Décision de Conformité et d'Enquêtes de Télécom CRTC 2026-140

Version PDF

Gatineau, le 18 juin 2026

Dossier public : 1011-NOC2025-0143

Élargissement du cadre de blocage à l'échelle des réseaux

Sommaire

Le Conseil aide à assurer que la population canadienne ait accès à des services de télécommunication sécuritaires et fiables grâce à ses activités réalisées en vertu de la *Loi sur les télécommunications* et de la Loi canadienne anti-pourriel. En vertu de la *Loi sur les télécommunications*, il joue un rôle restreint en promouvant la conformité aux Règles sur les télécommunications non sollicitées afin d'aider à empêcher la composition d'appels indésirables pour la population canadienne qui ne respectent pas ces règles. En vertu de la Loi canadienne anti-pourriel, il aide à protéger la population canadienne des messages indésirables en ligne de concert avec le Bureau de la concurrence Canada et le Commissariat à la protection de la vie privée du Canada, en promouvant et en surveillant la conformité par le biais d'un régime de réglementation civil.

Un réseau de zombies est un réseau d'ordinateurs, de téléphones cellulaires ou d'autres appareils infectés par des logiciels malveillants. Cela permet à des individus ou à des groupes de contrôler les appareils à l'insu et sans le consentement de leurs propriétaires. Les réseaux de zombies peuvent être utilisés pour envoyer des pourriels à la population canadienne ou pour d'autres activités néfastes.

Le blocage à l'échelle des réseaux peut aider à démanteler les réseaux de zombies. Il joue un role essential en aidant les fournisseurs de services de télécommunication à protéger la population canadienne contre les fraudes, les escroqueries et d'autres activités néfastes. Cela inclut aider à empêcher que les personnes reçoivent des courriels ou des messages texte conçus pour les inciter à partager leurs renseignements personnels avec des individus ou des groupes aux intentions malveillantes.

Dans la décision de Conformité et Enquêtes et de Télécom 2025-142, le Conseil a établi un cadre pour permettre aux entreprises canadiennes de bloquer les réseaux de zombies et d'autres activités néfastes sur leurs réseaux avant qu'ils n'atteignent les appareils des Canadiennes et des Canadiens. Le Conseil a ensuite amorcé une consultation pour recueillir les points de vue à savoir si la portée du cadre devrait être élargie.

Le Conseil a reçu les observations d'un large éventail de participants au cours de l'instance, notamment du Centre national de coordination en cybercriminalité de la Gendarmerie royale du Canada, de l'Independent Telecommunications Providers Association et de plusieurs entreprises. En

se fondant sur le dossier public, le Conseil élargit son cadre de blocage à l'échelle des réseaux afin d'autoriser toute méthode de blocage approuvée qui respecte les principes directeurs de nécessité, de précision et de protection de la vie privée des consommateurs. Le blocage doit être effectué conformément au cadre de blocage figurant en annexe de la présente décision, à compter du 18 juin 2026. En plus d'offrir plus de souplesse aux entreprises qui effectuent des activités de blocage à l'échelle des réseaux, la présente décision simplifie les exigences du cadre en matière de déclaration au Conseil et de diffusion de renseignements au public.

Le cadre révisé contribuera à réduire au minimum le fardeau administratif des entreprises de services de télécommunication, à diminuer les coûts relatifs à la conformité et à promouvoir l'innovation, tout en aidant ces entreprises à protéger plus efficacement la population canadienne contre la fraude, les escroqueries et autres activités néfastes.

Une opinion minoritaire du conseiller Bram Abramson est jointe à la présente décision.

Contexte

1. Dans la décision de Conformité et Enquêtes et de Télécom 2022-170, le Conseil a déterminé que l'approche réglementaire la plus appropriée pour traiter les réseaux de zombies[1] consiste à créer un cadre guidé par les principes de nécessité, de protection de la vie privée des clients, de reddition de comptes, de transparence et de précision. Ce cadre définit les conditions dans lesquelles les entreprises de services de télécommunication canadiennes peuvent procéder à un blocage à l'échelle des réseaux.

2. Dans la décision de Conformité et Enquêtes et de Télécom 2025-142, le Conseil a établi un cadre autorisant les entreprises de services de télécommunication à bloquer les réseaux de zombies et autres activités néfastes traversant leurs réseaux à l'aide de listes de blocage[2] qui répondent à des critères précis. Parallèlement, le Conseil a amorcé une instance au moyen de l'avis de consultation de Conformité et Enquêtes et de Télécom 2025-143 (instance) afin d'examiner si le cadre devrait être élargi pour inclure d'autres méthodes de blocage et, le cas échéant, si des mesures de protection de la vie privée et des exigences de déclaration supplémentaires sont nécessaires.

3. Des interventions ont été reçues du Centre national de coordination en cybercriminalité de la Gendarmerie royale du Canada, de l'Independent Telecommunications Providers Association et

---

[1] Un réseau de zombies est un réseau d'ordinateurs, de téléphones portables ou d'autres appareils infectés par des logiciels malveillants. Cela permet à des individus ou à des groupes de contrôler ces appareils à l'insu et sans le consentement de leurs propriétaires. Les réseaux de zombies peuvent être utilisés pour envoyer des pourriels à la population canadienne ou pour d'autres activités néfastes.

[2] Les listes de blocage sont des indicateurs de compromission qui aident à repérer les activités néfastes. Les entreprises peuvent utiliser ces listes pour empêcher le trafic en ligne suspect ou dangereux de passer par leurs réseaux.

de huit entreprises de services de télécommunication : Bragg Communications Inc., exerçant ses activités sous le nom d'Eastlink (Eastlink); Bell Canada; Cogeco Communications inc. (Cogeco); Québecor Média inc. (Québecor); Rogers Communications Canada Inc. (Rogers); Saskatchewan Telecommunications; TekSavvy Solutions Inc.; et TELUS Communications Inc. (TELUS). Bell Canada, Rogers et TELUS ont également répliqué aux interventions.

Questions

4. Le Conseil a identifié les questions suivantes à traiter :

    - La portée du cadre devrait-elle être élargie pour inclure des méthodes de blocage autres que les listes de blocage?
    - Le cadre devrait-il inclure des mesures supplémentaires pour protéger la vie privée?
    - Devrait-on réviser les exigences en matière de déclaration prévues par le cadre?

La portée du cadre devrait-elle être élargie pour inclure des méthodes de blocage autres que les listes de blocage?

Positions des parties

5. Les entreprises ont indiqué qu'elles s'appuient sur toute une gamme de méthodes de blocage autres que les listes de blocage pour bloquer les réseaux de zombies et autres cybermenaces, notamment le blocage de ports[3], le blocage des adresses source falsifiées[4] et le blocage du trafic sur la base d'anomalies de volume[5].

6. La plupart des entreprises ont averti que tout élargissement du cadre doit leur laisser la latitude nécessaire pour faire face à la nature dynamique des réseaux de zombies et autres cybermenaces. Elles ont souligné que les entreprises ont besoin d'indépendance et d'une marge de manœuvre opérationnelle pour mettre en œuvre et adapter leurs méthodes de blocage, parfois

---

[3] Le blocage de ports consiste à empêcher le trafic Internet d'utiliser des ports de communication particuliers connus pour être la cible d'activités malveillantes. Les entreprises bloquent certains ports afin de protéger les utilisateurs contre les attaques qui exploitent couramment ces ports.

[4] Les adresses source falsifiées sont des adresses IP (protocole Internet) qui ont été modifiées pour dissimuler l'identité de l'expéditeur et faire croire au système destinataire que le trafic provient d'une source fiable ou différente. Le blocage du trafic Internet comportant des adresses falsifiées aide les entreprises à prévenir les attaques qui reposent sur l'usurpation d'identité d'utilisateurs ou de systèmes légitimes.

[5] Les anomalies de volume de trafic désignent des changements inhabituels dans la quantité de données transitant par un réseau. Les entreprises surveillent et bloquent les anomalies de volume de trafic afin de maintenir la stabilité des réseaux et de les protéger contre les cyberattaques.

en temps réel, en réponse à des menaces en évolution rapide. Le Centre national de coordination en cybercriminalité a renforcé ce point en soulignant que les menaces à l'échelle des réseaux deviennent plus sophistiquées et plus dissimulées, et gagnent en ampleur, en vitesse et en précision.

7. Certaines entreprises ont également suggéré qu'un cadre qui n'autorise que certaines méthodes de blocage et impose des conditions d'utilisation strictes serait inefficace et potentiellement contre-productif. Bell Canada a fait remarquer que, dans le cadre actuel, une entreprise ne peut utiliser des listes de blocage tierces que si celles-ci répondent à une longue liste de critères auxquels les fournisseurs pourraient ne pas être en mesure ou disposés à se conformer. Cela pourrait contraindre les entreprises à cesser d'utiliser des listes de blocage tierces, ce qui compromettrait la sécurité même du réseau que le cadre est censé promouvoir.

8. TELUS a fait valoir que les exigences actuelles du cadre en matière de règlement des plaintes ne seraient pas applicables si d'autres méthodes de blocage étaient intégrées au cadre.

