Cour fédérale Federal Court

~~**TRÈS SECRET**~~
Date : 20251216

Dossier : C-1-24

Référence : 2025 CF 1978

Ottawa (Ontario), le 16 décembre 2025

En présence de madame la juge Kane

ENTRE :

DANS L'AFFAIRE concernant la demande de mandats présentée par [...] au titre des articles 12 et 21 de la *Loi sur le Service canadien du renseignement de sécurité*, LRC 1985, ch. C-23

ET DANS L'AFFAIRE VISANT DES CYBERACTIVITÉS D'ESPIONNAGE, DE SABOTAGE ET D'INGÉRENCE ÉTRANGÈRE

MOTIFS

I. Contexte

[1] Le 16 février 2024, la Cour a accueilli la demande de mandat présentée au titre des articles 12 et 21 afin d'autoriser le Service canadien du renseignement de sécurité [SCRS ou le Service] à faire enquête sur des menaces envers la sécurité du Canada que présentaient certaines cyberactivités d'espionnage, de sabotage et d'ingérence étrangère. Connu sous le nom de « cybermandat », ce mandat a été valide du [...] au [...].

[2] Le cybermandat autorisait le Service à intercepter toute communication destinée à l'infrastructure – ou en provenance de celle-ci – associée à des adresses de protocole Internet

[adresses IP], [...] et à toute autre infrastructure faisant l'objet d'une ordonnance de notre Cour conformément à la troisième condition du cybermandat. Le cybermandat autorisait également le Service à obtenir des informations [...] ayant trait à l'infrastructure en cause.

[3] La troisième condition du cybermandat autorisait le Service à présenter une demande supplémentaire à notre Cour dans l'éventualité où il a identifié une autre infrastructure.

[4] Le 29 février 2024, le Service a présenté une telle demande supplémentaire conformément à la troisième condition du cybermandat en vue d'exécuter des pouvoirs à l'égard de nouvelle infrastructure qu'il venait d'identifier, soit l'infrastructure liée à [...] adresses IP [la demande supplémentaire].

[5] Avant l'instruction de la demande supplémentaire, l'avocat du Procureur général du Canada [PGC] a signalé que la Cour suprême du Canada avait rendu, le 1er mars 2024, l'arrêt *R c Bykovets*, 2024 CSC 6 [*Bykovets*]. Dans cet arrêt, la majorité (cinq juges contre quatre) a déterminé qu'il existe une attente raisonnable au respect de la vie privée à l'égard des adresses IP, que les adresses IP bénéficient de la protection de l'article 8 de la *Charte canadienne des droits et libertés* [la *Charte*] et que la demande faite par la police à une tierce partie pour obtenir l'adresse IP de M. Bykovets sans avoir obtenu un mandat au préalable violait l'attente raisonnable au respect de sa vie privée. En revanche, la minorité a affirmé qu'il n'existe pas d'attente raisonnable au respect de la vie privée à l'égard de l'adresse IP de M. Bykovets.

[6] Dans la demande supplémentaire, selon la position initiale du PGC, la collecte des [...] adresses IP en cause est légale, et ce, parce que les adresses ont été obtenues avant l'arrêt *Bykovets*. Le PGC a toutefois offert d'autres observations par la suite.

[7] Le 6 mars 2024, la Cour a demandé au PGC de présenter ses observations sur les répercussions de l'arrêt *Bykovets* à l'égard de la demande supplémentaire et a nommé un *amicus curiae* [*amicus*] qui allait faire de même; un échéancier raisonnable a été établi pour la présentation des observations et l'audience. La demande supplémentaire a été suspendue en attendant l'opinion de la Cour sur les observations du PGC et de l'*amicus*.

[8] Dans une ordonnance de la Cour rendue le 15 avril 2024, M. Matthew Gourlay a été nommé *amicus*. M. Gourlay a présenté une analyse judicieuse de la portée de l'arrêt *Bykovets* et de ses répercussions sur la jurisprudence entourant la sécurité nationale et sur les questions précises que soulève la demande supplémentaire, dont les arguments subsidiaires du PGC.

[9] Le PGC a déposé ses observations écrites le 14 juin 2024.

[10] L'*amicus* a déposé ses observations écrites le 5 juillet 2024.

[11] Le PGC a déposé sa réponse le 18 juillet 2024.

[12] Les dates initiales proposées pour l'audience (les 14 et 15 août 2024) n'étaient pas réalistes; l'audience a donc été reportée.

[13] Dans une directive du 23 septembre 2024, la Cour a mentionné que l'arrêt *Bykovets* avait déjà été soulevé dans d'autres instances et qu'il y avait de fortes chances qu'il le soit à nouveau. La Cour a précisé que les observations du PGC et de l'*amicus* seraient pertinentes dans une autre instance, en l'occurrence, le dossier CSIS-24-22, et a proposé que le juge Gleeson, à qui l'on a confié ce dossier, copréside l'audience du dossier C-1-24. Les dossiers C-1-24 et CSIS-24-22 ne seront toutefois pas réunis ni instruits conjointement.

[14] Le PGC a transmis à l'*amicus* et à la Cour la jurisprudence pertinente des cours provinciales et supérieures ayant traité des répercussions de l'arrêt *Bykovets* sur les pratiques policières entourant la réception ou la collecte d'adresses IP; le PGC a continué de transmettre les décisions sur la question au fur et à mesure qu'elles étaient rendues.

[15] L'audience coprésidée par les juges Kane et Gleeson, qui portait sur les questions juridiques pertinentes soulevées par les dossiers C-1-24 et CSIS-24-22, a eu lieu le 15 octobre 2024. La Cour a ensuite tenu une audience uniquement sur le dossier C-1-24 afin, entre autres, d'entendre le témoignage du déclarant ainsi que les observations de l'avocat du PGC et de l'*amicus* concernant la demande supplémentaire.

[16] Ayant conclu que les [...] adresses IP ne sont pas visées par une attente raisonnable au respect de la vie privée et ne font pas intervenir l'article 8, la Cour a accueilli la demande supplémentaire le 23 octobre 2024.

[17] On a des motifs raisonnables de croire que les [...] adresses IP comprennent des adresses liées à des ressortissants étrangers se trouvant à l'extérieur du Canada, mais sans lien

reconnu avec le Canada, et à des victimes canadiennes d'attaques perpétrées par ces acteurs étrangers hostiles. Ces adresses IP ne sont pas visées par une attente raisonnable au respect de la vie privée et, en conséquence, c'est légalement que le Service les a obtenues au moyen d'une collecte non intrusive sans mandat conformément à l'article 12.

[18] Bien que la demande supplémentaire ait été accueillie sur cette base, le PGC a insisté pour que la Cour se penche sur ses arguments subsidiaires à l'appui de la collecte des [...] adresses IP et qu'elle se prononce sur d'éventuels scénarios dans lesquels la collecte de l'infrastructure (les adresses IP) pourrait être visée par une attente raisonnable au respect de la vie privée. L'*amicus* s'est opposé, arguant que la Cour devrait trancher la demande supplémentaire d'après les faits qui sont devant elle et en tenant compte qu'il n'y a pas d'attente raisonnable au respect de la vie privée. L'*amicus* a mis la Cour en garde contre la possibilité de se prononcer sur les arguments subsidiaires du PGC en l'absence d'un dossier factuel.

[19] Ayant décidé de réfléchir à la question des arguments subsidiaires, la Cour a déclaré qu'elle rendrait ses motifs à une date ultérieure. Les motifs de la Cour suivent et portent à la fois sur l'argument principal et les arguments subsidiaires à l'égard des [...] adresses IP en cause.

[20] Un résumé des conclusions de la Cour figure au paragraphe 223.

II. Le cybermandat

[21] Le paragraphe 1 du cybermandat autorise le directeur et tout employé du Service agissant sous l'autorité du directeur à intercepter toute communication destinée à une infrastructure – ou en provenance de celle-ci –, en l'occurrence [TRADUCTION] (a) « l'infrastructure liée aux

adresses IP, [...], ci-après » et énumère ensuite les adresses IP, [redacted]; ainsi que (b) [traduction] « toute autre infrastructure faisant l'objet d'une ordonnance de la Cour fédérale rendue en application de la troisième condition » [nous soulignons].

[22] On entend par « infrastructure » [TRADUCTION] « tout ordinateur, moyen d'entreposage de données électroniques, réseau, compte sur Internet ou compte auprès d'un fournisseur de services Internet qui est compromis, a fait l'objet d'une tentative de le compromettre ou est utilisé par un cyberacteur ».

[23] Au départ, le cybermandat autorisé identifiait initialement des adresses IP précises et d'autres infrastructures. L'affidavit déposé à l'appui de la demande de mandat présentée en vertu des articles 12 et 21 explique pourquoi l'infrastructure est potentiellement liée à des cyberactivités d'espionnage, de sabotage et d'ingérence étrangère et comment l'infrastructure a été identifiée. Le déclarant a également témoigné à l'appui de la demande. La Cour a été convaincue de la nécessité du cybermandat pour permettre au Service de faire enquête, au Canada ou à l'étranger, sur des menaces envers la sécurité du Canada que posent certaines cyberactivités d'espionnage, de sabotage et d'ingérence étrangère.

[24] La troisième condition du cybermandat prévoit ce qui suit :

> [TRADUCTION] Lorsque, conformément à l'alinéa 1b), le directeur général ou son remplaçant désigné a identifié une infrastructure, pour les fins de l'exécution du mandat, il présente sans délai une demande supplémentaire à la Cour en vue d'obtenir une ordonnance d'exécution des pouvoirs du mandat à l'égard de cette infrastructure.

[25] Conformément à la troisième condition du cybermandat, le SCRS a présenté une demande supplémentaire à la Cour à l'égard d'une infrastructure nouvellement identifiée, en l'occurrence, [...] adresses IP.

[26] L'affidavit déposé à l'appui de la demande supplémentaire décrit comment l'infrastructure a été identifiée et obtenue par le SCRS à partir de [...] ([...] adresses IP sont liées à des victimes de cyberacteurs; [...] adresses IP sont liées à des acteurs étrangers hostiles). Le SCRS a également fait des interrogations sans mandat sur les adresses IP en utilisant des outils sources ouverts afin d'identifier l'emplacement général et l'assignation d'un numéro aux adresses IP.

[27] À l'audience, le déclarant a donné davantage de renseignements. En résumé, la plupart des adresses IP ont été fournies par d'autres organismes ([...]). Le SCRS n'a pas, de façon proactive, tenté d'obtenir les adresses IP. En outre, la collecte des adresses IP a été effectuée avant l'arrêt *Bykovets*.

[28] Comme je l'ai mentionné ci-dessus, étant donné les grands principes affirmés dans l'arrêt *Bykovets* concernant l'attente raisonnable au respect de la vie privée à l'égard d'une adresse IP, la Cour a demandé d'autres observations afin d'apprécier la légalité de la collecte passive des [...] adresses IP par le SCRS.

III. Aperçu des positions des parties

A. *La position du PGC*

[29] Le principal argument du PGC est qu'il n'existe pas d'attente raisonnable au respect de la vie privée à l'égard des [...] adresses IP. Le PGC fait valoir que, si la Cour accepte son argument principal, avec lequel l'*amicus* est d'accord, les adresses IP ne sont pas visées par une attente raisonnable au respect de la vie privée et ne font pas intervenir l'article 8 de la *Charte*. En effet, les [...] adresses IP sont liées à des ressortissants étrangers se trouvant à l'extérieur du Canada, mais sans lien reconnu avec le Canada, et à des victimes canadiennes d'attaques perpétrées par ces acteurs étrangers hostiles. En conséquence, c'est légalement que le SCRS a obtenu les adresses IP au moyen d'une collecte non intrusive conformément à l'article 12, ce qui suffit pour que la Cour accueille la demande supplémentaire.

[30] Subsidiairement, le PGC fait valoir que l'article 12 de la *Loi sur le service canadien du renseignement de sécurité*, LRC 1985, ch C-23 [la *Loi sur le SCRS*] autorise la collecte des adresses IP suivant la norme des « motifs raisonnables de soupçonner » parce qu'il s'agit d'une fouille minimalement intrusive. Dans un second argument subsidiaire, le PGC avance que le critère de mise en balance établi dans la décision rendue en formation plénière (*Loi sur service canadien du renseignement de sécurité (Re)*, 2020 CF 616 [*Formation plénière*]) autorise également la collecte des adresses IP.

[31] Parce qu'il s'agit de questions récurrentes nécessitant une réponse, le PGC souhaite que la Cour se penche sur ses deux arguments subsidiaires, surtout l'argument selon lequel le SCRS peut obtenir les adresses IP (y compris au moyen d'une demande directe) sans mandat au moyen

d'une fouille minimalement intrusive conformément à l'article 12, et ce, même si les adresses IP sont visées par une attente raisonnable au respect de la vie privée.

[32] Le PGC soulève également des questions connexes quant à l'utilisation et à « l'enrichissement » d'adresses IP obtenues légalement.

B. *La position de l'amicus*

[33] Selon l'*amicus,* la demande supplémentaire peut être accueillie au regard des faits qui sont devant la Cour; aucun droit protégé par l'article 8 n'est en cause.

[34] L'*amicus* fait valoir que des acteurs étrangers hostiles sans lien avec le Canada ne jouissent pas de la protection de l'article 8 et que leurs adresses IP ne sont pas visées par une attente raisonnable au respect de la vie privée.

[35] Les victimes canadiennes de cyberattaques perpétrées par des acteurs étrangers hostiles quant à elles, jouissent de la protection de l'article 8. Toutefois, ces victimes ayant transmis volontairement leur adresse IP au SCRS, ou encore, leur adresse IP ayant été transmise au SCRS par d'autres au cours d'une enquête sur le cyberespionnage, l'article 8 ne trouve pas application. En effet, l'*amicus* souligne qu'une victime de cyberattaque verrait d'un bon œil les efforts déployés par le SCRS pour contrecarrer l'attaque.

[36] L'*amicus* établit une distinction entre les faits de la demande supplémentaire, notant que le SCRS n'a pas demandé les adresses IP, et d'autres circonstances dans lesquelles le SCRS pourrait tenter d'obtenir, de façon proactive, une adresse IP en la demandant à un fournisseur de

services Internet [FSI] canadien, par exemple. L'*amicus* avance que l'arrêt *Bykovets* ne s'appliquerait que dans ces autres circonstances. En effet, l'*amicus* soutient qu'une telle fouille serait plus que minimalement intrusive et nécessiterait un mandat.

[37] En l'absence d'un dossier factuel, l'*amicus* avance que la Cour ne devrait se concentrer que sur les faits de la demande supplémentaire et ne pas traiter les arguments subsidiaires du PGC.

[38] Toutefois, dans l'éventualité où la Cour se penche sur l'argument subsidiaire du PGC, l'*amicus* se dit en désaccord avec le point de vue selon lequel l'article 12 de la *Loi sur le SCRS* autorise le SCRS à tenter d'obtenir une adresse IP. Selon l'*amicus,* on ne peut invoquer l'arrêt *Bykovets* pour affirmer que, puisque la norme des « motifs raisonnables de soupçonner » suffit pour obtenir une adresse IP, l'article 12 autorise donc le SCRS à obtenir une telle adresse.

IV. L'interprétation et application de l'arrêt *Bykovets* à ce jour

A. *L'arrêt de la Cour suprême*

[39] Dans l'arrêt *Bykovets,* la Cour suprême conclut que la police a violé les droits de M. Bykovets en obtenant, sans autorisation judiciaire, son adresse IP auprès d'une tierce partie, en l'occurrence, une entreprise de traitement des cartes de crédit. Selon la Cour suprême, étant donné le risque qu'une adresse IP révèle l'activité en ligne de l'internaute et son identité, l'adresse IP fait intervenir une attente raisonnable au respect de la vie privée. En conséquence, d'après la Cour, la demande de l'État visant l'obtention d'une adresse IP est une fouille au sens de l'article 8 de la *Charte* et nécessite une autorisation judiciaire préalable.

