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

Avis de consultation de Conformité et Enquêtes et de Télécom CRTC 2021-9

Version PDF

Ottawa, le 13 janvier 2021

Dossier public : 1011-NOC2021-0009

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

Date limite de dépôt des interventions : 15 mars 2021

[Soumettre une intervention ou voir les documents connexes]

Le Conseil lance un appel aux observations par les présentes sur sa proposition de développer un cadre de blocage à l'échelle des réseaux qui limitera le préjudice causé aux Canadiens par les réseaux de zombies tout en préservant la vie privée et en assurant la transparence. Les réseaux de zombies sont à la base d'une part de plus en plus importante des cybermenaces qui pèsent sur les citoyens, les entreprises et les institutions du Canada, et le blocage du trafic des réseaux de zombies est un moyen efficace de réduire ces menaces.

Contexte

1. La cyberactivité malveillante vise les consommateurs et les entreprises du Canada, ainsi que les organisations qui fournissent des services essentiels comme les hôpitaux, les écoles et les organismes gouvernementaux. Cette activité malveillante compromet la vie privée et porte atteinte à l'intégrité et à la disponibilité du réseau. Elle impose également des coûts aux victimes et mine la confiance des Canadiens dans l'utilisation des communications électroniques pour mener leurs activités en ligne.

2. Une des tendances des cyberattaques est l'utilisation de réseaux de zombies pour contourner les défenses et donner aux attaquants une couche d'anonymat supplémentaire. Un réseau de zombies est un réseau d'ordinateurs infectés par des logiciels malveillants (zombies) qui sont sous le contrôle d'un serveur de commande et de contrôle (C2) exploité par un auteur malveillant. L'infection par un logiciel malveillant est causée par un programme informatique installé à l'insu ou sans le consentement du propriétaire de l'ordinateur. Chaque zombie[1] est un ordinateur ou

[1] Les zombies dont il est question dans le présent avis de consultation font référence exclusivement à des dispositifs infectés par des logiciels malveillants. Les « bons » zombies programmés pour effectuer des tâches utiles, tels que les robots conversationnels et les robots d'indexation, ne sont pas considérés.

autre dispositif d'un abonné aux services Internet qui communique par l'intermédiaire du fournisseur de services de l'abonné vers un serveur C2 associé.

3. Les réseaux de zombies sont à l'origine d'une part de plus en plus importante des logiciels malveillants et facilitent les formes les plus choquantes de cybermenaces. Les types de cyberattaques qui peuvent être perpétrées grâce aux réseaux d'ordinateurs zombies comprennent la distribution de pourriels, les attaques par déni de service distribué, le vol de renseignements et le déploiement de logiciels malveillants. Les Canadiens sont particulièrement préoccupés par les fréquentes attaques de logiciels de rançon[2], qui ont causé d'importantes interruptions de service et des dommages financiers.

4. Le Conseil réglemente le système canadien de télécommunication en vue de promouvoir les objectifs de la politique canadienne de télécommunication énoncés à l'article 7 de la *Loi sur les télécommunications* (*Loi*). Les activités malveillantes facilitées par les réseaux de zombies sont contraires à plusieurs des objectifs stratégiques de la *Loi*, notamment

    - favoriser le développement ordonné des télécommunications en un système qui contribue à sauvegarder, enrichir et renforcer la structure sociale et économique du Canada et de ses régions;
    - permettre l'accès aux Canadiens dans toutes les régions – rurales ou urbaines – du Canada à des services de télécommunication sûrs, abordables et de qualité;
    - satisfaire les exigences économiques et sociales des usagers des services de télécommunication;
    - contribuer à la protection de la vie privée des personnes.

