COUR SUPRÊME DU CANADA

RÉFÉRENCE : R. *c.* Bykovets, 2024 CSC 6

APPEL RÉENTENDU : 11 décembre 2023
JUGEMENT RENDU : 1er mars 2024
DOSSIER : 40269

ENTRE :

Andrei Bykovets
Appelant

et

Sa Majesté le Roi
Intimé

- et -

Directrice des poursuites pénales, procureur général de l'Ontario, procureur général de la Colombie-Britannique, Association canadienne des libertés civiles et British Columbia Civil Liberties Association
Intervenants

TRADUCTION FRANÇAISE OFFICIELLE

CORAM : Le juge en chef Wagner et les juges Karakatsanis, Côté, Rowe, Martin, Kasirer, Jamal, O'Bonsawin et Moreau

MOTIFS DE JUGEMENT : (par. 1 à 92)
La juge Karakatsanis (avec l'accord des juges Martin, Kasirer, Jamal et Moreau)

MOTIFS DISSIDENTS : (par. 93 à 165)	La juge Côté (avec l'accord du juge en chef Wagner et des juges Rowe et O'Bonsawin)

NOTE : Ce document fera l'objet de retouches de forme avant la parution de sa version définitive dans le *Recueil des arrêts de la Cour suprême du Canada*.

Andrei Bykovets *Appelant*

c.

Sa Majesté le Roi *Intimé*

et

Directrice des poursuites pénales,
procureur général de l'Ontario,
procureur général de la Colombie-Britannique,
Association canadienne des libertés civiles et
British Columbia Civil Liberties Association *Intervenants*

Répertorié : R. *c.* Bykovets

2024 CSC 6

N^{o} du greffe : 40269.

Audition : 17 janvier 2023.

Présents : Le juge en chef Wagner et les juges Karakatsanis, Côté, Brown, Martin, Jamal et O'Bonsawin.

Nouvelle audition : 11 décembre 2023.

Jugement : 1er mars 2024.

Présents : Le juge en chef Wagner et les juges Karakatsanis, Côté, Rowe, Martin, Kasirer, Jamal, O'Bonsawin et Moreau.

EN APPEL DE LA COUR D'APPEL DE L'ALBERTA

Droit constitutionnel — Charte des droits — Fouilles, perquisitions et saisies — Enquête sur des opérations en ligne frauduleuses menée par la police — Demande présentée par la police à une société de traitement des paiements afin d'obtenir la communication des adresses de protocole Internet (« IP ») associées aux opérations — Adresses IP communiquées volontairement à la police par la société de traitement des paiements, et accusé arrêté en conséquence — Les adresses IP sont-elles assorties d'une attente raisonnable au respect de la vie privée? — Une demande de communication d'adresse IP présentée par l'État à un tiers constitue-t-elle une fouille? — Charte canadienne des droits et libertés, art. 8.

Au cours d'une enquête sur des achats en ligne frauduleux effectués auprès d'un magasin de vins et spiritueux, la police a communiqué avec une société tierce de traitement qui gérait les ventes en ligne du magasin et a obtenu les adresses IP utilisées pour les achats. La police a par la suite obtenu une ordonnance de communication obligeant le fournisseur de services Internet (« FSI ») à révéler le nom et l'adresse du client pour chaque adresse IP. La police a utilisé ces renseignements relatifs à l'abonné pour solliciter et exécuter des mandats de perquisition. B a été arrêté.

B a contesté la demande de la police à la société de traitement en vue d'obtenir les adresses IP, alléguant que celle-ci avait violé son droit à la protection contre les fouilles, les perquisitions et les saisies abusives garanti par l'art. 8 de la *Charte*. La juge du procès a conclu que la demande faite par la police à la société de traitement ne constituait pas une fouille au sens de l'art. 8 de la *Charte* parce que B n'avait pas une attente raisonnable au respect de sa vie privée à l'égard de son adresse IP; le droit garanti à B par l'art. 8 n'entrait donc pas en jeu. B a été déclaré coupable de 14 infractions liées aux achats en ligne frauduleux. Les juges majoritaires de la Cour d'appel ont convenu que B n'avait aucune attente raisonnable au respect de sa vie privée à l'égard de ses adresses IP et ont rejeté l'appel interjeté par B contre ses déclarations de culpabilité. La juge dissidente aurait accueilli l'appel au motif qu'une attente raisonnable au respect de la vie privée s'appliquait aux adresses IP.

Arrêt (le juge en chef Wagner et les juges Côté, Rowe et O'Bonsawin sont dissidents) : Le pourvoi est accueilli et un nouveau procès est ordonné.

Les juges **Karakatsanis**, Martin, Kasirer, Jamal et Moreau : S'il doit protéger de manière significative la vie privée en ligne des Canadiens et des Canadiennes dans le monde actuel qui est très largement numérique, l'art. 8 de la *Charte* doit protéger leurs adresses IP. Une adresse IP est le lien crucial entre un internaute et son activité en ligne. Considérée de manière normative, elle est la clé donnant accès à l'activité Internet d'un utilisateur et, ultimement, à son identité. Une adresse IP suscite donc une attente raisonnable au respect de la vie privée. Par

conséquent, une demande d'adresse IP faite par l'État constitue une fouille au sens de l'art. 8 de la *Charte*.

L'article 8 de la *Charte* garantit le droit à la protection contre les fouilles, les perquisitions ou les saisies abusives. Il vise principalement à protéger la vie privée, y compris l'intimité informationnelle, à savoir le droit revendiqué par des particuliers, des groupes ou des institutions de déterminer eux-mêmes le moment, la manière et la mesure dans lesquels des renseignements les concernant sont communiqués. Le respect de la vie privée d'un individu est essentiel pour assurer la dignité, l'autonomie et la croissance personnelle de celui-ci. La protection de la vie privée est une condition préalable essentielle à l'épanouissement d'une démocratie libre et en santé.

Pour établir une violation de l'art. 8, le demandeur doit démontrer premièrement qu'il y a eu une fouille, une perquisition ou une saisie. 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 analysent l'attente au respect de la vie privée en examinant de nombreux facteurs interreliés, mais souvent concurrents, qui peuvent être regroupés en quatre catégories : (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 subjective au respect de la vie privée était objectivement

raisonnable. En l'espèce, les parties ont convenu que B avait un intérêt direct à l'égard des adresses IP ainsi qu'une attente subjective au respect de sa vie privée à l'égard de leur contenu informationnel.

En ce qui concerne l'objet de la fouille, celui-ci est défini sous l'angle non pas seulement des renseignements eux-mêmes, mais également de la tendance qui consiste à chercher à obtenir des renseignements pour permettre d'en tirer des inférences au sujet d'autres renseignements de nature personnelle. Le tribunal doit concevoir cet objet d'un point de vue holistique et doit être particulièrement prudent lorsqu'il décrit l'objet d'une fouille relative à des données électroniques. L'approche ne doit pas être mécanique et doit tenir compte de la réalité technologique. La fouille en l'espèce avait pour objet les renseignements que les adresses IP pouvaient révéler sur des internautes précis, y compris, ultimement, leur identité. Reconnaître que la police voulait l'adresse IP — en tant que lien entre un abonné et un endroit donnés et une activité Internet particulière — pour obtenir davantage de renseignements sur l'utilisateur permet au tribunal d'apprécier l'attente au respect de la vie privée à l'égard de tous les renseignements que cette adresse IP tend à révéler.

Pour ce qui est de la question de savoir si une attente subjective au respect de la vie privée est objectivement raisonnable, les tribunaux doivent prendre en considération l'ensemble des circonstances. Bien qu'il n'existe pas de liste définitive de facteurs, les tribunaux ont souvent examiné plus particulièrement le contrôle sur l'objet, le lieu de la fouille et le caractère privé de l'objet. Dans le contexte de l'intimité

informationnelle, le contrôle exercé par le demandeur sur l'objet n'est pas déterminant. Internet exige que les utilisateurs révèlent à leur FSI les renseignements relatifs à l'abonné pour pouvoir prendre part aux activités de cette nouvelle place publique, et les Canadiens et les Canadiennes n'ont pas à vivre en reclus du monde numérique afin de pouvoir conserver un semblant de vie privée. Le lieu où s'est déroulée la fouille n'est pas non plus préjudiciable à une attente raisonnable au respect de la vie privée dans un tel contexte. Les espaces en ligne sont qualitativement différents des espaces physiques. Les renseignements que renferme Internet peuvent révéler beaucoup plus que ce que sont susceptibles de révéler des renseignements assujettis aux limites d'un espace physique. Par conséquent, l'absence d'intrusion physique révèle peu sur le caractère raisonnable d'une attente au respect de la vie privée.

Quant au caractère privé de l'objet, l'art. 8 vise à protéger un ensemble de renseignements biographiques d'ordre personnel que les particuliers pourraient, dans une société libre et démocratique, vouloir constituer et soustraire à la connaissance de l'État. L'ensemble de renseignements biographiques ne touche pas uniquement à l'identité, mais s'étend notamment à des renseignements tendant à révéler des détails intimes sur le mode de vie et les choix personnels de l'individu. L'accent mis par l'art. 8 sur de tels renseignements signifie qu'une attente raisonnable au respect de la vie privée est appréciée de manière normative plutôt que simplement descriptive. Elle ne peut être appréciée en fonction d'une seule utilisation en particulier de la preuve; sa portée ne peut pas non plus être établie selon l'intention précise qu'avait la police en recherchant les renseignements. L'objectif de l'art. 8, apprécié normativement, exige plutôt de se

demander quels renseignements tend à révéler l'objet de la fouille. 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. De plus, 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. Une adresse IP peut aussi mettre l'État sur la trace d'une activité Internet qui mène directement à l'identité d'un utilisateur, même sans un mandat obligeant un FSI à révéler le nom et l'adresse du client associé à l'adresse IP. L'accès aux adresses IP sans autorisation judiciaire préalable pose de grands risques en matière de vie privée.

Définir une attente raisonnable au respect de la vie privée est une opération de mise en balance. En l'espèce, la balance penche en faveur de l'extension de l'attente raisonnable au respect de la vie privée 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. Internet a fait augmenter de manière exponentielle tant la qualité que la quantité de renseignements stockés à propos des internautes, et il englobe les comportements humains les plus publics comme les plus privés. Internet a permis aux sociétés privées non seulement de suivre leurs utilisateurs, mais aussi de bâtir des profils de ceux-ci remplis de renseignements que les utilisateurs n'ont jamais su qu'ils révélaient. En concentrant cette masse de renseignements entre les mains de tiers du secteur privé et en donnant à ces derniers les outils nécessaires

pour agréger et disséquer ces données, Internet a essentiellement modifié la topographie de la vie privée sous le régime de la *Charte*. Il a ajouté un tiers à l'écosystème constitutionnel, et a fait de la relation horizontale entre l'individu et l'État une relation tripartite. Bien que l'art. 8 ne s'applique pas aux tiers eux-mêmes, ceux-ci jouent le rôle de médiateurs dans une relation directement régie par la *Charte* — celle entre le défendeur et la police. Ce changement a accru la capacité informationnelle de l'État.

Ces préoccupations importantes relatives à la vie privée entrent en balance avec l'intérêt parfois conflictuel mais légitime de la société en ce qui a trait au besoin de sécurité. La police devrait disposer des outils d'enquête nécessaires pour s'occuper d'un crime commis et facilité en ligne. Toutefois, exiger que la police obtienne une autorisation judiciaire préalable avant d'obtenir une adresse IP ne constitue pas une lourde mesure d'enquête. 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. Reconnaître qu'une adresse IP est protégée par l'art. 8 vise 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. La surveillance judiciaire restreint ce qui est accessible à l'État en ligne et enlève aux sociétés privées le pouvoir de décider s'il convient de dévoiler des renseignements — et en quelle quantité — et renvoie la question au champ d'application de la *Charte*.