[40] En désaccord, la minorité plutôt conclut que M. Bykovets n'a pas d'attente raisonnable au respect de sa vie privée et que la police n'a pas besoin d'autorisation judiciaire avant de demander à l'entreprise de traitement des cartes de crédit les adresses IP afin de déterminer le FSI qui leur est associé. En outre, la minorité signale que sa conclusion n'exclut pas l'éventualité d'une attente raisonnable au respect de la vie privée si les faits sont différents.

[41] En guise de contexte, la police menait une enquête sur des achats frauduleux faits en ligne dans un magasin de vins et spiritueux. La police a contacté l'entreprise de traitement des cartes de crédit qui avait traité les ventes en ligne, obtenu les adresses IP utilisées pour les achats et ensuite obtenu une ordonnance de communication forçant le FSI à divulguer des renseignements sur l'abonné. La police a ensuite utilisé ces renseignements pour obtenir et exécuter des mandats de fouille.

[42] M. Bykovets a mis en doute la demande de la police visant l'obtention de ses adresses IP auprès de l'entreprise de traitement des cartes de crédit, faisant valoir qu'elle violait son droit de ne pas subir de fouille abusive en application de l'article 8.

[43] La Cour suprême affirme que l'adresse IP est la « clé donnant accès » à l'activité Internet d'un internaute et, ultimement, à son identité, de sorte qu'elle suscite une attente raisonnable au respect de la vie privée. L'article 8, qui protège la vie privée en ligne des Canadiens et des Canadiennes, doit protéger leurs adresses IP (au para 28).

[44] Aux paragraphes 60 à 70, la Cour suprême explique l'argumentaire justifiant sa conclusion que les adresses IP font intervenir une attente raisonnable au respect de la vie privée,

étant donné le risque qu'elles soient mises en corrélation avec d'autres renseignements en ligne, qui peuvent révéler une vaste gamme de renseignements, « qui touchent directement aux détails intimes sur le mode de vie et les choix personnels d'un utilisateur individuel », et qu'une autorisation judiciaire préalable à l'obtention de l'adresse IP est nécessaire.

[45] La Cour suprême affirme ce qui suit au paragraphe 60 :

> La Couronne suggère qu'une adresse IP ne sert à rien sans un mandat de type Spencer. Soit dit en tout respect, je ne peux souscrire à ce point de vue. Premièrement, en tant que lien qui relie une activité Internet précise à un endroit donné, l'adresse IP est susceptible de révéler des renseignements très personnels, même avant que la police n'essaie de relier l'adresse à l'identité de l'utilisateur. Deuxièmement, il est possible de mettre en corrélation l'activité associée à l'adresse IP avec une autre activité en ligne associée à cette adresse à laquelle l'État a accès — ce qui a des conséquences particulièrement préoccupantes lorsqu'y est combiné l'accès à des renseignements détenus par un tiers. Enfin une adresse IP peut mettre l'État sur la trace d'une activité Internet qui mène directement à l'identité d'un utilisateur, même sans un mandat de type Spencer. Les cas où une adresse IP peut révéler des renseignements biographiques ne sont pas tous visés par l'arrêt Spencer. À la lumière de ces trois points, que j'explique ci-dessous, l'accès aux adresses IP sans autorisation judiciaire préalable pose de grands risques en matière de vie privée et les adresses IP suscitent une attente raisonnable au respect de la vie privée.

[46] La Cour suprême remarque d'abord que « l'activité associée à l'adresse IP peut elle-même être très révélatrice, même avant toute tentative de déterminer l'identité » (au para 61) et que « [d]'autres activités en ligne peuvent révéler des renseignements qui touchent directement à l'ensemble des renseignements biographiques d'un utilisateur » (au para 63).

[47] La Cour suprême précise ensuite que « [d]euxièmement, l'activité précise associée à l'adresse IP par la fouille peut être mise en corrélation avec une autre activité en ligne associée à cette adresse IP » (au para 64) et a expliqué au para 65 :

> Sans la protection de l'art. 8, rien n'empêche l'État de recueillir de façon préventive des adresses IP et de comparer l'adresse IP de cet utilisateur avec ce que renferme sa base de données. De plus, et fait important, l'étendue des renseignements que peut révéler une adresse IP est énorme si elle est mise en corrélation avec des renseignements détenus par un tiers.

[48] Aux paragraphes 68 et 69, la Cour suprême ajoute que, « lien par lien, une adresse IP peut mettre l'État sur la trace d'une activité Internet anonyme qui mène directement à l'identité d'un utilisateur », que les adresses IP sont les « premiers "fragments numériques" sur la trace cybernétique de l'utilisateur », et que ces « fragments peuvent établir toute l'activité en ligne quotidienne, hebdomadaire, ou même mensuelle, d'un internaute, ce qui permet de dresser l'historique des cyberpérégrinations de ce dernier [...]. À l'instar de l'ordinateur dans l'affaire Reeves, une adresse IP fournit à l'État le moyen susceptible de le mener à un trésor de renseignements personnels » [références omises].

[49] La Cour suprême résume au paragraphe 70 :

> Par conséquent, une adresse IP peut révéler un éventail de renseignements éminemment privés qui touchent directement aux détails intimes sur le mode de vie et les choix personnels d'un utilisateur individuel (*Marakah*, au para 32; *Spencer*, au para 27).

[50] La Cour suprême reconnaît que les intérêts en matière de vie privée entrent en balance avec le besoin de sécurité et que la police devrait disposer des outils d'enquête nécessaires pour s'occuper d'un crime commis en ligne, notant le préjudice causé aux victimes, en particulier les

enfants. Malgré cette admission, la Cour suprême conclut qu'une autorisation judiciaire préalable est nécessaire, affirmant aux paragraphes 85 et 86 :

> [85] À mon avis, toutefois, exiger que la police obtienne une autorisation judiciaire préalable avant d'obtenir une adresse IP ne constitue pas une lourde mesure d'enquête, et ne porterait pas indûment atteinte à la capacité des forces de l'ordre de s'occuper de ce crime. Lorsqu'il existe un lien suffisant entre l'adresse IP, ou les renseignements relatifs à l'abonné, et la perpétration d'un crime, une autorisation judiciaire est facile à obtenir et requiert peu de renseignements de plus que ce que la police doit déjà fournir pour obtenir une ordonnance de communication de type *Spencer*. À titre d'exemple, suivant le par. 487.015(1) du *Code criminel*, L.R.C. 1985, c. C-46, une ordonnance de communication de renseignements relatifs à une transmission donnée d'une communication peut être obtenue s'il existe des motifs raisonnables de *soupçonner* qu'une infraction a été ou sera commise. La police sollicite et obtient souvent de multiples autorisations afin de protéger différents intérêts d'ordre territorial en matière de vie privée. Il en est de même lorsqu'il s'agit de protéger l'intimité informationnelle.
>
> [86] Tout bien pesé, le fardeau que l'on impose à l'État en reconnaissant une attente raisonnable au respect de la vie privée à l'égard des adresses IP est dérisoire par comparaison avec les préoccupations importantes relatives à la vie privée qui sont en cause en l'espèce. Les forces de l'ordre devront démontrer l'existence de motifs suffisants pour porter atteinte à la vie privée d'une personne, mais à l'ère des télémandats et de l'accès 24 h sur 24 à des juges de paix, ce fardeau n'est pas lourd. Les policiers qui se livrent à des activités d'enquête légitimes peuvent facilement établir les motifs constitutionnels requis. Reconnaître qu'une adresse IP est protégée par l'art. 8 ne contrecarrera pas les enquêtes policières faisant intervenir des adresses IP; une telle reconnaissance vise plutôt à faire en sorte que les enquêtes policières reflètent mieux ce à quoi chaque Canadien et Canadienne raisonnable s'attend du point de vue du respect de la vie privée *et* de la lutte contre la criminalité.

[51] La Cour suprême résume son argumentaire au paragraphe 90 :

> [90] Par conséquent, considéré normativement, l'art. 8 de la *Charte* devrait étendre l'attente raisonnable au respect de la vie privée aux

> adresses IP. Ces adresses fournissent à l'État le moyen d'obtenir des renseignements à caractère très personnel au sujet d'un internaute précis et, ultimement, son identité, qu'un autre mandat soit nécessaire ou non. Une adresse IP joue un rôle fondamental dans la sauvegarde de la vie privée sur Internet. C'est la clé donnant accès à l'activité en ligne d'un internaute et la clé servant à identifier l'utilisateur derrière une activité en ligne. Étant donné ces préoccupations sérieuses relatives à la vie privée, le droit du public de ne pas être importuné devrait l'emporter sur le fardeau relativement simple imposé aux forces de l'ordre. Reconnaître une attente raisonnable au respect de la vie privée à l'égard des adresses IP ferait en sorte que le voile de l'intimité auquel s'attendent tous les Canadiens et les Canadiennes quand ils accèdent à Internet serait levé uniquement lorsqu'un officier de justice indépendant est convaincu que le fait de fournir ces renseignements à l'État servira un objectif légitime d'application de la loi.
>
> [Nous soulignons.]

[52] En conclusion, la Cour suprême réitère que « la demande d'adresse IP faite par l'État constitue une fouille au sens de l'art. 8 de la *Charte* » (au para 92 [nous soulignons]).

B. *Conclusions clés de l'arrêt Bykovets*

- L'article 8 protège la vie privée en ligne des Canadiens; cette protection doit inclure les adresses IP.
- Une adresse IP est le lien crucial entre un internaute et son activité en ligne (au para 28). Étant donné le risque qu'une adresse IP révèle l'activité de l'internaute et son identité, une adresse IP fait intervenir une attente raisonnable au respect de la vie privée. Une demande d'adresse IP faite par l'État constitue une fouille au sens de l'article 8 de la *Charte*.
- Il y a fouille lorsque l'État frustre une attente raisonnable au respect de la vie privée. Une attente au respect de la vie privée est raisonnable quand le droit du public de ne pas être

importuné par le gouvernement l'emporte sur le droit du gouvernement de s'immiscer dans la vie privée des particuliers afin de réaliser ses fins, notamment d'assurer l'application de la loi. Les tribunaux ont établi qu'il existe une attente raisonnable au respect de la vie privée en tenant compte de facteurs concurrents : (1) l'objet de la fouille; (2) l'intérêt du demandeur à l'égard de l'objet; (3) l'attente subjective du demandeur au respect de sa vie privée; et (4) la question de savoir si l'attente au respect de la vie privée était objectivement raisonnablement (au para 31).

- Les tribunaux établissent si l'attente subjective au respect de la vie privée est objectivement raisonnable eu égard à l'ensemble des circonstances (aux para 44, 45).
- Définir une attente raisonnable au respect de la vie privée est une opération de mise en balance. D'après les faits de l'affaire *Bykovets*, la balance a penché en faveur d'une attente raisonnable au respect de la vie privée en ce qui a trait aux adresses IP. Le caractère éminemment privé des renseignements que peut révéler une adresse IP suggère fortement que le droit du public de ne pas être importuné devrait l'emporter sur le droit du gouvernement de réaliser ses objectifs d'application de la loi (aux para 71, 72).
- Bien que la police ait besoin d'outils d'enquête pour s'occuper d'un crime commis en ligne, il faut une autorisation judiciaire préalable avant d'obtenir une adresse IP et l'obtention d'une telle autorisation ne constitue pas une lourde mesure d'enquête (aux para 84, 85). La Cour suprême a mentionné à titre d'exemple l'ordonnance de communication prévue au paragraphe 487.015(1). La Cour suprême a également souligné que « [l]es forces de l'ordre devront démontrer l'existence de motifs suffisants pour porter atteinte à la vie privée d'une personne, mais à l'ère des télémandats et de l'accès 24 h sur 24 à des juges de paix, ce fardeau n'est pas trop lourd » (au para 86 [nous

soulignons]).

C. *L'interprétation et l'application de l'arrêt Bykovets par les cours provinciales et supérieures (contexte criminel)*

[53] Comme je l'ai mentionné plus haut, le PGC a présenté de la jurisprudence interprétant et appliquant l'arrêt *Bykovets*, ou établissant une distinction par rapport à ce dernier. Un bref résumé de cette jurisprudence et de la jurisprudence plus récente dont la Cour a pris connaissance figure ci-dessous.

[54] Dans la décision *R v Leger*, 2024 NBKB 72 [*Leger*], la Cour du Banc du Roi du Nouveau-Brunswick conclut que la transmission de l'adresse IP d'un accusé par la United Kingdom National Crime Agency (l'agence nationale du Royaume-Uni contre le crime) [UK NCA] à la Gendarmerie royale du Canada [GRC] ne fait pas intervenir la protection de l'article 8 en ce qui a trait aux droits de l'accusé; il n'y a pas d'acte de l'État et pas de fouille.

[55] La cour remarque au paragraphe 44 que la décision de Cour suprême dans l'arrêt *Bykovets* « est axée sur les mesures prises par les forces policières pour obtenir les renseignements, plutôt que de les recevoir à l'improviste », ce qui diffère des faits présentés à la cour. La cour conclut au para 45 :

> [45] Les faits de la présente cause ne font intervenir ni l'article 8 de la *Charte* ni les principes énoncés dans l'arrêt *R c Bykovets*. La GRC n'a ni pris des mesures d'enquête ni cherché à obtenir des renseignements pour trouver l'adresse IP qui, en définitive, a été rattachée à M. Leger. C'est plutôt l'UK NCA qui lui a fourni le nom d'utilisateur, l'ID TOX et l'adresse IP située au Canada qui était utilisée pour partager du matériel relatif à l'exploitation d'enfants et pour en discuter à une date donnée. Aucune

> perquisition n'a été menée par la GRC pour obtenir l'adresse IP de M. Leger.

[56] Dans la décision *R v Prys*, 2024 ABCJ 166, la Cour de justice de l'Alberta conclut que l'article 8 ne s'applique pas à la déclaration obligatoire d'activités entourant l'abus sexuel d'enfants dans un ressort étranger. L'adresse IP a été volontairement fournie par Dropbox, un organisme américain.

[57] La cour conclut que l'ordonnance de communication et le mandat de fouille ont tous deux été accordés légalement, expliquant au paragraphe 12 :

> [TRADUCTION] [12] Compte tenu de tout ce qui précède, je suis d'avis que l'article 8 de la *Charte* ne trouve pas application dans le cas de la déclaration obligatoire des instances détectées en ligne d'activités entourant l'abus sexuel d'enfants dans un ressort étranger, dont la déclaration volontaire d'adresses IP associées à de telles activités. Lorsque le NCMEC fait suivre une adresse IP à la police au Canada sans qu'une demande n'ait été faite par les forces de l'ordre, il s'agit simplement d'un moyen de déclarer un crime afin que la police puisse obtenir les autorisations judiciaires adéquates pour faire enquête sur les activités d'exploitation sexuelle d'enfants soupçonnées dans son propre ressort. Conformément à la décision de la Cour d'appel de l'Alberta *R v King*, 2021 ABCA 271, je suis d'avis que, lorsque l'information est transmise à la police par une tierce partie sans demande active, la police a le droit de recevoir et d'examiner cette information, et il n'y a pas de fouille, de perquisition ou de saisie par l'État qui fasse intervenir l'article 8 de la *Charte.*

[58] Dans la décision *R v Pengelly*, 2024 SKKB 192 [*Pengelly*], la Cour du Banc du Roi de la Saskatchewan conclut que, lorsque le National Center for Missing and Exploited Children (centre national pour les enfants disparus et exploités) [NCMEC], un organisme américain privé, transmet volontairement une adresse IP à la police, il ne s'agit pas d'une fouille faite par un acteur étatique au Canada et cette transmission ne fait pas intervenir l'article 8. La cour explique

au paragraphe 57 que l'aide offerte volontairement par le NCMEC pour détecter la pornographie juvénile n'engage pas la protection de la *Charte*; la réception par la police d'une plainte du NCMEC et l'utilisation d'un moteur de recherche public pour géolocaliser et identifier le fournisseur de services de communication [FSC] ne fait pas intervenir l'attente raisonnable au respect de la vie privée de M. Pengelly. En conséquence, les mesures initiales d'enquête prises par la police, y compris demander au FSI s'il détient des renseignements sur l'abonné (sans lui demander de fournir ces renseignements) ne nécessitent pas d'autorisation judiciaire préalable et ne violent pas le droit de l'accusé à la protection contre les fouilles, perquisitions ou saisies abusives (aux para 58-60).

