéa 1a)(iv) des Instructions de 2019²¹, car, en confirmant et en clarifiant l'applicabilité des règles relatives aux renseignements confidentiels sur les clients dans le contexte des applications technologiques numériques de recherche des contacts, le Conseil établira une certitude pour les parties et pour la population canadienne. La clarté et la transparence des règles relatives aux renseignements confidentiels sur les clients serviront à protéger les droits des consommateurs dans leurs relations avec leurs FST.

¹⁸ Le sous-alinéa 1b)(iii) des Instructions de 2006 précise que le Conseil devrait, lorsqu'il a recours à la réglementation, prendre des mesures qui, si elles ne sont pas de nature économique, sont mises en œuvre, dans toute la mesure du possible, de manière symétrique et neutre sur le plan de la concurrence.

¹⁹ *Décret donnant au CRTC des instructions relativement à la mise en œuvre de la politique canadienne de télécommunication pour promouvoir la concurrence, l'abordabilité, les intérêts des consommateurs et l'innovation*, DORS/2019-227, 17 juin 2019

²⁰ L'alinéa 1a) des Instructions de 2019 précise que le Conseil devrait examiner comment ses décisions peuvent promouvoir la concurrence, l'abordabilité, les intérêts des consommateurs et l'innovation.

²¹ Le sous-alinéa 1a)(iv) des Instructions de 2019 précise que, lorsque le Conseil évalue comment sa décision contribue à promouvoir la concurrence, l'abordabilité, les intérêts des consommateurs et l'innovation, il devrait examiner la mesure dans laquelle sa décision sert à renforcer et à protéger les droits des consommateurs dans leurs relations avec les FST.

85. En ce qui concerne la nouvelle exception proposée par le CDIP et le critère associé, le dossier de la présente instance ne démontre pas qu'une telle mesure réglementaire serait nécessaire pour protéger les intérêts des consommateurs.

Secrétaire général

Documents connexes

- *Application des obligations réglementaires directement aux entreprises autres que les entreprises de télécommunication qui offrent et qui fournissent des services de télécommunication*, Politique réglementaire de télécom CRTC 2017-11, 17 janvier 2017; modifiée par les Politiques réglementaires de télécom CRTC 2017-11-1, 10 juillet 2017, et 2017-11-2, 17 juillet 2018
- *Modifications apportées au cadre d'abstention concernant les services de données mobiles sans fil*, Décision de télécom CRTC 2010-445, 30 juin 2010
- *Mesures réglementaires liées aux dispositions relatives à la confidentialité et à la protection de la vie privée*, Politique réglementaire de télécom CRTC 2009-723, 25 novembre 2009
- *Examen des pratiques de gestion du trafic Internet des fournisseurs des services d'Internet*, Politique réglementaire de télécom CRTC 2009-657, 21 octobre 2009
- *Utilisation de l'information E9-1-1 pour fournir le service d'avis à la communauté évolué*, Décision de télécom CRTC 2007-13, 28 février 2007
- *Abstention de la réglementation des services locaux de détail*, Décision de télécom CRTC 2006-15, 6 avril 2006
- *Demande en vertu de la partie VII visant la révision du paragraphe 11 des Modalités de service*, Décision de télécom CRTC 2005-15, 17 mars 2005
- *Clauses de confidentialité des entreprises Canadiennes*, Décision de télécom CRTC 2003-33, 30 mai 2003; modifiée par la Décision de télécom CRTC 2003-33-1, 11 juillet 2003
- Ordonnance Télécom CRTC 99-991, 13 octobre 1999
- *Abstention de réglementation des services sans fil mobiles fournis par des compagnies de téléphone appartenant à une municipalité*, Décision de télécom CRTC 98-19, 9 octobre 1998
- *Réglementation des services de télécommunications sans fil mobile*, Décision de télécom CRTC 96-14, 23 décembre 1996
- *Abstention – Services fournis par des entreprises Canadiennes non dominantes*, Décision de télécom CRTC 95-19, 8 septembre 1995

- *AGT, NBTel et Newfoundland Tel – Modifications aux règlements généraux*, Décision de télécom CRTC 95-6, 27 avril 1995
- *Examen des règlements généraux des transporteurs publics de télécommunications terrestres assujettis à la réglementation fédérale*, Décision de télécom CRTC 86-7, 26 mars 1986; modifiée par l'Ordonnance de télécom CRTC 86-593, 22 septembre 1986

Annexe à la Décision de télécom CRTC 2022-238

Dans un souci de clarté, les règles générales relatives aux renseignements confidentiels sur les clients sont exposées ci-dessous.

Tous les fournisseurs de services de télécommunication (FST), qu'il s'agisse d'entreprises de télécommunication ou d'entreprises autres que les entreprises de télécommunication (p. ex. les revendeurs), doivent se conformer aux dispositions suivantes en ce qui concerne la fourniture de services de télécommunication, à l'exception des services sans fil mobiles non commutés.

À moins que le client ne donne son consentement exprès ou que la communication ne se fasse en vertu d'un pouvoir légal, tous les renseignements conservés par l'entreprise concernant le client, autres que le nom, l'adresse et le numéro de téléphone inscrit du client, et y compris, entre autres, les adresses IP et les numéros de téléphone sans fil mobiles non inscrits, sont confidentiels et ne peuvent être communiqués par l'entreprise à quiconque autre que :

- le client;
- une personne qui, de l'avis raisonnable de l'entreprise, cherche à obtenir les renseignements en qualité de mandataire du client;
- une autre compagnie de téléphone, sous réserve que les renseignements soient requis aux fins de la prestation efficace et rentable du service téléphonique et que la communication se fasse à titre confidentiel et que les renseignements ne soient utilisés qu'à cette fin;
- une entreprise qui s'occupe de fournir au client des services téléphoniques ou relatifs à l'annuaire téléphonique, sous réserve que les renseignements soient requis à cette fin, que la communication se fasse à titre confidentiel et que les renseignements ne soient utilisés qu'à cette fin;
- un mandataire de l'entreprise dont les services ont été retenus aux fins d'obtenir le règlement de l'état de compte du client, sous réserve que les renseignements soient requis et ne soient utilisés qu'à cette fin;
- une autorité publique ou un agent d'une autorité publique, à des fins d'alerte publique d'urgence, si une autorité publique a déterminé qu'il existe un danger imminent ou en cours qui menace la vie, la santé ou la sécurité d'un individu et que le danger pourrait être évité ou atténué par la communication des renseignements;
- une entreprise affiliée impliquée dans la fourniture au client de services de télécommunication ou de radiodiffusion, sous réserve que les renseignements soient requis à cette fin, que la communication se fasse à titre confidentiel et que les renseignements ne soient utilisés qu'à cette fin.

Bien que ce qui précède expose la série générale d'exceptions, le Conseil reconnaît qu'il a précédemment approuvé certaines exceptions particulières aux FST. Ces exceptions continuent de s'appliquer, le cas échéant.

Le consentement exprès peut être estimé comme donné par un client lorsque celui-ci fournit les éléments suivants :

- son consentement écrit;
- sa confirmation orale vérifiée par une tierce partie indépendante;
- sa confirmation électronique par l'utilisation d'un numéro sans frais;
- sa confirmation électronique au moyen d'Internet;
- son consentement oral, lorsqu'un enregistrement audio du consentement est conservé par l'entreprise;
- son consentement par d'autres méthodes, pour autant qu'une trace documentée objective du consentement du client soit créée par ce dernier ou par un tiers indépendant.

Pour qu'il soit valable, le consentement exprès doit être explicite et donc clair et éclairé.