Le juge en chef Wagner et les juges **Côté**, Rowe et O'Bonsawin (dissidents) : Le pourvoi devrait être rejeté. B n'avait pas une attente raisonnable au respect de sa vie privée à l'égard des adresses IP contenues sur les serveurs de l'entreprise de traitement des cartes de crédit, et du FSI qu'elles ont révélé. La police n'avait pas besoin d'une autorisation judiciaire avant de demander les adresses IP à l'entreprise afin de déterminer le FSI associé à celles-ci. Cependant, cette conclusion n'exclut pas la possibilité qu'une personne puisse avoir une attente raisonnable au respect de sa vie privée sur le fondement de faits différents.

L'article 8 de la *Charte* vise à assurer une protection contre l'intrusion de l'État dans la vie privée d'une personne et entre en jeu seulement lorsque les attentes raisonnables d'une personne en matière de vie privée sont affectées d'une manière ou d'une autre par une technique d'enquête. Le test relatif à l'attente raisonnable au respect de la vie privée est tributaire des faits et contextuel, et dépend de l'ensemble des circonstances d'un cas particulier. Le test est de nature normative, et non descriptive. Son objectif est de décider quel degré d'intimité une personne devrait avoir, et non pas quel degré d'intimité une personne a effectivement.

Déterminer l'objet de la fouille est une question clé dans l'analyse de l'ensemble des circonstances. Pour déterminer l'objet de la fouille, le tribunal doit se pencher sur le lien entre la technique d'enquête utilisée par la police et l'intérêt en matière de vie privée qui est en jeu. Il doit examiner non seulement la nature des renseignements précis recherchés, mais aussi la nature des renseignements qui sont

ainsi révélés. Le tribunal se préoccupe de la capacité des renseignements précis recherchés de donner lieu à des inférences ou de révéler d'autres renseignements. Ces inférences et ces autres renseignements font partie du véritable objet de la fouille. Une fois avoir déterminé l'objet de la fouille, il faut alors se demander si une attente subjective au respect de sa vie privée à l'égard de l'objet de la fouille est objectivement raisonnable. La question de savoir si une attente au respect de la vie privée est raisonnable dépend de plusieurs facteurs. Ils peuvent inclure le lieu fouillé, le contrôle sur l'objet de la fouille, le caractère privé de l'objet, si l'objet était à la vue du public, si l'objet a été abandonné, si des tiers possédaient déjà l'objet, si la méthode de fouille a porté atteinte à l'intérêt en matière de vie privée en cause, si la méthode de fouille était elle-même déraisonnable, et si la fouille a révélé des renseignements biographiques. Les facteurs ne seront pas tous pertinents pour l'analyse dans un cas donné et aucun facteur à lui seul n'est déterminant.

En l'espèce, les facteurs pertinents pour l'analyse du caractère raisonnable sont le caractère privé de l'objet, le contrôle sur l'objet et le lieu fouillé. Le caractère privé de l'objet d'une prétendue fouille peut appuyer une conclusion suivant laquelle une attente au respect de la vie privée est raisonnable. La question est de savoir non seulement si l'objet lui-même est privé, mais aussi s'il est susceptible de révéler d'autres renseignements privés essentiels. Ce facteur revêt une importance particulière en ce qui a trait aux intérêts en matière d'intimité informationnelle. Lorsque seule l'intimité informationnelle est en cause, il peut être presque essentiel que les renseignements eux-mêmes soient privés pour qu'il existe une attente raisonnable au

respect de la vie privée. Le contrôle sur l'objet de la fouille appuie généralement une conclusion selon laquelle il y avait une attente raisonnable au respect de la vie privée, alors que l'absence de contrôle peut militer contre une telle conclusion. Le lieu fouillé joue sur le caractère raisonnable de toute attente au respect de la vie privée à l'égard de celui-ci. L'idée du lieu se rapporte essentiellement au concept d'intimité territoriale et prend nécessairement moins d'importance dans les cas qui mettent en jeu l'intimité informationnelle.

Il y a désaccord avec l'appréciation que les juges majoritaires font de l'objet de la prétendue fouille en l'espèce. Les juges majoritaires incluent dans l'objet toute mesure menant à l'identification ultime du suspect, malgré le fait que de tels renseignements ne sont pas révélés par les adresses IP à elles seules, suivant la preuve au dossier. La façon correcte de qualifier l'objet de la fouille consiste à décrire celui-ci comme les adresses IP et le FSI révélé par ces adresses.

L'attente subjective de B au respect de sa vie privée à l'égard de l'objet de la fouille n'était pas objectivement raisonnable. Les adresses IP en cause n'étaient pas privées et, eu égard aux faits de l'affaire, ne révélaient pas de renseignements privés. Sans plus, tout ce qu'une adresse IP révèle à la police est le FSI d'un utilisateur — ce qui ne constitue guère un élément de nature particulièrement privée, et encore moins des renseignements biographiques. De plus, le facteur du contrôle tend à exclure une conclusion selon laquelle l'attente de B au respect de sa vie privée était raisonnable. B n'avait guère de contrôle sur les adresses IP, qu'un FSI peut changer à son gré et sans

préavis. Un internaute qui laisse derrière lui des données relatives à une adresse IP perd complètement le contrôle de ce qui se passe avec ces chiffres. Enfin, la prétendue fouille n'a pas été effectuée au domicile de B. Le lieu de la fouille était la base de données de l'entreprise de traitement des cartes de crédit. Il n'accroît pas le caractère objectivement raisonnable de l'attente subjective de B au respect de sa vie privée.

Jurisprudence

Citée par la juge Karakatsanis

Arrêts mentionnés : *R. c. Spencer*, 2014 CSC 43, [2014] 2 R.C.S. 212; *Hunter c. Southam Inc.*, [1984] 2 R.C.S. 145; *R. c. Marakah*, 2017 CSC 59, [2017] 2 R.C.S. 608; *R. c. Reeves*, 2018 CSC 56, [2018] 3 R.C.S. 531; *R. c. Tessling*, 2004 CSC 67, [2004] 3 R.C.S. 432; *R. c. Edwards*, [1996] 1 R.C.S. 128; *R. c. Jones*, 2017 CSC 60, [2017] 2 R.C.S. 696; *R. c. Ward*, 2012 ONCA 660, 112 O.R. (3d) 321; *R. c. Cole*, 2012 CSC 53, [2012] 3 R.C.S. 34; *R. c. Plant*, [1993] 3 R.C.S. 281; *R. c. Dyment*, [1988] 2 R.C.S. 417; *R. c. Ramelson*, 2022 CSC 44; *R. c. Vu*, 2013 CSC 60, [2013] 3 R.C.S. 657; *R. c. Patrick*, 2009 CSC 17, [2009] 1 R.C.S. 579; *R. c. Morelli*, 2010 CSC 8, [2010] 1 R.C.S. 253; *R. c. Spence*, 2005 CSC 71, [2005] 3 R.C.S. 458; *State c. Simmons*, 190 Vt. 141 (2011); *Breyer c. Bundesrepublik Deutschland*, C-582/14, EU:C:2016:779; *Vidal-Hall c. Google Inc.*, [2015] EWCA Civ 311, [2016] Q.B. 1003; *Québec (Procureure générale) c. 9147-0732 Québec inc.*, 2020 CSC 32, [2020] 3 R.C.S. 426; *R. c. Mills*, 2019 CSC 22, [2019] 2 R.C.S. 320; *R. c. Friesen*, 2020 CSC 9, [2020] 1 R.C.S. 424; *R. c. Wong*, [1990] 3 R.C.S. 36.

Citée par la juge Côté (dissidente)

R. c. Spencer, 2014 CSC 43, [2014] 2 R.C.S. 212; *R. c. Evans*, [1996] 1 R.C.S. 8; *R. c. Edwards*, [1996] 1 R.C.S. 128; *R. c. Tessling*, 2004 CSC 67, [2004] 3 R.C.S. 432; *R. c. Reeves*, 2018 CSC 56, [2018] 3 R.C.S. 531; *R. c. Marakah*, 2017 CSC 59, [2017] 2 R.C.S. 608; *R. c. Ward*, 2012 ONCA 660, 112 O.R. (3d) 321; *R. c. Trapp*, 2011 SKCA 143, 377 Sask. R. 246; *R. c. Kang-Brown*, 2008 CSC 18, [2008] 1 R.C.S. 456; *R. c. Gomboc*, 2010 CSC 55, [2010] 3 R.C.S. 211; *R. c. Plant*, [1993] 3 R.C.S. 281; *R. c. Vu*, 2013 CSC 60, [2013] 3 R.C.S. 657; *R. c. Stairs*, 2022 CSC 11; *R. c. Mills*, 2019 CSC 22, [2019] 2 R.C.S. 320; *Breyer c. Bundesrepublik Deutschland*, C-582/14, EU:C:2016:779; *Vidal-Hall c. Google Inc.*, [2015] EWCA Civ 311, [2016] Q.B. 1003; *Altimo Holdings c. Kyrgyz Mobil Tel Ltd*, [2011] UKPC 7, [2012] 1 W.L.R. 1804; *Hunter c. Southam Inc.*, [1984] 2 R.C.S. 145; *R. c. Feeney*, [1997] 2 R.C.S. 13; *R. c. McNeil*, 2009 CSC 3, [2009] 1 R.C.S. 66; *R. c. O'Brien*, 2023 ONCA 197, 166 O.R. (3d) 114; *R. c. Ilia*, 2023 ONCA 75, 523 C.R.R. (2d) 128; *R. c. Allen*, 2020 ONCA 664, 396 C.C.C. (3d) 1; *R. c. West*, 2020 ONCA 473, 392 C.C.C. (3d) 271; *R. c. Caza*, 2015 BCCA 374, 376 B.C.A.C. 258; *R. c. Smith*, 2005 BCCA 334, 199 C.C.C. (3d) 404; *R. c. Friesen*, 2020 CSC 9, [2020] 1 R.C.S. 424; *R. c. Find*, 2001 CSC 32, [2001] 1 R.C.S. 863; *R. c. McGregor*, 2023 CSC 4; *R. c. Sharma*, 2022 CSC 39; *R. c. Spence*, 2005 CSC 71, [2005] 3 R.C.S. 458; *In re The Board of Commerce Act, 1919, and The Combines and Fair Prices Act, 1919*, [1922] 1 A.C. 191.

Lois et règlements cités

Charte canadienne des droits et libertés, art. 8.

Code criminel, L.R.C. 1985, c. C-46, art. 487.015(1), 691 à 693.

Loi sur la Cour suprême, L.R.C. 1985, c. S-26, art. 40(3).

Doctrine et autres documents cités

Austin, Lisa M. « Getting Past Privacy? Surveillance, the Charter, and the Rule of Law » (2012), 27 *R.C.D.S.* 381.

Austin, Lisa M. « Technological Tattletales and Constitutional Black Holes : Communications Intermediaries and Constitutional Constraints » (2016), 17 *Theoretical Inquiries L.* 451.

Canada. Commissariat à la protection de la vie privée. *Ce qu'une adresse IP peut révéler à votre sujet : Rapport préparé par la Direction de l'analyse des technologies du Commissariat à la protection de la vie privée du Canada*, Gatineau, 2013.

Cockfield, Arthur J. « Who Watches the Watchers? A Law and Technology Perspective on Government and Private Sector Surveillance » (2003), 29 *Queen's L.J.* 364.