[59] Dans la décision *R v Cofell*, 2024 ONSC 7151 [*Cofell*], la Cour supérieure de justice de l'Ontario conclut que la transmission d'une adresse IP à la police par le Child Protection System (système de protection des enfants) [CPS], un organisme américain, ne constitue pas un acte de l'État, n'est pas une fouille et ne fait pas intervenir l'article 8 (au para 149). Subsidiairement, la cour précise que, si l'utilisation des renseignements du CPS avait été un acte de l'État, l'accusé n'aurait pas eu d'attente raisonnable au respect de sa vie privée suivant l'analyse de l'ensemble des circonstances, notamment parce qu'il a participé à l'échange de dossiers et que son adresse IP était déjà publique (au para 176).

[60] D'autres décisions rendues par des cours supérieures et provinciales concluent également que la réception passive d'une adresse IP par la police ne fait pas intervenir l'article 8.

[61] Dans la décision *R v Hillier*, 2024 NLSC 161, la Cour suprême de Terre-Neuve-et-Labrador conclut que les autorités canadiennes n'ont jamais demandé l'adresse IP de l'accusé,

mais que celle-ci a été fournie volontairement au Centre national contre l'exploitation d'enfants du Canada par le NCMEC et que, en conséquence, l'État n'a posé aucun acte direct à l'encontre du droit de l'accusé à la vie privée prévu à l'article 8 (aux para 68-71, 75). En outre, la cour signale que la portée de la *Charte* n'est pas extraterritoriale et qu'elle ne s'applique pas aux actes d'organismes de réglementation étrangers, ce qui inclut la façon dont ces derniers recueillent des éléments de preuve et les types de preuve qu'ils recueillent (aux para 68, 71).

[62] Dans la décision *R v Munro*, 2025 SKKB 20, la Cour du Banc du Roi de la Saskatchewan conclut que l'obtention de l'adresse IP de l'accusé par des acteurs privés (CPS) transmise volontairement aux forces de l'ordre ne fait pas intervenir l'article 8 de la *Charte*; les forces de l'ordre n'ont pas fait de demande, et il n'y a donc pas eu de fouille (aux para 44, 45).

[63] Dans la décision *R v Tate*, 2025 BCSC 1462 [*Tate*], la Cour suprême de la Colombie-Britannique conclut que l'obtention par la police de l'adresse IP d'un accusé, qui par ailleurs était disponible en ligne, ne fait pas intervenir l'article 8 de la *Charte*, puisqu'il n'y a pas d'attente raisonnable au respect de la vie privée à l'égard de cette adresse IP. Ainsi, il n'y a pas de fouille, de perquisition ou de saisie lorsque la police a obtenu l'information auprès du CPS ou l'a utilisée comme point de départ à enquête (au para 130).

[64] Dans les décisions *R v Brazeau*, 2024 ONCJ 611 [*Brazeau*] et *R v Done*, 2025 ONCJ 326 [*Done*], la Cour de justice de l'Ontario conclut que la réception passive par la police de détails entourant l'adresse IP de l'accusé ne constitue pas une fouille et ne fait pas intervenir la protection constitutionnelle de l'article 8. En conséquence, la police n'a pas besoin d'autorisation judiciaire, que ce soit avant de recevoir passivement un tel renseignement ou après l'avoir reçu

(*Brazeau* aux para 18 à 23; *Done* aux para 38-43). La Cour provinciale de la Colombie-Britannique en arrive à la même conclusion dans la décision *R v Cagoco* (BCPC, Courtenay, nº 44265-1, 1 novembre 2024 [non publiée], citée dans la décision *Cofell* aux para 115, 116).

[65] En outre, certaines décisions de cours supérieures et provinciales ont adopté une approche différente (*R v Asantarajah*, 2025 ONSC 1377; *R v Daniels*, 2025 ONSC 344; *R v Currie*, 2024 BCPC 175), mais la jurisprudence mentionnée ci-dessus a établi une distinction par rapport à celles-ci ou les a tout simplement écartées (voir *Tate* aux para 93, 94, 123-129; *Done* aux para 81, 82; *Cofell* au para 152).

[66] Toutes les décisions qui ont interprété ou appliqué l'arrêt *Bykovets*, ou qui ont établi une distinction par rapport à ce dernier, ont traité du rôle de la police dans les enquêtes criminelles, principalement dans le contexte de poursuites pour des infractions liées à la pornographie juvénile. Dans l'arrêt *Bykovets*, la Cour suprême a remarqué que l'équilibre entre la vie privée et « l'intérêt […] légitime de la société en ce qui a trait au besoin de sécurité » (au para 84) et a reconnu la gravité de la pornographie juvénile en ligne, mais a tout de même conclu qu'une autorisation judiciaire préalable est nécessaire, précisant que d'exiger une telle autorisation ne constitue pas une lourde mesure d'enquête. Les instances inférieures ayant appliqué l'arrêt *Bykovets*, ou ayant établi une distinction par rapport à cet arrêt, se sont concentrées sur la façon dont les adresses IP avaient été obtenues par la police, compte tenu de leur provenance et de l'existence d'une attente raisonnable au respect de la vie privée au départ dans les circonstances particulières de l'espèce. Les cours ont conclu que, lorsque des organismes des forces de l'ordre reçoivent des adresses IP d'organismes étrangers et d'acteurs non étatiques, cette réception passive ne fait pas intervenir l'article 8 et qu'il ne s'agit pas d'un acte de l'État.

[67] Dans les décisions *Leger* et *Pengelly*, la pratique de se fier à des outils sources ouverts pour enrichir une adresse IP transmise aux forces de l'ordre est acceptée (*Leger* aux para 51-55; *Pengelly* au para 58). Dans la décision *Tate*, la cour conclut également que ni la réception ni l'utilisation de l'adresse IP ne constitue une fouille (au para 130).

V. La position du PGC

[68] Le PGC reconnaît que la demande supplémentaire soulève une question précise, à savoir si le SCRS a recueilli légalement les [...] adresses IP. Le PGC estime que oui.

[69] Le PGC insiste sur le fait que la Cour suprême n'a pas envisagé si les adresses IP des titulaires de droits protégés par l'article 8 donnaient lieu à une attente raisonnable au respect de la vie privée en dehors du contexte factuel précis de l'affaire *Bykovets*, soit le cas d'un service de police canadien demandant une adresse IP à un fournisseur canadien, qui est une tierce partie. Le PGC signale que le contexte factuel de l'affaire *Bykovets* diffère du contexte factuel sous-tendant la demande supplémentaire et d'autres contextes dans lesquels le SCRS a obtenu des adresses IP.

[70] Le PGC fait valoir trois arguments et demande à la Cour de les prendre en compte tous les trois.

[71] L'argument principal du PGC est que la réception passive par le SCRS des [...] adresses IP ne fait pas intervenir l'article 8 de la *Charte*.

[72] L'*amicus* est d'accord avec l'argument principal, ainsi que la Cour, et la demande supplémentaire a été accueillie sur cette base. Les motifs de la Cour traitent néanmoins des observations du PGC et de l'*amicus* par souci d'intégralité.

A. *Aucune attente raisonnable au respect de la vie privée; l'article 8 ne s'applique pas*

[73] Le PGC explique que la collecte des [...] adresses IP ne fait pas intervenir l'article 8.

[74] En ce qui a trait aux [...] adresses IP liées aux acteurs étrangers hostiles se trouvant à l'extérieur du Canada, mais sans lien avec le Canada, il n'y a pas d'attente raisonnable au respect de la vie privée. Ces ressortissants étrangers ne jouissent pas de la protection de l'article 8 et ne peuvent pas faire valoir une violation de leur droit à la vie privée à l'égard de ces adresses IP. En effet, ces détenteurs d'adresses IP ne sont pas inclus dans la portée du mot « chacun » figurant à l'article 8 (*Loi sur le service canadien du renseignement de sécurité (CA) (Re)*, 2022 CF 1444 au para 170 [*Extérieur du Canada*]). Le PGC fait valoir que le Service peut recueillir ces adresses IP sans mandat au moyen d'une collecte non intrusive conformément à l'article 12.

[75] En ce qui a trait aux [...] adresses IP des victimes canadiennes de cyberattaques perpétrées par les acteurs étrangers, le PGC avance que ces adresses IP ne sont pas visées par une attente raisonnable au respect de la vie privée. Bien que les victimes canadiennes jouissent de la protection de l'article 8, l'ensemble des circonstances appuie la position selon laquelle ces victimes n'ont pas d'attente subjective que leurs adresses IP soient cachées au Service alors que cette information est recueillie à des fins non contradictoires ou bien qu'une attente subjective en matière de vie privée ne serait pas objectivement raisonnable, étant donné que le Service

recueille ces adresses IP pour alerter les victimes et/ou faire enquête sur des activités ayant trait à des menaces.

[76] Les adresses IP recueillies auprès d'organismes étrangers et canadiens sont issues de l'échange de renseignements entre organismes. Le PGC fait valoir que, lorsque des organismes étrangers ou canadiens [...] recueillent des informations légalement, en l'occurrence, des adresses IP, dans le cadre de leurs tâches ou de leur mandat en matière de sécurité nationale, la réception passive de cette information par le SCRS n'interfère pas avec l'attente raisonnable au respect de la vie privée.

[77] Le PGC maintient que, généralement, la réception et l'utilisation par le Service de toute adresse IP recueillie, par un organisme canadien ou étranger, et ensuite transmise au Service dans le cadre de l'échange de renseignements entre organismes (c'est-à-dire, la réception passive), et ce, même si l'adresse IP est liée à un titulaire de droits protégés par l'article 8, ne font pas intervenir l'article 8 de la *Charte*. Le PGC fait valoir que le Service peut recueillir et utiliser cette information au moyen d'une collecte non intrusive sans mandat conformément à l'article 12. Le PGC explique que, lorsqu'il n'y a pas d'attente raisonnable au respect de la vie privée au moment de la collecte ou de la transmission, l'information n'acquiert pas d'attente raisonnable au respect de la vie privée après le fait lorsque les autorités canadiennes la reçoivent ou l'utilisent.

[78] Le PGC signale en outre que les décisions rendues après l'arrêt *Bykovets*, dans lesquelles des instances inférieures ont conclu que, lorsque l'adresse IP d'un titulaire de droits protégés par

l'article 8 est recueillie par un organisme étranger et ensuite transmise aux forces de l'ordre canadiennes, l'article 8 ne s'applique pas; il n'y a pas de fouille.

B. *La Cour doit-elle se pencher sur l'argument subsidiaire concernant l'article 12?*

[79] Bien que l'*amicus* soit d'accord avec l'argument principal du PGC, ainsi que la Cour, et que la demande supplémentaire a été accueillie sur la base que les utilisateurs des [...] adresses IP n'ont pas d'attente raisonnable au respect de la vie privée, le PGC fait valoir que la Cour devrait traiter l'argument subsidiaire concernant l'article 12 pour plusieurs raisons :

- la collecte sans mandat d'adresses IP par le SCRS a été soulevée et continuera d'être soulevée dans d'autres demandes supplémentaires et d'autres contextes;
- par souci « d'économie et d'efficacité judiciaires », la Cour devrait trancher la question, car elle bénéficie du présent dossier;
- l'orientation de la Cour sur l'habileté du SCRS à recueillir des adresses IP sans mandat servira à résoudre des incertitudes juridiques dans la foulée de l'arrêt *Bykovets.*

(1) L'article 12 autorise la collecte minimalement intrusive des [...] adresses IP et d'autres adresses IP (réception passive et demandes directes)

[80] Le PGC fait valoir que, si la collecte, par le Service, des [...] adresses IP fait intervenir une attente raisonnable au respect de la vie privée et équivaut à une fouille à la lumière de l'arrêt *Bykovets*, le Service peut recueillir ces adresses IP sans mandat au moyen d'une collecte minimalement intrusive conformément à l'article 12 suivant la norme des « motifs raisonnables de soupçonner ». Le PGC remarque que la Cour a conclu que l'article 12 de la *Loi sur le SCRS*

donne l'autorité raisonnable et légale au SCRS d'effectuer des fouilles minimalement intrusives (*X (Re),* 2017 CF 1047 [*IMSI*]).

[81] Le PGC ajoute que, si le Service veut obtenir une adresse IP en faisant une **demande** à un fournisseur, qui est une tierce partie, comme c'est le cas dans l'arrêt *Bykovets,* le Service pourrait le faire au moyen d'une fouille minimalement intrusive conformément à l'article 12. Le PGC reconnaît que ce n'est pas le cas dans la demande supplémentaire, mais fait valoir que la Cour devrait néanmoins se pencher sur ces observations.

(a) *La norme des « motifs raisonnables de soupçonner » vise les fouilles minimalement intrusives, c'est-à-dire portant une atteinte minimale à la vie privée*

[82] Le PGC avance qu'il est implicite dans les motifs de la majorité de l'arrêt *Bykovets* que toute attente raisonnable au respect de la vie privée liée à une adresse IP n'est pas un intérêt accru en matière de vie privée, étant donné que la Cour suprême a conclu que la police aurait pu obtenir cette information suivant la norme des « motifs raisonnables de soupçonner », au moyen de l'ordonnance de communication prévue au *Code criminel*, LRC 1985, ch C-46 [*Code criminel*] (par opposition aux « motifs raisonnables de croire »). Le PGC signale que l'article 487.015 du *Code criminel* prévoit une ordonnance de communication de données de transmission s'il existe des motifs raisonnables de soupçonner qu'une infraction a été ou sera commise et que l'adresse IP est liée à la commission du crime.

[83] Le PGC remarque que la norme la moins exigeante des « motifs raisonnable de soupçonner » vise les fouilles portant une atteinte minimale à la vie privée (*Mahjoub c Canada*

(Citoyenneté et Immigration), 2017 CAF 157 au para 177 [*Mahjoub CAF*]; *IMSI* aux paras 218-219).

[84] Le PGC signale en outre que, aux paragraphes 234 à 242 de la décision *R c Kang- Brown*, 2008 CSC 18 [*Kang-Brown*], la Cour suprême a conclu que la fouille effectuée par un chien renifleur est une fouille minimalement intrusive pour laquelle la police n'a pas besoin de mandat. La Cour suprême a remarqué que la fouille n'a pas porté atteinte à l'intégrité physique de l'appelant, n'a pas causé d'inconvénients indus à l'appelant, était très ciblée et très précise et servait uniquement à déterminer la présence ou l'absence de marchandises de contrebande; en somme, la fouille était minimalement intrusive. Le PGC souligne que les mêmes critères ont été pris en compte dans les décisions *IMSI*, *Extérieur du Canada* et *Loi sur le Service canadien du renseignement de sécurité (Re)*, 2020 CF 697 [*Réseaux favoris*].

(b) *L'article 12 autorise les fouilles minimalement intrusives*

[85] Le PGC renvoie à la décision *Extérieur du Canada* dans laquelle le juge en chef précise que l'article 12 autorise le SCRS à mener des activités minimalement envahissantes à l'égard des droits protégés par l'article 8 (au para 176).

[86] Le PGC renvoie également à la décision *IMSI*, dans laquelle le juge en chef admet que, dans le contexte de la sécurité nationale, le public est probablement prêt à concéder une partie de ses droits en matière de vie privée afin de permettre au SCRS d'enquêter sur des activités dont il existe des motifs raisonnables de soupçonner qu'elles constituent des menaces envers la sécurité du Canada (au para 171).

[87] Le PGC précise que, dans la décision *IMSI*, le juge en chef fait une distinction entre une fouille minimalement intrusive et une fouille intrusive. La fouille minimalement intrusive est très précise et très ciblée; des renseignements personnels ou des renseignements d'une tierce partie recueillis fortuitement ne sont pas utilisés et sont détruits et la technologie est très fiable (aux para 209, 226, 246, 249, 252, 253).