Analyse du Conseil

Méthodes de blocage

9. Les entreprises utilisent diverses méthodes de blocage en combinaison pour protéger leurs réseaux, notamment les listes de blocage, le blocage de ports, le blocage des adresses sources falsifiées et le blocage du trafic en fonction d'anomalies de volume. Ces méthodes sont bien établies et s'alignent sur les pratiques exemplaires reconnues par l'industrie, élaborées par le Comité consultatif canadien pour la sécurité des télécommunications (CCCST) et l'Internet Engineering Task Force[6].

10. Limiter le cadre pourrait amener les entreprises à bloquer du trafic malveillant sans l'autorisation du Conseil ou à restreindre leur capacité à répondre à de nouvelles menaces. Si un modèle centralisé et normatif peut rendre la mise en œuvre plus cohérente, il pourrait contraindre les entreprises à cesser d'utiliser des méthodes de blocage largement répandues et conformes aux pratiques exemplaires de l'industrie. Il risque également de s'avérer inefficace, car toute tentative de définir des solutions à l'avance sera dépassée par des activités malveillantes en constante évolution.

11. L'adoption d'un modèle réglementaire simplifié, fondé sur des principes, soutiendra les

[6] Le CCCST est un comité consultatif qui permet aux secteurs privé et public d'échanger des renseignements et de collaborer de manière stratégique sur des questions actuelles et émergentes susceptibles d'avoir une influence sur l'infrastructure des télécommunications, y compris les menaces de cybersécurité. Le CCCST comprend le Groupe de travail canadien sur la cyberprotection des télécommunications, qui a élaboré des pratiques exemplaires à l'intention des fournisseurs de services de télécommunication canadiens. L'Internet Engineering Task Force est un organisme international qui élabore des normes pour la suite IP, à savoir le protocole de contrôle de transmission/protocole Internet (TCP/IP).

pratiques de blocage existantes des entreprises tout en leur accordant une marge d'appréciation pour choisir les outils, les fournisseurs et les détails de mise en œuvre. Conformément aux Instructions de 2023[7], ce modèle encouragera les entreprises à se faire concurrence et à innover à mesure que les technologies évoluent et que de nouvelles tactiques sont utilisées par les acteurs malveillants.

12. Étant donné que les entreprises utilisent diverses méthodes de blocage et qu'il existe un large consensus sur la nécessité de faire preuve de souplesse pour faire face à l'évolution des activités néfastes, le Conseil élargira le cadre réglementaire afin d'autoriser toute méthode de blocage conforme aux principes de nécessité, de précision et de protection de la vie privée des consommateurs. Ces principes soulignent que le blocage dans le cadre de ce dispositif doit être effectué exclusivement à des fins de cybersécurité, que toute incidence sur les services légitimes doit être limitée à ce qui est nécessaire pour bloquer le trafic malveillant, et que la vie privée des consommateurs doit être pleinement préservée.

Règlement des plaintes

13. Le principe de précision établi dans la décision de Conformité et Enquêtes et de Télécom 2022-170 et énoncé à la section 5 du cadre actuel précise que le public doit avoir la possibilité de signaler et de résoudre les faux positifs et les blocages excessifs de manière efficace et en temps opportun. Toutefois, il ne prescrit pas de délais fixes ni de mesures précises à prendre par les entreprises.

14. Le cadre actuel exige des entreprises qu'elles règlent les plaintes des clients dans un délai de deux jours ouvrables, soit en mettant à jour la liste de blocage concernée, soit en répondant au client.

15. Le dossier de l'instance suggère que ces exigences peuvent s'avérer peu réalistes compte tenu des mesures opérationnelles que les entreprises doivent prendre pour résoudre les plaintes et des diverses méthodes de blocage et solutions de fournisseurs utilisées. De plus, les exigences actuelles ne s'appliquent qu'aux plaintes liées aux listes de blocage.

16. Par conséquent, le Conseil exigera des entreprises qu'elles règlent les plaintes dans un délai de cinq jours ouvrables sans leur imposer de mesures précises à prendre. Cette approche garantit aux clients l'accès à un redressement en temps opportun tout en reconnaissant que les enquêtes sur les plaintes peuvent être complexes, nécessiter d'importantes ressources et dépendre de la coopération de tiers.

17. Compte tenu de ce qui précède, le Conseil détermine que le cadre sera révisé afin de :

---

[7] *Décret donnant au CRTC des instructions sur une approche renouvelée de la politique de télécommunication*, DORS/2023-23, 10 février 2023, alinéas 2a) et 2f).

- permettre aux entreprises d'utiliser toute méthode de blocage conforme aux principes directeurs du cadre;

- fournir aux entreprises une plus grande latitude dans la manière dont elles traitent les plaintes des clients.

18. Les définitions des termes « liste de blocage » et « fournisseur de liste de blocage » figurant dans le cadre précédent ont été remplacées par les définitions plus larges de « méthode de blocage » et de « fournisseur tiers » afin de refléter le champ d'application élargi du cadre.

Le cadre devrait-il inclure des mesures supplémentaires pour protéger la vie privée?

Positions des parties

19. La plupart des entreprises ont fait valoir qu'aucune mesure de protection supplémentaire de la vie privée n'était nécessaire, car les lois existantes en matière de protection de la vie privée ainsi que les règles et règlements du Conseil protègent déjà les Canadiennes et les Canadiens et leurs renseignements personnels dans le contexte du blocage à l'échelle des réseaux.

20. Les entreprises ont généralement convenu que la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) et les mesures de protection de la confidentialité des consommateurs du Conseil[8] offrent une protection suffisante de la vie privée. Québecor a indiqué que l'imposition de nouvelles interdictions concernant l'utilisation des renseignements personnels recueillis dans le cadre du cadre réglementaire pourrait entraver l'innovation, nuire à l'efficacité des mesures de cybersécurité et empêcher le développement d'outils bénéfiques pour les consommateurs. Cogeco a fait remarquer que de nouvelles interdictions pourraient entrer en conflit avec les exceptions et les exemptions prévues par les lois existantes en matière de protection de la vie privée.

21. Alors que la plupart des entreprises ont indiqué que les renseignements personnels recueillis dans le cadre de ce dispositif ne sont utilisés qu'à des fins de blocage, Québecor et TELUS ont suggéré que certaines utilisations secondaires, notamment à des fins de marketing, devraient être autorisées si elles sont menées dans le respect des lois et règlements applicables. TELUS a fait remarquer que le Commissariat à la protection de la vie privée du Canada a reconnu que la publicité comportementale en ligne peut être considérée comme une fin raisonnable au sens de

[8] En plus de la LPRPDE, les entreprises de services de télécommunication sont tenues de se conformer aux mesures de protection de la confidentialité des consommateurs imposées par le Conseil (voir par exemple la décision de télécom 2003-33; les politiques réglementaires de télécom 2009-723 et 2017-11; et la décision de télécom 2022-238).

la LPRPDE, à condition qu'elle soit menée selon certains paramètres[9].

Analyse du Conseil

22. Dans la décision de Conformité et Enquêtes et de Télécom 2022-170, le Conseil a fait de la protection de la vie privée des consommateurs un principe directeur du cadre réglementaire. Ce principe a ensuite été mis en œuvre à la section 8.2 du cadre publié dans la décision de Conformité et Enquêtes et de Télécom 2025-142. Les entreprises de services de télécommunication sont tenues de se conformer aux obligations existantes en matière de protection de la vie privée et d'adopter les pratiques exemplaires afin d'assurer le plus haut niveau de protection. Cela signifie qu'elles doivent veiller à ce que les renseignements personnels recueillis, utilisés ou divulgués aux fins de blocage se limitent à ce qui est essentiel à cette fin, ne soient conservés que pendant la durée nécessaire à cette fin et ne soient pas utilisés ou divulgués à d'autres fins.

23. Les entreprises répondent généralement aux attentes du cadre en matière de protection de la vie privée des consommateurs. Elles semblent limiter la collecte, l'utilisation et la divulgation des renseignements personnels à ce qui est nécessaire aux fins du blocage, ne les conservent que pendant de courtes périodes et les anonymisent et les agrègent une fois les activités de blocage terminées. L'accès est limité au personnel autorisé, et la divulgation n'est effectuée que lorsque la loi l'exige.

24. Compte tenu de ce qui précède, le Conseil détermine qu'aucune mesure de protection de la vie privée supplémentaire n'est nécessaire au-delà de celles déjà établies dans le cadre. Le Conseil estime toutefois qu'il convient de préciser, comme indiqué à la section 7.3 du cadre figurant en annexe de la présente décision, que toute utilisation issue de l'inspection approfondie des paquets[10] doit être limitée à des circonstances exceptionnelles, telles que l'exécution d'une ordonnance judiciaire ou l'ajustement des systèmes de gestion des menaces à la suite d'une cyberattaque. Dans de tels cas, l'inspection doit se limiter aux en-têtes de paquets et ne doit pas porter sur le contenu des communications.

25. En ce qui concerne la suggestion selon laquelle les renseignements personnels recueillis en vertu du cadre pourraient être utilisés à des fins secondaires, le Conseil estime, comme indiqué à la section 7.2 du cadre figurant en annexe à la présente décision, que le principe directeur de la protection de la vie privée des consommateurs se veut souple afin de permettre des utilisations secondaires licites, fondées sur le consentement ou autrement autorisées.