Hasan, Nader, et al. *Search and Seizure*, Toronto, Emond Montgomery, 2021.

Hogg, Peter W., and Wade K. Wright. *Constitutional Law of Canada*, 5th ed. Supp., Toronto, Thomson Reuters, 2022 (updated 2023, release 1).

Kennedy, Pagan. « William Gibson's Future Is Now », *The New York Times*, 13 janvier 2012 (en ligne : https://www.nytimes.com/2012/01/15/books/review/distrust-that-particular-flavor-by-william-gibson-book-review.html).

Magotiaux, Susan. « Out of Sync : Section 8 and Technological Advancement in Supreme Court Jurisprudence » (2015), 71 *S.C.L.R.* (2d) 501.

Matsumi, Hideyuki. « Predictions and Privacy : Should There Be Rules About Using Personal Data to Forecast the Future? » (2017), 48 *Cumb. L. Rev.* 149.

Olivetti Rason, Nino, and Sara Pennicino. « Comparative Law in the Jurisprudence of the Supreme Court of Canada », in Giuseppe Franco Ferrari, ed., *Judicial Cosmopolitanism : The Use of Foreign Law in Contemporary Constitutional Systems*, Boston, Brill/Nijhoff, 2019, 140.

Panneck, Travis. « Incognito Mode Is in the Constitution » (2019), 104 *Minn. L. Rev.* 511.

Sharpe, Robert J., and Kent Roach. *The Charter of Rights and Freedoms*, 7th ed., Toronto, Irwin Law, 2021.

Slane, Andrea. « Privacy and Civic Duty in *R v Ward* : The Right to Online Anonymity and the *Charter*-Compliant Scope of Voluntary Cooperation with Police Requests » (2013), 39 *Queen's L.J.* 301.

Tene, Omer. « What Google Knows : Privacy and Internet Search Engines », [2008] *Utah L. Rev.* 1433.

POURVOI contre un arrêt de la Cour d'appel de l'Alberta (les juges Veldhuis, Schutz et Crighton), 2022 ABCA 208, 55 Alta. L.R. (7th) 76, 509 C.R.R. (2d) 213, [2023] 5 W.W.R. 51, [2022] A.J. No. 738 (Lexis), 2022 CarswellAlta 1454 (WL), qui a confirmé une décision de la juge Ho, 2020 ABQB 70, 10 Alta. L.R. (7th) 103, 453 C.R.R. (2d) 347, [2020] A.J. No. 135 (Lexis), 2020 CarswellAlta 174 (WL). Pourvoi accueilli, le juge en chef Wagner et les juges Côté, Rowe et O'Bonsawin sont dissidents.

Heather Ferg et *Sarah Rankin*, pour l'appelant.

Rajbir Dhillon, pour l'intimé.

David W. Schermbrucker et *Allyson Ratsoy*, pour l'intervenante la directrice des poursuites pénales.

Andrew Hotke, pour l'intervenant le procureur général de l'Ontario.

Micah B. Rankin et *Michael Barrenger*, pour l'intervenant le procureur général de la Colombie-Britannique.

Anil K. Kapoor et *Cameron Cotton O'Brien*, pour l'intervenante l'Association canadienne des libertés civiles.

Daniel J. Song, c.r., et *Vibert M. Jack*, pour l'intervenante British Columbia Civil Liberties Association.

Version française du jugement des juges Karakatsanis, Martin, Kasirer, Jamal et Moreau rendu par

LA JUGE KARAKATSANIS —

I. Introduction

[1] Internet a grandement modifié l'expérience humaine, qui est passée des espaces physiques au cyberespace. Il en est venu à englober des places publiques, des bibliothèques, des marchés, des banques, des cinémas et des salles de concert, étant devenu l'objet culturel le plus vaste créé par notre espèce. Tout comme notre centre commercial et notre hôtel de ville, Internet est devenu pour bon nombre d'entre nous un fidèle compagnon, par l'entremise duquel nous confions nos espoirs, nos aspirations et nos craintes. Les gens utilisent Internet non pas seulement pour trouver des recettes,

payer des factures ou se faire indiquer le chemin à prendre, mais aussi pour explorer leur sexualité, planifier leur avenir et trouver l'amour.

[2] Ces nouvelles réalités ont forcé les tribunaux à se colleter avec « une multitude de questions inédites et épineuses à l'égard de la protection de la vie privée » (*R. c. Spencer*, 2014 CSC 43, [2014] 2 R.C.S. 212, par. 1). Dans *Spencer*, notre Cour a jugé qu'une attente raisonnable au respect de la vie privée s'applique aux renseignements relatifs à l'abonné — les nom, adresse et coordonnées — associés à l'adresse de protocole Internet (IP) d'une personne. Une demande de l'État en vue d'obtenir ces renseignements constitue une « fouille » ou « perquisition » au sens de l'art. 8 de la *Charte canadienne des droits et libertés*.

[3] Le présent pourvoi porte sur la question de savoir si une adresse IP elle-même suscite une attente raisonnable au respect de la vie privée. La réponse doit être affirmative.

[4] Une adresse IP est un numéro d'identification unique. De telles adresses identifient une activité connectée à Internet et permettent le transfert d'information d'une source à une autre. Elles sont nécessaires pour accéder à Internet. Une adresse IP identifie la source de toute activité en ligne et relie cette activité (au moyen d'un modem) à un endroit donné. De plus, le fournisseur de services Internet (FSI) conserve les renseignements relatifs à l'abonné qui se rattachent à chaque adresse IP.

[5] Cependant, comme les adresses IP sont composées de chiffres que le FSI peut habituellement changer sans préavis, la Couronne fait valoir — et les juges majoritaires de la Cour d'appel sont aussi de cet avis — qu'une adresse IP ne suscite pas une attente raisonnable au respect de la vie privée. En l'espèce, la Couronne soutient que la police ne recherchait rien de plus que l'ensemble de chiffres qui lui permettrait ultimement d'obtenir l'ordonnance de communication envisagée par l'arrêt *Spencer*. Par conséquent, la Couronne estime que l'État n'a pas porté atteinte au droit de l'appelant au respect de sa vie privée parce que l'arrêt *Spencer* protégeait suffisamment ses renseignements personnels.

[6] Soit dit en tout respect, je ne suis pas d'accord. Cette analyse est contraire à la jurisprudence de notre Cour concernant l'art. 8 de la *Charte*. Nous n'avons jamais abordé la question du respect de la vie privée fragment par fragment, en fonction de l'intention déclarée de la police d'utiliser d'une seule façon les renseignements qu'elle recueille. Le droit à la protection contre les fouilles, les perquisitions et les saisies abusives, comme tous les droits garantis par la *Charte*, doit recevoir une interprétation large et téléologique, qui reflète son origine constitutionnelle. Depuis l'arrêt *Hunter c. Southam Inc.*, [1984] 2 R.C.S. 145, nous avons conclu que l'art. 8 vise à empêcher les violations de la vie privée, plutôt qu'à condamner ou à admettre des violations eu égard à l'utilisation que fait ultimement l'État de ces renseignements. Le droit à la vie privée, une fois qu'il y a été porté atteinte, ne peut pas être rétabli.

[7] À cette fin, notre Cour a appliqué un critère normatif aux attentes raisonnables au respect de la vie privée. Nous avons défini l'art. 8 sous l'angle de ce que *devrait* être le droit à la vie privée — dans une société libre, démocratique et ouverte — en mettant en balance le droit d'une personne de ne pas être importunée et l'insistance que met la collectivité sur la protection. Ce critère normatif exige que nous appliquions une approche large et fonctionnelle à l'objet de la fouille, et que nous nous concentrions sur le *risque* qu'elle révèle des renseignements d'ordre personnel ou biographique (*R. c. Marakah*, 2017 CSC 59, [2017] 2 R.C.S. 608, par. 32).

[8] L'intimité informationnelle est une question particulièrement cruciale — et particulièrement difficile. Notre jurisprudence reconnaît que les ordinateurs sont uniques et présentent des risques en matière de vie privée qui diffèrent des risques traditionnellement visés par l'art. 8. La Cour a donc jugé que l'art. 8 empêche généralement la police de saisir un ordinateur sans mandat — même si l'appareil lui-même ne fournit aucun renseignement en l'absence d'une autorisation judiciaire de fouiller son contenu — parce que la saisie de l'ordinateur donne à l'État le moyen d'obtenir accès à son contenu (*R. c. Reeves*, 2018 CSC 56, [2018] 3 R.C.S. 531, par. 34).

[9] Considérer l'objet de la présente fouille comme une chaîne abstraite de chiffres utilisée uniquement pour obtenir un mandat de type *Spencer* va à l'encontre de ces précédents. Les adresses IP ne sont pas simplement des numéros dénués de sens. En tant que lien qui relie une activité Internet à un endroit donné, les adresses IP sont

plutôt susceptibles de révéler des renseignements très personnels — y compris l'identité de l'utilisateur de l'appareil — sans jamais faire naître l'obligation d'un mandat. L'activité en ligne précise associée à la fouille effectuée par l'État peut elle-même tendre à révéler des renseignements très privés. Lorsqu'elle est mise en corrélation avec d'autres renseignements en ligne qui y sont associés, comme ceux que fournissent de leur plein gré des sociétés privées ou que recueille autrement l'État, une adresse IP peut révéler un éventail d'activités en ligne très personnelles. De plus, lorsqu'elle est associée aux profils créés et conservés par des tiers du secteur privé, les risques en matière de vie privée liés aux adresses IP augmentent de façon exponentielle. L'information que recueillent, agrègent et analysent ces tiers leur permet de répertorier nos renseignements biographiques les plus intimes. Considérée de manière normative et dans son contexte, une adresse IP est le premier fragment numérique qui peut mener l'État sur la trace de l'activité Internet d'une personne. Elle est susceptible de révéler des renseignements personnels bien avant qu'un mandat de type *Spencer* ne soit sollicité.

[10] De plus, Internet a concentré cette masse d'information auprès de tiers du secteur privé dont les activités ne tombent pas sous le coup de la *Charte*. Ainsi, Internet a fondamentalement modifié la topographie de l'intimité informationnelle sous le régime de la *Charte* en introduisant des tiers médiateurs entre la personne et l'État — des médiateurs qui ne sont pas eux-mêmes assujettis à la *Charte*. Des sociétés privées répondent à des demandes fréquentes des forces de l'ordre et peuvent fournir de leur plein gré toute l'activité associée à l'adresse IP demandée. Des entreprises citoyennes

privées peuvent fournir de leur plein gré des profils granulaires de l'activité Internet d'un utilisateur individuel pendant des jours, des semaines ou des mois sans jamais tomber sous le coup de la *Charte*. Cette information peut toucher au cœur de l'ensemble des renseignements biographique d'un utilisateur et peut ultimement être reliée à l'identité d'un utilisateur, avec ou sans un mandat de type *Spencer*. Il s'agit d'une atteinte très grave à la vie privée.