[88] Le PGC fait valoir que si les [...] adresses IP en cause – ou d'autres adresses IP recueillies conformément à la demande supplémentaire – interfèrent un tant soit peu avec l'attente raisonnable au respect de la vie privée, la collecte de ces adresses est minimalement intrusive à l'égard de la vie privée. La méthode de collecte est très précise et très ciblée, ne recueille pas fortuitement les informations d'une tierce partie et les informations recueillies sont très fiables.

[89] D'ailleurs, fait valoir le PGC, le SCRS a avancé les mêmes raisons en invoquant l'article 12 pour demander des adresses IP.

[90] Le PGC reconnaît que le SCRS ne peut pas demander à des organismes étrangers de recueillir des informations sans mandat si, pour les recueillir lui-même, le SCRS a besoin d'un mandat. Le déclarant a confirmé que le SCRS ne l'a pas fait pour les [...] adresses IP et qu'il ne le fait pas.

[91] Le PGC admet que l'article 12 permet au SCRS d'exercer des activités minimalement intrusives. Toute activité plus que minimalement intrusive à l'égard d'un droit protégé par l'article 8 nécessite un mandat. Le PGC a précisé que, lorsque le SCRS obtient une adresse IP, il

demande un mandat conformément à l'article 21 pour obtenir d'autres renseignements auprès d'un FSC.

(c) *Les ordonnances de communication prévues au Code criminel sont un exemple; les adresses IP qui interfèrent avec l'attente raisonnable au respect de la vie privée peuvent être recueillies par la police au moyen d'une ordonnance de communication de données de transmission suivant la norme des « motifs raisonnables de soupçonner »*

[92] Le PGC fait valoir que la norme prévue à l'article 12 – à savoir, les « activités dont il existe des motifs raisonnables de soupçonner qu'elles constituent des menaces envers la sécurité du Canada » – est analogue à la norme des « motifs raisonnables de soupçonner », qui permet l'obtention de l'ordonnance de communication des données de transmission prévue à l'article 487.015 du *Code criminel*.

[93] Le PGC insiste sur le fait que l'arrêt *Bykovets* ne portait que sur la question de savoir si la police avait besoin d'un mandat pour demander l'adresse IP à une tierce partie. La Cour suprême a conclu que la police aurait pu obtenir l'adresse IP de l'accusé – malgré la conclusion que l'adresse IP est visée par une attente raisonnable au respect de la vie privée et que son obtention nécessite donc une autorisation judiciaire préalable – au moyen d'une ordonnance de communication des données de transmission pour une communication précise conformément à l'article 487.015 du *Code criminel*.

[94] Le PGC fait valoir que, bien que l'arrêt *Bykovets* qualifie l'adresse IP de « premier fragment numérique » qui, lorsqu'elle est combinée à d'autres renseignements, peut révéler des informations sur l'internaute, même d'après les faits de l'affaire *Bykovets*, la Cour suprême a précisé que la norme des « motifs raisonnables de soupçonner » autorise la police à recueillir

légalement cette information. Si la police peut obtenir l'ordonnance de communication prévue à l'article 487.015 du *Code criminel* pour obtenir une adresse IP suivant la norme des « motifs raisonnables de soupçonner », cela indique qu'il s'agit d'une fouille minimalement intrusive.

[95] Le PGC avance que le paragraphe 85 de l'arrêt *Bykovets* indique clairement à la police que, si elle avait voulu obtenir l'adresse IP de M. Bykovets auprès d'une tierce partie, telle une entreprise de traitement des cartes de crédit, la police aurait dû demander une ordonnance de communication des données de transmission suivant la norme des « motifs raisonnables de soupçonner », laquelle circonscrit les fouilles minimalement intrusives. Seules les fouilles plus que minimalement intrusives nécessitent une autorisation judiciaire préalable suivant la norme des « motifs raisonnables de croire ».

[96] Le PGC avance que les passages de l'arrêt *Bykovets* invoqués par l'*amicus* pour faire valoir les intérêts accrus en matière de vie privée à l'égard d'une adresse IP et la nécessité d'une autorisation judiciaire préalable suivant la norme des « motifs raisonnables de croire » sont des remarques incidentes. Le PGC affirme que ces passages isolés, qui n'appuient pas les conclusions de l'arrêt *Bykovets*, n'établissent pas de principes juridiques.

[97] Le PGC avance que l'*amicus* a invoqué les paragraphes 60 à 70 de l'arrêt *Bykovets,* alors que ces paragraphes ne peuvent pas être invoqués séparément du paragraphe 85 et que l'on ne peut interpréter les paragraphes 60 à 70 pour affirmer que la collecte d'adresses IP de titulaires de droits protégés par l'article 8 est plus que minimalement intrusive et nécessite donc une autorisation judiciaire préalable suivant la norme des « motifs raisonnables de croire ». Une telle

interprétation est irréconciliable avec le paragraphe 85, selon lequel on peut obtenir un mandat suivant la norme des « motifs raisonnables de soupçonner ».

[98] Le PGC maintient que, aux paragraphes 56, 76 et 77 de la décision *R v Otto*, 2019 ONSC 2473 [*Otto*], les dispositions du *Code criminel* entourant les données de transmission, qui exigent des « motifs raisonnables de soupçonner », respectent l'article 8. Dans la décision *Otto,* la cour conclut que l'obtention des données de transmission est minimalement intrusive à l'égard de la vie privée et que la norme des « motifs raisonnables de soupçonner » offre une protection constitutionnelle suffisante. La cour précise également que l'on ne peut pas utiliser les données de transmission obtenues avec mandat pour obtenir le contenu des communications; l'obtention du contenu des communications fait intervenir la protection de la vie privée et exige le respect de la norme des « motifs raisonnables de croire ». Le PGC met en doute l'observation de l'*amicus* selon laquelle l'arrêt *Bykovets* contredit les conclusions de la décision *Otto.*

[99] Le PGC fait valoir que, si la police peut obtenir l'ordonnance de communication prévue au *Code criminel* suivant la norme des « motifs raisonnables de soupçonner » en vue de recueillir des données de transmission (une fouille minimalement intrusive), le SCRS devrait donc être en mesure d'obtenir ce type d'information au moyen d'une collecte minimalement intrusive conformément à l'article 12 dans le contexte de la sécurité nationale. Le PGC précise que, dans le contexte de l'application de la loi, la police aura besoin d'un mandat, mais seulement suivant la norme des « motifs raisonnables de soupçonner », soit la norme s'appliquant aux collectes sans mandat conformément à l'article 12 (si tous les autres critères sont remplis). Le SCRS devrait pouvoir obtenir ce type d'information conformément à l'article 12 suivant la même

norme dans le contexte de la sécurité nationale; une norme plus rigoureuse ne devrait pas être imposée dans le contexte de la sécurité nationale (*Mahjoub CAF* aux para 265-267).

C. *L'utilisation ultérieure à la collecte des adresses IP*

[100] Le PGC signale que l'arrêt *Bykovets* ne se penche pas sur l'utilisation ultérieure à la collecte (aussi appelée « enrichissement ») et l'exploitation d'une adresse IP.

[101] Le PGC souligne que le déclarant du SCRS a expliqué que le SCRS utilise des outils pour enrichir les adresses IP recueillies (avec ou sans mandat). Les outils sources ouverts sont des outils publics qui, généralement, permettent d'obtenir des informations sur la géolocalisation et le FSC. Le PGC avance que l'enrichissement au moyen d'outils sources ouverts accessibles au public constitue une collecte non intrusive. Le déclarant du SCRS a précisé que, dans le cybercontexte, le SCRS ne recueille pas d'informations personnelles liées à une adresse IP, à moins que l'information ne soit déjà publique. Sinon, il faut un mandat.

[102] Le PGC remarque que, dans la décision *Leger*, la cour accepte le recours par la police à de tels outils et conclut que l'utilisation par la GRC de l'adresse IP – au moyen d'informations provenant d'outils sources ouverts que la police a utilisées pour obtenir une ordonnance de communication et un mandat de perquisition – ne fait pas intervenir l'article 8.

[103] Le PGC fait valoir que, lorsque les adresses IP des titulaires de droits protégés par l'article 8 ont été recueillies de façon indépendante par des organismes étrangers et ensuite transmises au SCRS dans le cadre d'un échange de renseignements entre organismes, ou lorsqu'elles ont été recueillies légalement d'une autre façon, la réception et l'utilisation de cette

information par le SCRS ne font pas intervenir l'article 8. En conséquence, l'article 8 n'intervient pas non plus à l'égard de l'utilisation ultérieure des informations par le SCRS. Autrement dit, l'information ne peut pas être visée par une attente raisonnable au respect de la vie privée après sa collecte si elle ne l'était pas au moment de la collecte. Le PGC maintient que le SCRS peut effectuer des interrogations à l'aide d'outils sources ouverts sur ces adresses IP pour établir leur emplacement géographique général et leur FSC.

[104] Le PGC fait en outre valoir que, s'il a effectué une collecte légale d'adresses IP, avec ou sans mandat, le SCRS [TRADUCTION] « traite cette information dans ses propres systèmes » et est en droit de le faire.

D. *Mise en balance; invoquer l'approche décrite dans la décision Formation plénière*

[105] Enfin, le PGC avance que, si l'une ou l'autre des [...] adresses IP a été recueillie en violation de l'article 8 et que la Cour conclut également que l'article 12 n'autorise pas la collecte, la Cour pourrait, en vertu de son pouvoir discrétionnaire, autoriser le Service à recueillir les adresses IP suivant le critère en trois volets établi dans la décision *Formation plénière*. Le PGC remarque que ce second argument subsidiaire est une position de dernier recours.

[106] Le PGC avance que, les mêmes facteurs, adaptés au contexte, guideraient la Cour dans l'exercice de son pouvoir discrétionnaire, soit la gravité de l'acte illégal, l'équité (p. ex. : l'importance de l'empiètement de l'acte illégal sur les droits ou les intérêts individuels et si le caractère illégal de l'acte remet en cause la crédibilité ou la fiabilité des informations) et l'intérêt de la collectivité, dont la nature et la gravité d'une menace pour la sécurité du Canada.

[107] Le PGC avance que toute illégalité liée à la collecte des [...] adresses IP effectuée par le SCRS est mineure, étant donné que le SCRS a reçu l'information passivement et en l'absence de conduite illégale répétée. Toutes les adresses IP en cause ont été recueillies avant l'arrêt *Bykovets* et, à ce moment-là, on n'envisageait pas que les adresses IP puissent être protégées par l'article 8.

[108] En ce qui a trait à l'équité, toute illégalité liée à la collecte des [...] adresses IP ne met pas en doute la crédibilité ou la fiabilité des informations. En outre, il existe un intérêt pour la collectivité que le SCRS puisse faire enquête sur des menaces envers la sécurité du Canada et, dans les circonstances de la demande supplémentaire, des preuves viennent étayer une menace immédiate envers la sécurité de Canada posée par les cyberactivités d'espionnage et de sabotage. Le PGC fait valoir que l'imminence et la gravité de cette menace sont des circonstances atténuantes appuyant l'admissibilité des adresses IP malgré toute illégalité qui pourrait entacher leur collecte.

VI. La position de l'*amicus*

A. *La demande supplémentaire peut être accueillie; il n'y a pas d'attente raisonnable au respect de la vie privée*

[109] L'*amicus* admet que la demande supplémentaire peut être accueillie sur la base que les [...] adresses IP en cause ne font pas intervenir d'attente raisonnable au respect de la vie privée. L'*amicus* souligne toutefois que des circonstances différentes pourraient soulever d'autres préoccupations.

[110] L'*amicus* reconnaît qu'une entité étrangère sans lien avec le Canada ne bénéficie pas de la protection de l'article 8. L'*amicus* fait valoir que le PGC (et le SCRS) doit établir l'absence de lien avant que la collecte d'adresses IP sans mandat ne puisse être autorisée. C'est ce que le déclarant du PGC a fait, dans la demande supplémentaire, lorsqu'il a expliqué que [...] adresses IP recueillies ont été utilisées par des acteurs étrangers hostiles sans lien avec le Canada ni protection de l'article 8 et que les autres [...] adresses IP ont été victimes de cyberattaques.

[111] L'*amicus* soutient que, en cas de doute concernant la protection de l'article 8, en vue de protéger les personnes contre les fouilles abusives, le SCRS devrait invoquer un autre moyen juridique pour obtenir l'adresse IP – soit l'échange de renseignements entre organismes, une collecte conformément à l'article 12 ou un mandat en application de l'article 21.

[112] L'*amicus* soutient que l'on devrait présumer de l'existence d'une attente raisonnable au respect de la vie privée à l'égard des adresses IP des victimes canadiennes. L'échange de renseignements entre organismes étrangers ou canadiens peut toutefois donner au SCRS l'autorisation légale nécessaire pour obtenir l'adresse IP d'une victime canadienne, ce qui est le cas pour les adresses IP en cause.

B. *Le SCRS peut recueillir sans mandat les adresses IP d'organismes étrangers et canadiens dans le cadre de l'échange de renseignements entre organismes*

[113] L'*amicus* reconnaît que la *Charte* ne s'applique généralement pas aux renseignements reçus d'organismes étrangers au terme d'une collaboration entre organismes.

[114] L'*amicus* reconnaît également que les [...] adresses IP fournies [...] au SCRS proviennent d'une collecte légale sans mandat. D'après les éléments de preuve, ces adresses IP étaient liées à l'infrastructure compromise par les acteurs étrangers.

[115] L'*amicus* admet que, de façon générale, le SCRS peut recevoir des adresses IP [...] et peut présumer que [...] a recueilli légalement ces adresses IP dans le cadre de son mandat.

[116] L'*amicus* maintient toutefois que, au même titre que pour les adresses IP fournies par des organismes étrangers, l'exploitation ultérieure par le SCRS de ces adresses IP (p. ex. : au moyen de moteurs de recherche publics ou autrement) dans le contexte d'une enquête menée sur une personne (c'est-à-dire, une cible) au Canada peut faire intervenir l'attente raisonnable au respect de la vie privée.

C. *Les répercussions de l'arrêt Bykovets*

[117] L'*amicus* et le PGC conviennent des conclusions clés sur les faits de l'arrêt *Bykovets*, mais leurs avis divergent quant à la portée de l'application de cet arrêt, notamment la question de savoir si la Cour suprême considère une demande d'adresse IP comme une intrusion minimale à l'attente raisonnable au respect de la vie privée et la norme entourant l'autorisation nécessaire pour obtenir une adresse IP.

[118] L'*amicus* fait remarquer que la majorité dans l'arrêt *Bykovets* souligne la nature inhérente à la vie privée d'une adresse IP, car elle est le « premier fragment numérique » qui mène à d'autres renseignements et peut ultimement révéler des renseignements hautement personnels sur

l'internaute. L'*amicus* maintient que ce premier fragment recèle déjà la vie privée de l'internaute.

D. *L'article 12 ne suffit pas pour autoriser l'obtention d'une adresse IP*

[119] L'*amicus* est d'avis que la Cour devrait se concentrer seulement sur les [...] adresses IP en cause et ne pas traiter les arguments subsidiaires du PGC.

[120] Toutefois, si la Cour choisit de se pencher sur les arguments subsidiaires, la position de l'*amicus* est que l'article 12 n'autorise pas le SCRS à demander une adresse IP.

(1) La collecte d'une adresse IP n'est pas toujours une fouille minimalement intrusive

[121] L'*amicus* met en doute l'argument du PGC selon lequel l'arrêt *Bykovets* affirme que de tenter d'obtenir une adresse IP est une fouille minimalement intrusive, que des « motifs raisonnables de soupçonner » que l'information concerne des activités qui sont des menaces envers la sécurité du Canada suffit et que l'article 12 autorise le SCRS à procéder à une collecte sans mandat.