---

[9] *Commissariat à la protection de la vie privée du Canada* (2015). Position de principe sur la publicité comportementale en ligne.

[10] L'inspection approfondie des paquets est une méthode permettant d'examiner le contenu des paquets de données qui transitent par un réseau. Elle peut être utilisée pour détecter les paquets contenant du contenu malveillant.

Devrait-on réviser les exigences en matière de déclaration prévues par le cadre?

Positions des parties

26. La plupart des entreprises ont exprimé des préoccupations concernant les exigences actuelles du cadre en matière de déclaration.

27. De nombreuses entreprises ont averti que la publication de rapports détaillés sur leurs pratiques de blocage et leurs résultats pourrait indirectement aider des acteurs malveillants à cerner des vulnérabilités potentielles, à adapter leurs attaques et à contourner les mesures de protection du réseau.

28. Certaines entreprises ont émis des doutes quant à l'intérêt pour les consommateurs des renseignements techniques concernant les solutions de blocage à l'échelle des réseaux mises en œuvre par les entreprises. Elles ont suggéré que le Canadien moyen n'est probablement pas intéressé par les renseignements communiqués ni en mesure de les comprendre pleinement.

29. Plusieurs entreprises ont également fait valoir qu'il serait compliqué et coûteux en ressources de mettre en place et de réorganiser leurs systèmes pour se conformer aux exigences en matière de déclaration. Elles ont fait remarquer que les solutions de blocage ne sont généralement pas conçues pour fournir des données détaillées à des fins de rapport. TELUS et Eastlink ont laissé entendre que de telles limitations techniques pourraient empêcher les entreprises de se conformer aux exigences en matière de déclaration.

30. Bell Canada a recommandé que le Conseil demande au Groupe de travail Réseaux (GTR)[11] du Comité directeur du CRTC sur l'interconnexion (CDCI) de réexaminer la question des indicateurs de rapport appropriés. À titre subsidiaire, Bell Canada a suggéré que les exigences actuelles en matière de déclaration soient remplacées par les deux indicateurs proposés par le GTR du CDCI dans le rapport examiné dans la décision de Conformité et Enquêtes et de Télécom 2025-142 : le nombre d'indicateurs de compromission (IC) bloqués et le nombre de faux positifs signalés. À titre de solution de rechange, Bell Canada a suggéré de réduire et de clarifier les règles de déclaration existantes et de permettre aux entreprises de déposer leurs rapports à titre confidentiel.

Analyse du Conseil

31. Dans la décision de Conformité et Enquêtes et de Télécom 2022-170, le Conseil a fait de la transparence un principe directeur du cadre et a établi ce qui suit :

---

[11] Le CDCI est un organisme créé par le Conseil pour aider à élaborer les renseignements, les procédures et les lignes directrices qui peuvent être nécessaires dans divers aspects des activités réglementaires du Conseil. Le GTR s'occupe des tâches liées à l'exploitation des réseaux et aux questions connexes.

- Les entreprises doivent publier sur leur site Web suffisamment de renseignements sur leurs solutions de blocage pour permettre aux clients de choisir en connaissance de cause l'entreprise avec laquelle ils souhaitent faire affaire, sans pour autant en divulguer trop, ce qui aiderait des acteurs malveillants à contourner ces solutions;

- Les entreprises sont tenues de communiquer des indicateurs de rendement au Conseil afin de permettre la divulgation publique de statistiques agrégées et l'évaluation de la nécessité de mesures réglementaires supplémentaires.

32. Ce principe a ensuite été mis en œuvre dans les sections 6 et 7 du cadre publié dans la décision de Conformité et Enquêtes et de Télécom 2025-142.

Renseignements sur les sites Web des entreprises

33. Le Conseil estime que les renseignements généraux figurant sur les sites Web des entreprises concernant les pratiques de blocage sont suffisants pour éclairer le choix des consommateurs. De plus, le Conseil estime que l'obligation de publier un avis préalable pour chaque modification apportée à une méthode de blocage pourrait alerter les acteurs malveillants et compromettre l'efficacité du cadre réglementaire.

34. Par conséquent, le Conseil révisera le cadre réglementaire afin d'exiger des entreprises qu'elles publient moins de détails techniques sur leurs sites Web, tout en veillant à ce qu'elles divulguent publiquement suffisamment de renseignements sur leurs pratiques de blocage pour aider les clients à prendre des décisions éclairées. Cela permettra de réduire le fardeau administratif pesant sur les entreprises et le risque d'exposer des renseignements sensibles à des acteurs malveillants, tout en garantissant un niveau minimal de transparence concernant les activités de blocage des entreprises.

Déclaration au Conseil

35. Le Conseil fait remarquer que, dans le cadre actuel, les exigences en matière de rapports sont beaucoup plus détaillées que ce que prévoient les deux indicateurs recommandés par le GTR du CDCI (IC uniques bloqués et faux positifs signalés). Ces indicateurs ont été jugés suffisants par l'industrie pour fournir un aperçu significatif du rendement des entreprises. Le Conseil estime que limiter les exigences à ces indicateurs contribuerait à réduire les coûts de mise en conformité pour les entreprises.

36. Cependant, le Conseil estime qu'il a besoin de plus de renseignements que ceux fournis par ces deux indicateurs pour exercer une surveillance efficace. Bien que le nombre d'IC bloqués et de faux positifs reçus donne une indication de base de l'ampleur du blocage et de son incidence sur les services légitimes, ils ne fournissent pas suffisamment de renseignements pour évaluer si les pratiques de blocage des entreprises sont conformes aux principes directeurs du cadre. Limiter les exigences de déclaration répond aux préoccupations soulevées concernant le fardeau administratif, mais cela supprime également des indicateurs importants de l'activité et du

rendement des entreprises en matière de blocage.

37. Le nouveau modèle réglementaire n'est pas non plus aussi normatif que l'approche initiale, qui s'appuyait sur des critères techniques détaillés pour garantir le respect des conditions générales. Dans le cadre de la nouvelle approche, les entreprises disposent d'une plus grande latitude dans le choix des méthodes de blocage et des détails opérationnels. Par conséquent, le Conseil estime que, dans le cadre révisé, les entreprises doivent adapter la manière dont elles démontrent leur reddition de comptes.

38. Compte tenu des exigences simplifiées du cadre révisé, le Conseil détermine que les entreprises seront tenues de lui présenter des rapports annuels simplifiés. Le rapport doit inclure les éléments suivants :

    - le nombre total d'IC bloqués par l'entreprise;
    - le nombre total de plaintes pour faux positifs et blocage excessif reçues des clients;
    - une description des mesures de blocage utilisées à l'échelle des réseaux;
    - une explication de la manière dont les mesures de blocage sont conformes au cadre.

39. Cette approche permettra une surveillance efficace tout en protégeant les renseignements sensibles et en laissant aux entreprises la latitude nécessaire pour démontrer leur conformité d'une manière qui reflète leur environnement réseau unique. Elle fournira également au Conseil les renseignements dont elle a besoin pour cerner les problèmes potentiels (p. ex. les fournisseurs à haut risque, les outils portant atteinte à la vie privée et les risques de blocage excessif) et vérifier la conformité. Au besoin, le Conseil pourra prendre des mesures pour remédier à la non-conformité, notamment en demandant des renseignements supplémentaires, en collaborant avec les entreprises pour clarifier ou ajuster leurs pratiques, ou en utilisant d'autres outils d'enquête et d'application prévus par la *Loi sur les télécommunications* (*Loi*).

40. Afin de renforcer la transparence publique, le Conseil rendra publics, à sa discrétion, le nombre d'IC bloqués et le nombre de plaintes pour faux positifs ou blocage excessif signalées, car il est peu probable que ces renseignements soient exploités par des acteurs malveillants. Le Conseil a également l'intention d'utiliser les renseignements fournis dans les rapports annuels confidentiels pour établir des résumés agrégés des activités de blocage à l'échelle de l'industrie. Ces résumés expliqueront la portée, l'incidence et les avantages des activités de blocage des entreprises d'une manière accessible et significative pour la population canadienne, tout en protégeant les renseignements sensibles.

41. Le Conseil estime que cette approche établit un juste équilibre entre la transparence envers le public, la reddition de comptes et la confidentialité des pratiques de blocage des entreprises.

Conclusion

42. Le Conseil approuve, conformément à l'article 36 de la *Loi*, le cadre révisé pour le blocage à l'échelle des réseaux figurant en annexe de la présente décision. Il entrera en vigueur le 18 juin 2026.

43. En vertu de l'article 36 de la *Loi*, les entreprises canadiennes doivent obtenir l'approbation du Conseil pour contrôler ou influencer le contenu des télécommunications. En bloquant le trafic des réseaux de zombies et d'autres activités néfastes, les entreprises canadiennes peuvent empêcher la transmission de télécommunications aux utilisateurs, contrôlant ainsi le contenu des télécommunications qu'elles acheminent pour le public. Par conséquent, cette activité relève du champ d'application de l'article 36 de la *Loi*.