[11] L'intérêt légitime de la société au respect de la vie privée entre en balance avec son intérêt légitime dans « [l]a répression du crime et la sécurité » (*R. c. Tessling*, 2004 CSC 67, [2004] 3 R.C.S. 432, par. 17). Bien que le droit de ne pas être importuné doive suivre l'évolution technologique, la manière de commettre un crime et d'enquêter sur celui-ci évolue également. La facilité d'accès à Internet et l'anonymat de l'utilisateur se conjuguent pour faciliter la perpétration d'un crime et mettent à rude épreuve l'application efficace de la loi. Il est clair que la nature particulièrement insidieuse d'un grand nombre de cybercrimes, y compris la pornographie juvénile et le leurre d'enfant, pose un préjudice social grave et urgent. La police doit disposer des outils nécessaires pour enquêter sur ces crimes. De plus, lorsqu'une adresse IP (ou l'information relative à l'abonné) est clairement liée à un crime — comme elle peut manifestement l'être dans le cas de la pornographie juvénile ou du leurre d'enfant —, une autorisation judiciaire préalable est facile à obtenir. Une ordonnance de communication d'une adresse IP exigerait peu de renseignements de plus que ce que la police doit déjà fournir pour obtenir un mandat de type *Spencer*. Tant l'intérêt de la société à l'application efficace de la loi que son intérêt à la protection des droits à

l'intimité informationnelle de tous les Canadiens et les Canadiennes doivent être respectés et mis en balance.

[12] Tout bien pesé, le fardeau qu'impose à l'État le fait de reconnaître une attente raisonnable au respect de la vie privée à l'égard des adresses IP n'est pas lourd. Cette reconnaissance ajoute une autre étape aux enquêtes criminelles en exigeant que l'État démontre l'existence de motifs pour porter atteinte à la vie privée en ligne. Cependant, à l'ère des télémandats, cet obstacle est facilement surmonté lorsque la police recherche l'adresse IP dans le cadre de l'enquête sur une infraction criminelle. La protection conférée par l'art. 8 laisserait la police suivre une activité Internet liée à ses objectifs d'application de la loi tout en l'empêchant de demander librement l'adresse IP associée à une activité en ligne *non* liée à l'enquête. La surveillance judiciaire enlèverait également aux sociétés privées le pouvoir de décider s'il convient de révéler des renseignements — et en quelle quantité — et renverrait la question au champ d'application de la *Charte*.

[13] En tant qu'élément inhérent crucial dans la structure d'Internet, une adresse IP est la clé susceptible de guider l'État dans le labyrinthe de l'activité Internet d'un utilisateur ainsi que le lien par lequel des intermédiaires peuvent fournir de leur plein gré à l'État des renseignements relatifs à cet utilisateur. Par conséquent, l'art. 8 devrait protéger les adresses IP. Cela aurait pour effet de préserver le premier « fragment numérique » et d'obscurcir la trace du parcours d'un internaute dans le cyberespace; cela aurait également pour effet de favoriser la réalisation de l'objectif de l'art. 8

consistant à empêcher les possibles atteintes à la vie privée plutôt que de circonscrire sa portée suivant les intentions déclarées de l'État quant à la manière dont il utilisera cette clé.

[14] Je suis d'avis d'accueillir le pourvoi. Il existe une attente raisonnable au respect de la vie privée à l'égard d'une adresse IP. Une demande d'adresse IP faite par l'État constitue une fouille.

II. Contexte

[15] L'appelant, Andrei Bykovets, a été déclaré coupable de 14 infractions d'utilisation de données de carte de crédit non autorisées pour l'achat de cartes-cadeaux en ligne, d'utilisation de ces cartes-cadeaux pour des achats effectués en magasin, et de possession de matériel lié à la fraude par carte de crédit.

[16] Au cours de l'enquête qu'a menée le Service de police de Calgary sur les achats en ligne frauduleux effectués auprès d'un magasin de vins et spiritueux, la police a appris que les ventes en ligne du magasin étaient gérées par Moneris, une société tierce de traitement des paiements. La police a communiqué avec Moneris pour obtenir les adresses IP utilisées pour les opérations, et l'entreprise en a volontairement signalé deux. La police a par la suite obtenu une ordonnance de communication obligeant le FSI des adresses à révéler les renseignements relatifs à l'abonné — le nom et l'adresse du client — pour chaque adresse IP, comme l'exige l'arrêt *Spencer*. L'une d'elles était enregistrée au nom de l'appelant et l'autre à celui de son père.

[17] La police a ensuite utilisé ces renseignements pour solliciter et exécuter des mandats de perquisition visant les adresses résidentielles de l'appelant et de son père. L'appelant a été arrêté, a été déclaré coupable après la tenue d'un procès, et ses déclarations de culpabilité ont été confirmées en appel.

[18] Avant le procès, l'appelant a allégué que la demande faite par la police à Moneris avait violé son droit à la protection contre les fouilles, les perquisitions et les saisies abusives garanti par l'art. 8 de la *Charte*. La question clé au voir-dire était celle de savoir si l'appelant avait une attente raisonnable au respect de sa vie privée à l'égard de son adresse IP.

[19] L'avocat de la défense a soumis le rapport d'un enquêteur judiciaire contenant un résumé technique des adresses IP et de leurs rôles. Le rapport indique qu'il y a des adresses IP internes et des adresses IP externes. Les adresses IP externes sont utilisées pour transférer de l'information d'une source à une autre sur Internet au moyen d'un modem loué du FSI. L'adresse IP externe ressemble beaucoup à l'adresse municipale de la maison d'une personne. Sans celle-ci, un utilisateur ne peut ni envoyer ni recevoir de données. Un modem ou un routeur attribue également une adresse IP interne à chaque appareil sur un réseau local, ce qui correspond à peu près aux différentes pièces d'une maison.

[20] Les adresses IP peuvent également être statiques ou dynamiques. La plupart d'entre elles sont dynamiques, ce qui signifie que le FSI peut changer l'adresse IP externe d'un utilisateur sans préavis et pour différentes raisons. Le FSI tient un

registre indiquant à quel abonné chaque adresse IP externe a été attribuée et pour quelle période.

[21] Il est possible de déterminer le FSI d'un utilisateur en entrant son adresse IP dans un site Web de recherche d'adresse IP. La police peut par la suite demander au FSI de lui fournir les renseignements relatifs à l'abonné à qui l'adresse IP a été attribuée, comme le prévoit l'arrêt *Spencer*. Cela dit, l'expert a expliqué qu'il est toujours possible de prendre des mesures pour déterminer l'identité d'un utilisateur, sans avoir recours au FSI, au moyen des renseignements enregistrés sur le site Web d'une société tierce. Des sociétés tierces, comme Google ou Facebook, peuvent suivre les adresses IP externes de chaque utilisateur qui visite leur site et enregistrer ces renseignements à divers degrés. Ces sociétés peuvent déterminer l'identité de ces utilisateurs individuels en fonction de leur activité Internet sur leur site (rapport d'expertise, reproduit au d.a., p. 311). L'effet est amplifié lorsque des renseignements de multiples sites sont recueillis (p. 312).

[22] Par conséquent, de l'avis de l'expert, si ceux qui cherchent à identifier un internaute particulier ont accès aux renseignements enregistrés par des sociétés tierces, [TRADUCTION] « il n'est pas nécessaire d'obtenir les renseignements relatifs à l'abonné détenus par le FSI pour identifier correctement un internaute particulier » (p. 312).

III. Décisions des juridictions inférieures

A. *Cour du Banc de la Reine de l'Alberta, 2020 ABQB 70, 10 Alta. L.R. (7th) 103 (la juge Ho)*

[23] La juge du procès a conclu que la demande faite par la police à Moneris ne constituait pas une fouille au sens de l'art. 8 de la *Charte* parce que l'appelant n'avait pas une attente raisonnable au respect de sa vie privée à l'égard de son adresse IP. Eu égard aux facteurs énoncés par notre Cour dans *Tessling*, elle a défini l'objet de la prétendue fouille comme étant les adresses IP recherchées pour faire avancer l'enquête. Elle a examiné le rapport d'expertise et a estimé qu'à elles seules, les adresses IP n'établissent pas un lien avec, ni ne fournissent aucune autre information sur, un internaute (par. 44).

[24] Par conséquent, l'attente subjective de l'appelant au respect de sa vie privée à l'égard de son adresse IP n'était pas raisonnable parce que l'adresse en question ne révélait pas un « ensemble de renseignements biographiques d'ordre personnel » sans accès au site Web d'un tiers (par. 56). La juge du procès a considéré qu'il n'y avait [TRADUCTION] « guère à gagner d'un point de vue normatif » au fait d'« exiger de la police qu'elle sollicite une autorisation judiciaire » lorsqu'elle accède à l'adresse IP elle-même plutôt que lorsqu'elle accède aux renseignements relatifs à l'abonné liés à cette adresse IP (par. 64, citant *Spencer*).

B. *Cour d'appel de l'Alberta, 2022 ABCA 208, [2023] 5 W.W.R. 51 (les juges Schutz et Crighton, la juge Veldhuis, dissidente)*

[25] Les juges majoritaires de la Cour d'appel ont rejeté l'appel, en grande partie pour les motifs exposés par la juge du procès. Les juges Schutz et Crighton ont convenu que l'appelant n'avait aucune attente raisonnable au respect de sa vie privée à l'égard de son adresse IP parce que, prise isolément, cette adresse ne révèle rien sur le mode de vie ou les renseignements biographiques d'une personne. Le peu d'information qu'a communiqué l'adresse IP a été supplanté par [TRADUCTION] « des préoccupations légitimes tout aussi valables » : « . . . la répression du crime et la sécurité . . . » (par. 22).

[26] La juge Veldhuis, dissidente, aurait accueilli l'appel au motif que la juge du procès n'a pas [TRADUCTION] « entrepris son analyse en tenant compte de l'approche normative » (par. 62). Qualifié adéquatement, l'objet de la fouille n'était pas l'adresse IP elle-même, mais [TRADUCTION] « l'identité d'un internaute qui correspond à une adresse IP particulière liée à une activité Internet particulière sous surveillance » (par. 77).

[27] La juge Veldhuis a conclu que l'attente de l'appelant au respect de sa vie privée à l'égard de l'objet de la fouille était raisonnable. Une personne ayant communiqué des données financières pour effectuer un achat en ligne s'attendrait à ce que l'adresse IP utilisée demeure privée, et ce renseignement était de nature privée parce qu'il était susceptible d'identifier un internaute [TRADUCTION] « sans aucune exigence de soupçons ou de motifs raisonnables étayant une autorisation judiciaire » (par. 88). Par conséquent, une attente raisonnable au respect de la vie privée

s'appliquait à ces adresses IP parce que [TRADUCTION] « celles-ci étaient liées à une activité Internet particulière sous surveillance qui était susceptible de révéler des renseignements biographiques » (par. 94).

IV. Analyse

[28] Le présent pourvoi soulève une seule question : Une attente raisonnable au respect de la vie privée s'applique-t-elle à une adresse IP? À mon avis, la réponse est affirmative. Comme je vais l'expliquer, une adresse IP est le lien crucial entre un internaute et son activité en ligne. Par conséquent, la présente fouille avait pour objet les renseignements que les adresses IP en cause pouvaient révéler sur des internautes précis, y compris, ultimement, leur identité. Conclure que l'art. 8 ne vise pas une adresse IP parce que la police l'a recueillie uniquement pour obtenir un mandat de type *Spencer* ne tient aucun compte des renseignements qu'elle *peut* révéler sans mandat. Une telle analyse reflète un raisonnement fragment par fragment, fondé sur la manière dont l'État entend utiliser l'information dans une situation donnée, ce qui est contraire à l'approche large et téléologique que requiert le statut constitutionnel de l'art. 8. L'analyse ne peut pas non plus se limiter aux intérêts en matière de vie privés touchés par ce qu'est susceptible de révéler l'adresse IP *à elle seule*, sans qu'il ne soit tenu compte de ce qu'elle est susceptible de révéler lorsque combinée à d'autres renseignements disponibles, en particulier auprès de sites Web de tiers. Considérée de manière normative, une adresse IP est la clé donnant accès à l'activité Internet d'un utilisateur et, ultimement, à son identité, de sorte qu'elle suscite une attente raisonnable

au respect de la vie privée. S'il doit protéger de manière significative la vie privée en ligne des Canadiens et des Canadiennes dans le monde actuel qui est très largement numérique, l'art. 8 doit protéger leurs adresses IP.