5. Le Conseil est également le principal organisme d'application de la *Loi visant à promouvoir l'efficacité et la capacité d'adaptation de l'économie canadienne par la réglementation de certaines pratiques qui découragent l'exercice des activités commerciales par voie électronique et modifiant la Loi sur le Conseil de la radiodiffusion et des télécommunications canadiennes, la Loi sur la concurrence, la Loi sur la protection des renseignements personnels et les documents électroniques et la Loi sur les télécommunications* (*Loi canadienne anti-pourriel* [LCAP]). Il est chargé de veiller au respect des dispositions relatives à la distribution de pourriels (article 6), à la redirection du trafic vers les réseaux malveillants (article 7) et à l'installation de logiciels malveillants (article 8) ainsi que de faire respecter l'interdiction d'aider quiconque se livre à ces activités (article 9). Le personnel du Conseil mène des enquêtes et prend des mesures coercitives lorsque des infractions ont déjà été commises; il travaille également de manière proactive pour prévenir les

[2] Les logiciels de rançon sont un type de logiciel malveillant conçu pour dénier l'accès à un système informatique ou à des données en les cryptant jusqu'au versement d'une rançon. La méthode la plus courante de distribution du logiciel de rançon est le pourriel par hameçonnage, où une victime ouvre un courriel contenant une pièce jointe malveillante et la télécharge sur son ordinateur sans le savoir.

infractions en utilisant des mécanismes de promotion de la conformité et de sensibilisation. L'activité du réseau de zombies est par définition une violation de la LCAP, tout comme le réseau de zombies lui-même.

6. Dans le bulletin d'information de Conformité et Enquêtes 2018-415, le Conseil a fait remarquer que l'article 9 de la LCAP peut s'appliquer aux personnes et aux organisations, y compris aux entreprises canadiennes et autres fournisseurs de services de télécommunication (FST), qui fournissent des services techniques et d'autres services qui facilitent l'activité commerciale électronique. Le Conseil a déclaré que, conformément à l'article 9, il s'attendait à ce que les FST prennent des mesures appropriées pour réduire et limiter les comportements anti-LCAP sur leurs réseaux.

7. L'un des moyens dont disposent les FST pour limiter les comportements anti-LCAP est de bloquer le trafic des réseaux de zombies. Certains mécanismes de blocage peuvent être mis en œuvre au niveau des points d'extrémité par les utilisateurs, et d'autres à l'échelle des réseaux par les fournisseurs de services, y compris les entreprises canadiennes et d'autres FST. Toutefois, l'article 36 de la *Loi* contient également une interdiction sur le contrôle du contenu des télécommunications par les entreprises canadiennes.

8. Le Conseil ne peut généralement pas affronter les attaques facilitées par les réseaux de zombies à leur source, car elles ont lieu le plus souvent à l'étranger. Toutefois, le Conseil a le pouvoir et le mandat d'utiliser les mécanismes réglementaires de la *Loi* pour lutter contre les activités malveillantes facilitées par les réseaux de zombies. Le Conseil envisage donc de mettre en place un cadre de blocage à l'échelle des réseaux pour prévenir les préjudices et atteindre les objectifs de la *Loi*.

Cadre de blocage à l'échelle des réseaux

9. Les fournisseurs de services peuvent introduire le blocage à l'échelle des réseaux en utilisant diverses techniques. Trois des techniques les plus courantes sont le blocage basé sur le domaine, le blocage basé sur le protocole Internet (IP) et le blocage basé sur le protocole.

10. Les internautes accèdent aux sites Web en cliquant sur des liens ou en saisissant des domaines (www.exemple.com) dans un navigateur. Pour accéder à une page Web, le domaine doit d'abord être traduit dans l'adresse IP du serveur qui héberge la page Web. Cette traduction se fait au moyen du système de noms de domaine (DNS), qui associe les noms de domaine aux adresses IP. Une fois l'adresse IP trouvée, l'appareil de l'internaute peut alors acheminer la communication vers le serveur du site Web et télécharger la page Web.

11. Lorsque le blocage basé sur le domaine est en place et qu'un appareil infecté demande un domaine C2 bloqué, la réponse du DNS indiquera que le domaine est inconnu ou redirigera l'utilisateur vers un site indiquant que le domaine demandé n'est pas autorisé.

12. Cependant, tous les logiciels malveillants ne se connectent pas aux serveurs C2 en utilisant des domaines; certains se connectent en communiquant directement avec l'adresse IP d'un serveur C2. Le blocage basé sur le domaine n'est pas efficace pour ce type de logiciel malveillant, car il contourne le DNS, de sorte que des techniques de remplacement sont nécessaires. Une possibilité est le blocage basé sur l'IP, qui utilise un filtre appelé pare-feu pour empêcher la communication vers les adresses IP des serveurs C2 suspects tout en laissant passer d'autres communications. Une autre est le blocage basé sur le protocole, qui est une forme plus ciblée de blocage basé sur l'IP, limité à un groupe de services sur un serveur spécifique.

