Conseil de la radiodiffusion et des télécommunications canadiennes
Canadian Radio-television and Telecommunications Commission

Décision de Conformité et Enquêtes et de Télécom CRTC 2025-142

Version PDF

Gatineau, le 13 juin 2025

Dossier public : 1011-NOC2021-0009

Développement d’un cadre pour limiter le trafic des réseaux de zombies

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* (*Loi*) et de la Loi canadienne anti-pourriel (LCAP). En vertu de la *Loi*, il joue un rôle restreint en réglementant les fournisseurs de services de télécommunication (FST). En vertu de la LCAP, 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. Dans la décision de Conformité et Enquêtes et de Télécom 2022-170, le Conseil a conclu que des mesures réglementaires étaient nécessaires afin que les FST aident à démanteler les réseaux de zombies et à protéger la population canadienne des dommages qu’ils causent. Dans cette décision, le Conseil a précisé les lignes directrices d’un cadre de réglementation en vue de bloquer les activités malveillantes des réseaux de zombies.

Le Conseil a demandé au Groupe de travail Réseau (GTR) du Comité directeur du CRTC sur l’interconnexion (CDCI) de lui remettre un rapport sur les activités néfastes devant être bloquées par le cadre ainsi que sur des méthodes de blocage potentielles. Le GTR est composé de groupes d’experts techniques comprenant des FST, des ministères fédéraux ayant un mandat de protection de la sécurité publique et d’autres experts de l’industrie.

En s’appuyant sur le dossier de la présente instance et sur le rapport du GTR du CDCI, le Conseil établit un cadre précisant les modalités permettant aux entreprises canadiennes de bloquer les réseaux de zombies et toute autre activité néfaste dans leurs réseaux avant que ces menaces n’atteignent les appareils de la population canadienne. Ce blocage doit être effectué conformément au cadre de blocage énoncé à l’annexe de la présente décision, à compter du **12 août 2025**.

Canada

Dans l’avis de consultation de Conformité et Enquêtes et de Télécom 2025-143, également publié aujourd’hui, le Conseil sollicite des observations sur la question de savoir si la portée du cadre devrait être élargie pour inclure des méthodes de blocage autres que les listes de blocage.

Contexte

1. Dans la décision de Conformité et Enquêtes et de Télécom 2022-170 (Décision), le Conseil a conclu que des mesures réglementaires sont nécessaires pour résoudre le problème du trafic[1] des réseaux de zombies néfastes. Le Conseil a déterminé que l’approche réglementaire la plus appropriée consiste à créer un cadre qui établit les normes minimales afin que les entreprises canadiennes puissent obtenir l’approbation du Conseil de bloquer le trafic de réseaux de zombies au niveau du réseau.

2. Dans la Décision, le Conseil a également déterminé que le cadre serait guidé par les principes de nécessité, de protection de la vie privée des clients, de responsabilité, de transparence et d’exactitude. Le Conseil a demandé au Comité directeur du CRTC sur l’interconnexion (CDCI) d’examiner plusieurs questions pour aider à élaborer des normes minimales conformes à ces principes directeurs.

3. Le 31 mai 2023, le Groupe de travail Réseau du CDCI a déposé un rapport intitulé *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* (NTRE080) [Rapport], qui formulait des recommandations concernant le type d’activités à bloquer par le cadre, la façon dont les listes de blocage devraient être utilisées par les entreprises et si des méthodes de blocage supplémentaires devraient être incluses dans le cadre.

4. Les contributeurs au Rapport comprenaient des fournisseurs de services de télécommunication (FST), Bell Canada, Rogers Communications Canada Inc. (Rogers), Saskatchewan Telecommunications, Shaw Communications Inc. (Shaw), TekSavvy Solutions Inc. et TELUS Communications Inc. (TELUS), ainsi que l’Autorité canadienne pour les enregistrements Internet, le Centre canadien pour la cybersécurité (CCC) du Centre de la sécurité des télécommunications, le Groupe national de coordination contre la cybercriminalité (GNC3) de la Gendarmerie royale du Canada, l’Independent Telecommunications Providers Association (ITPA) et les Opérateurs de réseaux concurrentiels Canadiens.

---

[1] Un réseau de zombies est un réseau d’appareils infectés par des logiciels malveillants, appelés zombies, et contrôlé en groupe à l’insu et sans le consentement de leurs propriétaires, dans un but malveillant. Le trafic des réseaux de zombies est le trafic Internet qui circule entre les appareils infectés et leurs points de contrôle, appelés serveurs de commande et de contrôle.

5. Le Conseil a reçu des observations sur le Rapport de Bell Canada, du Centre pour la défense de l'intérêt public (CDIP), du CCC, du GNC3, de l'ITPA, de Rogers, de TELUS et d'un particulier.

6. Dans la présente décision, le Conseil établit un cadre qui autorise les entreprises canadiennes à bloquer les réseaux de zombies à l'échelle des réseaux en utilisant des listes de blocage autorisées. Le cadre établit les normes minimales afin que les entreprises canadiennes puissent obtenir l'approbation du Conseil pour adhérer au système de blocage à l'échelle du réseau, conformément à l'article 36 de la *Loi sur les télécommunications* (*Loi*). Cet article précise que les entreprises canadiennes ont besoin de l'approbation du Conseil pour contrôler ou influencer le contenu des télécommunications.

Questions

7. D'après le Rapport et les observations reçues à son sujet, le Conseil a déterminé qu'il devait se pencher sur les questions suivantes :

    - Quelle devrait être la portée du cadre?
    - Comment les listes de blocage devraient-elles être mises en œuvre?
    - Quelles méthodes de blocage le cadre devrait-il autoriser?
    - Quels autres aspects du cadre devraient être pris en considération?

Quelle devrait être la portée du cadre?