[122] L'*amicus* fait valoir que l'arrêt *Bykovets* n'appuie pas la conclusion selon laquelle la collecte de l'adresse IP d'une cible est toujours minimalement intrusive et tombe sous l'application de l'article 12.

[123] L'*amicus* avance que la protection dont bénéficient les détenteurs d'adresses IP quant à leur vie privée n'est pas moindre dans le contexte de la sécurité nationale que celle dont bénéficient les cibles d'enquêtes criminelles.

[124] L'*amicus* insiste sur le fait que, dans la foulée de l'arrêt *Bykovets*, il faut dorénavant considérer une adresse IP du point de vue du risque qu'elle révèle des renseignements et non pas y voir une simple série de chiffres, comme c'était le cas auparavant. En conséquence, lorsque la collecte d'une l'adresse IP outrepasse la fouille minimalement intrusive (très ciblée et très précise), un mandat est nécessaire.

[125] L'*amicus* reconnaît que l'adresse IP n'est qu'une série de chiffres et qu'elle ne comporte pas à elle seule de renseignements personnels; toutefois, un mandat peut s'avérer nécessaire lorsque les « fragments numériques » de l'adresse IP risquent de révéler des détails intimes touchant les renseignements biographiques d'ordre personnel de la cible mettant en jeu sa vie privée.

[126] L'*amicus* admet que, dans le contexte du cybermandat, la possibilité d'une enquête ciblée visant une personne précise (c'est-à-dire, une « cible »), encore moins une personne protégée par l'article 8, est infime. Toutefois, dans des circonstances où, par exemple, la cible d'une enquête du SCRS aurait un lien avec le Canada et bénéficierait de la protection de l'article 8, cette cible pourrait avoir une attente raisonnable au respect de la vie privée à l'égard de son adresse IP (conformément à l'arrêt *Bykovets*). L'*amicus* fait valoir que, dans un tel cas, la collecte de l'adresse IP de la cible serait plus que minimalement intrusive.

[127] L'*amicus* mentionne en outre un autre scénario dans lequel le SCRS demande à une tierce partie, soit une entreprise de traitement des cartes de crédit, l'adresse IP liée à des achats effectués en ligne qui suggèrent une menace envers la sécurité nationale. En obtenant l'adresse IP, le SCRS pourrait, au moyen d'autres techniques d'enquête, découvrir la vie en ligne de la cible, le tout sans mandat. L'*amicus* soutient que, dans un tel scénario, l'intrusion est plus que minimale; l'article 12 ne suffit pas, et un mandat est nécessaire.

[128] L'*amicus* fait valoir que la demande directe d'une adresse IP formulée par le SCRS nécessiterait une autorisation judiciaire préalable; on ne peut pas présumer qu'une telle fouille serait minimalement intrusive.

(2) L'ordonnance de communication prévue au *Code criminel* n'est pas analogue

[129] Selon l'*amicus*, l'arrêt *Bykovets* ne conclut pas que la norme des « motifs raisonnables de soupçonner » suffit pour obtenir une adresse IP. La majorité, dans l'arrêt *Bykovets* mentionne, au paragraphe 85, qu'une autorisation judiciaire serait relativement facile à obtenir et qu'un télémandat visant une ordonnance de communication des données de transmission pourrait être obtenu suivant la norme des « motifs raisonnables de soupçonner »; toutefois, l'*amicus* avance qu'il ne s'agit là que d'un exemple, lequel ne s'applique qu'aux faits de l'affaire *Bykovets.*

[130] L'*amicus* réitère que, lorsque le SCRS demande à un FSI ou à une tierce partie l'adresse IP d'une cible canadienne faisant l'objet d'une enquête, cette cible a une attente raisonnable au respect de sa vie privée. L'*amicus* maintient que l'exemple relatif à une ordonnance de communication cité dans l'arrêt *Bykovets* ne répond pas à la question de savoir quelle norme permet d'obtenir une adresse IP – les « motifs raisonnables de croire » ou les

« motifs raisonnables de soupçonner » – ni ne détermine l'importance des soupçons nécessaires pour outrepasser la norme des « motifs raisonnables de soupçonner ».

[131] L'*amicus* maintient que, dans l'arrêt *Bykovets*, la Cour suprême a justifié sa conclusion que l'attente raisonnable au respect de la vie privée doit être protégée en raison du risque qu'une adresse IP révèle des renseignements très intimes. L'*amicus* avance qu'il est impossible de concilier cette conclusion avec l'argument du PGC selon lequel l'État peut demander une adresse IP sans qu'il s'agisse d'une fouille plus que minimalement intrusive. L'*amicus* avance que l'on ne peut faire fi des paragraphes 60 à 70 et d'autres passages reconnaissant la protection liée à la vie privée en ce qui a trait à une adresse IP; la Cour suprême pense ce qu'elle dit!

[132] L'*amicus* fait valoir que, dans les circonstances de la décision *Bykovets*, la Cour suprême n'a pas eu à déterminer le type d'autorisation judiciaire qui peut ou non suffire pour faire tomber l'attente raisonnable au respect de la vie privée à l'égard d'une adresse IP simplement parce qu'aucune autorisation judiciaire n'a été demandée. L'*amicus* est d'avis que le renvoi du PGC à la mention, au paragraphe 85, de la facilité avec laquelle on peut obtenir une ordonnance de communication est une remarque incidente et non pas la décision de la Cour suprême sur les faits. L'*amicus* admet toutefois qu'il faut [TRADUCTION] « s'y attarder sérieusement ».

E. *L'utilisation ultérieure des adresses IP*

[133] L'*amicus* fait valoir que le recours aux outils technologiques sources ouverts pour enrichir des adresses IP est de mise seulement lorsqu'une adresse IP n'est pas visée par une attente raisonnable au respect de la vie privée ou, si l'adresse IP est visée par une telle attente, l'adresse IP a été obtenue légalement au départ. Les [...] adresses IP en cause dans la demande

supplémentaire ne sont pas visées par une attente raisonnable au respect de la vie privée et ont été recueillies légalement. L'enrichissement ultérieur des [...] adresses IP ne fait pas intervenir d'attente raisonnable au respect de la vie privée, puisqu'une telle attente n'existait pas au moment de la collecte.

[134] L'*amicus* explique que, dans ses observations faites au juge Gleeson dans le dossier CSIS-24-22, il a adopté la position selon laquelle l'exploitation du dispositif en cause nécessitait un mandat. L'*amicus* signale la distinction entre un dispositif et une simple adresse IP.

[135] Dans le dossier CSIS-24-22, l'*amicus* a reconnu que la *Charte* ne s'applique pas à la réception passive de renseignements issus de la collaboration entre organismes. Toutefois, l'*amicus* fait valoir que l'exploitation par le SCRS de cette information dans le contexte d'une enquête visant une personne se trouvant au Canada pourrait faire intervenir l'article 8 s'il existe une attente résiduelle au respect de la vie privée à l'égard de ce matériel [TRADUCTION] « selon le contexte ».

[136] Dans la demande supplémentaire, l'*amicus* affirme que [TRADUCTION] « une adresse IP est, évidemment, très différente d'un dispositif électronique […], elle ne contient en elle-même rien de privé. En conséquence, la dichotomie acquisition-exploitation articulée par l'*amicus* dans [l'affaire CSIS-24-22] ne s'applique pas dans le contexte qui nous occupe. »

[137] L'*amicus* reconnaît qu'une adresse IP demeure une « série de chiffres » (par opposition à un dispositif qui pourrait être exploité davantage), mais réitère que, bien que les chiffres ne

contiennent pas de renseignements personnels, ceux-ci risquent d'être mis en corrélation avec d'autres activités en ligne et mener à d'autres informations, d'où la conclusion qu'une adresse IP est visée par une attente raisonnable au respect de la vie privée. L'*amicus* renvoie au paragraphe 65 de l'arrêt *Bykovets,* qui mentionne que la Cour a tenu compte de la disponibilité des outils sources ouverts et d'autres bases de données dans sa conclusion qu'il existe une attente raisonnable au respect de la vie privée à l'égard du premier fragment numérique, soit l'adresse IP.

[138] L'*amicus* reconnaît également, dans ses observations écrites, qu'il ne serait pas logique que la police ait besoin d'un mandat pour exploiter les adresses IP qu'elle a par ailleurs obtenues légalement. Conformément à l'arrêt *Bykovets,* [TRADUCTION] « les implications indirectes sur la vie privée de l'acquisition par l'État de l'adresse IP sont déjà prises en compte dans l'analyse de l'acquisition elle-même ».

[139] La Cour comprend que la position de l'*amicus* est la suivante : si l'adresse IP n'est pas visée par une attente raisonnable au respect de la vie ou si l'adresse IP est reçue passivement et/ou obtenue légalement d'une autre façon, il est possible d'enrichir l'adresse IP au moyen d'outils sources ouverts accessibles au public pourvu que cet enrichissement ne révèle pas de renseignements personnels. L'*amicus* remarque que le SCRS aurait besoin d'un mandat pour recourir à toute méthode intrusive contre une cible protégée par l'article 8 après avoir obtenu son adresse IP.

VII. Dispositions pertinentes de la *Loi sur le SCRS*

[140] L'article 12 prévoit ce qui suit :

> 12(1) Le Service recueille, au moyen d'enquêtes ou autrement, dans la mesure strictement nécessaire, et analyse et conserve les informations et renseignements sur les activités dont il existe des motifs raisonnables de soupçonner qu'elles constituent des menaces envers la sécurité du Canada; il en fait rapport au gouvernement du Canada et le conseille à cet égard.
>
> (2) Il est entendu que le Service peut exercer les fonctions que le paragraphe (1) lui confère même à l'extérieur du Canada.
>
> [Nous soulignons.]

[141] Le paragraphe 21(1) prévoit ce qui suit :

> 21(1) Le directeur ou un employé désigné à cette fin par le ministre peut, après avoir obtenu l'approbation du ministre, demander à un juge de décerner un mandat en conformité avec le présent article s'il a des motifs raisonnables de croire que le mandat est nécessaire pour permettre pour permettre au Service de faire enquête, au Canada ou à l'étranger, sur des menaces envers la sécurité du Canada ou d'exercer les fonctions qui lui sont conférées en vertu de l'article 16.

[142] D'autres dispositions prévoient les exigences liées à la demande de mandat et les faits dont le juge doit être convaincu pour le décerner. Le paragraphe 21(2) prévoit les questions qui doivent être traitées dans la demande de mandat, notamment les faits invoqués pour justifier les « motifs raisonnables de croire », toute autre procédure d'enquête tentée sans succès ou qui n'est pas réalisable; le cas échéant, l'impossibilité d'obtenir, sans mandat, des renseignements importants en ce qui a trait à une menace envers la sécurité du Canada ou à l'exécution de tâches et fonctions du SCRS prévues à l'article 16. Le paragraphe 21(3) précise les fait dont le juge doit être convaincu pour décerner le mandat (ce qui peut inclure des conditions « indiquées dans l'intérêt public » (alinéa 21(4)f)).

VIII. Les ordonnances de communication prévues au *Code criminel* : articles 487.014, 487.0141, 487.015 et 492.2

[143] La police est régie par les dispositions du *Code criminel*, qui prévoient que des mandats sont nécessaires pour obtenir des renseignements, des documents ou des biens. Dans une enquête visant des crimes perpétrés en ligne ou des cybercrimes, la police dispose d'options précises pour obtenir une autorisation judiciaire selon les circonstances. Voici quelques exemples.

[144] L'article 487.013 dispose qu'un juge de paix ou un juge peut, sur demande *ex parte*, ordonner à toute personne de préserver des données informatiques qui sont en sa possession s'il existe des « motifs raisonnables de soupçonner » qu'une infraction a été ou sera commise et que les données informatiques seront utiles à l'enquête relative à l'infraction.

[145] L'article 487.014 dispose qu'un juge de paix ou un juge peut, sur demande *ex parte*, ordonner à toute personne de communiquer un document comportant des données qui est en sa possession s'il existe des motifs raisonnables de croire qu'une infraction a été ou sera commise et que le document ou les données fourniront une preuve concernant la perpétration de l'infraction.

[146] L'article 487.015 dispose que, afin d'identifier tout dispositif ayant servi à la transmission de la communication ou toute personne y ayant participé, un juge de paix ou un juge, sur demande *ex parte*, peut ordonner à toute personne d'établir et de communiquer un document comportant des données de transmission qui ont trait à l'identification et qui, si le juge de paix ou le juge est convaincu qu'il existe des motifs raisonnables de soupçonner qu'une infraction a été ou sera commise; que l'identification de tout dispositif ayant servi à la

transmission d'une communication ou de toute personne y ayant participé sera utile à l'enquête relative à l'infraction; et que les données de transmission en la possession ou à la disposition d'une ou de plusieurs personnes – dont l'identité n'est pas connue au moment de la présentation de la demande – permettront cette identification. (Comme je l'ai mentionné, dans l'arrêt *Bykovets*, la Cour suprême a suggéré l'ordonnance de communication en vue de retracer une communication donnée prévue à l'article 487.015 comme alternative pour la police souhaitant obtenir une autorisation judiciaire visant à obtenir une adresse IP.)

[147] L'article 487.016 dispose qu'un juge de paix ou un juge peut, sur demande *ex parte*, ordonner à toute personne d'établir et de communiquer un document comportant des données de transmission qui sont en sa possession ou à sa disposition, si le juge de paix ou le juge est convaincu qu'il existe des motifs raisonnables de soupçonner qu'une infraction a été ou sera commise et que les données de transmission seront utiles à l'enquête relative à l'infraction.

[148] L'article 487.017 prévoit une ordonnance de communication des données de localisation également s'il existe des « motifs raisonnables de soupçonner ».

[149] L'article 492.2 dispose qu'un juge de paix ou un juge qui est convaincu qu'il existe des motifs raisonnables de soupçonner qu'une infraction a été ou sera commise et que les données de transmission seront utiles à l'enquête peut délivrer un mandat autorisant un agent de la paix ou un fonctionnaire public (police) à obtenir de telles données au moyen d'un enregistreur de données de transmission.

[150] Sauf pour le mandat visant la communication d'un document contenant des données, la police doit respecter la norme des « motifs raisonnables de soupçonner » qu'une infraction a été ou sera commise en vue d'obtenir divers mandats, dont le mandat pour identifier un dispositif.

IX. Analyse

[151] Selon le PGC, la question clé est de savoir si la collecte, par le SCRS, des [...] adresses IP est autorisée par l'article 12 à titre de fouille non intrusive ou minimalement intrusive ou si la collecte est plus que minimalement intrusive; si la collecte est plus que minimalement intrusive, l'autorisation prévue par l'article 21 est nécessaire pour que la collecte soit légale et conforme à l'article 8 de la *Charte*. Il a été conclu que les [...] adresses IP ont été légalement recueillies au moyen d'une collecte non intrusive parce qu'il n'y a pas d'attente raisonnable au respect de la vie privée à l'égard de ces adresses précises; il ne s'agit pas d'une fouille.

[152] La Cour suprême est arrivée à ses conclusions dans l'arrêt *Bykovets* d'après les faits qui lui ont été présentés; la police a demandé une adresse IP à une tierce partie sans avoir obtenu de mandat, et cette adresse IP a été utilisée pour obtenir d'autres mandats qui ont mené aux accusations portées contre M. Bykovets. La Cour suprême a conclu qu'une adresse IP est visée par une attente raisonnable au respect de la vie privée et doit être protégée contre les fouilles abusives et, en conséquence, une autorisation judiciaire préalable est nécessaire. Bien que le contexte de l'affaire *Bykovets* diffère de celui de la demande supplémentaire – notamment en ce que le SCRS n'a pas demandé les adresses IP et que le mandat du SCRS est d'enquêter sur les menaces envers la sécurité nationale –, la Cour suprême a insisté sur la vie privée en lien avec

une adresse IP en raison du risque qu'elle révèle d'autres informations; en conséquence, notre Cour estime devoir analyser minutieusement la portée de l'article 12.