A. *Cadre juridique*

[29] L'article 8 de la *Charte* garantit le « droit à la protection contre les fouilles, les perquisitions ou les saisies abusives ». Il vise principalement à protéger la vie privée ou le droit individuel « de ne pas être importuné » (*R. c. Edwards*, [1996] 1 R.C.S. 128, par. 67). Le respect de la vie privée d'un individu est essentiel pour assurer la dignité, l'autonomie et la croissance personnelle de celui-ci (*R. c. Jones*, 2017 CSC 60, [2017] 2 R.C.S. 696, par. 38). La protection de sa vie privée est une condition préalable essentielle à l'épanouissement d'une démocratie libre et en santé.

[30] Pour établir une violation de l'art. 8, le demandeur doit démontrer qu'il y a eu une fouille, une perquisition ou une saisie, et que la fouille, la perquisition ou la saisie était abusive. Seule la première exigence — si la demande des adresses IP constituait une fouille — est en cause en l'espèce.

[31] 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 (*Hunter*, p. 159-160). Les tribunaux

analysent l'attente au respect de la vie privée en examinant de nombreux facteurs interreliés, mais souvent concurrents, qui peuvent être regroupés en quatre catégories : (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 subjective au respect de la vie privée était objectivement raisonnable (*Spencer*, par. 18, citant *Tessling*, par. 32).

[32] La présente affaire porte sur l'intimité informationnelle, ou [TRADUCTION] « le droit revendiqué par des particuliers, des groupes ou des institutions de déterminer eux-mêmes le moment, la manière et la mesure dans lesquels des renseignements les concernant sont communiqués » (*Tessling*, par. 23, citant A. F. Westin, *Privacy and Freedom* (1970), p. 7). Autrement dit, cet aspect du droit à la vie privée concerne « l'autodétermination informationnelle » (*Jones*, par. 39).

[33] Les parties conviennent que l'appelant avait un intérêt direct à l'égard des adresses IP ainsi qu'une attente subjective au respect de sa vie privée à l'égard de leur contenu informationnel. Dans les sections qui suivent, je me penche sur l'objet de la fouille et sur la question de savoir si l'attente de l'appelant au respect de sa vie privée à l'égard de cet objet était raisonnable.

B. *L'objet de la fouille*

[34] Examiner l'objet de la prétendue fouille permet au tribunal de déterminer les intérêts en matière de vie privée qui sont en cause (*Spencer*, par. 22). Une question

directrice lorsqu'il s'agit de définir l'objet de la prétendue fouille consiste à établir [TRADUCTION] « ce que la police recherchait vraiment » (*Marakah*, par. 15, citant *R. c. Ward*, 2012 ONCA 660, 112 O.R. (3d) 321, par. 67). Le tribunal doit concevoir l'objet de la fouille d'un point de vue holistique. L'approche ne doit pas être mécanique et doit tenir compte de la réalité technologique (*Spencer*, par. 26 et 31; *Marakah*, par. 17).

[35] En l'espèce, l'appelant nous demande d'adopter la façon dont la juge dissidente a qualifié l'objet. Ce que la police recherchait vraiment, affirme-t-il, était [TRADUCTION] « de relier une activité Internet à une personne précise. Obtenir une adresse IP était une étape essentielle pour identifier l'internaute s'étant livré à l'activité Internet précise » (m.a., par. 37).

[36] La Couronne intimée préconise la qualification donnée par la juge du procès et les juges majoritaires de la Cour d'appel. La police [TRADUCTION] « voulait les adresses IP pour faire progresser son enquête » (m.i., par. 53).

[37] À mon avis, la juge du procès et les juges majoritaires de la Cour d'appel ont adopté une description artificiellement étroite de l'objet de cette prétendue fouille. Cette description est incompatible avec l'approche normative suivie dans nos précédents et ne prend pas en compte les intérêts en matière de vie privée qui sont en jeu en l'espèce.

[38] Notre Cour n'a jamais décrit le droit constitutionnel à la vie privée en fonction de l'intention déclarée de l'État, ou d'une utilisation particulière des

renseignements. Nous avons plutôt systématiquement adopté une approche large et fonctionnelle à l'égard de l'objet de la fouille, « en examinant le lien entre la technique d'enquête utilisée par la police et l'intérêt en matière de vie privée qui est en jeu » (*Spencer*, par. 26). L'objet est défini sous l'angle non pas seulement des renseignements eux-mêmes, mais également de « la tendance qui consiste à chercher à obtenir des renseignements pour permettre d'en tirer des inférences au sujet d'autres renseignements qui, eux, sont de nature personnelle » (par. 31). Dans l'arrêt *Marakah*, par exemple, la question était de savoir si l'expéditeur d'un message texte a une attente raisonnable au respect de sa vie privée à l'égard de ce message dans l'appareil du destinataire. S'exprimant au nom des juges majoritaires, la juge en chef McLachlin a statué que l'objet de la fouille n'était pas le téléphone du destinataire, ni même le message texte lui-même, mais une « conversation électronique » y compris « toute inférence que l'on peut tirer de ces renseignements quant aux fréquentations et aux activités » (par. 20).

[39] Les tribunaux doivent être particulièrement prudents lorsqu'ils décrivent l'objet d'une fouille relative à des données électroniques (*Marakah*, par. 14). Dans *R. c. Cole*, 2012 CSC 53, [2012] 3 R.C.S. 34, où la police avait examiné le contenu d'un ordinateur, notre Cour a décrit l'objet de la prétendue fouille comme étant « les données, ou le *contenu informationnel* [. . .] de l'ordinateur portatif, [. . .] non pas [l'appareil] lui-même » (par. 41 (en italique dans l'original)).

[40] De même, dans l'arrêt *Reeves*, où la police avait saisi l'ordinateur domestique partagé de l'appelant, la fouille ne visait pas uniquement l'ordinateur lui-même, mais « ultimement, les données qu'il renfermait sur l'utilisation de M. Reeves, y compris les fichiers auxquels il avait accédé et ceux qu'il avait sauvegardés et supprimés » (par. 30). L'État a fait intervenir l'art. 8 en saisissant l'ordinateur *même si* la police avait besoin d'un mandat pour fouiller son contenu, parce que la saisie a été pour la police « le moyen d'obtenir accès à [d]es renseignements [de nature éminemment personnelle] » (par. 34).

[41] C'est la même chose en l'espèce. La police ne « recherchait [pas] vraiment » les adresses IP dans l'abstrait. En tant qu'« ensemble de chiffres », une adresse IP n'est d'aucun intérêt pour la police. Cette dernière recherchait plutôt les renseignements qu'une adresse IP tend à révéler sur un internaute précis, y compris son activité en ligne et, ultimement, son identité « en tant que source, possesseur ou utilisateur des renseignements visés » (*Spencer*, par. 47). Constituant l'identifiant d'une activité connectée à Internet provenant d'un endroit donné, l'adresse IP est un outil puissant qui permet à l'État — avec ou sans un autre mandat — de recueillir l'activité Internet d'un utilisateur pendant la période où une adresse IP particulière est liée à cette source. Par conséquent, comme dans l'affaire *Reeves*, l'adresse IP a fourni à l'État le *moyen* de tirer des inférences immédiates et directes sur l'utilisateur derrière une activité Internet précise. Les renseignements inférés d'une activité Internet sur un appareil peuvent être très personnels, y compris en liant cette activité à l'identité d'un utilisateur particulier (voir *Spencer*, par. 47).

[42] Cette description constitue une conception large et fonctionnelle de l'objet. En « se gard[ant] [. . .] à juste titre de toute approche mécanique qui définirait l'objet en fonction d'actes matériels, de lieux physiques ou de modalités de transmission [informationnelle] », elle « tient [. . .] compte de la réalité technologique » (*Marakah*, par. 17). Cette description n'étend pas le bouclier protecteur de la *Charte* à toutes les étapes d'une enquête. Elle confirme plutôt que les techniques d'enquête qui révèlent des renseignements qui semblent inoffensifs doivent tout de même être examinées par rapport aux intérêts en matière de vie privée qui sont en jeu (*Spencer*, par. 26) Reconnaître que la police voulait l'adresse IP — en tant que lien entre un abonné et un endroit donnés et une activité Internet particulière — pour obtenir davantage de renseignements sur l'utilisateur permet au tribunal d'apprécier l'attente au respect de la vie privée à l'égard de *tous* les renseignements que cette adresse IP « ten[d] à révéler » (*Spencer*, par. 27 (soulignement dans l'original), citant *R. c. Plant*, [1993] 3 R.C.S. 281, p. 293), et donc en [TRADUCTION] « t[enant] compte de la nature des droits en matière de vie privée auxquels l'action de l'État pourrait porter atteinte » (*Marakah*, par. 15, citant *Ward*, par. 65 (je souligne)).

[43] Par conséquent, l'objet de la prétendue fouille en l'espèce est une adresse IP en tant que clé permettant d'obtenir davantage de renseignements sur un internaute particulier, y compris son activité en ligne et, ultimement, son identité en tant que source de ces renseignements. Dans la présente affaire, la police a cherché à obtenir ces renseignements au moyen d'une ordonnance de communication telle que l'envisage l'arrêt *Spencer*. Cependant, comme l'indique le rapport d'expertise, un mandat de type

Spencer ne constitue pas la seule façon dont une adresse IP peut révéler des détails intimes sur le mode de vie et les choix personnels d'un internaute. L'activité en ligne associée à l'adresse IP peut elle-même révéler des renseignements très personnels sans les mesures de protection relatives à l'autorisation judiciaire préalable. Je passe maintenant à cette question.

C. *L'attente au respect de la vie privée était-elle raisonnable?*

[44] L'article 8 est mis en jeu uniquement lorsqu'une attente subjective au respect de la vie privée est objectivement raisonnable. La question, dans tous les cas, est celle de savoir « si, dans une situation donnée, le droit du public de ne pas être importuné par le gouvernement doit céder le pas au droit du gouvernement de s'immiscer dans la vie privée des particuliers afin de réaliser ses fins et, notamment, d'assurer l'application de la loi » (*Hunter*, p. 159-160).

[45] Les tribunaux doivent trancher cette question eu égard à l'ensemble des circonstances. Bien qu'il n'existe pas de liste définitive de facteurs (*Cole*, par. 45), les tribunaux ont souvent examiné plus particulièrement le contrôle sur l'objet exercé par le demandeur, le lieu de la fouille et le caractère privé de l'objet (voir, p. ex., *Marakah*, par. 24).

(1) Contrôle sur l'objet

[46] Dans le contexte de l'intimité informationnelle, le contrôle exercé par le demandeur sur l'objet n'est pas déterminant (*Reeves*, par. 38). L'autodétermination au cœur de l'intimité informationnelle signifie qu'une personne « peut [. . .] choisir de divulguer certains renseignements soit pour une fin précise, soit encore à une catégorie restreinte de personnes, et néanmoins conserver une attente raisonnable au respect de sa vie privée » (*Jones*, par. 39). L'anonymat est une conception particulièrement importante du droit à la vie privée quand il est question d'Internet (*Spencer*, par. 45, citant Westin, p. 32).