13. Toutes ces techniques de blocage utilisent des renseignements provenant de sources publiques et privées pour repérer et bloquer l'accès aux serveurs C2 au moyen de leurs noms de domaine, de leurs adresses IP ou de modèles de communication connus des réseaux de zombies.

14. Selon l'avis préliminaire du Conseil, le blocage à l'échelle des réseaux est une stratégie viable pour prévenir le préjudice que les réseaux de zombies causent aux Canadiens et pour promouvoir les objectifs stratégiques de la *Loi*.

15. Bien que le blocage à l'échelle des réseaux puisse être mis en œuvre sans accéder au contenu des transmissions Internet, le Conseil estime néanmoins que tout cadre réglementaire de blocage ou de filtrage du trafic doit comporter des garanties pour assurer la protection des intérêts des utilisateurs. Tout cadre approuvé par le Conseil devra comprendre, au minimum, des dispositions i) qui garantissent la protection de la vie privée des abonnés aux services Internet, ii) qui permettent aux abonnés de choisir d'accepter ou de refuser le blocage, iii) qui prévoient un mécanisme de correction des faux positifs, iv) qui garantissent que les décisions de blocage sont impartiales et prises dans l'intérêt des Canadiens et v) qui minimisent la surveillance, la collecte et l'utilisation des renseignements relatifs aux abonnés.

Appel aux observations

16. Afin de mieux protéger les Canadiens contre les communications malveillantes et de renforcer la cybersécurité, le Conseil s'engage à faire des efforts qui contribuent à prévenir, réduire et interrompre les attaques des réseaux de zombies et autres communications anti-LCAP.

17. Le Conseil lance par les présentes un appel aux observations pour guider l'élaboration d'un cadre de blocage à l'échelle des réseaux afin de limiter les dommages causés aux Canadiens par les réseaux de zombies. Le Conseil sollicite l'avis des abonnés aux services Internet sur la première question ci-dessous, et celui de tous les intervenants sur les autres questions.

Q1. En tant qu'internaute canadien, quel serait l'avantage pour vous de voir votre fournisseur de services de télécommunication (FST) bloquer les communications malveillantes des réseaux de zombies? Quelles sont vos préoccupations?

18. La neutralité du Net est le concept selon lequel tout le trafic Internet devrait être traité de manière égale par les FST, avec peu ou pas de priorité, de discrimination ou de préférence, quel que soit le contenu du trafic. Le Conseil a approuvé ce concept en principe, bien qu'il soit favorable à des exceptions limitées, par exemple aux programmes qui bloquent l'accès au matériel d'exploitation des enfants et aux services tels que les filtres anti-pourriels des FST.

19. Le trafic des réseaux de zombies expose les Canadiens aux pourriels, aux logiciels espions, au vol d'information et aux logiciels de rançon. Compte tenu des risques associés à cette exposition, une exception limitée à la neutralité du réseau peut être garantie afin d'offrir aux Canadiens une protection supplémentaire contre ces menaces.

20. Le Conseil demande aux abonnés canadiens aux services Internet s'ils pensent pouvoir bénéficier d'un cadre permettant à leur FST de bloquer le trafic des réseaux de zombies, et les raisons qui motivent cette opinion.

Q2. Quelles conditions rattachées au cadre sont requises pour protéger la vie privée des abonnés aux services Internet lors de la surveillance du trafic et du signalement grâce aux programmes de blocage?

21. Les réseaux de zombies constituent une menace importante pour la vie privée des consommateurs. Ils sont utilisés pour obtenir un accès illégal à des renseignements personnels sensibles qui peuvent ensuite être utilisés à des fins malveillantes. Le blocage des communications des réseaux de zombies peut contribuer à protéger les consommateurs; toutefois, cette protection est assurée par la surveillance du trafic Internet. Les conséquences pour la vie privée des consommateurs que la surveillance entraîne doivent être traitées pour tout cadre de blocage potentiel.