[153] Selon le PGC, certains passages de la décision *Bykovets* sont des remarques incidentes, tandis que l'*amicus* est d'avis que ce sont d'autres passages qui sont des remarques incidentes et non pas ceux identifiés par le PGC. D'après notre Cour, aucun passage ne peut être ignoré, même s'ils sont difficiles à concilier entre eux. L'orientation fournie par la Cour suprême peut être adaptée au contexte du SCRS, lequel doit pouvoir faire enquête sur des menaces envers la sécurité du Canada, rôle ayant été décrit comme central et essentiel au sein de « l'appareil de sécurité nationale du Canada » (*IMSI* au para 203). La principale question soulevée par la demande supplémentaire peut être tranchée sans incohérence par rapport aux principes établis dans l'arrêt *Bykovets* parce qu'il n'existe pas d'attente raisonnable au respect de la vie privée à l'égard des [...] adresses IP.

[154] Pour établir si le SCRS peut recueillir ou non les adresses IP dans d'autres contextes, il faut tenir compte des principes de l'arrêt *Bykovets* ainsi que de la jurisprudence de notre Cour et de la Cour d'appel fédérale ayant pris en compte les paramètres de l'article 12 et les implications pour la vie privée du recours par le SCRS à la nouvelle technologie.

[155] Dans l'arrêt *Bykovets*, la Cour suprême a fait part d'importantes préoccupations au sujet du risque qu'une adresse IP révèle des renseignements biographiques d'ordre personnel. Néanmoins, dans une enquête sur des menaces envers la sécurité nationale, en particulier dans le cybercontexte, le SCRS ne souhaite pas obtenir l'adresse IP pour recueillir de l'information au sujet du mode de vie de l'internaute, mais plutôt pour remédier à une menace envers la sécurité

nationale. À elle seule, l'adresse IP recueillie par le SCRS ne révèle pas de renseignements personnels.

[156] Le déclarant du SCRS a expliqué que l'obtention de tout renseignement personnel au sujet de l'utilisateur de l'adresse IP, à l'exception de tout renseignement personnel déjà public, nécessite un mandat.

A. *Les [...] adresses IP de la demande supplémentaire ont été recueillies légalement*

[157] Étant d'accord avec le PGC et l'*amicus*, la Cour estime également que la réception passive et la collecte des [...] adresses IP ne font pas intervenir l'article 8; il n'y a pas d'attente raisonnable au respect de la vie privée et pas de fouille.

[158] Les [...] adresses IP d'acteurs étrangers hostiles sans aucun lien avec le Canada ne font pas intervenir l'article 8 de la *Charte*, car ces ressortissants étrangers ne sont pas inclus dans la portée du mot « chacun » figurant dans le libellé de l'article 8.

[159] Comme l'a souligné le juge en chef dans la décision *Extérieur du Canada* au paragraphe 6, « les ressortissants étrangers dépourvus de lien reconnu avec le Canada ne peuvent faire valoir les protections prévues à l'article 8 ». Le juge en chef a expliqué, au paragraphe 170, que les ressortissants étrangers qui n'ont pas l'un des trois liens reconnus avec le Canada (la citoyenneté canadienne, la présence au Canada ou faire l'objet de poursuites pénales au Canada) ne sont pas visés par le mot « chacun » qui figure à l'article 8.

[160] Bien que les [...] victimes canadiennes de cyberattaques soient protégées par l'article 8, compte tenu de l'ensemble des circonstances, leurs adresses IP ne sont pas visées par une attente raisonnable au respect de la vie privée.

[161] La demande supplémentaire a été accueillie sur la base que les [...] adresses IP en cause ne font pas intervenir d'attente raisonnable au respect de la vie privée; c'est légalement que le SCRS a obtenu les adresses IP sans mandat au moyen d'une collecte non intrusive conformément à l'article 12.

B. *La collecte minimalement intrusive des [...] adresses IP conformément à l'article 12 était possible*

[162] Dans l'arrêt *Bykovets,* la Cour suprême a conclu qu'« une adresse IP peut révéler un éventail de renseignements éminemment privés qui touchent directement aux détails intimes sur le mode de vie et les choix personnels d'un utilisateur individuel » (au para 70 [nous soulignons]). Toutefois, dans le contexte du cybermandat, l'adresse IP ne révèle pas de tels renseignements; le SCRS ne cherche qu'à contrecarrer une cyberattaque, ce pourquoi il demande l'adresse IP. Dans ce contexte, l'adresse IP ne révèle pas de renseignements d'ordre personnel sur le mode de vie. Comme en a témoigné le déclarant, l'obtention de tout renseignement personnel par le SCRS nécessite un mandat, car elle est plus que minimalement intrusive.

[163] En outre, lorsque l'adresse IP est recueillie uniquement pour contrecarrer une cyberattaque, en de telles circonstances, toute attente au respect de la vie privée n'est pas raisonnable.

[164] Même si l'on avait conclu à l'existence d'une attente raisonnable au respect de la vie privée, les [...] adresses IP auraient tout de même pu être recueillies au moyen d'une fouille minimalement intrusive conformément à l'article 12. En outre, la collecte de l'adresse IP est également très ciblée et très précise (dans la mesure du possible, étant donné la nature changeante des adresses IP), et aucune autre information n'a été recueillie fortuitement (et si tel avait été le cas, l'information n'aurait pas été retenue) (*IMSI* au para 236).

[165] Les futures demandes supplémentaires pourraient autoriser la réception passive des adresses IP d'acteurs étrangers hostiles et/ou de victimes de cyberattaques, au moyen de l'échange de renseignements entre organismes, au moyen soit d'une collecte non intrusive (s'il n'y a pas d'attente raisonnable apparente au respect de la vie privée) soit d'une collecte minimalement intrusive. [...]

C. *Réception passive des adresses IP*

[166] Comme je l'ai mentionné, le SCRS a reçu passivement la plupart des [...] adresses IP de la part d'organismes étrangers et canadiens. En outre, le SCRS reçoit passivement des adresses IP dans d'autres contextes. L'*amicus* signale qu'une telle réception passive, étant donné que les organismes étrangers et canadiens ont recueilli légalement les adresses IP et les ont transmises, ne fait pas intervenir la *Charte*.

[167] La Cour a tenu compte de l'interprétation et de l'application de l'arrêt *Bykovets* par les cours supérieures et provinciales. Comme je l'ai mentionné ci-dessus, cette jurisprudence appuie la position selon laquelle la réception passive par les forces de l'ordre d'adresses IP obtenues

auprès d'organismes étrangers et d'acteurs non étatiques ne fait pas intervenir la protection de l'article 8.

[168] La Cour convient que, d'après la jurisprudence analogue dans le contexte criminel, lorsque le SCRS reçoit passivement des adresses IP de la part d'organismes étrangers ou canadiens sans que le SCRS n'ait fait de demande ou posé d'[TRADUCTION]« acte de l'État », il ne s'agit pas d'une fouille.

[169] Dans des circonstances analogues à celles de l'espèce, ou dans d'autres contextes entourant la réception passive d'adresses IP par le SCRS, invoquer l'article 12 suffit pour recueillir les adresses IP; il s'agit d'une collecte minimalement intrusive (ou non intrusive).

D. *L'article 12 autorise les fouilles minimalement intrusives si tous les critères de l'article 12 sont remplis*

(1) L'article 12 autorise les fouilles minimalement intrusives, dont la demande d'adresse IP

[170] La jurisprudence de notre Cour et de la Cour d'appel fédérale s'est penchée sur la portée de l'article 12. Bien que l'arrêt *Bykovets* précise qu'une attente raisonnable au respect de la vie privée existe à l'égard d'une adresse IP et conclut qu'une autorisation judiciaire préalable est nécessaire pour que la police puisse demander une adresse IP dans le cadre d'une enquête sur un crime, la jurisprudence de notre Cour a traité le contexte différent de la sécurité nationale et cette jurisprudence peut coexister parallèlement à l'arrêt *Bykovets.* Selon la jurisprudence de notre Cour en matière de sécurité nationale, l'article 12 n'autorise pas les fouilles plus que minimalement intrusives (c'est-à-dire, celles qui permettent d'intercepter des renseignements

biographiques d'ordre personnel ayant trait à une personne). En outre, l'article 12 comporte d'autres mesures de contrôle.

[171] Dans la décision *Extérieur du Canada,* le juge en chef a affirmé aux paragraphes 176 et 178 :

> [176] Selon la jurisprudence constante de la Cour, l'article 12 autorise seulement le SCRS à mener sans mandat des activités qui sont minimalement envahissantes. Or, cette jurisprudence intéresse des personnes faisant l'objet d'enquêtes pouvant faire valoir les droits que confère l'article 8 de la *Charte*.
>
> […]
>
> [178] Certes, « une autorisation préalable, qui prend habituellement la forme d'un mandat vide, a toujours été la condition préalable d'une fouille, d'une perquisition et d'une saisie valides sous le régime de la common law et de la plupart des lois » *Hunter*, p 160. Toutefois, l'article 12 l'emporte sur la *common law*, car il habilite expressément le SCRS à recueillir, dans la mesure strictement nécessaire, et à analyser et conserver les renseignements sur les activités dont on a des motifs raisonnables de soupçonner qu'elles constituent des menaces envers la sécurité du Canada.

[172] L'arrêt *Bykovets* précise nettement la nécessité d'une autorisation préalable à une demande d'adresse IP faite par la police dans le cadre d'une enquête criminelle; toutefois, l'article 12 n'exige pas d'autorisation judiciaire préalable si le SCRS veut recueillir des renseignements – « dans la mesure strictement nécessaire » – concernant des activités dont il existe des motifs raisonnables de soupçonner qu'elles constituent des menaces envers la sécurité du Canada.

[173] Dans la décision *Mahjoub (Re),* 2013 CF 1096 au para 33, le juge Blanchard a signalé que, bien que l'article 12 semble être d'une large portée, il est néanmoins limité par les exigences

relatives aux mandats prévues aux articles 21 à 24. Le juge Blanchard a précisé que l'article 12 n'autorise pas les fouilles et les saisies attentatoires d'informations privées.

[174] Le juge Blanchard a conclu, au paragraphe 35, que l'article 12 exige que le SCRS ait une raison précise et objective pour recourir à une technique d'enquête la moins attentatoire possible et il atteint le juste équilibre « entre l'intérêt du public à ce que l'on fasse enquête sur les menaces envers la sécurité du Canada et les droits à la vie privée de la cible en question ».

[175] La Cour d'appel fédérale a pris en compte trois appels connexes, dont la décision du juge Blanchard, citée ci-dessus, et a affirmé au paragraphe 176 de la décision *Mahjoub CAF* :

> L'article 12 […] permet la collecte des informations et des renseignements sur les activités dont il existe des motifs raisonnables de soupçonner qu'elles constituent des menaces envers la sécurité du Canada. Contrairement à l'allégation de M. Mahjoub, ce pouvoir n'est pas absolu : des enquêtes peuvent être entreprises uniquement s'il existe des « motifs raisonnables de soupçonner » que des activités constituent « des menaces envers la sécurité du Canada », et alors seulement « dans la mesure strictement nécessaire ». Je suis d'accord avec la Cour fédérale quand elle dit que l'article 12 n'est ni imprécis ni trop large dans sa portée. L'article 12 est limité par l'article 2, qui définit en détail ce qui constitue des « menaces envers la sécurité du Canada » d'une manière qui se conforme aux normes exposées par la Cour suprême du Canada [dans la jurisprudence portant sur la portée trop large et le caractère vague].

[176] Dans la décision *Mahjoub CAF*, au paragraphe 177, la Cour d'appel fédérale a confirmé les conclusions du juge Blanchard selon lesquelles l'article 12 et les dispositions connexes sur les mandats sont constitutionnelles et la norme des « motifs raisonnables de soupçonner » de l'article 12 respecte l'article 8 de la *Charte* étant donné l'atteinte minimale à la vie privée que représentent les fouilles autorisées en vertu de l'article 12.

[177] Dans la décision *IMSI*, le juge en chef a pris en compte le fait que le SCRS a invoqué l'article 12 et a conclu que l'exigence des « motifs raisonnables de soupçonner » prévue à l'article 12 « est un critère "solide" qui est bien connu en droit canadien […] », soulignant que la portée de l'article 12 est d'autant plus restreinte en raison de l'exigence que l'information recueillie soit « strictement nécessaire » (au para 213).

[178] Au paragraphe 218, le juge en chef a précisé ce qui suit :

> […] l'article 12 n'autorise par la SCRS à enquêter sur des personnes qui mènent des activités dont il n'existe pas de motifs raisonnables de soupçonner qu'elles constituent des menaces envers la sécurité du Canada. Les pouvoirs d'enquête prévus à l'article 12 visent uniquement les personnes dont les activités respectent ce critère rigoureux. […]

[179] Dans la décision *IMSI*, la question posée à la Cour concerne l'utilisation par le SCRS d'un émulateur de station de base [ESB] afin d'obtenir les caractéristiques distinctives des appareils mobiles faisant l'objet d'une enquête, en particulier l'identité internationale de l'abonné mobile [*International Mobile Subscribe Identity* ou IMSI] et l'identité internationale d'équipement mobile [*International Mobile Equipment Identity* ou IMEI]. Le juge en chef conclut que l'article 12 donne l'autorité raisonnable et légale au SCRS de recueillir, au moyen d'une fouille minimalement intrusive, l'information concernant les IMSI et IMEI, car il s'agit de sous-ensembles de données de transmission.

[180] Le juge O'Reilly résume de façon succincte la décision du juge en chef dans la décision *Réseaux favoris* aux paragraphes 105, 107, 109 et 110 reproduits ci-dessous.

> [105] Sous la plume du juge en chef Paul Crampton, la Cour a traité du recours aux ESB dans le contexte de l'article 12 de la *Loi*

sur le SCRS, c'est-à-dire aux fins d'enquêtes sur des menaces pour la sécurité nationale (*X*(*Re) (ESB)*, 2017 CF 1047). Le juge en chef a conclu que l'utilisation d'un ESB était assimilable à une fouille, parce que l'utilisateur d'un appareil mobile avait une attente raisonnable en matière de vie privée relativement aux informations qu'un ESB pourrait capturer. Toutefois, il a conclu à la légalité de l'utilisation d'un ESB sans mandat, tant que le Service prenait des mesures pour minimiser l'empiètement sur la vie privée, notamment éviter d'intercepter le contenu de communications et les informations sur l'appareil, détruire toute information de tiers recueillie de manière incidente et ne pas utiliser les informations à des fins de géolocalisation. Bien que les informations que l'ESB permet d'obtenir puissent aider le Service à créer un mince profil personnel de l'utilisateur, ce qui met en cause l'article 8 de la *Charte canadienne des droits et libertés* [*Charte*], le juge en chef a conclu que les fouilles sans mandat n'étaient pas abusives, étant très ciblées, très précises et minimalement envahissantes.

[…]

[107] D'entrée de jeu, le juge en chef a clairement souligné que les fouilles effectuées sans mandat sont présumées abusives et contreviennent donc à la protection contre les fouilles, les perquisitions et les saisies abusives garantie par l'article 8 de la *Charte*. Néanmoins, une telle fouille pourrait être jugée non abusive si elle est autorisée par une loi, si la disposition législative l'autorisant est raisonnable et si elle n'a pas été effectuée de manière abusive. Il a conclu qu'en vertu de l'article 12, le Service est tenu de recueillir, d'analyser et de conserver des informations et des renseignements sur des activités qui constituent des menaces pour la sécurité nationale (au paragraphe 196). En outre, l'article 21 de la *Loi sur le SCRS* établit les circonstances entourant l'obtention d'un mandat par le Service. Par contre, la *Loi sur le SCRS* n'exige pas que le Service obtienne un mandat chaque fois qu'il cherche à recueillir des informations ayant trait à la sécurité nationale, même quand la collecte met en cause l'attente raisonnable d'une personne et égard à sa vie privée. Il a constaté l'existence d'une gamme d'activités minimalement envahissantes que peut mener le Service pour assumer son rôle en matière de sécurité nationale sans devoir obtenir de mandat (au paragraphe 198), encore une fois, tant qu'elles sont autorisées par une loi, que la disposition législative les autorisant est raisonnable et que les fouilles ainsi effectuées ne le sont pas de manière abusive.