[47] Notre approche diffère de celle des États-Unis, où ce qu'on appelle la [TRADUCTION] « doctrine du tiers » exclut l'attente raisonnable au respect de la vie privée « si les renseignements sont détenus ou connus par des tiers » (T. Panneck, « Incognito Mode Is in the Constitution » (2019), 104 *Minn. L. Rev.* 511, p. 520, citant D. J. Solove, « A Taxonomy of Privacy » (2006), 154 *U. Pa. L. Rev.* 477, p. 528). Notre Cour a rejeté l'approche américaine très tôt dans sa jurisprudence relative à l'art. 8 (*R. c. Dyment*, [1988] 2 R.C.S. 417, p. 429-430, le juge La Forest).

[48] Le caractère non déterminant du contrôle dans notre analyse est particulièrement pertinent en ce qui concerne Internet, qui exige que les utilisateurs révèlent à leur FSI les renseignements relatifs à l'abonné pour pouvoir prendre part aux activités de cette nouvelle place publique. Comme nous l'avons affirmé dans l'arrêt *Jones*, « la seule façon qu'avait l'intéressé de conserver, vis-à-vis du fournisseur de services, un contrôle sur l'objet de la fouille, était de s'abstenir complètement d'utiliser

ses services. Il ne s'agit évidemment pas là d'un véritable choix. [. . .] Les Canadiens n'ont pas à vivre en reclus du monde numérique afin de pouvoir conserver un semblant de vie privée » (par. 45).

(2) Lieu fouillé

[49] Le lieu où s'est déroulée la fouille n'est pas non plus préjudiciable à une attente raisonnable au respect de la vie privée en l'espèce. Ce facteur a été élaboré en grande partie dans le contexte de l'intimité territoriale, et un objet numérique « cadre mal dans les paramètres établis par la jurisprudence » (*Marakah*, par. 27). Comme l'a récemment fait remarquer notre Cour, « les espaces en ligne sont *qualitativement* différents » des espaces physiques (*R. c. Ramelson*, 2022 CSC 44, par. 49 (en italique dans l'original)).

[50] L'architecture d'Internet a mené à un registre permanent large, précis et en continuelle expansion qui est [TRADUCTION] « sans précédent dans notre société » (*R. c. Vu*, 2013 CSC 60, [2013] 3 R.C.S. 657, par. 40 (soulignement dans l'original), citant A. D. Gold, « Applying Section 8 in the Digital World : Seizures and Searches », document préparé pour le 7th Annual Six-Minute Criminal Defence Lawyer (9 juin 2007), par. 3). Les renseignements que renferme Internet peuvent révéler beaucoup plus que ce que sont susceptibles de révéler des renseignements assujettis aux limites d'un espace physique (voir *Vu*, par. 44 et 47). Par conséquent, l'absence d'intrusion physique soulignée par la juge du procès nous renseigne peu sur le caractère raisonnable d'une attente au respect de la vie privée.

(3) Caractère privé de l'objet

[51] L'article 8 vise à « prot[éger] un ensemble de renseignements biographiques d'ordre personnel que les particuliers pourraient, dans une société libre et démocratique, vouloir constituer et soustraire à la connaissance de l'État » (*Plant*, p. 293). L'« ensemble de renseignements biographiques » ne touche pas uniquement à l'identité, mais s'étend « notamment [à] de[s] renseignements tendant à révéler des détails intimes sur le mode de vie et les choix personnels de l'individu » (p. 293).

[52] L'accent mis par l'art. 8 sur les renseignements que les particuliers « pourraient [. . .] vouloir constituer et soustraire à la connaissance de l'État » signifie qu'une attente raisonnable au respect de la vie privée est appréciée de manière normative plutôt que simplement descriptive (*Spencer*, par. 27, citant *Plant*, p. 293). L'approche normative exprime un idéal. « La question à se poser consiste à savoir si le droit à la vie privée revendiqué doit [TRADUCTION] "être considéré comme à l'abri de toute intrusion par l'État — sauf justification constitutionnelle — pour que la société canadienne demeure libre, démocratique et ouverte" » (*Reeves*, par. 28, citant *Ward*, par. 87). Par conséquent, l'art. 8 s'étendra aussi loin que devrait s'étendre le droit à la vie privée pour protéger la dignité, l'autonomie et la croissance personnelle de l'individu, et pas plus. Ou, comme l'a dit le juge d'appel Doherty, reconnaître une attente raisonnable au respect de la vie privée signifie que [TRADUCTION] « la conduite étatique contestée a atteint le stade où les valeurs qui sous-tendent la société canadienne contemporaine dictent que l'État doit respecter la vie privée des individus sauf s'il est

en mesure de justifier sur le plan constitutionnel toute atteinte à cette vie privée personnelle » (*Ward*, par. 82). Cette analyse « abonde [inévitablement] en jugements de valeur énoncés du point de vue indépendant de la personne raisonnable et bien informée, qui se soucie des conséquences à long terme des actions gouvernementales sur la protection du droit au respect de la vie privée » (*R. c. Patrick*, 2009 CSC 17, [2009] 1 R.C.S. 579, par. 14).

[53] Par conséquent, on ne peut apprécier une attente raisonnable au respect de la vie privée, en tant que composante clé de l'art. 8, en fonction d'une seule utilisation en particulier de la preuve. Sa portée ne peut pas non plus être établie selon l'intention précise qu'avait la police en recherchant les renseignements. L'objectif de l'art. 8, apprécié normativement, exige plutôt que nous nous demandions quels renseignements tend à révéler l'objet de la fouille. Comme cette analyse vise à déterminer « si, d'une manière générale, les citoyens ont un droit au respect de leur vie privée » à l'égard de l'objet de la fouille effectuée par l'État, nous examinons non seulement les renseignements que la police cherche à découvrir dans un cas donné, mais aussi tous les renseignements que l'objet peut tendre à révéler (*Patrick*, par. 32).

[54] Ce principe est particulièrement clair en cas de fouille de renseignements numériques. Les ordinateurs sont différents. Ces appareils stockent d'immenses quantités de renseignements — dont certains sont générés automatiquement et conservés à l'insu de l'utilisateur — qui peuvent toucher à l'ensemble de renseignements biographiques d'ordre personnel (*Vu*, par. 41). Ces intérêts en matière

de vie privée peuvent être encore plus manifestes si l'appareil sert à se connecter à Internet (*Cole*, par. 47). En effet, « il est difficile d'imaginer une atteinte plus grave à la vie privée » que les fouilles relatives à l'utilisation d'Internet par une personne (*R. c. Morelli*, 2010 CSC 8, [2010] 1 R.C.S. 253, par. 105).

[55] Les intérêts uniques et accrus en matière de vie privée à l'égard des données d'un ordinateur personnel découlent du *risque* qu'elles dévoilent des renseignements très révélateurs. Dans l'arrêt *Vu*, notre Cour a estimé que la fouille d'un ordinateur doit faire l'objet d'une autorisation expresse préalable parce que les ordinateurs abritent un univers presque illimité d'informations (au par. 41), et que les renseignements liés à l'activité Internet d'un utilisateur « peuvent également permettre aux enquêteurs d'avoir accès à des détails intimes concernant les intérêts, les habitudes et l'identité de l'utilisateur » (par. 42). Même si la police dans cette affaire essayait simplement de savoir qui habitait dans la maison, la Cour a néanmoins conclu que la fouille mettait en jeu des intérêts sérieux en matière de vie privée.

[56] De même, dans *Reeves*, l'intention précise des policiers de fouiller l'ordinateur pour voir s'il contenait de la pornographie juvénile n'a eu aucune incidence sur le caractère sérieux des préoccupations en matière de vie privée qui découlaient de la saisie d'un ordinateur. Au contraire, ces préoccupations résultaient du « caractère personnel ou confidentiel des données conservées grâce à la saisie de l'ordinateur et auxquelles la police pourrait ainsi avoir accès » (par. 33 (je souligne), citant *Marakah*, par. 32). La Constitution devrait assurer une protection contre la saisie d'un ordinateur

parce qu'une telle saisie a été, pour la police, « le moyen d'obtenir accès à [d]es renseignements [de nature éminemment personnelle] » (*Reeves*, par. 34).

[57] L'intention précise des policiers de restreindre l'usage de renseignements dans une affaire donnée — si bien intentionnés qu'ils soient — n'est donc pas pertinente en ce qui a trait à l'art. 8. L'analyse de l'« attente raisonnable au respect de la vie privée » est axée sur le *risque* qu'un objet particulier révèle à l'État l'ensemble des renseignements biographiques d'une personne, et non pas sur la question de savoir si les adresses IP ont révélé des renseignements sur l'appelant *eu égard aux faits*. La juge en chef McLachlin a été explicite à cet égard dans l'arrêt *Marakah*, où elle a écrit que « le risque de divulgation de renseignements privés est un facteur dont il faut tenir compte pour décider si une conversation électronique suscite des attentes raisonnables en matière de respect de la vie privée » (par. 31; voir aussi par. 32). Les messages textes suscitaient donc une attente raisonnable au respect de la vie privée, indépendamment de la question de savoir si les messages textes recherchés révélaient ou non des renseignements au vu des faits de cette affaire.

[58] De plus, en appliquant un critère normatif, il n'est pas utile de mettre l'accent sur l'interprétation la plus étroite de la preuve d'expert. Nous devons plutôt apprécier la preuve en tenant compte du contexte plus large dans lequel elle s'inscrit, et notamment des réalités sociales actuelles et de l'incidence de notre décision dans d'autres circonstances. Notre Cour a fréquemment pris connaissance d'office de ces « faits sociaux » plus larges afin d'« établir le cadre de référence ou le contexte pour

trancher des questions factuelles cruciales pour le règlement d'un litige [. . .] [;] ils contribuent à expliquer certains aspects de la preuve » (*R. c. Spence*, 2005 CSC 71, [2005] 3 R.C.S. 458, par. 57; voir aussi P. W. Hogg et W. K. Wright, *Constitutional Law of Canada* (5e éd. suppl.), § 60:8). À mon avis, il faut prendre en considération l'intrusion sans cesse croissante d'Internet dans nos vies privées pour trancher le présent pourvoi. Il est largement reconnu qu'Internet est omniprésent et qu'un grand nombre d'internautes laissent derrière eux une trace de renseignements que d'autres recueillent à différentes fins, des renseignements qui peuvent être assemblés de manière à révéler des détails profondément privés. De plus, comme l'indique la preuve d'expert, une adresse IP se rattache à toute activité en ligne; il s'agit d'un élément constitutif fondamental de toute utilisation d'Internet. Ce contexte social du monde numérique est nécessaire lorsqu'une approche fonctionnelle est utilisée pour définir l'intérêt en matière de vie privée que confère la *Charte* aux renseignements qu'est susceptible de révéler une adresse IP.

[59] De même, les intervenants jouent un rôle essentiel dans les décisions de notre Cour — non seulement en mettant en évidence les conséquences de décisions juridiques particulières, mais aussi en reflétant la diversité de points de vue sur laquelle repose notre approche normative. [TRADUCTION] « L'acceptation des intervenants reflète le fait que la décision du tribunal sur une question constitutionnelle aura de vastes ramifications publiques, et reconnaît le fait que ceux qui ont des intérêts particuliers qui sont touchés et qui peuvent aider le tribunal devraient être entendus » (R. J. Sharpe et K. Roach, *The Charter of Rights and Freedoms* (7e éd. 2021), p. 128).

[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.

[61] Premièrement, l'activité associée à l'adresse IP peut elle-même être très révélatrice, même avant toute tentative de déterminer l'identité. En l'espèce, l'activité consistait en une série d'opérations financières réalisée au moyen d'un intermédiaire en ligne, Moneris. Lorsqu'elle est reliée à des intermédiaires financiers tels que Moneris ou PayPal, une adresse IP peut révéler toutes les opérations qu'a effectuées un utilisateur sur cet intermédiaire pendant la période où l'adresse IP lui a été assignée.