Définitions

8. Dans le Rapport, le CDCI a fait remarquer que la plupart des contributeurs étaient d'accord avec les définitions de la cybersécurité et des cyberattaques proposées dans la Décision.

Analyse du Conseil

9. Compte tenu de ce large consensus, les définitions suivantes seront utilisées aux fins du cadre :

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

    Cyberattaque : l'utilisation de moyens électroniques pour interrompre, manipuler, détruire ou obtenir un accès non autorisé à un système, à un réseau ou à un appareil informatique.

10. Le Conseil fait remarquer que le terme « cybersécurité » dans ce contexte s'applique à la sécurité des services Internet que les entreprises fournissent aux consommateurs. Le terme ne s'applique pas à l'utilisation par les entreprises de pratiques de gestion du trafic Internet pour gérer la congestion sur leurs réseaux et protéger leur intégrité (voir la politique réglementaire de télécom 2009-657).

Définition d'« indicateur de compromission »

11. Les contributeurs au Rapport n'ont pas été en mesure de s'entendre sur une définition unique d'« indicateur de compromission » (IC) à recommander au Conseil. Certains contributeurs n'étaient pas d'accord avec la définition proposée dans la Décision en se fondant sur l'argument selon lequel un IC est composé de plusieurs points de données plutôt que d'un seul. D'autres ont fait remarquer qu'ils ne pouvaient pas évaluer adéquatement l'exactitude de la définition proposée par le Conseil sans en savoir plus sur la façon dont les IC seront utilisés dans le contexte du cadre.

Positions des parties

12. Étant donné qu'un IC est composé de données, Bell Canada et Rogers ont suggéré de supprimer le terme « criminalistique » de la définition. Bell Canada a également soutenu qu'un IC ne devrait pas être défini comme une combinaison ou une série de points de données parce qu'il est difficile de maintenir les IC en fonction de plusieurs points de données dans une liste de blocage de réseaux de zombies.

Analyse du Conseil

13. Le Conseil est d'avis que, dans le contexte du cadre, le terme « IC » fait simplement référence aux identificateurs à bloquer à des fins de cybersécurité. Les identificateurs peuvent inclure un ou plusieurs éléments de données, y compris, par exemple, un nom de domaine, une adresse de protocole Internet (IP) et un numéro de port.

14. Le Conseil convient qu'il n'est pas nécessaire d'inclure le terme « criminalistique » dans la définition d'« IC ». Il estime également que les deux dernières phrases de la définition proposée sont inutiles, car elles font référence à la façon dont les IC sont généralement utilisés par la communauté de la cybersécurité.

15. Par conséquent, la définition initiale d'« IC » sera révisée comme suit :

> Un IC est un identifiant utilisé par les entreprises pour bloquer le trafic de réseau à des fins de cybersécurité qui indique, avec un degré élevé de confiance, une intrusion sur un système et que des activités malveillantes se produisent. En d'autres termes, un IC est une caractéristique technique d'une cyberattaque particulière. Dans le contexte d'une liste de blocage, un IC peut se composer, par exemple i) d'un nom de domaine, ou ii) d'une adresse IP et d'un numéro de port.

Application du cadre au blocage de tous les IC

16. Dans le Rapport, le CDCI a fait remarquer que la plupart des contributeurs ont recommandé que le cadre ne s'applique qu'au blocage de réseaux de zombies, car c'était la portée initiale proposée par le Conseil.

17. Toutefois, l'Autorité canadienne pour les enregistrements Internet et le GNC3 ont fait remarquer que, d'un point de vue technique, le cadre pourrait s'appliquer au blocage de tous les IC et pas seulement du trafic de réseaux de zombies. Ils ont soutenu que tout blocage qui respecte les principes directeurs du cadre et qui est effectué à des fins de cybersécurité devrait être autorisé.

Positions des parties

18. Bell Canada a recommandé que le cadre se concentre sur la prévention du trafic de réseaux de zombies, et le CDIP a proposé de limiter le blocage au trafic de réseaux de zombies afin de réduire le risque de blocage du trafic non malveillant.

19. Bell Canada, Shaw et TELUS ont soulevé des préoccupations techniques au sujet des types et du volume d'IC à bloquer. Elles ont fait remarquer que l'utilisation de listes de blocage qui incluent des IC pour les cybermenaces qui ne sont pas liées aux réseaux de zombies nécessiterait une grande capacité de traitement, ce qui pourrait nuire au rendement du réseau.

20. Cependant, le CCC et le GNC3 ont souligné que le blocage uniquement du trafic de réseaux de zombies ne résoudrait qu'une partie des dommages causés par le trafic malveillant, et qu'il serait difficile de définir uniquement les IC liés au trafic de réseaux de zombies dans les flux de menaces. Par conséquent, ils ont suggéré d'inclure le blocage du trafic malveillant qui n'est pas lié aux réseaux de zombies dans le cadre.

Analyse du Conseil

21. Dans la Décision, le Conseil a déclaré que les réseaux de zombies, les logiciels malveillants et les intrusions informatiques sont imbriqués, ce qui rend peu pratique et inefficace le fait de bloquer uniquement le trafic des réseaux de zombies et de ne pas bloquer les autres types d'IC. Le Conseil a également fait remarquer qu'il n'est peut-être pas pratique d'isoler le trafic de réseaux de zombies identifié au moyen d'IC particuliers parce que les IC utilisés dans le but de bloquer le trafic ne ciblent pas particulièrement les réseaux de zombies. Les IC recensent plutôt plus généralement le trafic de logiciels malveillants ou le trafic suggérant des intrusions informatiques.

22. Dans la Décision, le Conseil a également fait remarquer que la justification de la politique pour bloquer le trafic de réseaux de zombies (c.-à-d. le préjudice à la population canadienne) s'applique également au trafic identifié par d'autres IC.