44. Le cadre définit les modalités permettant aux entreprises canadiennes de bloquer les réseaux de zombies et autres activités néfastes. La participation à ce cadre est volontaire; les entreprises ne sont pas tenues de bloquer le trafic Internet transitant par leurs réseaux pour se protéger contre les cyberattaques. Toutefois, si elles choisissent de le faire, elles doivent se conformer aux modalités énoncées dans le cadre.

45. Le Conseil encourage les fournisseurs de services de télécommunication autres que les entreprises de services de télécommunication à adopter une approche similaire. Si des fournisseurs de services de télécommunication autres que les entreprises de services de télécommunication choisissent de bloquer le trafic réseau à des fins de cybersécurité d'une manière non conforme au cadre, le Conseil pourra examiner s'il y a lieu de prendre des mesures réglementaires supplémentaires.

Instructions de 2023

46. Le Conseil estime que le cadre fera progresser les objectifs stratégiques en matière de télécommunications énoncés dans la *Loi*[12] ainsi que les intérêts des consommateurs et les objectifs d'innovation des Instructions de 2023 en aidant à protéger la population canadienne contre les réseaux de zombies et les autres activités néfastes ainsi qu'en rendant les services de télécommunication plus fiables. Le cadre est conçu pour être neutre sur le plan technologique et souple afin d'encourager les entreprises à innover dans la lutte contre les cybermenaces et d'aider à protéger la vie privée des personnes en interdisant l'accès et la collecte non autorisés de leurs renseignements personnels.

Secrétaire général

---

[12] Les objectifs cités sont les suivants : 7b) permettre l'accès aux Canadiens dans toutes les régions — rurales ou urbaines — du Canada à des services de télécommunication sûrs, abordables et de qualité ; 7g) stimuler la recherche et le développement au Canada dans le domaine des télécommunications ainsi que l'innovation en ce qui touche la fourniture de services dans ce domaine ; 7h) satisfaire les exigences économiques et sociales des usagers des services de télécommunication; et 7i) contribuer à la protection de la vie privée des personnes.

Annexe à la Décision de Conformité et Enquêtes et de Télécom CRTC 2026-140

Cadre pour le blocage à l'échelle des réseaux

Définitions

Blocage excessif : Blocage appliqué à du trafic malveillant, mais trop général et s'appliquant aussi à du contenu non malveillant.

Client : Personne abonnée aux services de l'entreprise qui font l'objet du blocage.

Cyberattaque : Utilisation malveillante de moyens électroniques pour interrompre, manipuler, détruire ou obtenir un accès non autorisé à un système, un réseau ou un dispositif informatique.

Cybersécurité : Ensemble des technologies, processus, pratiques et mesures d'intervention et d'atténuation conçus afin de protéger contre les cyberattaques et de garantir la confidentialité, l'intégrité et la disponibilité des renseignements électroniques.

Entreprise canadienne (selon la définition de la *Loi sur les télécommunications*) : Propriétaire ou exploitant d'une installation de transmission grâce à laquelle sont fournis par lui-même ou une autre personne des services de télécommunication au public moyennant contrepartie.

Faux positif : Se produit lorsque du contenu non malveillant est bloqué à tort.

Fournisseur tiers : Toute personne ou entité qui fournit des systèmes, de l'équipement ou des logiciels qu'une entreprise utilise pour mettre en œuvre une méthode de blocage.

Indicateur de compromission (IC) : Identifiant utilisé par les entreprises pour bloquer le trafic réseau afin d'assurer une protection contre les cyberattaques et qui indique, avec un degré de confiance élevé, qu'il y a une intrusion dans un système et qu'une activité malveillante est en cours. En d'autres termes, un IC est une caractéristique technique d'une cyberattaque particulière.

Méthode de blocage : Toute mesure pouvant être utilisée par une entreprise pour bloquer le trafic Internet malveillant transitant par son réseau.

Période de déclaration : Année civile du 1er janvier au 31 décembre (12 mois), la première période de déclaration commençant le jour de l'entrée en vigueur du cadre énoncé à l'annexe de la Décision de Conformité et Enquêtes et de Télécom CRTC 2026-140 et se terminant le 31 décembre de cette année.

***

Conformément à l'article 36 de la *Loi sur les télécommunications*, le Conseil autorise les entreprises

canadiennes à prendre des mesures de cybersécurité pour bloquer le trafic Internet passant par leurs réseaux, uniquement dans le but de se protéger contre les cyberattaques, sous réserve du respect des modalités énoncées ci-dessous. Les modalités entreront en vigueur le 18 juin 2026.

Cette autorisation ne s'applique pas au blocage du trafic à d'autres fins, y compris le blocage d'activités par ailleurs illégales, ou le blocage à des fins commerciales, concurrentielles ou politiques.

1.0. Blocage par défaut

1.1. Le blocage doit fonctionner au niveau du réseau par défaut : un client ne peut y adhérer ou s'en retirer.

1.2. Toutefois, l'entreprise ne doit mettre en œuvre aucune mesure qui pourrait empêcher les clients d'utiliser des services légitimes permettant de contourner le blocage, tels que des services de réseau privé virtuel ou d'autres résolveurs du système de noms de domaine.

2.0. Mesures de blocage autorisées

2.1. L'entreprise ne peut bloquer le trafic Internet malveillant qu'en utilisant des mesures conformes aux principes directeurs de nécessité, de précision et de protection de la vie privée des consommateurs énoncés à l'annexe 1 de la Décision de Conformité et Enquêtes et de Télécom CRTC 2022-170.

2.2. Il incombe à l'entreprise de démontrer que ses mesures sont conformes à ces principes, comme le prévoit la sous-section 6.1d) du présent cadre.

2.3. Les fournisseurs tiers auxquels fait appel une entreprise doivent répondre, au minimum, aux critères suivants :

a) Le fournisseur tiers possède l'expertise technique nécessaire, comme le démontrent, par exemple, des années d'activité dans la recherche sur les cybermenaces nouvelles et changeantes, par l'acceptation du marché et l'approbation certifiée des professionnels de l'industrie, ou par des certifications selon des normes internationales reconnues.

b) Le fournisseur tiers n'a aucun conflit d'intérêts potentiel (p. ex. propriété et contexte géopolitique) qui pourrait compromettre le fonctionnement de ses systèmes, de son équipement ou de ses logiciels de manière impartiale et dans l'intérêt supérieur de la population canadienne.

3.0. Nécessité

3.1. Une entreprise ne peut recourir à une méthode de blocage que dans le but de protéger ses réseaux et les ordinateurs de ses clients contre les réseaux de zombies malveillants (c.-à-d. contre l'intégration à un réseau d'appareils infectés par des logiciels malveillants contrôlés par un acteur malveillant à l'insu et sans le consentement des clients) et contre d'autres

cybermenaces, notamment les logiciels malveillants et le phishing.

4.0. Précision

4.1. Une entreprise doit s'assurer que ses méthodes de blocage sont précises et réduisent au minimum le risque de faux positifs et de blocage excessif.

4.2. Une entreprise devrait prendre des mesures pour limiter l'incidence de ses activités de blocage sur les services légitimes à ce qui est nécessaire pour bloquer le trafic malveillant. Cela peut inclure des mécanismes permettant de vérifier que le trafic bloqué est bien malveillant, des processus visant à évaluer les dommages collatéraux potentiels sur les services légitimes, ainsi que des processus visant à mettre à jour ou à affiner les méthodes de blocage.

4.3. Une entreprise doit disposer d'un processus permettant de recevoir, de valider et de résoudre les plaintes des clients liées aux faux positifs et au blocage excessif[1]. Ce processus devrait inclure l'examen du problème signalé, l'ajustement ou la mise à jour de la méthode de blocage si nécessaire, et la notification du client si nécessaire.

4.4. L'entreprise doit résoudre une plainte dans les cinq jours ouvrables suivant sa réception.

5.0. Transparence (divulgation publique)

5.1. L'entreprise doit divulguer, clairement et bien en évidence sur son site, des renseignements sur le blocage de cybersécurité effectué en vertu de ce cadre. Ces renseignements doivent être mis en évidence par un en-tête « Blocage de cybersécurité » distinct[2]. L'entreprise doit également faire référence à ses divulgations en ligne dans le matériel promotionnel pertinent, les contrats avec les clients et les modalités d'utilisation.

5.2. La divulgation en ligne doit fournir i) suffisamment de renseignements, rédigés dans un langage clair, pour que la population canadienne comprenne le type et la portée du blocage en place, ii) si l'entreprise fait appel à des fournisseurs tiers pour soutenir ses activités de blocage (y compris si ces fournisseurs sont situés à l'extérieur du Canada), iii) le processus de dépôt et d'enquête sur les plaintes liées à des faux positifs et à un blocage excessif potentiels; iv) tout renseignement pertinent lié à la confidentialité et les déclarations nécessaires. À tout le moins, les renseignements suivants doivent être inclus :

---

[1] Les clients peuvent également déposer leurs plaintes directement au Conseil via la page « Communiquez avec nous ».