22. Le Conseil invite les parties à présenter leurs observations sur les conditions qui peuvent protéger la vie privée des consommateurs, telles que

    - interdire aux entreprises de surveiller, de collecter ou de divulguer des contenus ou des métadonnées qui ne servent pas à bloquer le trafic des réseaux de zombies;
    - limiter la surveillance et la collecte au nom de domaine de destination ou à l'adresse IP demandée et au nombre de fois où le service malveillant est demandé;
    - restreindre la divulgation des données surveillées aux parties participant au programme de blocage.

23. Le Conseil sollicite également des observations sur les mesures appropriées à utiliser pour faire en sorte que le cadre fonctionne comme prévu. Il s'agit par exemple de l'enregistrement de la date et de l'heure et du volume des événements bloqués et du taux de faux positifs.

Q3. Quelles sont les exigences de divulgation nécessaires pour les entreprises et les FST pour garantir que les abonnés aux services Internet disposent de renseignements suffisants pour prendre des décisions éclairées sur la participation à un programme de blocage?

24. La transparence des programmes de blocage est importante pour garantir la responsabilité et pour aider les consommateurs à faire des choix éclairés lorsqu'ils choisissent leur FST ou décident de participer à un programme de blocage. Les abonnés aux services Internet devraient être informés par leur FST que le blocage est utilisé et ils devraient pouvoir vérifier si un domaine ou une adresse IP en particulier est bloqué par leur fournisseur. Toutefois, pour garantir qu'un programme de blocage reste efficace, il peut être raisonnable de fixer des limites quant aux renseignements mis à disposition, car des auteurs malveillants pourraient utiliser n'importe quelle information publique pour contourner les mesures de blocage.

25. Le Conseil invite les intéressés à faire part de leurs observations sur les dispositions qui assureront la transparence des programmes de blocage, par exemple en informant les clients de la portée du mécanisme de filtrage ou en créant un portail où les abonnés peuvent vérifier si un domaine particulier est bloqué. Dans leurs observations, les parties doivent aborder quelconque risque relatif à l'efficacité ou à la réussite associé à la divulgation d'information sur le fonctionnement du programme.

Q4. Quelles sont les parties les plus aptes à décider de ce qui doit être bloqué?

26. Les décisions relatives au blocage ne devraient pas être prises à la légère et doivent tenir compte de facteurs comme le degré de préjudice potentiel pour les internautes et si d'autres effets imprévus résulteront du blocage. Les décisions relatives au blocage ne doivent pas être influencées par des intérêts commerciaux et elles doivent reposer sur des données solides provenant de sources fiables. L'avis préliminaire du Conseil est qu'une partie indépendante spécialisée en cybersécurité serait la mieux placée pour évaluer l'impact du blocage d'un domaine ou d'une adresse IP en particulier en vue de protéger l'intérêt public et pour décider si le blocage est justifié.

27. Le Conseil est également d'avis que bien que les entreprises et les FST peuvent avoir besoin d'une certaine souplesse pour retirer de la liste de blocage les indicateurs qui conduisent à de faux positifs, ils devraient, pour protéger l'intégrité du cadre, demander l'approbation de l'évaluateur indépendant avant d'ajouter de nouveaux indicateurs.

28. Le Conseil invite les parties à commenter les méthodes et les dispositions garantissant l'impartialité et l'exactitude des décisions de blocage, et à désigner des parties viables et indépendantes susceptibles de servir d'autorité décisionnelle.

Q5. Le trafic des réseaux de zombies serait-il mieux traité par un blocage par défaut à option de retrait ou par un modèle qui permet un blocage à option d'adhésion?

29. Les appareils infectés connectés à Internet et fonctionnant comme des zombies le font généralement à l'insu de leur propriétaire ou sans son consentement. Les abonnés aux services Internet peuvent ne pas voir l'intérêt de participer à un programme de blocage à l'échelle des réseaux, même si leur appareil est infecté par un logiciel malveillant, ce qui peut rendre un modèle à option d'adhésion moins efficace qu'un modèle à option de retrait.