23. En ce qui concerne la crainte que l'utilisation de grandes listes de blocage ne nuise au rendement du réseau, le Conseil fait remarquer que le cadre n'exige pas l'utilisation d'une liste de blocage précise ni n'impose un seuil de blocage minimal. Les entreprises qui optent pour le cadre peuvent contrôler les types et le volume d'IC qu'ils bloquent tant qu'ils respectent ses modalités.

24. Le Conseil estime qu'un cadre qui met l'accent sur tous les IC plutôt que sur ceux qui n'identifient que le trafic de réseaux de zombies maximiserait son efficacité à protéger la population canadienne, serait techniquement faisable et serait approprié en tant que politique.

25. Le Conseil détermine donc que la portée du cadre s'étendra au blocage de tous les IC.

Comment les listes de blocage devraient-elles être mises en œuvre?

Liste de blocage centralisée

26. Dans la Décision, le Conseil a demandé au CDCI s'il existe un organisme d'experts indépendants qui peut tenir à jour une liste de blocage centralisée à l'intention des FST, et comment cet organisme d'experts traiterait les plaintes de faux positif lorsque du trafic non malveillant est bloqué à tort. Il a également demandé si les FST et d'autres intervenants peuvent demander l'ajout ou le retrait de certains IC de la liste de blocage.

27. Bien que le CDCI n'ait pas été en mesure d'identifier un organisme d'experts indépendant pour maintenir une liste de blocage centralisée, il a recommandé que si un organisme d'experts est identifié pour traiter les plaintes de faux positif, il devrait être responsable du traitement de ces plaintes et de la mise à jour de la liste de blocage.

Positions des parties

28. Bell Canada et Rogers ont suggéré que, compte tenu de son expérience et de son expertise en matière de cybersécurité, le CCC devrait gérer une liste de blocage centralisée. TELUS a pour sa part proposé que les FST canadiens gèrent une liste de blocage centralisée.

29. Le CCC a déclaré qu'il ne peut pas tenir une liste de blocage centralisée parce que cette fonction de réglementation est incompatible avec son mandat.

Analyse du Conseil

30. Étant donné qu'aucun organisme d'experts indépendants en mesure de gérer une liste de blocage centralisée n'a été identifié, le Conseil ne se prononcera pas sur cette question pour le moment.

Listes de blocage de tierces parties

31. Dans la Décision, le Conseil a demandé au CDCI comment les listes de blocage de tierces parties devraient être accréditées si elles sont incluses dans le cadre et comment le public devrait déposer des plaintes de faux positif pour s'assurer que les listes de blocage de tierces parties sont mises à jour.

32. Dans le Rapport, le CDCI n'a pas été en mesure de déterminer un organisme capable de gérer l'accréditation des listes de blocage de tierces parties. Toutefois, il a suggéré qu'un organisme central au sein du gouvernement ou de l'industrie des télécommunications pourrait remplir cette fonction.

33. Le CDCI a ajouté que l'accréditation de plusieurs listes de blocage donnerait entre autres aux FST la souplesse nécessaire pour choisir une liste de blocage qui correspond à leurs préférences. Il a également recommandé que les propriétaires de listes de blocage de tierces parties soient responsables du traitement des plaintes de faux positif et de la mise à jour de leurs listes de blocage au besoin.

Positions des parties

34. Bell Canada, Rogers et TELUS ont convenu de la nécessité d'un processus d'accréditation centralisé pour s'assurer que les listes de blocage de tierces parties répondent aux critères minimaux. Bell Canada a recommandé que le CCC gère ce processus et a proposé des critères d'accréditation pour les fournisseurs de listes bloquées.

35. Le CCC a recommandé qu'un comité central gère le processus d'accréditation. Il a indiqué qu'il apporterait son expérience en matière de cybersécurité au comité, mais qu'il ne devrait pas avoir le pouvoir de prendre des décisions.

36. L'ITPA a fait valoir qu'un processus d'accréditation centralisé n'est pas nécessaire et a recommandé que les FST soient autorisés à utiliser toute liste de blocage d'une tierce partie qui répond à des critères préétablis. L'ITPA a suggéré que les FST présentent les listes de blocage qu'ils utilisent à une entité comme le Conseil, qui pourrait publier un registre des listes de blocage utilisées par les FST canadiens.

37. TELUS a indiqué que les entreprises pourraient avoir besoin d'utiliser plusieurs listes de blocage puisqu'il y a un chevauchement limité entre elles.

38. En ce qui concerne les plaintes de faux positif, Bell Canada et l'ITPA ont suggéré qu'un portail Web centralisé soit créé pour permettre à la population canadienne de vérifier et de signaler les faux positifs. Cependant, Rogers a indiqué que des acteurs malveillants pourraient utiliser ce portail pour identifier les adresses IP.

39. Le CDIP a soutenu que le dépôt de plaintes de faux positif devrait être facile pour la personne moyenne et que des réponses rapides à ces plaintes sont cruciales.

Analyse du Conseil

40. Le Conseil estime que les entreprises devraient être responsables de s'assurer que les listes de blocages qu'elles utilisent répondent à des critères minimaux, étant donné que l'on n'a pas identifié d'organisation pouvant gérer un processus d'accréditation centralisé. Les critères minimaux entourant les listes de blocage sont énoncés aux sections 3.0 et 4.0 du cadre décrit à l'annexe de la présente décision.

41. En ce qui concerne les plaintes de faux positif, le Conseil convient qu'elles devraient être traitées en temps opportun. Par conséquent, la section 5.0 du cadre exigera que les entreprises règlent les plaintes concernant un faux positif potentiel dans les deux jours ouvrables suivant leur réception.