[2] Ces renseignements peuvent être publiés sur la même page Web que les renseignements divulgués conformément aux exigences actuelles du Conseil relatives aux pratiques de gestion du trafic Internet ou à tout autre endroit pertinent.

a) Que le blocage respecte les modalités énoncées dans le présent cadre;

b) Une description générale des méthodes de blocage utilisées et de leur fonctionnement;

c) Les coordonnées de l'entreprise pour déposer des plaintes et le processus à suivre;

d) Que le blocage a pour but de fournir des services Internet plus sécuritaires, mais qu'il ne remplace pas les mesures de protection au niveau de l'utilisateur : les fournisseurs de services fournissent des mesures de protection en matière de cybersécurité pour leurs réseaux et les consommateurs fournissent des mesures de protection en matière de cybersécurité pour leurs propres appareils. Par conséquent, il reste important que les clients continuent de sécuriser leurs appareils et leur connexion Internet contre les cybermenaces (p. ex. en installant et en mettant à jour des solutions antivirus, en mettant régulièrement à jour leurs logiciels, en gérant un pare-feu, en utilisant des mots de passe forts, en activant l'authentification à deux facteurs et en sécurisant leur connexion sans fil).

5.3. La divulgation en ligne doit être accessible aux personnes en situation de handicap, conformément aux conclusions sur l'accessibilité énoncées dans la Politique réglementaire de radiodiffusion et de télécom CRTC 2009-430.

6.0. Transparence (rapports du Conseil)

6.1. L'entreprise doit déposer auprès du Conseil[3] les renseignements suivants sur les activités de blocage pendant la période de déclaration, dans les 30 jours civils suivant la fin de celle-ci[4] :

a) L'identification de toutes les listes de blocage utilisées par l'entreprise, y compris celles provenant de fournisseurs ou de produits tiers auxquels elle fait appel;

b) le nombre total d'IC bloqués par l'entreprise;

c) le nombre total de plaintes pour faux positifs ou blocage excessif reçues des clients;

d) une justification détaillée expliquant en quoi le blocage est conforme aux conditions générales du présent cadre;

e) un hyperlien vers la page Web utilisée pour remplir les exigences de divulgation établies à

---

[3] En ce qui concerne la méthode de dépôt, consulter la page Web « Soumettre des demandes et autres documents auprès du CRTC en utilisant Mon compte CRTC ».

[4] Le Conseil peut, à sa discrétion, rendre publiques les mesures indiquées aux points b) et c). Le Conseil peut également utiliser les renseignements issus des rapports annuels confidentiels pour établir des résumés agrégés des activités de blocage à l'échelle des réseaux dans l'ensemble de l'industrie.

la section 5.0.

7.0. Reddition de comptes et protection de la vie privée

7.1. L’entreprise doit examiner périodiquement tous ses systèmes de blocage assujettis à ce cadre afin de vérifier qu’ils fonctionnent comme prévu.

7.2. Si l’entreprise recueille, utilise ou a l’intention de divulguer des renseignements personnels aux fins des activités exercées en vertu du présent cadre, elle doit se conformer pleinement à toutes les lois et à tous les règlements applicables relatifs à la protection des renseignements personnels. Ce cadre ne permet pas la collecte, l’utilisation ou la divulgation supplémentaire de renseignements personnels, sauf lorsque ces activités sont autorisées par les lois et règlements applicables ou par une ordonnance d’un tribunal compétent.

7.3. Toute utilisation de l’inspection approfondie des paquets dans le cadre du présent cadre doit être limitée à des circonstances exceptionnelles, telles que le respect d’une ordonnance d’un tribunal ou l’ajustement des systèmes de gestion des menaces à la suite d’une cyberattaque. Dans de tels cas, l’inspection doit se limiter aux en-têtes des paquets et ne doit pas impliquer l’inspection du contenu des communications.

8.0. Autres conditions

8.1. L’entreprise doit se conformer à toute autre condition que le Conseil peut établir de temps à autre à la suite d’un processus public.

Opinion minoritaire du conseiller Bram Abramson

1. La *Loi sur les télécommunications* (*Loi*) interdit aux entreprises de contrôler le contenu ou d'influencer le sens ou l'objet des télécommunications qu'elles transmettent au public, sauf autorisation contraire du Conseil. Le cadre existant autorisait le blocage à l'échelle des réseaux du trafic des réseaux de zombies. Le cadre révisé approuve davantage et surveille moins : moins de divulgation, moins de structure pour le traitement des plaintes, moins de protection de la vie privée. Le pouvoir discrétionnaire des entreprises a été accru. La gouvernance de ce pouvoir discrétionnaire s'est réduite.

2. C'est cette inversion qui motive mon opinion minoritaire. La conséquence n'est pas abstraite. Lorsque des communications légitimes seront bloquées à tort ou que des données sensibles seront surveillées et détournées, personne ne sera en mesure de s'en apercevoir, et personne qui surveille le système n'aura l'obligation de découvrir ces situations. Je suis d'accord avec la majorité pour dire que le cadre de blocage des réseaux de zombies approuvé devrait être élargi afin d'englober plus généralement les mesures de blocage liées à la cybersécurité, afin de mieux structurer le pouvoir discrétionnaire que les entreprises exercent inévitablement dans un environnement de trafic où les menaces sont multiples. Toutefois, le cadre adopté affaiblit les mesures de protection qui confèrent à cette approbation sa légitimité et sa pérennité. Il réduit à la fois l'information disponible pour vérifier l'intégrité du système et la clarté des limites régissant son utilisation. Le cadre ne comporte pas de régime de rapports structuré et contrôlable qui permettrait de garantir la protection des intérêts légitimes en matière de confidentialité grâce à une surveillance efficace. Enfin, il restreint une garantie de protection de la vie privée existante qui n'a jamais été remise en question dans l'avis de consultation de Conformité et Enquêtes et de Télécom 2025-143 (avis), lequel définissait la portée de la présente instance et sur lequel les parties se sont raisonnablement fondées pour décider d'intervenir ou non.

3. L'instance écrite qui a mené à l'élaboration du cadre révisé, menée selon un calendrier serré entre la mi-juin et la fin juillet 2025, a réuni huit fournisseurs de services de télécommunication (FST[1]) et un organisme d'application de la loi[2], mais aucun défenseur de l'intérêt public, groupe

---

[1] Bell Canada, Bragg Communications Inc. (exerçant ses activités sous le nom d'Eastlink), Cogeco Communications inc., Québecor Média inc., Rogers Communications Canada Inc., Saskatchewan Telecommunications, TekSavvy Solutions Inc. et TELUS Communications Inc. L'Independent Telecommunications Providers Association s'est inscrite en tant qu'intervenant, mais n'a formulé aucune observation.

[2] Le Centre national de coordination en cybercriminalité de la Gendarmerie royale du Canada.

d'utilisateurs ou intervenant en matière de protection de la vie privée[3]. Dans ce contexte, la majorité a procédé à l'élargissement d'une exception sensible à une interdiction réglementaire sans que l'élargissement soit soumis à un test comparatif, à des preuves d'intérêt public ou à un examen axé sur la protection de la vie privée proportionné à cet élargissement.

Les fournisseurs de services de télécommunication en tant qu'« agents de confiance »

4. Les services de télécommunication « de base » offrent la capacité de transmission pure sur une voie de communication, qui est, à toutes fins pratiques, transparente pour ce qui est de son interaction avec l'information[4]. Dans l'Internet, les protocoles communs de numérotation et de routage relient entre eux des liaisons de télécommunication de base[5] qui ne sont pas utilisables sans des mesures visant à préserver leur capacité de transmission pure[6]. Les FST doivent donc nécessairement faire preuve de discernement opérationnel pour gérer le trafic nuisible ou indésirable. Cela confère aux FST un rôle délicat, que le Commissariat à la protection de la vie privée décrit à juste titre comme celui d'« agents de confiance » :

> Les fournisseurs de services de télécommunication […] font office d'« agents de confiance »; ils offrent à leur clientèle des services d'accès à Internet, de téléphonie cellulaire et de téléphonie filaire et servent pour ainsi dire de conduit à toutes les communications mobiles, téléphoniques et Internet de leurs clients, qu'elles soient sensibles ou non. Les clients confient leurs communications privées à leurs fournisseurs de services de télécommunication et s'attendent à ce que celles-ci soient transmises de façon sécuritaire et ne fassent pas généralement l'objet de surveillance, à moins que ce ne soit pour un motif lié directement à la prestation du service[7].

---

[3] Par exemple, l'avis de consultation de Conformité et Enquêtes et de Télécom 2021-9 a recueilli des interventions de la part du commissaire à la protection de la vie privée du Canada et de la B.C. Civil Liberties Association; de l'Association des Sourds du Canada; de l'Association des consommateurs du Canada, de l'Organisation nationale anti-pauvreté et d'Option consommateurs, représentées conjointement par le Centre de défense de l'intérêt public; de la Canadian Internet Policy and Public Interest Clinic; du Conseil des Canadiens avec déficiences et de l'ARCH Disability Law Centre; de l'Open Internet Coalition; de la Participatory Culture Foundation; de l'Union des consommateurs ainsi que d'associations de créateurs, de syndicats et d'associations professionnelles et de fournisseurs d'applications et de contenu, entre autres.

[4] Décision de télécom 84-18, paragraphe II.C.

[5] David D. Clark, *Designing an Internet*, Cambridge, MA, MIT Press, 2018.

[6] Craig McTaggart, « Was the Internet ever neutral? », Telecommunications Policy Research Conference, 15 août 2006.