30. Le Conseil invite les parties à évaluer les avantages et les inconvénients relativement à l'efficacité des modèles de blocage par défaut par rapport aux modèles de type à option d'adhésion pour traiter les communications des réseaux de zombies. Les parties devraient déterminer quel est leur modèle préféré et quelles sont les dispositions requises pour sa mise en œuvre.

Q6. Quelles dispositions ou conditions rattachées au cadre sont nécessaires pour prévenir et atténuer les risques liés au blocage excessif et aux faux positifs?

31. Plusieurs services en ligne peuvent se résoudre à la même adresse IP, et les serveurs de réseau de zombies C2 ne restent généralement pas sur le même appareil pendant de longues périodes. Le blocage d'une adresse IP peut donc empêcher par inadvertance l'accès à un service légitime, et le blocage d'un serveur C2 ne sera efficace que pendant une durée limitée. Par conséquent, la liste de blocage doit changer régulièrement pour rester exacte, ce qui amène des risques de blocage excessif et de faux positifs.

32. Le Conseil invite les intéressés à formuler des observations sur les dispositions ou les conditions rattachées au cadre de blocage qui pourraient empêcher le blocage excessif et les faux positifs, ou qui pourraient atténuer les risques associés. Les parties sont invitées à

    - commenter la probabilité de l'apparition d'un blocage excessif et de faux positifs et les conséquences de cette situation dans le cadre de l'utilisation de mesures de protection contre le trafic des réseaux de zombies;
    - définir les attentes en matière de résolution des faux positifs et les dispositions pour garantir la rapidité et l'équité procédurale dans le processus de résolution;
    - suggérer des options, accompagnées des avantages et des inconvénients que chacune représente, de moyens automatisés pour résoudre le problème causé par le blocage incorrect des services.

Q7. Quel mécanisme réglementaire est le mieux adapté pour garantir la mise en œuvre d'un cadre de blocage à l'échelle des réseaux qui traite efficacement les communications des réseaux de zombies?

33. Le Conseil estime qu'il dispose d'un certain nombre de pouvoirs en vertu de la *Loi* qui lui permettraient d'établir un cadre obligatoire ou facultatif, notamment ceux prévus aux articles 24, 24.1, 36 et 41. Par exemple, le Conseil pourrait envisager

    - d'autoriser les entreprises canadiennes à procéder au blocage en vertu de l'article 36 de la *Loi*;
    - d'imposer aux entreprises canadiennes et aux autres FST l'obligation d'effectuer un blocage à l'échelle des réseaux comme condition de service, conformément aux articles 24 et 24.1;
    - d'interdire l'utilisation des installations de télécommunication d'une entreprise canadienne pour transmettre des communications de réseau de zombies, dans la mesure où il s'agit de communications non sollicitées au sens de l'article 41 de la *Loi*.

34. Le Conseil pourrait également envisager d'utiliser l'article 42 de la *Loi* pour étendre ce cadre à d'autres personnes qui ont le contrôle des installations de télécommunication.

35. Le Conseil invite les intéressés à lui faire part de leurs observations sur la pertinence et l'efficacité des mécanismes de réglementation mentionnés ci-dessus pour remédier au préjudice causé par les réseaux de zombies. Les parties sont encouragées à examiner toutes les options énumérées et à formuler des observations sur chacune d'entre elles.

Q8. Quelles techniques de blocage à l'échelle des réseaux sont les mieux adaptées pour arrêter ou limiter la communication entre les réseaux de zombies?

36. Les réseaux de zombies et les logiciels malveillants sur lesquels ils reposent varient en fonction de leur conception et de leur objectif. Ces variations peuvent limiter l'efficacité de certaines techniques de blocage contre le trafic des réseaux de zombies.

37. Le Conseil sollicite des observations sur l'efficacité des techniques de blocage des réseaux de zombies, en particulier celles qui bloquent les communications entre un dispositif infecté au Canada et les serveurs C2 situés à l'intérieur ou à l'extérieur du Canada.

38. Compte tenu de l'augmentation significative des attaques facilitées par les réseaux de zombies, le Conseil se concentrera sur les techniques qui concilient efficacité et facilité de mise en œuvre et qui n'entraînent pas de coûts supplémentaires aux abonnés des services Internet. Les techniques qui tirent profit des technologies, services et infrastructures existants présentent donc un intérêt particulier.