Listes de blocage internes

42. Dans le Rapport, le CDCI a fait remarquer que la plupart des FST n'ont pas la capacité de créer et de tenir à jour leurs propres listes de blocage.

Analyse du Conseil

43. L'un des avantages des listes de blocage internes est qu'elles peuvent permettre aux entreprises de bloquer les IC qui ne figurent pas sur des listes de blocage de tierces parties, en particulier les IC qui sont propres au Canada.

44. Étant donné que certaines entreprises utilisent déjà des listes de blocage internes et que d'autres pourraient être en mesure de créer les leurs, le Conseil permettra l'utilisation de listes de blocage internes en vertu du cadre, sous réserve des modalités énoncées à la section 4.0.

Quelles méthodes de blocage le cadre devrait-il autoriser?

Types de blocage

45. Dans le Rapport, le CDCI a recommandé que le cadre n'autorise que le blocage basé sur l'adresse IP, car il s'agit de la capacité la plus courante prise en charge par les FST.

Positions des parties

46. Bell Canada et TELUS ont convenu que le cadre devrait se limiter au blocage basé sur les adresses IP. Toutefois, le CCC et le GNC3 ont soutenu qu'une telle limitation limiterait la capacité des entreprises à s'adapter, et ont donc recommandé que d'autres types de blocage soient autorisés.

Analyse du Conseil

47. L'objectif d'un cadre large et technologiquement neutre est de permettre aux entreprises de mettre en œuvre le blocage à l'échelle du réseau au mieux de leurs capacités techniques. Limiter le cadre au blocage basé sur les adresses IP ne

donnerait pas aux entreprises individuelles la souplesse nécessaire pour bloquer au maximum de leur capacité technique et limiterait leur capacité à s’adapter.

48. Par conséquent, le Conseil détermine que le cadre ne se limitera pas au blocage basé sur les adresses IP.

Méthodes de blocage autres que les listes de blocage

49. Dans la Décision, le Conseil a reconnu que chaque méthode de blocage présente ses propres avantages et inconvénients, et que les entreprises pourraient vouloir utiliser plusieurs méthodes pour obtenir les meilleurs résultats. Par conséquent, le Conseil a demandé au CDCI s’il y avait des questions techniques que le Conseil devrait examiner avant d’autoriser d’autres méthodes de blocage en vertu du cadre.

50. Le CDCI a fait valoir que pour que le blocage soit efficace, les entreprises doivent utiliser plusieurs méthodes différentes en même temps. Par conséquent, il a recommandé que les entreprises disposent de la flexibilité nécessaire pour choisir parmi différentes méthodes de blocage.

Positions des parties

51. Rogers a déclaré que puisque les FST utilisent déjà diverses techniques pour protéger les clients contre les activités en ligne malveillantes, ils devraient avoir la souplesse nécessaire pour mettre en œuvre d’autres mesures parallèlement aux méthodes de blocage autorisées en vertu du cadre.

52. Un particulier a fait remarquer que le dossier de la présente instance ne traite pas du blocage de ports, du blocage basé sur la signature ou du blocage basé sur les caractéristiques comportementales et du blocage basé sur l’inspection dynamique des paquets.

Analyse du Conseil

53. Le dossier de l’instance qui a mené à la Décision a montré que de nombreuses entreprises ont utilisé des méthodes de blocage fondées sur la détection de tendances inhabituelles ou malveillantes dans le trafic de réseau.

54. Le Conseil estime que toutes les méthodes de blocage devraient être autorisées en vertu du cadre afin de s’assurer qu’elles sont conformes aux critères minimaux du cadre.

55. Toutefois, le Conseil dispose actuellement de peu de renseignements sur les méthodes de blocage autres que les listes de blocage. Par conséquent, dans l’avis de consultation de Conformité et Enquêtes et de Télécom 2025-143, le Conseil examinera si et comment les méthodes de blocage autres que les listes de blocage devraient être intégrées au cadre.

Quels autres aspects du cadre devraient être pris en considération?

Options d'adhésion et de retrait pour les clients

56. Dans la Décision, le Conseil a demandé au CDCI s'il y avait un besoin technique de permettre à des clients individuels d'adhérer au système de blocage ou de s'en retirer.

57. Dans le Rapport, le CDCI a indiqué qu'il n'y a aucun besoin technique ni aucun moyen de permettre aux clients de choisir d'adhérer au système de blocage à l'échelle des réseaux ou de s'en retirer.

Positions des parties

58. Bien que le particulier ait appuyé une option de retrait pour les clients, Bell Canada et TELUS ont convenu avec le CDCI qu'il n'est pas possible pour la plupart des entreprises de permettre à leurs clients de refuser le blocage, parce que les entreprises ne sont généralement pas en mesure de reconnaître le trafic des utilisateurs individuels à l'échelle des réseaux.

59. Bell Canada et Rogers ont également fait remarquer que l'inclusion d'une option de retrait réduirait l'efficacité du cadre en augmentant la probabilité que les appareils de ceux qui s'en retirent s'infectent et propagent des réseaux de zombies et des logiciels malveillants à d'autres Canadiennes et Canadiens.

Analyse du Conseil

60. Dans la Décision, le Conseil était d'avis que le blocage devrait se faire par défaut, sans donner aux clients la possibilité de choisir d'y adhérer ou de s'en retirer. La Décision a souligné que les approches d'adhésion ont de faibles taux d'adoption et que les approches d'adhésion et de retrait minent la sécurité du réseau et augmentent considérablement le fardeau et les coûts de mise en œuvre supportés par les entreprises.