[…]

> [109] Le juge en chef a conclu au caractère raisonnable de l'article 12, compte tenu de sa nature et de son objet, de l'ampleur de l'intrusion qu'il autorise, du mécanisme d'intrusion qu'il permet d'utiliser, de la supervision judiciaire qu'il prévoit ainsi que d'autres mesures de contrôle. Comme il en est question plus haut, les premiers de ces éléments, c'est-à-dire la nature et l'objet de la disposition, diffèrent de façon importante entre les articles 12 et 16.
>
> [110] Selon le juge en chef, la nature et l'objet de l'article 12 consistent en l'octroi, au Service, de la responsabilité de recueillir, d'analyser et de conserver, dans la mesure strictement nécessaire, des informations et des renseignements sur des activités pour lesquelles le Service a des motifs raisonnables de croire qu'elles constituent des « menaces envers la sécurité du Canada », au sens de l'article 2 de la *Loi sur le SCRS*. Il s'agit, selon le juge en chef, d'un rôle : « central et, sans doute, essentiel ». Il a rejeté les arguments des *amici*, qui estimaient que le critère des motifs raisonnables de soupçonner était faible sur le plan constitutionnel, soulignant que ce critère avait été approuvé par la Cour suprême dans des affaires où le droit au respect de la vie privée était réduit, qui mettaient en cause des intérêts publics de premier plan ou qui traitaient de méthodes de fouilles très précises (aux paragraphes 206 et 207). Il a conclu que les fouilles réalisées au moyen d'ESB pour l'application de l'article 12 comportaient chacun de ces éléments : intrusion minimale, préoccupations urgente liées à la sécurité nationale et très grande précision.
>
> [Nous soulignons.]

[181] De façon semblable, la collecte d'une adresse IP visée par une attente raisonnable au respect de la vie privée serait une fouille minimalement intrusive parce que l'adresse IP, à elle seule, ne révèle aucun renseignement personnel. Bien qu'une adresse IP puisse être utilisée pour créer un « mince profil personnel de l'utilisateur » si elle est « enrichie » au moyen d'une interrogation faite sur un moteur de recherche public, la collecte de l'adresse IP autorisée par l'article 12 – si tous les critères de l'article 12 sont remplis, notamment qu'il s'agit d'une enquête sur une menace envers la sécurité nationale et que l'information est strictement nécessaire – n'est pas une fouille abusive. La demande d'adresse IP ferait partie de la « gamme d'activités

minimalement envahissantes que peut mener le Service pour assumer son rôle en matière de sécurité nationale ».

[182] Dans la décision *IMSI*, le juge en chef conclut que le recours à un ESB constitue une fouille parce que la personne a une « attente raisonnable au respect de la vie privée […] relativement aux informations que le SCRS, en ayant accès aux IMSI et aux IMEI de ses appareils mobiles, pouvait commencer à recueillir à son endroit ou pouvait utiliser pour tirer des inférences plus fondées » et « [d]ans la mesure où ceci a permis au SCRS de mieux comprendre certains aspects des renseignements biographiques d'ordre personnel de […] ou de tirer des inférences plus fondées à leur égard, cette activité implique les droits qui lui sont garantis par l'article 8 de la *Charte* » (au para 6).

[183] La même justification sous-tend la conclusion de la Cour suprême dans l'arrêt *Bykovets* selon laquelle il existe une attente raisonnable au respect de la vie privée à l'égard des adresses IP. Toutefois, dans le contexte du SCRS, l'adresse IP à elle seule ne lui permet généralement pas de tirer des inférences concernant les renseignements biographiques d'ordre personnel. Néanmoins, l'arrêt *Bykovets* établit que les utilisateurs d'adresses IP (toutes les adresses IP) ont une attente raisonnable au respect de la vie privée quant à leur adresse IP, attente qui fait intervenir la protection de l'article 8. La question est de savoir si la fouille servant à obtenir une adresse IP est ou non abusive.

[184] Dans la décision *IMSI*, le juge en chef conclut que, bien que la cueillette de IMSI et de IMEI fasse intervenir l'article 8, la collecte sans mandat de cette information (c'est-à-dire, la

fouille) n'est pas abusive parce qu'elle est très ciblée, très précise et minimalement envahissante (au para 7).

[185] Le juge en chef remarque, au paragraphe 112, que « [l]'ensemble des circonstances à évaluer lorsqu'il s'agit de déterminer si la personne visée s'attendait raisonnablement au respect de sa vie privée quant à l'objet de la fouille ou de la perquisition présumée comprend divers facteurs directement liés aux attentes de la personne en matière de respect de la vie privée, d'un point de vue tant subjectif qu'objectif ». Le juge en chef mentionne les facteurs établis par la jurisprudence, qui sont les même que ceux énoncés par la Cour suprême dans l'arrêt *Bykovets.*

[186] Le juge en chef conclut également, au paragraphe 198, que l'article 12 « confère au SCRS toute la latitude nécessaire pour enquêter sans mandat sur des activités dont il existe des motifs raisonnables de soupçonner qu'elles constituent des menaces envers la sécurité du Canada, sauf si la common law l'exige. »

[187] Au paragraphe 200, le juge en chef se penche sur la différence entre l'exigence pour les services de police d'obtenir un mandat et la possibilité pour le SCRS d'invoquer l'article 12, :

> [200] Les *amici* suggèrent en outre que le fait d'exiger un mandat avant de tenter d'obtenir des IMSI et des IMEI au moyen de la technologie relative aux ESB correspondrait à l'exigence implicite selon laquelle les services de police doivent obtenir un mandat général, en vertu de l'article 487.01 du *Code criminel*, ou un mandat pour un enregistreur de données de transmission, en vertu de l'article 492.2, avant de pouvoir utiliser un ESB pour obtenir des IMSI et des IMEI et les attribuer à un suspect. Toutefois, le fait que le Parlement *peut* avoir déterminé que les *services de police* doivent avoir un mandat pour utiliser un ESB et attribuer un IMSI et une IMEI à une personne ne suffit pas à conclure que le SCRS doit également obtenir un mandat dans de telles circonstances.

> Entre autres, les services de police ne disposent pas des pouvoirs conférés par l'article 12 de la *Loi sur le SCRS*.

[188] Cette différence existe en l'espèce : les dispositions du *Code criminel* concernant le mandat s'appliquent aux services de police lorsqu'ils demandent une adresse IP tandis que l'article 12 s'applique au SCRS lorsque ce dernier demande ou recueille une adresse IP.

[189] Dans la décision *IMSI*, le juge en chef a répondu aux *amici* au sujet de l'intention du Parlement dans l'adoption de l'article 12, affirmant au 201 :

> [201] Les *amici* soutiennent également qu'il incombe au Parlement de décider de permettre au SCRS d'utiliser un ESB pour intercepter l'IMSI et l'IMEI d'un appareil mobile pour attribuer celui-ci à une cible selon des « motifs raisonnables de soupçonner ». Je suis d'accord, et je crois que c'est ce qu'a fait le Parlement lorsqu'il a adopté l'article 12 de la *Loi sur le SCRS*. Donc, l'utilisation, par le SCRS, d'un ESB à cette fin précise est « autorisée par la loi », conformément à la jurisprudence citée au paragraphe 133.

[190] De façon semblable, l'article 12 autorise le SCRS à demander ou à recueillir les adresses IP suivant la norme des « motifs raisonnables de soupçonner » si tous les critères de l'article 12 sont remplis. S'il veut restreindre le pouvoir du SCRS, le Parlement peut le faire, mais il devra également mettre en balance le besoin de s'assurer que le SCRS a les outils nécessaires pour faire enquête et, idéalement, contrecarrer les menaces envers la sécurité nationale.

[191] Dans la décision *IMSI*, le juge en chef a conclu que l'article 12 est une disposition législative raisonnable, a expliqué sa conclusion aux paragraphes 202 à 235 et a résumé son raisonnement au paragraphe 236, signalant l'objet de l'article 12, la mesure de l'atteinte

autorisée par l'article 12, la mesure dans laquelle la *Loi sur le SCRS* prévoit une supervision, à son article 21, qui se déclenche dès que le SCRS tente d'obtenir les pouvoirs nécessaires pour mener des activités plus que minimalement envahissantes, ainsi que le rôle important de contrôle assumé par le Comité de surveillance des activités de renseignement de sécurité [CSARS] (maintenant l'Office de surveillance des activités en matière de sécurité nationale et de renseignement [l'OSSNR]). Le même raisonnement s'applique au SCRS lorsqu'il invoque l'article 12 pour recueillir une adresse IP sans mandat.

(2) La fouille visant l'obtention d'une adresse IP est-elle toujours minimalement intrusive?

[192] L'*amicus* fait valoir que la fouille visant l'obtention d'une adresse IP n'est pas toujours minimalement intrusive.

[193] L'*amicus* reconnaît que l'adresse IP à elle seule n'est qu'une série de chiffres ne comportant aucun renseignement personnel. Néanmoins, l'*amicus* avance qu'un mandat peut s'avérer nécessaire lorsque les « fragments numériques » que constitue l'adresse IP risquent de révéler des détails intimes entourant les renseignements biologiques d'ordre personnel de la cible. Bien que ce potentiel existe, ce ne sont pas toutes les adresses IP qui entraînent une telle révélation. Le déclarant a traité de cette question dans la demande supplémentaire, et la preuve a révélé que le SCRS n'obtient pas de renseignements biographiques d'ordre personnel à partir d'une adresse IP, sauf avec un mandat. Le SCRS fait une demande de mandat en application de l'article 21 en vue d'obtenir toute information concernant une adresse IP (suivant la norme plus exigeante des « motifs raisonnables de croire » que l'information est nécessaire pour permettre

au SCRS de faire enquête sur une menace envers la sécurité du Canada et que toutes les autres exigences de l'article 21 sont remplies). Le déclarant a confirmé que c'est ce que fait le SCRS.

[194] Dans la décision *IMSI* au paragraphe 219, le juge en chef définit la portée de l'article 12 dans les termes suivants :

> [219] Le SCRS peut recueillir, analyser et conserver des informations obtenues de façon non envahissante ou très envahissante au sujet des quelques activités qui s'inscrivent dans le cadre très étroit qu'établit l'article 12. Toutefois, lorsqu'il passe à des activités de collecte plus envahissantes, le Service doit obtenir un mandat. En bref, en ajoutant les dispositions de l'article 21 concernant les mandats à la *Loi sur le SCRS*, le législateur prévoyait implicitement que le SCRS ne mènerait pas, en vertu de l'article 12, d'activités de collecte plus que minimalement envahissantes sans obtenir une autorisation judiciaire préalable au titre de l'article 21. Il peut être inféré de ce cadre qu'en l'absence d'un mandat, l'article 12 permet au SCRS de mener uniquement des activités non envahissantes ou minimalement envahissantes.

[195] Il n'est pas mis en doute que les fouilles sans mandat effectuées conformément à l'article 12 se limitent aux fouilles minimalement intrusives. Si le SCRS demande une adresse IP dans un contexte qui fournit déjà des renseignements au sujet de la cible d'une enquête ayant une attente raisonnable au respect de la vie privée à l'égard de son adresse IP, l'adresse IP peut laisser entrevoir plus qu'un « mince profil personnel ». Dans de tels contextes, la collecte de l'adresse IP serait plus que minimalement intrusive et nécessiterait un mandat.

[196] L'*amicus* avance en outre que le respect de la vie privée à l'égard d'une adresse IP recueillie dans le contexte de la sécurité nationale n'est pas moindre que dans le contexte d'une enquête criminelle. Toutefois, la question de savoir si l'attente raisonnable au respect de la vie

privée – peu importe le degré de respect – est la même dans le contexte de la sécurité nationale et dans le contexte criminel dépend des circonstances.

[197] Même si les adresses IP sont visées par une attente raisonnable au respect de la vie privée, les attentes de certains internautes peuvent ne pas être raisonnables. Au départ, il faut déterminer l'existence d'une attente raisonnable au respect de la vie privée dans la totalité des circonstances. Dans l'arrêt *Bykovets*, la Cour suprême remarque qu'une attente au respect de la vie privée est raisonnable quand le droit de ne pas être importuné par le gouvernement l'emporte sur le droit du gouvernement de s'immiscer dans la vie privée des particuliers afin de réaliser ses fins. Dans le cadre de l'enquête d'une menace envers la sécurité nationale, l'intérêt du gouvernement à demander et à recueillir l'adresse IP peut outrepasser celui de la personne, dépendant de la nature de la menace et des autres circonstances.

[198] Dans la décision *IMSI* au para 166, à laquelle renvoie l'*amicus*, le juge en chef répond à l'argument du PGC selon lequel il est moins probable qu'une personne soit poursuivie à cause de renseignements personnels recueillis par le SCRS qu'à cause de renseignements de même nature obtenus par les services de la police; <u>à elle seule</u>, cette explication ne suffit pas pour conclure qu'un individu a des attentes moindres en matière de vie privée. Le juge en chef conclut que plusieurs facteurs – dont les conséquences potentielles – informent l'attente raisonnable au respect de la vie privée.

[199] En analysant la portée de l'article 12 à l'égard des fouilles minimalement intrusives, le juge en chef signale, entre autres, le rôle essentiel joué par le SCRS dans la sécurité nationale (au para 203). Le juge en chef ajoute, au para 206 :

> La Cour [CSC] a alors réitéré qu'un « exercice de pondération des intérêts en jeu peut justifier une fouille en application d'une norme moins rigoureuse lorsque les droits à la vie privée sont réduits ou lorsque les objectifs d'ordre public de l'État sont prédominants » (*Chehil*, précité, au paragraphe 23). Bref, le critère requis pour résister à un examen approfondi en vertu de l'article 8 « peut varier selon le contexte » (*Rogers*, précité, au paragraphe 35). [Nous soulignons.]

[200] En ce qui a trait à la raisonnabilité de la fouille autorisée par l'article 12, le juge en chef affirme dans la décision *IMSI* au para 211 :

> En effet, je crois que les objectifs relatifs à la sécurité nationale qui figurent à l'article 12 suffiront habituellement à faire pencher la balance en faveur des intérêts de l'État, lorsque les fouilles menées par le SCRS sont minimalement envahissantes (*Jarvis*, précité, au paragraphe 71; *Mahjoub CAF*, précité). Comme la Cour suprême l'a reconnu, « [l]'une des responsabilités les plus fondamentales d'un gouvernement est d'assurer la sécurité de ses citoyens. »
>
> (Voir *Charkaoui c Canada (Citoyenneté et Immigration)*, 2007 CSC 9 au para 1.)

[201] Comme je l'ai mentionné plus haut, dans la décision *IMSI*, le juge en chef réitère l'importance du rôle du SCRS dans les enquêtes sur des menaces envers la sécurité nationale, un rôle « central et, sans doute, essentiel » (au para 203).

[202] L'*amicus* reconnaît que la nature de l'enquête – p. ex. : l'enquête du SCRS sur une menace envers la sécurité nationale – est un facteur pertinent ainsi que d'autres renseignements dont pourrait disposer le SCRS lorsqu'il demande une adresse IP.

[203] Malgré la mise en garde de l'*amicus* contre la jurisprudence existante portant sur l'article 12 en lien avec les répercussions de l'arrêt *Bykovets*, la Cour conclut que la jurisprudence de la Cour fédérale et de la Cour d'appel fédérale demeure contraignante. Cette

jurisprudence, en tenant compte des intrusions à l'attente raisonnable au respect de la vie privée et de la portée de l'article 12, a traité de plusieurs questions semblables sur lesquelles s'est penchée la Cour suprême dans l'arrêt *Bykovets,* notamment la question de savoir en quoi consiste l'attente raisonnable au respect de la vie privée, le besoin de prendre en compte la totalité des circonstances et le besoin d'équilibre, bien que ce soit dans le contexte de la sécurité nationale. L'arrêt *Bykovets* confirme l'existence d'une attente raisonnable au respect de la vie privée à l'égard d'une adresse IP, tout comme, par exemple, dans la décision *IMSI,* la Cour confirme l'existence d'une attente raisonnable au respect de la vie privée à l'égard des numéros IMSI et IMEI, mais conclut que l'on peut invoquer l'article 12 pour effectuer une collecte minimalement intrusive très ciblée et très précise, compte tenu de toutes les autres mesures de contrôle prévues à l'article 12.