39. Les parties sont priées d'indiquer leurs techniques de blocage préférées et de fournir une justification détaillée qui expose les avantages, les inconvénients, les coûts, la rapidité de mise en œuvre et les obstacles à la mise en œuvre de ces techniques. Dans le cadre de leur description des inconvénients, les parties sont invitées à formuler des observations précises sur les lacunes liées à la défense de réseau qui subsisteraient malgré la mise en œuvre, sur les taux de faux positifs et sur les risques de blocage excessif.

40. Les observations ne doivent pas se limiter aux méthodes basées sur le domaine, l'IP ou le protocole. Les parties sont encouragées à proposer des solutions de rechange et à établir tous les avantages et inconvénients associés à ces solutions.

Q9. S'il est déterminé que le blocage basé sur le domaine s'avère une technique privilégiée, quelles considérations relatives à la sélection du résolveur de domaine un cadre de blocage devrait-il prendre en compte?

41. Les résolveurs de domaine sont des ordinateurs spécialisés gérés par des fournisseurs de services qui lancent le processus de traduction d'un nom de domaine en son adresse IP correspondante. De nombreux résolveurs de domaine et de services sont disponibles pour assurer le blocage de domaine et empêcher l'accès aux serveurs C2 du réseau de zombies.

42. Le Conseil invite les intéressés à lui faire part de leurs observations sur l'utilisation potentielle des résolveurs de domaine ou de services existants pour bloquer le trafic des réseaux de zombies, notamment le Bouclier canadien de l'Autorité canadienne pour les enregistrements Internet, Quad9, OpenDNS, Comodo Secure DNS et CleanBrowsing.

43. Les parties devraient examiner les considérations relatives à l'utilisation des résolveurs de domaine existants adaptés aux communications des réseaux de zombies. Les parties peuvent également proposer l'utilisation de résolveurs de domaine particuliers en incluant une justification indiquant les avantages et les inconvénients de chacun de ces résolveurs.

Q10. Comment les changements technologiques doivent-ils être traités dans le cadre du blocage à l'échelle des réseaux?

44. Les réseaux de zombies sont dynamiques et flexibles en raison de leur conception. Les logiciels malveillants des réseaux de zombies sont fréquemment modifiés et mis à jour afin de reconstituer ou d'étendre le bassin de zombies, d'ajouter des fonctionnalités et d'améliorer la performance. Les serveurs C2 sont également régulièrement déplacés et dupliqués sur différents serveurs pour échapper à la détection et résister aux démantèlements. Les nombreux réseaux de zombies en activité adoptent divers comportements de communication qui sont de plus en plus codés et donc difficiles à détecter. Les opérateurs malveillants adaptent la conception des réseaux de zombies pour contourner toutes les méthodes de blocage connues; un cadre de blocage efficace doit pouvoir s'adapter en conséquence.

45. Le Conseil invite les parties à formuler des suggestions et des observations sur les dispositions du cadre qui aideraient les entreprises et autres FST à s'adapter aux variations de conception des réseaux de zombies et aux ajustements de leurs opérateurs. Par exemple, quelles dispositions le cadre devrait-il inclure pour tenir compte des changements dans la conception des logiciels malveillants ou des types de dispositifs ciblés par les opérateurs de réseaux de zombies?

Procédure

46. Les *Règles de pratique et de procédure du Conseil de la radiodiffusion et des télécommunications canadiennes* (*Règles de procédure*) s'appliquent à la présente instance. Les *Règles de procédure* établissent, entre autres choses, les règles concernant le contenu, le format, le dépôt et la signification des interventions, des réponses, des répliques et des demandes de renseignements; la procédure de dépôt d'information confidentielle et des demandes de divulgation et le déroulement de l'audience publique. Par conséquent, la procédure établie ci-dessous doit être lue en parallèle aux *Règles de procédure* et aux documents connexes, que l'on peut consulter sur le site Web du Conseil à l'adresse www.crtc.gc.ca, sous la rubrique « Lois et règlements ». Les lignes directrices établies dans le bulletin d'information de radiodiffusion et de télécom 2010-959 donnent des renseignements pour aider les intéressés et les parties à comprendre les *Règles de procédure* afin qu'ils puissent participer aux instances du Conseil de manière plus efficace[3].