61. Le Conseil estime qu'il n'est pas techniquement possible de permettre aux clients de choisir d'adhérer au système de blocage à l'échelle du réseau fourni par les entreprises ou de s'en retirer et que cela irait à l'encontre de l'objectif du cadre. Une approche de blocage par défaut garantirait que tous les clients de l'entreprise bénéficient du blocage de la manière la plus efficace possible. Comme il est indiqué dans la Décision, cette approche est conforme à d'autres approches de blocage du trafic Internet de premier plan, notamment le modèle de blocage de Cleanfeed et le modèle de blocage de l'Autorité canadienne pour les enregistrements Internet.

62. Le Conseil détermine donc que le blocage en vertu du cadre sera appliqué par défaut.

Comment maximiser l'efficacité du cadre

63. Dans la Décision, le Conseil a demandé au CDCI quels autres éléments techniques aideraient à maximiser l'adoption du cadre et son efficacité.

64. Dans le Rapport, le CDCI a suggéré que le format de données pour le blocage de l'IC devrait être uniforme afin d'assurer la compatibilité entre les plateformes, que les FST devraient adopter des mécanismes d'échange de renseignements et que les IC devraient avoir des dates d'expiration.

Analyse du Conseil

65. En ce qui concerne les dates d'expiration pour les IC, le Conseil estime qu'un mélange de révision manuelle et de retrait de la liste automatisé des IC contribuerait à réduire les faux positifs et à s'assurer que les listes de blocage sont exactes et à jour.

66. En ce qui concerne l'échange de renseignements, le Conseil croit que l'échange d'IC entre les entreprises aiderait à maximiser l'efficacité du cadre. Cependant, cet échange peut être problématique en raison des conditions d'utilisation des listes de blocage commerciales qui peuvent ne pas permettre le partage ouvert des IC, et de la résistance possible des entreprises à échanger les IC à partir de leurs propres listes de blocage élaborées à l'interne. Par conséquent, le Conseil n'encouragera les entreprises à échanger les IC que dans le but de s'entraider.

67. Quant à l'exigence d'un format de données uniforme, cette suggestion va à l'encontre de l'idée que le cadre devrait être neutre sur le plan technologique et pourrait avoir une incidence directe sur d'autres parties qui ne sont pas réglementées par le Conseil, y compris les fournisseurs de listes de blocage. Par conséquent, le Conseil laissera l'industrie et les fournisseurs de listes de blocage s'entendre sur les normes de format de données.

Divulgation au public

68. Dans le Rapport, le CDCI a proposé que les exigences de divulgation des pratiques de gestion du trafic Internet énoncées dans la politique réglementaire de télécom 2009-657 servent de modèle pour informer les clients au sujet du cadre. Il a ajouté que le cadre devrait décrire clairement quels renseignements concernant la transparence sont nécessaires pour que la population canadienne puisse prendre des décisions éclairées sur les entreprises qu'elle souhaite utiliser.

Positions des parties

69. TELUS a déclaré que la divulgation au public de tous les IC bloqués pourrait réduire l'efficacité des programmes de cybersécurité, tandis que Bell Canada a recommandé que le cadre soit divulgué, mais pas les IC.

70. Le CDIP a souligné que la divulgation de détails pertinents dans un langage simple est très importante pour les consommateurs.

71. Le Conseil a également reçu des observations sur le besoin de transparence quant à ce qui est bloqué et à la façon dont c'est bloqué.

Analyse du Conseil

72. Le Conseil estime qu'il est essentiel que les renseignements sur le blocage dans le cadre devraient être rendus disponibles pour permettre aux consommateurs de prendre des décisions éclairées concernant leurs services Internet. Pour assurer la transparence, ces renseignements devraient être rédigés en langage clair et comprendre des détails sur le type et la portée du blocage en place, ainsi que sur le moment et la façon dont il sera appliqué.

73. Le Conseil convient que la liste des IC bloqués par une entreprise ne devrait pas être rendue publique, car cela fournirait aux acteurs malveillants des renseignements qu'ils pourraient exploiter.

74. Par conséquent, l'article 6.0 du cadre exigera que les entreprises divulguent, clairement et bien en vue sur leurs sites Web, certains renseignements liés à leur blocage. Ces exigences de divulgation sont globalement conformes aux exigences actuelles du Conseil relatives aux pratiques de gestion du trafic Internet.

Exigences en matière d'établissement de rapports

75. Le Rapport suggérait que chaque FST devrait fournir au Conseil le nombre d'IC bloqués et le nombre de faux positifs signalés.

Positions des parties

76. Bell Canada a suggéré qu'au lieu de demander aux entreprises de déclarer continuellement les paramètres au Conseil, il serait plus efficace d'établir des critères d'accréditation complets et d'avoir un tiers indépendant qui accrédite les fournisseurs de listes de blocage.

Analyse du Conseil

77. Les pratiques actuelles de blocage des réseaux de zombies des entreprises ne sont pas claires, même après une consultation publique et la publication du Rapport. La population canadienne sait peu de choses sur ce que font les entreprises en matière de blocage de cybersécurité. La mise en œuvre d'exigences en matière de rapports aiderait le Conseil à surveiller et à évaluer le rendement du cadre et à déterminer s'il fonctionne efficacement et atteint son objectif.

78. Le Conseil estime qu'il est dans l'intérêt public que la population canadienne soit au courant du rendement des entreprises en matière de blocage à l'échelle du réseau, car la sécurité du réseau fait partie du service Internet pour lequel elles paient. De plus, cette transparence pourrait stimuler la concurrence et l'innovation entre les entreprises en permettant au public d'examiner leurs rendements et de les aider à prendre des décisions éclairées.

79. Toutefois, le Conseil est d'avis que les exigences en matière de rapports ne devraient pas se limiter aux deux paramètres proposés par le CDCI. Il estime qu'aux fins de

l’évaluation de l’efficacité du cadre, il serait approprié d’exiger des renseignements plus détaillés sur le rendement des entreprises en matière de blocage.