(3) Les ordonnances de communication prévues au *Code criminel* et l'article 12 de la *Loi sur le SCRS*

[204] Comme je l'ai mentionné, d'après la mise en garde de l'*amicus,* il ne faut pas donner à l'arrêt *Bykovets* une interprétation appuyant la conclusion selon laquelle l'article 12 autorise l'obtention d'une adresse IP. L'*amicus* fait valoir que, bien que la majorité dans l'arrêt *Bykovets* suggère que l'obtention d'une autorisation judiciaire préalable – par exemple, un télémandat autorisant l'ordonnance de communication de données de transmission prévue au *Code criminel* – est relativement aisée, il ne faut pas en conclure de façon plus générale que la Cour suprême est d'avis que la demande d'adresse IP est une fouille minimalement intrusive.

[205] L'*amicus* convient, dans ses réponses aux questions de la Cour, que l'arrêt *Bykovets* appuie le point de vue selon lequel une ordonnance de communication de données de

transmission prévue à l'article 487.015 du *Code criminel* aurait permis d'éviter la conclusion de l'arrêt *Bykovets*, mais il s'oppose en ce que cette approche devrait être généralement retenue ou qu'il s'agit d'une fouille minimalement intrusive.

[206] Notre Cour est d'avis que la Cour suprême n'a pas d'autres motifs de donner l'exemple précis du télémandat autorisant l'ordonnance de communication de données de transmission prévue à l'article 487.015, sinon que pour signaler que c'est le moyen par lequel la police aurait pu obtenir l'adresse IP de M. Bykovets – et que c'est le moyen auquel la police devrait recourir pour obtenir des adresses IP dans des circonstances semblables à l'avenir. L'article 487.015 prévoit une ordonnance de communication afin d'identifier tout dispositif ayant servi à la transmission de données (y compris une adresse IP). Les autres options du *Code criminel* sont conçues pour obtenir des renseignements précis et, à l'exception de l'ordonnance de communication d'un document contenant des données (c'est-à-dire, du contenu), elles sont toutes fondées sur la norme des « motifs raisonnables de soupçonner ».

[207] Dans les dispositions analogues du *Code criminel*, seule l'ordonnance de communication d'un document contenant des données (que ce soit une ordonnance générale ou pour des dates précises) exige des motifs raisonnables de croire qu'une infraction a été ou sera commise et que le document ou les données fourniront des preuves concernant la commission de l'infraction. Or, une adresse IP à elle seule ne contient pas de données.

[208] De l'avis de l'*amicus*, l'exemple de télémandat visé à l'article 487.015 du *Code criminel* n'est pas valable parce que, dans l'arrêt *Bykovets*, on n'avait pas demandé à la Cour suprême de déterminer le type d'autorisation judiciaire préalable adéquat, étant donné que la police n'avait

demandé aucune autorisation. Toutefois, si la police avait tenté d'obtenir une autorisation judiciaire, l'affaire ne se serait pas retrouvée devant la Cour. La Cour suprême s'est penchée sur la violation de la *Charte*, qui émanait des faits, et s'est prononcée sur les façons d'éviter une telle violation – ce qu'elle fait habituellement dans d'autres circonstances où sont constatées des violations à la *Charte*. Selon notre Cour, la Cour suprême a affirmé qu'il aurait fallu demander un mandat et, en présence de motifs « suffisants » au regard de la norme des « motifs raisonnables de soupçonner » qu'une infraction a été ou sera commise, l'ordonnance de communication des données de transmission prévue au *Code criminel* aurait donné à la police le pouvoir de demander l'adresse IP à l'entreprise de traitement des payements, la tierce partie. Les concepts de motifs raisonnables, que ce soit de soupçonner ou de croire, ne sont pas des concepts nouveaux pour la police, le SCRS ou les cours. Déterminer ce qui est « suffisant » pour respecter l'une ou l'autre norme est une décision prise au cas par cas suivant les circonstances.

[209] En dépit des grands principes de l'arrêt *Bykovets* concernant le droit à la vie privée en jeu dans cette affaire, principes qui suggèrent qu'une adresse IP est une information fortement protégée par le droit à la vie privée (parce qu'elle peut révéler des informations et parce qu'elle est le premier fragment numérique), j'estime que la Cour suprême n'aurait pas suggéré que l'ordonnance de communication des données de transmission prévue à l'article 487.015 puisse être une meilleure solution si la norme des « motifs raisonnables de soupçonner » n'avait pas suffi à prévenir une fouille abusive.

[210] En ce qui a trait aux messages contradictoires de l'arrêt *Bykovets*, l'*amicus* admet qu'il existe une « tension » entre les passages qui signalent l'importance du droit à la vie privée à l'égard d'une adresse IP et le paragraphe 85, qui propose, comme pouvoir requis, l'ordonnance

de communication suivant des « motifs raisonnables de soupçonner ». L'*amicus* est d'avis que ces passages sont des remarques incidentes, tandis que le PGC croit que d'autres passages sont des remarques incidentes.

[211] Dans certains paragraphes, les renvois de la Cour suprême portent sur les faits précis de l'affaire *Bykovets* tandis que d'autres sont d'ordre plus général, par exemple, sur le droit à la vie privée à l'égard d'une adresse IP. Notre Cour a tenté de concilier l'arrêt de la Cour suprême avec les faits qui se trouvent devant elle et d'appliquer les principes de cette décision, et ce, en tenant également compte des circonstances de la demande supplémentaire, qui sont différentes, et du contexte de la *Loi sur le SCRS* ainsi que de la jurisprudence de la Cour fédérale et de la Cour d'appel fédérale sur la portée de l'article 12 dans le contexte de la sécurité nationale.

[212] Comme l'a mentionné le PGC, le mandat du SCRS, qui est prévu à l'article 12, concernant la collecte sans mandat est circonscrit par de nombreuses mesures de contrôle : les exigences législatives; l'examen judiciaire dans le cas où le SCRS utilise de l'information recueillie pour demander un mandat ultérieurement; la supervision du ministre de la Sécurité publique; les exigences du directeur du SCRS en matière de rapports au PGC et au ministre lorsqu'un employé peut avoir agi illégalement; et l'imputabilité envers l'OSSNR et le Comité des parlementaires sur la sécurité nationale et le renseignement ainsi que les examens effectués par ces deux entités.

E. *Le SCRS ne devrait pas être astreint à une norme plus élevée que la police*

[213] Dans l'arrêt *Bykovets*, la majorité est d'avis que ce n'est pas un lourd fardeau pour les forces de l'ordre de respecter la norme des « motifs raisonnables de soupçonner » quant à

l'obtention d'une ordonnance de communication des données de transmission prévue à l'article 487.015 par l'entremise d'un télémandat. Je suis d'accord avec le PGC : le SCRS ne devrait pas être astreint à une norme plus élevée dans le contexte de la sécurité nationale, alors que tous les critères de l'article 12 sont remplis.

[214] Le SCRS ne peut pas se prévaloir des télémandats. Le SCRS peut conformément à l'article 12 effectuer une fouille minimalement intrusive sans mandat (si tous les critères sont remplis) ou encore demander le mandat prévu à l'article 21 et se plier aux exigences supplémentaires, y compris les affidavits détaillés, les audiences *ex parte* à huis clos, le contre-interrogatoire des déclarants et la détermination par un juge désigné. Demander le mandat prévu à l'article 21 afin d'obtenir une adresse IP, laquelle ne sera pas utilisée pour obtenir d'autres renseignements biographiques d'ordre personnel, est un lourd fardeau et ne permettait pas au SCRS de faire enquête et de contrecarrer des cybermenaces ou d'autres menaces à la sécurité nationale au moment où elles surviennent.

[215] Si la police peut obtenir l'ordonnance de communication prévue à l'article 487.015 du *Code criminel* en vue d'identifier un dispositif suivant la norme des « motifs raisonnables de soupçonner » et ainsi obtenir une adresse IP, le SCRS devrait être en mesure de recueillir ce type d'information conformément à l'article 12 suivant la même norme dans le contexte de la sécurité nationale; une norme plus élevée ne devrait pas être imposée dans le contexte de la sécurité nationale (*Mahjoub CAF* aux para 265-267).

[216] Toutefois, le SCRS devra obtenir un mandat s'il veut recueillir d'autres informations qui révèlent des renseignements biographiques d'ordre personnel.

F. *L'utilisation ultérieure des adresses IP*

[217] Comme je l'ai mentionné, la Cour reconnaît que les [...] adresses IP de la demande supplémentaire ont été recueillies sans mandat dans le cadre d'une collecte non intrusive et, subsidiairement, qu'elles auraient pu être recueillies au moyen d'une collecte minimalement intrusive. Les utilisateurs des [...] adresses IP n'ont pas d'attente raisonnable au respect de la vie privée et, en conséquence, la collecte de leurs adresses IP ne fait pas intervenir l'article 8 (il ne s'agit pas d'une fouille).

[218] On pose à la Cour une question connexe, à savoir si le SCRS peut utiliser ou enrichir les [...] adresses IP. Le PGC et l'*amicus* conviennent que l'utilisation ultérieure ou l'enrichissement des [...] adresses IP n'est pas une fouille. Leur argument est que, parce que la collecte des [...] adresses IP ne fait pas intervenir l'article 8, l'utilisation plus avant de ces adresses ne fait pas elle non plus intervenir l'article 8. Il n'y a pas d'attente raisonnable au respect de la vie privée au départ et il n'y a pas de telle attente non plus après le fait (la collecte).

[219] L'*amicus* remarque que c'est la capacité des adresses IP de révéler d'autres informations qui justifie l'attente raisonnable au respect de la vie privée (*Bykovets* aux para 63-65), et si l'adresse IP est obtenue légalement, l'utilisation ultérieure ou l'enrichissement de l'adresse IP, au moyen d'outils sources ouverts, limitée aux données de géolocalisation et le FSC ne devrait pas nécessiter de mandat. L'*amicus* met en garde, toutefois, contre la collecte plus intrusive, laquelle devrait respecter la norme des « motifs raisonnables de croire ».

[220] Dans l'arrêt *Bykovets*, la Cour suprême n'a pas commenté l'utilisation ultérieure de l'adresse IP après qu'elle ait été obtenue légalement, mais a précisé que d'autres mandats

seraient nécessaires pour obtenir le contenu des communications – tout comme ils le seraient dans le contexte du SCRS. Dans une enquête plus ciblée menée par le SCRS, un mandat serait nécessaire pour obtenir plus d'informations à partir d'une adresse IP recueillie légalement qui révèlerait des renseignements biographiques d'ordre personnel.

[221] Que d'autres adresses IP recueillies légalement (avec ou sans mandat) puissent être enrichies au moyen d'outils publics sources ouverts n'est pas une question que je dois trancher en l'espèce. Bien que le PGC reconnaît que l'enrichissement se produit et fait valoir que l'enrichissement d'adresses IP au moyen d'outils sources ouverts, qui sont également utilisés par la police (tel que mentionné dans les décisions *Leger* et *Pengelly)*, ne fait pas intervenir l'article 8; cette question devra être tranchée dans le contexte d'une demande appropriée dotée d'un dossier factuel qui explique pleinement la capacité des outils sources ouverts d'enrichir une adresse IP.

X. Second argument subsidiaire du PGC

[222] Il n'est pas nécessaire que je me penche sur le second argument subsidiaire du PGC, qui se fonde sur le critère de mise en balance établi dans la décision *Formation plénière*. Cette approche serait une détermination après le fait de la légalité de la collecte de renseignements et/ou d'adresses IP. Si jamais la question se pose à l'avenir, on y répondra le moment venu.

XI. Conclusion

[223] En somme, la Cour conclut ce qui suit :

- Les [...] adresses IP en cause dans la demande supplémentaire ont été obtenues

légalement en application de l'article 12 au moyen d'une collecte non intrusive; les [...] adresses IP ne sont pas visées par une attente raisonnable au respect de la vie privée et ne font pas intervenir l'article 8.

- Les adresses IP recueillies conformément au cybermandat, dans des conditions analogues (par exemple, en cas de réception passive ou en l'absence d'attente raisonnable au respect de la vie privée) peuvent être recueillies légalement de façon non intrusive ou minimalement intrusive conformément à l'article 12.
- Les adresses IP dans d'autres contextes, dans lesquels le SCRS reçoit passivement les adresses IP et où il n'y a pas d'[TRADUCTION]« acte de l'État », peuvent être recueillies légalement conformément à l'article 12.
- Le SCRS peut demander des adresses IP conformément à l'article 12 dans le cadre d'une fouille minimalement intrusive lorsque tous les critères de l'article 12 sont remplis (dans la mesure où l'information est strictement nécessaire et l'information a trait aux activités dont il existe des motifs raisonnables de soupçonner qu'elles constituent des menaces envers la sécurité du Canada). La collecte doit être minimalement intrusive, très ciblée et très précise. Comme je l'ai mentionné ci-dessus, cette conclusion est appuyée par la jurisprudence portant sur l'article 12, qui, entre autres, reconnaît que, bien qu'un mandat soit nécessaire pour la police – suivant la norme des « motifs raisonnables de soupçonner » – l'article 12 prévoit une autorisation analogue et sans mandat pour le SCRS dans le contexte de la sécurité nationale.
- Toute collecte d'adresses IP plus que minimalement intrusive nécessite une autorisation judiciaire préalable.
- Par exemple, lorsque le SCRS demande une adresse IP dans un contexte qui, au départ,

fournit des renseignements sur la cible d'une enquête ayant une attente raisonnable au respect de la vie privée à l'égard de son adresse IP, l'adresse IP risque de révéler des renseignements biographiques d'ordre personnel; dans de tels contextes, la collecte de l'adresse IP serait plus que minimalement intrusive et nécessiterait l'obtention d'un mandat.

- En ce qui a trait à l'utilisation ou l'enrichissement des [...] adresses IP en cause dans la demande supplémentaire, parce qu'il n'y a pas d'attente raisonnable au respect de la vie privée en l'espèce, l'utilisation ultérieure ou l'enrichissement des [...] adresses IP ne soulève pas de préoccupations liées à l'application de l'article 8.

"Catherine M. Kane"
Juge

Traduction certifiée conforme
Nathalie Ayotte, jurilinguiste principale

COUR FÉDÉRALE

AVOCATS INSCRITS AU DOSSIER

DOSSIER :	C-1-24
INTITULÉ :	DANS L'AFFAIRE concernant la demande de mandats présentée par [...] au titre des articles 12 et 21 de la *Loi sur le Service canadien du renseignement de sécurité*, LRS 1985, ch. C-23 ET DANS L'AFFAIRE VISANT DES CYBERACTIVITÉS D'ESPIONNAGE, DE SABOTAGE, ET D'INGÉRENCE ÉTRANGÈRE
LIEU DE L'AUDIENCE :	OTTAWA
DATE DE L'AUDIENCE :	LES 15 ET 24 OCTOBRE 2024
MOTIFS CLASSIFIÉS :	LA JUGE KANE
DATE DES MOTIFS :	LE 16 DÉCEMBRE 2025

COMPARUTIONS

JEFFREY JOHNSTON ZORICA GUZINA	POUR LE PROCUREUR GÉNÉRAL DU CANADA
MATTHEW GOURLAY	*AMICUS CURIAE*

AVOCATS INSCRITS AU DOSSIER

Procureur Général du Canada Ottawa (Ontario)	POUR LE PROCUREUR GÉNÉRAL DU CANADA
Henein Hutchison Robitaille LLP Toronto (Ontario)	*AMICUS CURIAE*