[7] *Résultats de l'enquête sur le Programme de publicité pertinente de Bell lancée par le commissaire*, Rapport de conclusions d'enquête en vertu de la LPRPDE [*Loi sur la protection des renseignements personnels et les documents électroniques*] nº 2015-001 (Commissariat à la protection de la vie privée), le 7 avril 2015, citant Éloïse Gratton, *Internet and Wireless Privacy: A Legal Guide to Global Business Practices*, Toronto, CCH Canada Ltd., 2003.

5. Compte tenu du caractère sensible de ce rôle, la réglementation sur les télécommunications prévoit des mesures de protection propres aux entreprises de télécommunication afin d'encadrer le pouvoir discrétionnaire dont peuvent disposer les FST. Au Canada, ces mesures de protection sont inscrites dans deux dispositions de la *Loi* : le paragraphe 27(2), qui interdit toute discrimination injuste et toute préférence indue, et l'article 36, qui interdit à une entreprise de régir le contenu ou d'influencer le sens ou l'objet des télécommunications qu'elle transmet au public sans l'approbation du Conseil.

6. Dans le réseau téléphonique public commuté centralisé, la mise en œuvre de ces mesures de protection était relativement simple. La gestion du trafic devait être « sous réserve uniquement des paramètres techniques de fidélité ou des critères de distorsion ou d'autres facteurs de conditionnement ». Par exemple, « [les techniques] facilitant l'acheminement économique et fiable d'information […] ne [modifient] pas la nature du service de base ». Il en va de même pour « la conversion interne de vitesse, de code et de protocole qui ne se manifeste pas dans les résultats du service », ainsi que pour « [le] service [et] la mémoire du réseau »[8].

7. La manière d'appliquer les principes relatifs aux entreprises de télécommunication à Internet, dont l'architecture de base est bien moins centralisée, est par conséquent moins bien définie.

Évaluabilité et reddition de comptes

8. Le cadre de 2009 du Conseil relatif à la gestion du trafic Internet exigeait que les FST adaptent ces pratiques afin de répondre à un besoin précis « sans plus[9] ». À ce moment, le Conseil n'a pas cherché à déterminer dans quelle mesure le trafic Internet pouvait être purement et simplement bloqué, ce qui relève de l'article 36, tout en demeurant un service de télécommunication de base.

---

[8] Décision de télécom 84-18, paragraphe II.C.

[9] Politique réglementaire de télécom 2009-657, paragraphe 43, à la suite d'une consultation amorcée par une plainte plus précise déposée en 2008 : voir la décision de télécom 2008-108 et l'avis public de télécom 2008-19 (tel que modifié).

9. La décision majoritaire ci-dessus[10] d'une réunion plénière du Conseil[11] change cette situation. La participation des entreprises reste facultative. Toutefois, pour les abonnés des entreprises participantes, le blocage est activé par défaut. Des solutions techniques, telles que les services de réseau privé virtuel et des résolveurs du système de noms de domaine, doivent être mises à la disposition des abonnés qui en font la demande. Cependant, les solutions techniques ne sauraient se substituer à la reddition de comptes quant à la manière dont ce pouvoir discrétionnaire est exercé.

10. Le cadre réglementaire relatif au blocage des réseaux de zombies accordait une grande importance à la transparence et aux exigences en matière d'établissement de rapports. Le cadre révisé relatif au blocage à l'échelle des réseaux privilégie un recours accru à l'auto-évaluation des entreprises et aux signalements confidentiels, sans pour autant que cela s'accompagne d'un renforcement correspondant de la reddition de comptes au public. Alors que le cadre précédent limitait l'autorisation au seul appariement basé sur des indicateurs par rapport à des listes de blocage approuvées, le cadre révisé autorise toute mesure qu'une entreprise peut mettre en œuvre pour bloquer le trafic malveillant, dans le respect de principes généraux plutôt que de mécanismes définis, et sans processus d'évaluation des dommages collatéraux, de mécanismes de mise à jour et d'expiration, ni de traitement des plaintes conforme à des normes de service. Le fait de se fier aux plaintes émanant des utilisateurs n'est pas non plus une solution miracle : lorsque le blocage est automatisé, déclenché en amont ou difficile à reconnaître pour les utilisateurs, les blocages erronés risquent de ne pas donner lieu à des plaintes de manière fiable. La petite entreprise dont l'adresse de protocole Internet a hérité de la mauvaise réputation d'un ancien locataire ou dont le site légitime partage une infrastructure d'hébergement avec un voisin malveillant, constate simplement que les clients ne viennent plus. Cette entreprise n'aura aucune raison de soupçonner un blocage établi par l'entreprise de services de télécommunication, ne recevra aucune notification indiquant qu'un tel blocage a eu lieu et ne disposera d'aucune voie de recours supervisée par un tiers pour le contester.

11. Un minimum de transparence aide les utilisateurs à comprendre en quoi leurs communications pourraient être touchées. Cela permet aux chercheurs, aux groupes de défense de l'intérêt public

---

[10] À la suite d'une instance lancée en 2021 : avis de consultation de Conformité et Enquêtes et de Télécom 2021-9; décision de Conformité et Enquêtes et de Télécom 2022-170; *Développement d'un cadre de blocage à l'échelle des réseaux pour limiter le trafic des réseaux de zombies et renforcer la sécurité en ligne des Canadiens*, Rapport NTRE080 du Groupe de travail Réseau du Comité directeur du CRTC sur l'interconnexion, 31 mai 2023; décision de Conformité et Enquêtes et de Télécom 2025-142; avis de consultation de Conformité et Enquêtes et de Télécom 2025-143.

[11] Par « réunion plénière du Conseil », je fais référence, comme dans mes opinions minoritaires précédentes, à une décision qui n'est ni déléguée à un sous-comité constitué par voie de règlement du Conseil, ni confiée à un comité de conseillers, et non à la participation ou à la non-participation d'un conseiller en particulier à la décision. En ce qui concerne les sous-comités constitués par règlement, voir l'alinéa 11(1)b) et le paragraphe 12(3) de la *Loi sur le Conseil de la radiodiffusion et des télécommunications canadiennes*, L.R.C. 1985, ch. C-22. En ce qui concerne le pouvoir de la présidence de constituer des comités en attribuant des affaires et en désignant des membres pour les traiter, voir *Shoan c. Canada (Procureur général)*, 2016 CAF 261, para. 6.

et aux autres intervenants de dégager des tendances et des problèmes potentiels. Cela permet aux abonnés de tenir compte des pratiques d'un fournisseur lorsqu'ils prennent leurs décisions d'achat. La concurrence ne peut pas réguler ce que les abonnés ne sont pas en mesure d'évaluer. Le cadre révisé allège considérablement les obligations de divulgation, tant pour ce qui est de la précision que de l'exigence, ce qui simplifie la divulgation de renseignements, mais réduit la transparence. La divulgation de renseignements susceptibles de révéler des méthodes de protection, des seuils ou des configurations précises soulève des préoccupations légitimes en matière de sécurité. Ce n'est pas le cas des indicateurs de rendement correctement agrégés, des procédures de traitement des plaintes et des mécanismes de reddition de comptes à un niveau supérieur.

12. La diminution de la transparence entraîne la diminution de la capacité d'encadrer le comportement des entreprises par la concurrence, l'examen public et le choix éclairé des consommateurs. L'accent est donc davantage mis sur le traitement des plaintes et le contrôle exercé par le Conseil. Un processus de plainte est toujours nécessaire, mais n'est plus structuré de manière efficace. Le cadre de blocage des réseaux de zombies considérait les plaintes comme des éléments permettant d'assurer la qualité et l'intégrité du système, ce qui entraînait une vérification de l'indicateur concerné, une correction si nécessaire et une communication adressée au plaignant. Le cadre révisé présente désormais les plaintes comme des situations relevant du service à la clientèle plutôt que comme des données structurées servant l'assurance qualité du système. Laissé en grande partie à la discrétion des entreprises, sans faire l'objet d'un examen plus large, et dépourvu de classification, de suivi ou de lien avec des mesures correctives, un tel cadre ne permet pas de détecter ni de corriger de manière fiable les erreurs systémiques. Il ne peut donc pas non plus assumer la fonction de gouvernance sur laquelle repose l'approche d'autorisation fondée sur des principes du cadre. Si le contrôle exercé par le Conseil revêt une importance capitale lorsque celui-ci est le seul acteur à avoir accès à des données sensibles issues des rapports, cela signifie que nous avons une responsabilité particulière. Il s'agit d'examiner les renseignements dont nous disposons en exclusivité, de cerner les tendances à l'échelle du système et de résumer nos conclusions à l'intention du public, de manière à préserver la confidentialité tout en favorisant l'intégrité du système.