80. Par conséquent, la section 7.0 du cadre exigera que les entreprises présentent chaque année au Conseil certains renseignements sur leur blocage de cybersécurité. Cela comprend des détails sur les listes de blocage utilisées, le nombre et les types d’IC uniques bloqués, le nombre et les types d’événements de blocage et le nombre de plaintes de faux positif ou de blocage excessif de la part des clients. Toutefois, afin de réduire le fardeau administratif immédiat associé à la mise en œuvre du cadre, ces exigences en matière de rapports n’entreront en vigueur qu’après la fin de la consultation publique amorcée par l’avis de consultation de Conformité et Enquêtes et de Télécom 2025-143.

Respect de la vie privée

81. Dans le Rapport, le CDCI a fait remarquer que l’évaluation du trafic à l’échelle des réseaux ne nécessite pas de renseignements sur les abonnés et n’implique donc pas le traitement de données sur les renseignements personnels.

Positions des parties

82. Le CDIP a soulevé des préoccupations quant à la possibilité que certaines méthodes de détermination et de blocage des réseaux de zombies puissent impliquer la collecte et l’exposition des renseignements personnels des consommateurs.

83. Bell Canada et TELUS ont fait valoir qu’il n’est pas nécessaire d’avoir plus de mesures de protection de la vie privée parce que le blocage des réseaux de zombies à l’échelle du réseau n’implique pas l’examen du contenu des messages ou des sites Web.

84. TELUS a fait remarquer qu’étant donné que les mesures de sécurité à l’échelle du réseau ciblent les activités malveillantes en fonction des noms de domaine, des adresses IP, des localisateurs de ressources universels, des tendances inhabituelles dans le trafic et d’autres paramètres des réseaux, le blocage à l’échelle du réseau s’applique à tous les clients d’un FST, et pas seulement à des clients précis.

Analyse du Conseil

85. Comme il est indiqué dans la Décision, le blocage des réseaux de zombies au niveau du réseau n’implique généralement pas l’identification de clients précis. Si une entreprise recueille ou expose des renseignements personnels pour se protéger contre les cyberattaques, elle doit respecter les obligations légales et réglementaires existantes, y compris celles énoncées dans la *Loi sur la protection des renseignements personnels et les documents électroniques* et dans diverses décisions du Conseil, comme la décision de télécom 2003-33 et les politiques réglementaires de télécom 2009-723 et 2017-11.

86. Compte tenu de ce qui précède, le paragraphe 8.2 du cadre indiquera explicitement que si une entreprise recueille, utilise ou divulgue des renseignements personnels pour des activités en vertu du cadre, elle doit se conformer à toutes les lois et à tous les règlements applicables. Il indiquera également clairement que le cadre ne permet pas la collecte, l'utilisation ou la communication supplémentaire de renseignements personnels.

Conclusion

87. Le Conseil approuve, conformément à l'article 36 de la *Loi*, le cadre énoncé à l'annexe de la présente décision. Il prendra effet le **12 août 2025**.

88. En vertu de l'article 36 de la *Loi*, les entreprises canadiennes ont besoin de l'approbation du Conseil pour contrôler ou influencer le contenu des télécommunications. En bloquant le trafic de réseaux de zombies et d'autres activités néfastes, les entreprises canadiennes peuvent empêcher la livraison de télécommunications aux utilisateurs, contrôlant ainsi le contenu des télécommunications qu'elles acheminent pour le public. Par conséquent, une telle activité relève de l'article 36 de la *Loi*.

89. Le cadre établit les modalités qui permettent aux entreprises canadiennes de bloquer le trafic Internet à des fins de cybersécurité. Pour l'instant, le cadre se limite à l'utilisation de listes de blocage de tierces parties et internes. Toutefois, dans l'avis de consultation de Conformité et Enquêtes et de Télécom 2025-143, le Conseil examinera si et comment les méthodes de blocage autres que les listes de blocage devraient être intégrées au cadre.

Instructions de 2023

90. Le Conseil estime que le cadre fera progresser les objectifs stratégiques de télécommunication énoncés dans la *Loi*[2] ainsi que les intérêts des consommateurs et les objectifs d'innovation des Instructions de 2023[3] en aidant à protéger la population canadienne contre les réseaux de zombies et 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 préjudices en ligne et d'aider à protéger la vie privée des personnes en interdisant l'accès et la collecte non autorisés de leurs renseignements personnels.

---

[2] 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.

[3] *Décret donnant au CRTC des instructions sur une approche renouvelée de la politique de télécommunication*, DORS/2023-23, 10 février 2023.

Secrétaire général

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 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

- *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

- *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

- *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

Annexe à la Décision de Conformité et Enquêtes et de Télécom CRTC 2025-142

Cadre pour limiter le trafic de réseaux de zombies

Définitions

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

Client : Personne qui est 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 se 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 de manière incorrecte.

Fournisseur de listes de blocage : Personne qui possède et gère une liste de blocage. Cette personne peut être une entreprise (liste de blocage interne) ou toute autre personne, comme un fournisseur de liste de blocage (liste de blocage de tierce partie).

Indicateur de compromission : Identifiant utilisé par les entreprises pour bloquer le trafic de 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. Dans le contexte d'une liste de blocage, un IC peut se composer, par exemple i) d'un nom de domaine ou ii) d'une adresse IP et d'un numéro de port.

Liste de blocage : Liste des indicateurs de compromission (IC) qui peuvent être utilisés par une entreprise pour bloquer le trafic Internet malveillant qui passe 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 de l'article 7.0 du cadre 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, à l'exception des exigences de la section 7.0, entreront en vigueur le **12 août 2025**. La section 7.0 entrera en vigueur dès l'approbation de la version finale du cadre de blocage.