Par exemple, Moneris a associé cinq opérations en ligne différentes aux adresses IP en question (motifs exposés au terme du voir-dire, par. 7-8).

[62] Ces achats peuvent « diffuser une foule de renseignements personnels susceptibles de révéler des informations biographiques d'ordre personnel sur [l'acheteur] » (*Marakah*, par. 33), allant des restaurants qu'il fréquente, des destinations qu'il visite, de ses passe-temps, aux suppléments alimentaires qu'il utilise. Les internautes peuvent même avoir « un important intérêt en matière de respect de la vie privée en ce qui concerne la seule *existence* de leurs [achats] électroniques », d'autant plus que nos marchés migrent rapidement en ligne (par. 33 (en italique dans l'original)).

[63] D'autres activités en ligne peuvent révéler des renseignements qui touchent directement à l'ensemble des renseignements biographiques d'un utilisateur. Les sites Web qui offrent des services de rencontre ou de la pornographie adulte peuvent donner à l'État une description des préférences sexuelles de l'utilisateur. L'historique d'un internaute dans des salons de cyberbavardage médical, politique, ou autre salon de cyberbavardage semblable, peut révéler ses préoccupations de santé ou ses opinions politiques. Si l'adresse IP n'est pas protégée, ces renseignements sont librement accessibles à l'État sans la protection de la *Charte*, qu'ils aient ou non un rapport avec l'enquête sur un crime donné.

[64] Deuxièmement, 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.

[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. Des décisions tendent à indiquer que des tiers fournissent ces renseignements sans qu'on le leur demande. À titre d'exemple, dans l'affaire *State c. Simmons*, 190 Vt. 141 (2011), la police, après avoir identifié un suspect, a contacté MySpace, un site de média social, et lui a demandé de lui communiquer les adresses IP qui avaient accédé au profil MySpace de celui-ci (par. 3). MySpace a fourni des registres indiquant non seulement les adresses IP elles-mêmes, mais aussi *toutes les fois* que chaque adresse IP s'était connectée au compte MySpace de M. Simmons — notamment le fait qu'une adresse IP s'était connectée au compte [TRADUCTION] « plus de 100 fois sur une période d'une semaine » (par. 3).

[66] Comme l'a expliqué l'expert, les sites Web de tiers peuvent suivre l'adresse IP externe de chaque utilisateur qui visite leur site. Certains sites Web, tels que Google, recueillent également d'énormes quantités d'autres renseignements comme l'historique sur YouTube, les recherches sur Google et l'historique des localisations. Ces renseignements peuvent être de nature extrêmement personnelle.

[67] Beaucoup d'activités en ligne sont exercées de façon anonyme (*Spencer*, par. 48; *Ward*, par. 75). Les gens agissent de manière différente en ligne qu'ils ne le feraient en personne (*Ramelson*, par. 5). « Certains lieux en ligne, tels les moteurs de

recherche, permettent aux gens d'explorer des notions qu'ils hésiteraient à évoquer en public; d'autres, comme les médias sociaux, permettent aux utilisateurs de se dissimuler derrière la façade de leur choix » (par. 46). Nous ne voudrions pas que les profils de médias sociaux auxquels nous nous attardons parviennent à la connaissance de l'État. Nous ne voudrions pas non plus que la version intimement privée de nous-mêmes révélée par l'ensemble de termes clés que nous avons récemment entrés dans un moteur de recherche se répande dans le monde hors ligne. Les internautes devraient pouvoir s'attendre à ce que l'État n'obtienne pas ces renseignements sans un fondement constitutionnel valable.

[68] Enfin, 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. L'expert utilise l'exemple d'une adresse IP qui se connecte à un profil de média social en particulier ou d'un compte de courriel qui contient des renseignements permettant d'inférer l'identité de l'utilisateur, comme son nom. À partir de là, une petite inférence suffit pour découvrir l'identité de l'utilisateur. Il ne suffit pas d'affirmer — comme le fait l'avocate de la Couronne — qu'un mandat de type *Spencer* est requis si l'adresse IP est recherchée à l'égard de renseignements susceptibles de dévoiler l'identité de l'internaute. Il ne peut revenir à la police ou à des sociétés privées de déterminer si les renseignements fournis sur le site Web auront pour effet (peut-être s'ils sont combinés à d'autres renseignements) d'aider à identifier la source de l'activité ou l'identité de l'utilisateur, ou encore de compromettre autrement des intérêts en matière de vie privée.

[69] L'affirmation selon laquelle un mandat de type *Spencer* assure une protection contre les préoccupations en matière de vie privée que soulèvent les adresses IP n'est donc tout simplement pas étayée par les réalités technologiques modernes. Les adresses IP jouent un rôle crucial dans la structure inhérente d'Internet. Elles sont le moyen par lequel les appareils connectés à Internet envoient et reçoivent des données. Elles sont donc la clé donnant accès à l'activité en ligne d'un internaute — les premiers [TRADUCTION] « fragments numériques » sur la trace cybernétique de l'utilisateur (*Jones*, par. 42, citant S. Magotiaux, « Out of Sync : Section 8 and Technological Advancement in Supreme Court Jurisprudence » (2015), 71 *S.C.L.R.* (2d) 501, p. 502). 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 (*Morelli*, par. 3). 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.

[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*, par. 32; *Spencer*, par. 27).

(4) La balance penche-t-elle en faveur d'une attente raisonnable au respect de la vie privée?

[71] Définir une attente raisonnable au respect de la vie privée est une opération de mise en balance. Les particuliers ont le droit de revendiquer leur droit de ne pas être

importunés par l'État. « En même temps, la vie économique et sociale crée des demandes concurrentes. Les citoyens tiennent à leur vie privée, mais ils veulent également être protégés » (*Tessling*, par. 17).

[72] En l'espèce, 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. Je m'explique.

[73] Internet a fait augmenter de manière exponentielle tant la qualité que la quantité de renseignements stockés à propos des internautes, et il englobe les comportements humains les plus publics comme les plus privés (*Ramelson*, par. 45). Ces renseignements sont fortement centralisés, sont aisément accessibles, et [TRADUCTION] « ne sont pas filtrés par la mémoire et la motivation humaines, mais peuvent être produits en tant que copie de leur forme originale » (L. M. Austin, « Technological Tattletales and Constitutional Black Holes : Communications Intermediaries and Constitutional Constraints » (2016), 17 *Theoretical Inquiries L.* 451, p. 457). Les renseignements, autrefois révélés à l'État fragment par fragment, peuvent maintenant être « compilé[s], disséqué[s] et analysé[s] afin de mieux comprendre qui nous sommes en tant qu'individus ou en tant que populations » (*Ramelson*, par. 48). Une adresse IP se rattache à chacun de ces fragments. C'est la clé qui les relie l'un à l'autre.

[74] Même les [TRADUCTION] « renseignements qui peuvent à première vue sembler banals et ne pas faire partie de l'ensemble des renseignements biographiques peuvent être profondément révélateurs lorsqu'on les met en contexte avec d'autres points de données » (N. Hasan et autres, *Search and Seizure* (2021), p. 59). L'agrégation [TRADUCTION] « crée des synergies. Analysés, les renseignements agrégés peuvent révéler sur une personne de nouveaux faits qu'elle ne s'attendait pas à ce qu'on sache à son sujet quand les données originales isolées ont été recueillies » (O. Tene, « What Google Knows : Privacy and Internet Search Engines », [2008] *Utah L. Rev.* 1433, p. 1458, citant Solove, p. 507). Vu l'omniprésence d'Internet, nous devons examiner de plus en plus [TRADUCTION] « les façons dont différents ensembles de données *combinés* à d'autres ensembles de données portent atteinte aux droits à la vie privée » (Hasan, p. 60 (en italique dans l'original)).

[75] Non seulement Internet garde un registre permanent précis, mais il a concentré cette masse de données entre les mains de tiers et investi ces derniers d'un immense pouvoir informationnel. Il a donné à de grandes sociétés privées la capacité de recueillir de vastes quantités de renseignements relatifs à l'utilisateur et d'agréger ces données en images claires de l'activité en ligne de leurs utilisateurs afin de savoir ce que veulent ceux-ci et à quel moment ils le veulent. En échange, ces sociétés [TRADUCTION] « bâtissent ce qui représente peut-être l'objet culturel le plus durable, le plus lourd et le plus important dans l'histoire de l'humanité » (Tene, p. 1435, citant J. Battelle, *The Search : How Google and Its Rivals Rewrote the Rules of Business and Transformed Our Culture* (2005), p. 6).

[76] Internet a permis aux sociétés privées non seulement de suivre leurs utilisateurs, mais aussi de bâtir des profils de ceux-ci remplis de renseignements que les utilisateurs n'ont jamais su qu'ils révélaient. « L'historique de navigation, par exemple, permet d'obtenir des renseignements détaillés sur les intérêts des utilisateurs. Les moteurs de recherche peuvent recueillir des renseignements sur les termes recherchés par les utilisateurs. Les annonceurs peuvent suivre leurs utilisateurs à travers les réseaux de sites Web et obtenir un aperçu de leurs intérêts et de leurs préoccupations » (*Spencer*, par. 46). Des commentateurs ont même suggéré que les entreprises peuvent utiliser les données qu'elles recueillent pour déterminer [TRADUCTION] « ce que vous allez acheter, le genre de personne avec qui vous allez vous mettre en couple, si vous ferez bien un nouveau travail, combien de temps vous resterez à ce poste, et si vous tomberez malade » (H. Matsumi, « Predictions and Privacy : Should There Be Rules About Using Personal Data to Forecast the Future? » (2017), 48 *Cumb. L. Rev.* 149, p. 149).

[77] C'est loin d'être une conjecture. En effet, il est notoire que les plus grandes sociétés de médias sociaux dans le monde utilisent les adresses IP pour, par exemple, personnaliser les publicités que voient leurs utilisateurs, établir les préférences de ceux-ci et inférer encore plus de renseignements à leur sujet, comme leur âge, leur sexe et leurs intérêts. Quand il s'agit de suivre les utilisateurs sur Internet, pour paraphraser l'auteur de science-fiction William Gibson, [TRADUCTION] « [l]e futur est déjà là » (P. Kennedy, « William Gibson's Future Is Now », *The New York Times*, 13 janvier 2012 (en ligne)).

[78] En concentrant cette masse de renseignements entre les mains de tiers du secteur privé et en donnant à ces derniers les outils nécessaires pour agréger et disséquer ces données, Internet a essentiellement modifié la topographie de la vie privée sous le régime de la *Charte*. Il a ajouté un tiers à l'écosystème constitutionnel, et a fait de la relation horizontale entre l'individu et l'État une relation tripartite. Bien que l'art. 8 ne s'applique pas aux tiers eux-mêmes, ceux-ci [TRADUCTION] « joue[nt] le rôle de médiateur[s] dans une relation directement régie par la *Charte* — celle entre le défendeur et la police » (A. Slane, « Privacy and Civic Duty in *R v Ward* : The Right to Online Anonymity and the *Charter*-Compliant Scope of Voluntary Cooperation with Police Requests » (2013), 39 *Queen's L.J.* 301, p. 311).