47. Le Conseil encourage les réponses, entre autres, des entreprises de services locaux titulaires et concurrentes, des sociétés d'hébergement Web, des fournisseurs de DNS de protection et d'autres organisations gouvernementaux dont le mandat comprend la protection des infrastructures critiques ou des réseaux informatiques.

48. Les intéressés qui souhaitent devenir des parties à la présente instance doivent déposer auprès du Conseil une intervention concernant les questions susmentionnées, au plus tard le **15 mars 2021**. L'intervention doit être déposée conformément à l'article 26 des *Règles de procédure*.

49. Les parties sont autorisées à coordonner, organiser et déposer, en un mémoire unique, des interventions au nom d'autres intéressés qui partagent leur opinion. Des renseignements sur la manière de déposer ce type de mémoire, qu'on appelle une intervention favorable conjointe, ainsi qu'un modèle de la lettre d'accompagnement qui doit être déposée par les parties sont présentés dans le bulletin d'information de télécom 2011-693.

50. Tous les documents devant être signifiés aux parties à l'instance doivent être signifiés en utilisant les coordonnées figurant dans les interventions.

---

[3] Les articles 30 à 34 des *Règles de procédure* et les articles 38 à 39 de la *Loi* définissent un processus par lequel les parties aux instances du Conseil peuvent déposer de l'information confidentielle au dossier d'une instance publique. Consultez le bulletin d'information de radiodiffusion et de télécom 2010-961 pour plus de détails sur le processus.

51. Toutes les parties peuvent déposer des répliques aux interventions auprès du Conseil, au plus tard le **14 avril 2021**. Les mémoires, y compris leur résumé, ne doivent pas dépasser 20 pages.

52. Le Conseil encourage les intéressés et les parties à examiner le contenu du dossier public de la présente instance sur le site Web du Conseil à l'adresse www.crtc.gc.ca pour obtenir tout renseignement additionnel qu'ils pourraient juger utile à la préparation de leurs mémoires.

53. Les mémoires de plus de cinq pages devraient inclure un résumé. Chaque paragraphe des mémoires devrait être numéroté. La mention ***Fin du document*** devrait également être ajoutée après le dernier paragraphe du mémoire. Cela permettra au Conseil de s'assurer que le document n'a pas été détérioré lors de la transmission par voie électronique.

54. En vertu du bulletin d'information de radiodiffusion et de télécom 2015-242, le Conseil s'attend à ce que les entités constituées et les associations déposent leurs mémoires dans le cadre des instances du Conseil dans des formats accessibles (p. ex. des formats de fichier texte dont le texte peut être agrandi ou modifié, ou lu par un lecteur d'écran), et il encourage tous les Canadiens à faire de même. Pour leur faciliter la tâche, le Conseil a affiché sur son site Web des lignes directrices pour la préparation des documents en formats accessibles.

55. Les mémoires doivent être déposés auprès du secrétaire général du Conseil selon **une seule** des façons suivantes :

en remplissant le
[formulaire d'intervention]

ou

par la poste, à l'adresse
CRTC, Ottawa (Ontario) K1A 0N2

ou

par télécopieur, au numéro
819-994-0218

56. Les parties qui envoient des documents par voie électronique doivent s'assurer de pouvoir prouver au Conseil, sur demande, le dépôt ou la signification d'un document en particulier. Par conséquent, elles doivent conserver la preuve de l'envoi et de la réception d'un document pour une période de 180 jours à compter de la date du dépôt ou de la signification du document. Le Conseil recommande aux parties qui déposent un document et en signifient copie par voie électronique de se montrer prudentes lors de la signification de documents par courriel, car la preuve de la signification peut être difficile à faire.