13. Le pouvoir discrétionnaire de l'entreprise ne peut se justifier lui-même. Ce qui lui confère sa légitimité, c'est une structure de gouvernance garantissant la transparence, le contrôle et la correction. L'obligation de produire un rapport annuel ne porte désormais que sur des indicateurs agrégés, sans les renseignements contextuels nécessaires pour évaluer la qualité du système. C'est de la comptabilité, pas de la gestion. Une entreprise pourrait afficher des volumes de blocage élevés et un faible nombre de plaintes tout en continuant à fonctionner avec des règles mal configurées, des indicateurs dépassés, des signatures trop générales ou des faux positifs que les utilisateurs n'ont pas détectés ou n'ont pas pu attribuer facilement au blocage. Sans information sur les dénominateurs, sur la correction des erreurs et sur le cycle de vie, les volumes divulgués ne permettent guère de se prononcer sur leur précision ou leur représentativité. La reddition de comptes exige des renseignements qui peuvent être évalués, et pas seulement des renseignements qui peuvent être comptabilisés. Le cadre de déclaration n'impose pas non plus au Conseil de

regrouper les rapports confidentiels des entreprises en un rapport public précis mais cohérent et permettant de suivre l'évolution d'une année à l'autre. Il prévoit uniquement que le Conseil « peut » publier certains indicateurs ou établir des résumés agrégés pour l'industrie. Un tel cadre ne devrait pas reposer sur une divulgation discrétionnaire décidée a posteriori. Sans données permettant de relier les résultats aux processus sous-jacents, les rapports ne peuvent pas servir de base à une évaluation pertinente par des tiers.

14. Un modèle fondé sur des principes peut être rendu administrable sans avoir recours à des règles techniques contraignantes. J'aurais exigé trois mesures, chacune visant à permettre à l'abonné concerné, dans chaque cas particulier, ainsi qu'au Conseil et au public dans l'ensemble du système, de détecter les blocages erronés.

15. Tout d'abord, établir des rapports annuels structurés. Le rapport annuel de chaque entreprise participante comporterait, au minimum :

    a) le volume de trafic évalué par rapport au trafic bloqué;

    b) les renseignements de base sur le cycle de vie (ajouts, retraits) des mesures et des fournisseurs tiers actuellement utilisés;

    c) les corrections apportées après avoir relevé les faux positifs;

    d) les résultats des plaintes classés par type de décision : blocage confirmé, modifié, annulé ou non vérifiable.

16. Ce type de rapport permet de relier les résultats aux processus sans divulguer les méthodes de protection, les seuils ou les configurations.

17. Deuxièmement, redonner aux processus de plainte leur rôle d'assurance de l'intégrité du système. Le cadre sur les réseaux de zombies considérait les plaintes comme des données servant à l'assurance qualité. J'aurais donné suite à cette mesure en exigeant que les plaintes relatives au blocage fassent l'objet d'un accusé de réception contenant un minimum de renseignements, soient consignées, classées de manière à permettre un audit et une analyse des tendances, et fassent l'objet d'une procédure de transmission à l'échelon supérieur incluant le Conseil.

18. Troisièmement, un engagement du Conseil plutôt qu'un pouvoir discrétionnaire du Conseil. J'aurais souhaité que nous nous engagions à publier régulièrement des indicateurs agrégés cohérents permettant de suivre l'évolution d'une année à l'autre, de manière à permettre un examen par le marché, un débat et une comparaison au sein de l'écosystème, sans pour autant compromettre la sécurité opérationnelle.

19. De telles exigences pour les FST d'importance pour l'ensemble du système[12] auraient permis de mettre en place un système de reddition de comptes adapté au pouvoir discrétionnaire qui leur est accordé, sans pour autant imposer de technologies ou de méthodes, et de manière à promouvoir une bonne gouvernance tant au niveau interne qu'à l'échelle de l'industrie, sous la supervision du Conseil. Il ne s'agit pas de déterminer si les renseignements sont communiqués de manière confidentielle par les entreprises au Conseil et par le Conseil au public. La question est de savoir si ces renseignements peuvent, à chaque étape, étayer l'évaluation.

Mesures de protection de la vie privée

20. Le Conseil n'est pas une autorité générale de protection de la vie privée. Mais il assume des responsabilités propres à son secteur qui l'obligent expressément à contribuer à la protection de la vie privée[13]. Un principe général en matière de protection de la vie privée veut que les renseignements personnels « ne doivent pas être utilisés ou communiqués à des fins autres que celles auxquelles ils ont été recueillis à moins que la personne concernée n'y consente ou que la loi ne l'exige[14] ». Conformément à ces responsabilités et à ce principe de protection de la vie privée, le dispositif mis en place pour limiter le trafic des réseaux de zombies n'autorisait « pas la collecte, l'utilisation ou la communication supplémentaire de renseignements personnels[15] ».

21. L'avis lançant la présente instance[16] posait cinq questions relatives à la vie privée (sur douze questions). Des renseignements factuels ont été fournis pour deux de ces questions. Les trois autres, intitulées « Ajout de mesures de protection au cadre pour aider à protéger la vie privée », demandaient si des mesures de protection supplémentaires étaient nécessaires en plus de celles déjà en place. Le traitement de la vie privée dans le cadre révisé présente trois problèmes distincts. Premièrement, il n'apporte aucune mesure de protection supplémentaire, malgré un renforcement significatif de la sensibilité et de la précision des techniques qu'il autorise. Deuxièmement, la seule nouvelle restriction qu'il impose à l'inspection approfondie des paquets n'est pas applicable telle qu'elle est formulée. Troisièmement, le cadre restreint une mesure de

---

[12] Les FST dont la taille globale ou la position en tant que fournisseur clé dans une région dépasse un certain seuil, les premiers parce que leurs décisions de blocage ont un large impact, et les seconds parce que leurs abonnés ne peuvent pas facilement contourner ces blocages. Concernant ces seuils et leur lien avec l'échelle minimale efficace (et donc l'entrée sur le marché et la participation), voir mes remarques lors de la conférence annuelle de l'Association canadienne des fournisseurs de services Internet sans fil (CanWISP), le 31 mars 2026.

[13] *Loi*, alinéas 7i) et 47a).

[14] *Loi sur la protection des renseignements personnels et les documents électroniques* (L.C. 2000, ch. 5), annexe 1, article 4.5.

[15] Décision de Conformité et Enquêtes et de Télécom 2025-142, annexe, section 8.2.

[16] Avis de consultation de Conformité et Enquêtes et de Télécom 2025-143, paragraphe 4, questions 6 à 10.

protection existante que l'avis n'a jamais remise en cause.

22. Tout d'abord, il convient de garder à l'esprit une distinction importante. Le cadre précédent, qui se limitait essentiellement à un blocage par liste de blocage, se situait à l'extrémité inférieure du spectre de l'intrusion. L'élargissement de la portée pour englober des techniques telles que les signatures de fichiers, la détection des anomalies de volume de trafic et les empreintes de réseau constitue une différence notable. La comparaison statique avec des indicateurs de compromission, tels que les adresses de protocole Internet, les numéros de systèmes autonomes, les noms d'hôtes ou d'autres identifiants similaires, consiste à vérifier si le trafic correspond à une chaîne de caractères identifiée. L'analyse comportementale nécessaire pour étayer certaines des techniques récemment adoptées exige une observation plus soutenue du trafic, avec un niveau de précision proche du contenu, voire révélateur de celui-ci, qu'il s'agisse d'établir un modèle de référence du trafic « normal » en vue de la détection des anomalies ou de cerner les caractéristiques des flux de trafic telles que la synchronisation, le volume, les modèles de protocole ou les signatures de charge utile pour l'empreinte réseau. Même lorsqu'elles ne servent pas à analyser le contenu en tant que tel, ces techniques peuvent permettre de générer ou de confirmer des hypothèses concernant des comptes identifiables, des terminaux ou des habitudes d'utilisation. Les répercussions en matière de vie privée sont d'une nature différente, et pas seulement d'un degré différent.

23. Lorsque la portée des mesures autorisées s'étend pour inclure des techniques davantage axées sur l'observation, l'inférence ou la persistance, la structure de gouvernance correspondante doit évoluer en conséquence. La conclusion selon laquelle aucune mesure de protection supplémentaire n'est requise n'est pas entièrement compatible avec l'augmentation considérable de la sensibilité et de la précision des renseignements recueillis. Malgré cette augmentation considérable, la majorité conclut qu'aucune mesure de protection supplémentaire en matière de protection de la vie privée n'est nécessaire au-delà de celles qui sont déjà en place, puis indique du même souffle que l'inspection approfondie des paquets doit être limitée à des circonstances exceptionnelles. Cette juxtaposition résume tout le problème. Si l'une des nouvelles techniques envisagées nécessite des règles explicites en raison de ses répercussions en matière de protection de la vie privée, l'hypothèse selon laquelle aucune mesure de protection supplémentaire n'est nécessaire devient difficile à défendre. La majorité n'explique pas pourquoi les mesures de protection existantes étaient suffisantes, compte tenu de la diversité accrue des techniques utilisées et de la nature plus sensible des renseignements en jeu. Ce cadre aurait dû préciser comment les FST sont censés gérer ces techniques et en rendre compte.

24. Deuxièmement, la majorité reconnaît que l'inspection approfondie des paquets soulève des préoccupations précises en matière de protection de la vie privée et affirme donc que son utilisation doit être limitée à des « circonstances exceptionnelles ». Cette précision est nécessaire, mais ce cadre ne permet pas d'appliquer la règle de manière efficace. Il ne précise pas ce qui constitue des circonstances exceptionnelles; combien de temps une telle utilisation peut se poursuivre après la violation; quels documents doivent être établis ni comment le Conseil doit vérifier la cohérence entre les entreprises, ni comment le public peut s'en assurer.