Cette autorisation ne s'applique pas au blocage du trafic à d'autres fins, y compris le blocage d'activités autrement 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 qui pourraient contourner le blocage, tels que des services de réseau privé virtuel ou d'autres résolveurs du système de noms de domaine.

2.0. Ce qui est autorisé à être bloqué et de quelle façon

2.1 L'entreprise ne peut bloquer le trafic Internet malveillant qu'en fonction des indicateurs de compromission (IC) qui sont répertoriés sur une liste de blocage autorisée, comme indiqué à la section 2.2.

2.2. Sous réserve de la conformité d'une entreprise aux exigences énoncées dans la présente section et aux sections 3.0 et 4.0, les listes de blocage qui peuvent être utilisées par une entreprise sont les suivantes :

a) une liste de blocage de tierce partie qui peut être accessible à une entreprise par toute méthode automatisée ou plateforme de son choix;

b) une liste de blocage propriétaire interne.

2.3. L'entreprise peut utiliser une ou plusieurs listes de blocage autorisées, en totalité ou en partie, au meilleur de sa capacité technique[1].

2.4. L'entreprise doit utiliser une liste de blocage autorisée de la manière spécifiée par son fournisseur (p. ex. le fournisseur peut spécifier une fréquence de mise à jour particulière pour assurer l'expiration correcte des IC). Toutefois, en cas de conflit,

[1] Cette capacité technique peut être limitée, par exemple, en termes de volume d'IC à bloquer (limites dans les ressources informatiques) ou en termes de nature des IC et de la couche du modèle d'interconnexion des systèmes ouverts (OSI) à laquelle le blocage est effectué. En conséquence, toute liste de blocage autorisée peut être réduite ou personnalisée par l'entreprise.

les modalités imposées aux présentes par le Conseil l'emportent sur toute exigence contradictoire d'un fournisseur de listes de blocage.

3.0. Liste de blocage de tierce partie

3.1. Une entreprise ne peut utiliser une liste de blocage de tierce partie que s'il est convaincu que la liste de blocage et son fournisseur répondent, au minimum, aux critères suivants :

a) le fournisseur de listes de blocage 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 bien connues de l'Organisation internationale de normalisation (ISO) ou d'autres normes;

b) le fournisseur de listes de blocage n'a aucun conflit d'intérêts potentiel (p. ex. propriété et contexte géopolitique) qui pourrait compromettre le fonctionnement de sa liste de blocage de manière impartiale et dans l'intérêt supérieur de la population canadienne;

c) les exigences communes énoncées à la section 4.0 sont respectées.

4.0. Exigences applicables à toutes les listes de blocage autorisées

4.1. Une entreprise ne peut utiliser qu'une liste de blocage autorisée conforme aux critères minimaux suivants :

a) la liste de blocage recense uniquement les IC qui sont associés à des cyberattaques;

b) le fournisseur de la liste de blocage a la capacité de recevoir des IC de tierces parties;

c) le fournisseur de la liste de blocage a un mécanisme en place pour vérifier si chaque IC sur la liste est malveillant et évaluer s'il peut causer des dommages indirects. Le fournisseur de la liste de blocage a un mécanisme en place pour s'assurer que le blocage n'aura qu'une incidence minimale sur les services légitimes, strictement limitée à ce qui est nécessaire pour atteindre l'objectif de bloquer le trafic malveillant;

d) la liste de blocage est continuellement actualisée au moyen, par exemple, d'un mélange de révision manuelle, de retrait de la liste automatisé des IC ou de dates d'expiration;

e) le fournisseur de la liste de blocage a un processus en place, avec des normes de services, pour répondre aux plaintes relatives aux faux positifs et au

blocage excessif. À tout le moins, le processus de traitement des plaintes doit comprendre

i) une révision de l'IC en cause;

ii) la mise à jour de la liste de blocage, s'il y a lieu, pour en retirer l'IC (faux positif) ou le remplacer par un IC plus précis (blocage excessif);

iii) informer rapidement l'entreprise d'origine de la mesure prise, conformément aux exigences énoncées à l'article 5.2.

5.0. Exactitude (faux positifs et blocage excessif)

5.1. À la réception d'une plainte d'un client concernant un faux positif potentiel ou un blocage excessif, l'entreprise doit déterminer si la cause fondamentale est imputable à une liste de blocage assujettie au présent cadre et, le cas échéant, transmettre la plainte au fournisseur de la liste.

5.2. L'entreprise doit régler une plainte dans les deux jours ouvrables suivant sa réception de l'une des deux façons suivantes :

a) si un faux positif ou un blocage excessif est confirmé, l'entreprise doit actualiser la liste de blocage, comme il est établi au 4.1e.ii) ci-dessus (c.-à-d. déblocage);

b) si l'IC est confirmé comme étant malveillant et que le blocage est maintenu, l'entreprise doit en informer le client.

6.0. Transparence (exigences de divulgation)

6.1. 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 aussi faire référence à ses divulgations en ligne dans le matériel promotionnel pertinent, les contrats avec les clients et les modalités de service.