57. Conformément aux *Règles de procédure*, un document doit être déposé auprès du Conseil et de toutes les parties concernées au plus tard à 17 h, heure de Vancouver (20 h, heure d'Ottawa) à la date d'échéance. Les parties sont tenues de veiller à ce que leur mémoire soit déposé en temps opportun et ne seront pas informées s'il est reçu après la date limite. Les mémoires déposés en retard, y compris en cas de retard causé par la poste, ne seront pas pris en compte par le Conseil et ne seront pas versés au dossier public.

58. Le Conseil n'accusera pas officiellement réception des mémoires. Il en tiendra toutefois pleinement compte et les versera au dossier public de l'instance, pourvu que la procédure de dépôt énoncée ci-dessus ait été suivie.

Avis important

59. Tous les renseignements fournis par les parties dans le cadre de ce processus public, sauf ceux désignés confidentiels, qu'ils soient envoyés par la poste, par télécopieur, par courriel ou au moyen du site Web du Conseil à l'adresse www.crtc.gc.ca, seront versés à un dossier public et affichés sur le site Web du Conseil. Ces renseignements comprennent les renseignements personnels, tels que le nom, l'adresse électronique, l'adresse postale ainsi que les numéros de téléphone et de télécopieur.

60. Les renseignements personnels fournis par les parties peuvent être divulgués et seront utilisés aux fins auxquelles ils ont été recueillis ou compilés par le Conseil, ou pour un usage qui est compatible avec ces fins.

61. Les documents reçus en version électronique ou autrement seront affichés intégralement sur le site Web du Conseil, tels qu'ils ont été reçus, y compris tous les renseignements personnels qu'ils contiennent, dans la langue officielle et le format d'origine dans lesquels ils sont reçus. Les documents qui ne sont pas reçus en version électronique seront affichés en version PDF.

62. Les renseignements fournis au Conseil par les parties dans le cadre de ce processus public sont déposés dans une base de données impropre à la recherche et réservée exclusivement à ce processus public. Cette base de données ne peut être consultée qu'à partir de la page Web de ce processus public. Par conséquent, une recherche généralisée du site Web du Conseil, à l'aide de son moteur de recherche ou de tout autre moteur de recherche, ne permettra pas d'accéder directement aux renseignements fournis dans le cadre de ce processus public.

Disponibilité des documents

63. On peut consulter sur le site Web du Conseil les versions électroniques des interventions et des autres documents dont il est question dans le présent avis. On peut y accéder à l'adresse www.crtc.gc.ca au moyen du numéro de dossier public indiqué au début du présent avis ou en consultant la rubrique « Consultations et audiences – Donnez votre avis! », puis en cliquant sur « les instances en période d'observations ouverte ». On peut alors accéder aux documents en cliquant sur les liens dans les colonnes « Sujet » et « Documents connexes » associées au présent avis.

64. Les documents peuvent également être consultés à l'adresse suivante, sur demande, pendant les heures normales de bureau.

Les Terrasses de la Chaudière
Édifice central
1, promenade du Portage
Gatineau (Québec) J8X 4B1
Téléphone : 819-997-2429
Télécopieur : 819-994-0218

Téléphone sans frais : 1-877-249-2782
ATS sans frais : 1-877-909-2782

Secrétaire général

Documents connexes

- *Lignes directrices sur l'approche du Conseil concernant l'article 9 de la Loi canadienne anti-pourriel (LCAP)*, Bulletin d'information de Conformité et Enquêtes CRTC 2018-415, 5 novembre 2018

- *Dépôt de mémoires en formats accessibles pour les instances du Conseil*, Bulletin d'information de radiodiffusion et de télécom CRTC 2015-242, 8 juin 2015

- *Dépôt d'interventions favorables conjointes*, Bulletin d'information de télécom CRTC 2011-693, 8 novembre 2011

- *Procédure à suivre pour le dépôt et la demande de communication de renseignements confidentiels dans le cadre d'une instance du Conseil*, Bulletin d'information de radiodiffusion et de télécom CRTC 2010-961, 23 décembre 2010, modifié par le Bulletin d'information de radiodiffusion et de télécom CRTC 2010-961-1, 26 octobre 2012

- *Lignes directrices à l'égard des* Règles de pratique et de procédure du CRTC, Bulletin d'information de radiodiffusion et de télécom CRTC 2010-959, 23 décembre 2010