25. Une mesure de protection efficace devrait, au minimum, exiger que les circonstances exceptionnelles soient expressément justifiées, limitées dans le temps, documentées, qu'elles puissent être attribuées à un décideur désigné et soient susceptibles d'être réexaminées a posteriori. Ce cadre ne prévoit rien de tout cela. Il n'explique pas non plus si les exemples cités (ordonnances d'un tribunal et ajustements à la suite d'un incident) sont exhaustifs ou simplement donnés à titre d'exemples, si les utilisateurs concernés peuvent se plaindre spécifiquement d'une telle utilisation, ni comment cette règle s'inscrit dans le cadre existant du Conseil en matière de pratiques de gestion du trafic Internet. Sans ces éléments, la règle n'est pas facilement vérifiable ni applicable de manière uniforme par toutes les entreprises.

26. Troisièmement, alors que le cadre relatif aux réseaux de zombies interdisait la réutilisation des renseignements personnels déjà recueillis à d'autres fins, telles que la publicité comportementale, le cadre révisé assouplit cette mesure de protection en précisant que le cadre n'autorise pas la collecte, l'utilisation ou la communication supplémentaire de renseignements personnels, « sauf lorsque ces activités sont autorisées par les lois et règlements applicables ou par une ordonnance d'un tribunal compétent ». Cela ouvre la voie à des utilisations secondaires que le cadre précédent excluait.

27. La surveillance du trafic justifiée par des raisons de sécurité peut fournir des profils utiles à des fins de marketing. Le nouveau libellé laisse aux entreprises le soin de déterminer elles-mêmes dans quelle mesure l'un peut alimenter l'autre. Ce changement est à la fois préoccupant sur le fond et dépourvu de fondement sur le plan procédural. Il affaiblit la mesure de protection du principe de finalité, alors même que le cadre s'étend à des techniques capables de générer des renseignements plus sensibles liés au trafic. Cet affaiblissement se produit alors que l'avis demandait s'il fallait ajouter des mesures de protection, et non s'il fallait restreindre celles qui existent déjà. La question centrale de l'avis consistait à déterminer s'il fallait renforcer la protection. Les intervenants potentiels adaptent leur participation aux questions posées; un assouplissement qui n'était pas mentionné dans l'avis n'était pas de nature à être examiné dans le cadre du dossier de l'instance[17]. J'aurais conservé la formulation actuelle relative au principe de finalité et, si le Conseil avait jugé utile d'envisager un assouplissement, j'aurais inscrit cette proposition dans un dossier constitué à cette fin.

28. Les agents de confiance ne devraient pas avoir à deviner, sans qu'on leur communique quoi que ce soit, dans quelle mesure ils peuvent réutiliser les renseignements obtenus dans le cadre de la protection des communications. La majorité reconnaît que le Commissariat à la protection de la vie privée a mis en place un cadre réglementaire pour la publicité comportementale en ligne. Ce

---

[17] *Bell Canada c. Canada (Procureur général)*, 2016 CAF 217, paragraphe 38, *a contrario* (l'avis de consultation indiquait clairement que l'ensemble de la pratique de la substitution simultanée faisait l'objet de la discussion; c'est l'inverse qui s'applique en l'espèce). Voir également mon opinion minoritaire dans l'avis de consultation de télécom 2024-293 (en raison de la formulation de l'avis de consultation, « des mises à jour sur la fin des rabais et la fin de contrat au Code des fournisseurs de services de télévision semblables à celles envisagées pour le Code sur les services sans fil et le Code sur les services Internet ne seront pas possibles dans le cadre de la présente instance »).

cadre, publié dans un autre contexte mais peu de temps après que le Commissariat à la protection de la vie privée ait désigné les entreprises de services de télécommunication comme des agents de confiance dont les clients s'attendent à ce qu'elles « ne fassent pas généralement l'objet de surveillance, à moins que ce ne soit pour un motif lié directement à la prestation du service[18] », met en garde contre le fait que la publicité comportementale en ligne « ne devrait pas être considérée comme une condition permettant aux personnes d'utiliser Internet en général[19] ». Il exige que les utilisateurs soient informés de l'utilisation envisagée de manière claire et compréhensible et qu'ils puissent d'emblée retirer facilement leur consentement, de manière à ce que ce retrait prenne effet immédiatement et de façon durable.

29. Ces exigences concernent les avis aux consommateurs et leur consentement. Ces dispositions s'appliquent avant toute anonymisation ou regroupement des données sur le trafic[20] : le consentement ne doit pas être obtenu a posteriori en supprimant les identifiants de renseignements personnels qui n'auraient jamais dû être réutilisés. Les entreprises souhaitant mettre en place des utilisations secondaires, ainsi que les intervenants souhaitant les contester, trouveront le site naturel de ce débat dans les conditions générales, destinées aux consommateurs, qui régissent les modalités des contrats de services de télécommunication.

Conclusion

30. La majorité autorise un élargissement de l'éventail de techniques de cybersécurité s'appliquant à un ensemble plus vaste et plus sensible de données sur le trafic, dans un cadre qui fonctionne par défaut, mais qui reste pratiquement invisible pour ceux qui y sont soumis. Cet élargissement est nécessaire. L'affaiblissement des mesures de protection qui le sous-tendent n'est pas nécessaire. L'accroissement du pouvoir discrétionnaire des entreprises devrait s'accompagner d'un accroissement proportionnel de la transparence, de la reddition de comptes et des mesures de protection de la vie privée qui régissent ce pouvoir discrétionnaire. Au contraire, le cadre révisé inverse cette relation. Le statut d'« agent de confiance » n'est pas un titre que portent les entreprises. C'est une norme à laquelle elles doivent se conformer. Je suis respectueusement en désaccord.

---

[18] Rapport de conclusions d'enquête en vertu de la LPRPDE nº 2015-001, cité en note de bas de page 7 dans la présente opinion minoritaire.

[19] *Commissariat à la protection de la vie privée du Canada* (2015), Position de principe sur la publicité comportementale en ligne.

[20] Voir la décision majoritaire, ci-dessus, à la note de bas de page 9.

Documents connexes

- *Appel aux observations – Modifications proposées au cadre pour limiter le trafic des réseaux de zombies*, Avis de consultation de Conformité et Enquêtes et de Télécom CRTC 2025-143, 13 juin 2025

- *Développement d'un cadre pour limiter le trafic des réseaux de zombies*, Décision de Conformité et Enquêtes et de Télécom CRTC 2025-142, 13 juin 2025

- *Appel aux observations – Faciliter le choix d'un service téléphonique sans fil ou d'un service Internet – Améliorer les avis aux clients*, Avis de consultation de télécom CRTC 2024-293, 22 novembre 2024, modifié par les Avis de consultation de télécom CRTC 2024-293-1, 20 décembre 2024; 2024-293-2, 14 février 2025; et 2024-293-3, 28 février 2025

- *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*, Décision de télécom CRTC 2022-238, 6 septembre 2022

- *Développement d'un cadre de blocage à l'échelle des réseaux pour limiter le trafic des réseaux de zombies et renforcer la sécurité en ligne des Canadiens*, Décision de Conformité et Enquêtes et de Télécom CRTC 2022-170, 23 juin 2022, modifiée par la Décision de Conformité et Enquêtes et de Télécom CRTC 2022-170-1, 11 octobre 2022

- *Appel aux observations – Développement d'un cadre de blocage à l'échelle des réseaux pour limiter le trafic des réseaux de zombies et renforcer la sécurité en ligne des Canadiens*, Avis de consultation de Conformité et Enquêtes et de Télécom CRTC 2021-9, 13 janvier 2021, modifié par l'Avis de consultation de Conformité et Enquêtes et de Télécom CRTC 2021-9-1, 29 juin 2021

- *Application des obligations réglementaires directement aux entreprises autres que les entreprises de télécommunication qui offrent et 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

- *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 de services Internet*, Politique réglementaire de télécom CRTC 2009-657, 21 octobre 2009

- *Accessibilité des services de télécommunication et de radiodiffusion*, Politique réglementaire de radiodiffusion et de télécom CRTC 2009-430, 21 juillet 2009, modifiée par la Politique

réglementaire de radiodiffusion et de télécom CRTC 2009-430-1, 17 décembre 2009

- *Demande de l'Association canadienne des fournisseurs Internet relative au lissage du trafic du service d'accès par passerelle de gros de Bell Canada*, Décision de télécom CRTC 2008-108, 20 novembre 2008

- *Examen des pratiques de gestion du trafic Internet des fournisseurs de services Internet*, Avis public de télécom CRTC 2008-19, 20 novembre 2008, modifié par les Avis public de télécom CRTC 2008-19-1, 11 février 2009; 2008-19-2, 12 février 2009; 2008-19-3, 18 mars 2009; et 2008-19-4, 16 juillet 2009

- *Clauses de confidentialité des entreprises canadiennes*, Décision Télécom CRTC 2003-33, 30 mai 2003, modifiée par la Décision Télécom CRTC 2003-33-1, 11 juillet 2003

- *Services améliorés*, Décision Télécom CRTC 84-18, 12 juillet 1984