6.2. La divulgation en ligne doit fournir suffisamment de renseignements en langage clair pour que la population canadienne comprenne le type et la portée du blocage en place; quand et comment il sera appliqué; le processus de dépôt et d'enquête sur les plaintes liées à des faux positifs et à un blocage excessif potentiels; tout renseignement pertinent lié à la confidentialité et les déclarations nécessaires. À

[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.

tout le moins, les renseignements suivants doivent être inclus pour satisfaire à cette exigence :

a) Que le blocage respecte les modalités énoncées dans la décision *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. Par conséquent, le blocage est effectué exclusivement à des fins de protection contre les cyberattaques et non à d'autres fins, telles que le blocage d'autres activités illégales ou le blocage à des fins commerciales, concurrentielles ou politiques. L'objectif est de protéger les ordinateurs des clients contre les réseaux de zombies malveillants (c.-à-d. contre l'adhésion à un réseau d'appareils infectés par des logiciels malveillants contrôlés par un auteur de menaces à l'insu et sans le consentement des clients) et contre d'autres cybermenaces, notamment les logiciels malveillants et l'hameçonnage. Le blocage n'implique aucune appréciation du contenu des sites Web visités. Par exemple, ce blocage n'examine pas les sites Web qui offrent des biens ou des services illicites, ou des sites Web qui publient des nouvelles fausses ou trompeuses, des commentaires offensants ou du matériel obscène.

b) Que le blocage est appliqué à l'échelle des réseaux par défaut, ce qui signifie que les clients ne peuvent pas demander d'adhérer au système de blocage ou de s'en retirer.

c) Le type de blocage employé (c.-à-d. un blocage basé sur une liste de blocage d'indicateurs qui ont été validés comme étant malveillants) et le type d'indicateurs utilisé pour le blocage (p. ex. adresse IP et numéro de port, nom de domaine).

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

e) Que le blocage a pour but de fournir des services Internet plus sécuritaires, mais qu'il ne remplace pas les protections au niveau de l'utilisateur : les fournisseurs de services fournissent des protections en matière de cybersécurité pour leurs réseaux et les consommateurs fournissent des protections en matière de cybersécurité pour leurs propres appareils. Par conséquent, il demeure important que les clients continuent de sécuriser leurs appareils et leur connexion Internet contre les cybermenaces (p. ex. installer et mettre à jour des solutions antivirus, mettre à jour régulièrement leurs logiciels, gérer un pare-feu, utiliser de solides mots de passe, activer l'authentification à deux facteurs et sécuriser leur connexion sans fil).

6.3 Lorsqu'une entreprise met en place un nouveau mécanisme de blocage ou en modifie un qu'elle a déjà, elle doit remplir les exigences de divulgation du présent article au moins 30 jours avant le changement.

6.4. La divulgation en ligne doit être accessible aux personnes en situation de handicap, conformément aux décisions énoncées dans la politique *Accessibilité des services de télécommunication et de radiodiffusion* dans la 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.

7.0. Transparence (mesures de performance)

(La section 7.0 entrera en vigueur dès l'approbation de la version finale du cadre de blocage.)

7.1. L'entreprise doit déposer les renseignements suivants devant le Conseil[3] au sujet des listes de blocage qu'elle a utilisées pendant la période de déclaration, dans les 30 jours civils suivant la fin de celle-ci :

a) l'identification de toutes les listes de blocage utilisées par l'entreprise (de tierces parties ou internes), avec les noms des listes et le nom de leur fournisseur;

b) si une liste de blocage n'a pas été utilisée pendant toute la période de déclaration, les dates de début et de fin de son utilisation; si une liste de blocage de tierce partie n'est pas utilisée dans son intégralité, mais seulement en partie, des détails sur la façon dont la personnalisation est appliquée;

c) le nombre total d'IC uniques efficacement bloqués par l'entreprise, y compris une ventilation par nombre i) d'adresses IP, ii) de domaines et iii) d'autres types d'IC uniques;

d) le nombre total d'événements de blocage, y compris une ventilation par type de cybermenace : i) réseaux de zombies, ii) logiciels malveillants, iii) hameçonnage et iv) autres cybermenaces;

e) en ce qui concerne les IC détectés et bloqués au moyen de listes de blocage internes, le nombre total d'IC uniques hors du réseau de l'entreprise, et le nombre total d'IC échangés avec d'autres entreprises pour atténuer la menace correspondante sur d'autres réseaux, ainsi que la méthode employée pour échanger les IC (automatisée ou manuelle)[4];

---

[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] Conformément aux sections 3.1.4 (11) et 6.1 du document *Pratiques exemplaires de sécurité pour les fournisseurs de services de télécommunications canadiens (FST)*, Comité consultatif canadien pour la sécurité des télécommunications (CCCST), 31 octobre 2013 (Pratiques exemplaires du CCCST en matière de sécurité)

f) le nombre total d'avis envoyés aux clients pour les avertir que leur ordinateur a été infecté[5];

g) le nombre d'événements de blocage par abonné par mois (c.-à-d. le résultat mathématique du rapport suivant : le nombre total d'événements de blocage [section 7.1.d], divisé par le nombre total d'abonnés aux services Internet, divisé par le nombre de mois sur la période de déclaration). Inclure tous les chiffres utilisés pour calculer le nombre par abonné;

h) le nombre total de plaintes pour faux positifs ou blocage excessif reçues des clients pour chaque liste de blocage utilisée, et le nombre de faux positifs et d'événements de blocage excessif qui ont été confirmés;

i) un hyperlien vers la page Web utilisée pour remplir les exigences de divulgation établies à l'article 6.0;

j) lorsqu'une entreprise utilise des listes de blocage internes, une description détaillée du fonctionnement de chaque liste de blocage interne, y compris, par exemple, une référence aux exigences établies à l'article 4.1.

8.0. Responsabilisation et protection de la vie privée

8.1. L'entreprise doit examiner périodiquement tous ses systèmes de blocage assujettis à ce cadre pour vérifier qu'ils fonctionnent comme prévu.

8.2. 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 communication supplémentaire de renseignements personnels.

9.0. Autres conditions

9.1 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.

---

[5] Conformément aux articles 5 et 6 du document *Recommendations for the Remediation of Bots in ISP Networks* [en anglais seulement], Request for comments (RFC) 6561, The Internet Society (Internet Engineering Task Force), mars 2012 et à la section 5.2.1 des Pratiques exemplaires du CCCST en matière de sécurité