[79] Ce changement a accru, plutôt que restreint, la capacité informationnelle de l'État. [TRADUCTION] « [L]es progrès technologiques permettent aux acteurs gouvernementaux d'étendre considérablement leurs pouvoirs de surveillance, notamment en exploitant des renseignements détaillés recueillis par le secteur privé » (A. J. Cockfield, « Who Watches the Watchers? A Law and Technology Perspective on Government and Private Sector Surveillance » (2003), 29 *Queen's L.J.* 364, p. 406). La professeure Austin décrit cette situation comme le [TRADUCTION] « nouveau lien de surveillance public/privé », où des intermédiaires peuvent « permet[tre] à l'État d'accéder au contenu de nos communications ainsi qu'à une mine d'autres données connexes » (p. 453). Par conséquent, [TRADUCTION] « dans le contexte de la collaboration d'intermédiaires, le pouvoir de l'État s'accroît » (p. 458).

[80] Même si l'adresse IP ne révèle pas en soi l'identité de l'utilisateur, la disponibilité et la facilité d'obtention d'un mandat de type *Spencer* signifient que cette identité peut être révélée ultérieurement, à l'égard non seulement de l'activité Internet potentiellement criminelle en question, mais aussi de tous les renseignements qui peuvent être inférés de l'activité Internet de l'utilisateur. Comme le soutient l'appelant, comparer l'adresse IP d'un utilisateur identifié avec d'autres activités en ligne [TRADUCTION] « brise complètement l'anonymat [en ligne] » (m.a., par. 45).

[81] Certaines juridictions étrangères ont réagi en reconnaissant que les adresses IP constituent des renseignements privés qui méritent d'être protégés, même s'il est nécessaire de recourir à des renseignements détenus par des tiers. Dans l'arrêt *Breyer c. Bundesrepublik Deutschland*, C-582/14, EU:C:2016:779, la Cour européenne de justice a conclu qu'une adresse IP était une donnée à caractère personnel concernant une « personne [. . .] identifiable » suivant l'art. 2 de la *Directive 95/46/CE du Parlement européen et du Conseil*, [1995] J.O. L. 281/31. Il était sans importance qu'il faille recourir à un tiers pour rendre cette personne « identifiable » : l'adresse IP d'un utilisateur est *en soi* une « donné[e] à caractère personnel » parce qu'elle peut raisonnablement tendre à révéler l'identité de l'utilisateur — dans cette affaire, au moyen de renseignements détenus par un intermédiaire du secteur privé (par. 44).

[82] De même, la Cour d'appel d'Angleterre et du Pays de Galles a conclu que la question de savoir si des [TRADUCTION] « renseignements générés par un navigateur » — comme une adresse IP — étaient des données à caractère personnel au

sens de la *Data Protection Act 1998* (R.-U.), 1998, c. 29, était une question sérieuse à juger au fond (*Vidal-Hall c. Google Inc.*, [2015] EWCA Civ 311, [2016] Q.B. 1003, par. 107). La cour a estimé qu'il était clairement possible de soutenir que de tels renseignements constituent des données à caractère personnel parce qu'ils [TRADUCTION] « "individualisent" l'individu, en ce sens qu'il est distingué de tous les autres » (par. 115). Le fait que les renseignements ne nomment pas l'utilisateur n'a eu [TRADUCTION] « aucune incidence » sur sa conclusion, car, « dans la plupart des cas — notamment ceux où une adresse IP dynamique est attribuée —, les données nécessaires seront disponibles pour permettre d'identifier le ou les utilisateurs de l'adresse IP » (par. 117).

[83] Je conviens avec l'intervenante la British Columbia Civil Liberties Association que ces décisions décrivent de façon convaincante l'interaction entre les adresses IP et l'approche normative que notre Cour a systématiquement appliquée à l'art. 8 de la *Charte*. Elles reconnaissent les adresses IP en tant que renseignements privés parce qu'elles pourraient raisonnablement révéler — c'est-à-dire qu'elles tendent à révéler — l'identité de l'utilisateur, qu'il soit nécessaire ou non de faire appel à un tiers. Ces décisions « *appu[ient]* ou [. . .] *confirme[nt]* » la méthodologie appliquée par la Cour à l'égard de la protection de la vie privée (*Québec (Procureure générale) c. 9147-0732 Québec inc.*, 2020 CSC 32, [2020] 3 R.C.S. 426, par. 22 (en italique dans l'original)). Notre Cour a, tout au long de son histoire, examiné des décisions comparatives pour leur force convaincante (voir N. Olivetti Rason et S. Pennicino, « Comparative Law in the Jurisprudence of the Supreme Court of Canada »,

dans G. F. Ferrari, dir., *Judicial Cosmopolitanism : The Use of Foreign Law in Contemporary Constitutional Systems* (2019), 140, p. 146).

[84] Ces préoccupations importantes relatives à la vie privée entrent en balance avec l'intérêt parfois conflictuel mais légitime de la société en ce qui a trait au besoin de sécurité. Au fur et à mesure qu'évolue la technologie, la manière de commettre un crime et d'enquêter sur celui-ci évolue également (*R. c. Mills*, 2019 CSC 22, [2019] 2 R.C.S. 320, par. 38-39). La facilité d'accès à Internet et l'anonymat de l'utilisateur se conjuguent pour permettre la perpétration d'un large éventail de crimes, y compris des infractions et des crimes d'ordre sexuel contre des enfants. L'effet amplifié et la permanence du préjudice causé aux victimes de cybercriminalité, en particulier les enfants, doivent être pris en compte lorsqu'il s'agit de définir et de calibrer l'intérêt dans l'application de la loi que met en cause le présent pourvoi (voir *R. c. Friesen*, 2020 CSC 9, [2020] 1 R.C.S. 424, par. 1, 5 et 50-73; Magotiaux, p. 502). La police devrait disposer des outils d'enquête nécessaires pour s'occuper d'un crime commis et facilité en ligne.

[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.

[87] Une attente raisonnable au respect de la vie privée fait en sorte que l'État ne peut effectuer que des fouilles motivées par des préoccupations légitimes d'application de la loi. Les avantages pour le respect de la vie privée sont importants. Une autorisation judiciaire préalable restreint considérablement ce qui est accessible à l'État en ligne, et l'empêche d'obtenir les détails sur la vie en ligne d'un utilisateur que révèle l'adresse IP de ce dernier et qui ne sont pas pertinents pour l'enquête. Cela réduit considérablement la possibilité d'exercices [TRADUCTION] « arbitraire[s] et même discriminatoire[s] » du pouvoir discrétionnaire qui autoriseraient l'État à découvrir des renseignements sur l'internaute qu'il veut pour toute raison qu'il juge indiquée (L. M. Austin, « Getting Past Privacy? Surveillance, the Charter, and the Rule of Law » (2012), 27 *R.C.D.S.* 381, p. 392). Dans une société démocratique, il est « inconcevable que l'État ait le pouvoir discrétionnaire illimité de soumettre qui il veut à une surveillance [numérique] effectuée subrepticement » (*R. c. Wong*, [1990] 3 R.C.S. 36, p. 47).

[88] La surveillance judiciaire en ce qui a trait à une adresse IP est le moyen de réaliser l'objectif de l'art. 8 d'empêcher les atteintes à la vie privée. Depuis l'arrêt *Hunter,* nous avons statué que cette disposition vise à empêcher les violations de la vie privée, et non à condamner ou à admettre des violations après le fait eu égard à l'utilisation que fait l'État de ces renseignements. Le droit à la vie privée, une fois qu'il y a été porté atteinte, ne peut pas être rétabli.

[89] Enfin, la surveillance judiciaire enlève aux sociétés privées le pouvoir de décider s'il convient de dévoiler des renseignements — et en quelle quantité — et renvoie la question au champ d'application de la *Charte*. L'accroissement du pouvoir de l'État occasionné par Internet est donc compensé par une interprétation large et téléologique de l'art. 8 qui répond à nos « nouvelles réalités sociales, politiques et historiques » (*Hunter*, p. 155). Laisser le secteur privé décider de fournir ou non à la police des renseignements qui risquent de révéler l'aspect le plus intime de notre personne porte un coup inacceptable à l'art. 8. Laisser la protection de la *Charte* s'appliquer à la prochaine étape envisagée de l'enquête ne suffit pas. Comme je l'ai expliqué, il pourrait alors être trop tard.

[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 d'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.

[91] À mon avis, la personne raisonnable et bien informée qui se soucie des conséquences à long terme des actions gouvernementales sur la protection du droit au respect de la vie privée conclurait que les adresses IP devraient susciter une attente raisonnable au respect de la vie privée. Étendre la portée de l'art. 8 aux adresses IP protège le premier « fragment numérique » et obscurcit donc la trace du parcours d'un internaute dans le cyberespace.

V. Dispositif

[92] J'estime que la demande d'adresse IP faite par l'État constitue une fouille au sens de l'art. 8 de la *Charte*. Je suis d'avis d'accueillir le pourvoi, d'annuler la déclaration de culpabilité et d'ordonner la tenue d'un nouveau procès.

Version française des motifs du juge en chef Wagner et des juges Côté, Rowe et O'Bonsawin rendus par

LA JUGE CÔTÉ —

I. Introduction

[93] En cette ère numérique, tant les préoccupations relatives au respect de la vie privée en ligne que celles relatives à la cybercriminalité sont répandues.

[94] En l'espèce, la police de Calgary a enquêté sur une série d'achats frauduleux faits en ligne. À la suite de cette enquête, l'appelant, Andrei Bykovets, a été arrêté, jugé et déclaré coupable d'un certain nombre d'infractions liées à une fraude commise en utilisant Internet. La police a pu l'identifier en prenant plusieurs mesures, notamment en obtenant une ordonnance de communication comme l'exige l'arrêt *R. c. Spencer*, 2014 CSC 43, [2014] 2 R.C.S. 212. La première mesure prise dans l'enquête a été de récupérer auprès d'un intermédiaire les adresses de protocole Internet (« IP ») de l'appelant, ce que la police a fait sans mandat. L'appelant allègue qu'il avait une attente raisonnable au respect de sa vie privée à l'égard de ses adresses IP, de sorte que les droits que lui garantit l'art. 8 de la *Charte canadienne des droits et libertés* ont été violés lorsque la police a obtenu ces adresses de l'intermédiaire. Selon l'appelant, la police avait besoin d'une autorisation judiciaire préalable pour les obtenir.

[95] Notre Cour est appelée à décider si l'appelant avait une attente raisonnable au respect de sa vie privée à l'égard des adresses IP elles-mêmes — sans autre renseignement reliant ces adresses à celui-ci en tant qu'internaute — dans les circonstances de l'espèce. Je conclus que l'appelant n'avait pas d'attente raisonnable au respect de sa vie privée. Je suis donc d'avis de rejeter le pourvoi.

II. Faits

[96] Les faits ne sont pas contestés par les parties.

[97] En septembre 2017, la police de Calgary a entrepris une enquête liée à l'achat de cartes-cadeaux virtuelles au moyen de données de carte de crédit frauduleuses. Les achats ont été faits en ligne par l'entremise d'entreprises, dont un magasin de vins et spiritueux appelé Co-op Wine Spirits Beer. Les paiements ont été traités par une filiale de Moneris, l'entreprise de traitement des cartes de crédit.

[98] Au cours de son enquête sur la fraude, la police a communiqué avec Moneris et lui a demandé les adresses IP associées aux achats. Moneris a fourni les adresses IP figurant dans ses journaux des opérations. La police a ensuite utilisé un site Web de recherche accessible au public et a appris que les adresses IP avaient été émises par TELUS. Elle a obtenu une ordonnance de communication intimant à TELUS de fournir les renseignements relatifs à l'abonné associés aux adresses IP. Une adresse était enregistrée au nom de l'appelant et l'autre l'était à celui de son père. Je souligne qu'il n'y a aucune distinction entre ces deux adresses pour les besoins du présent pourvoi.

[99] La police a ensuite demandé et obtenu des mandats de perquisition des deux résidences associées aux adresses IP. Pendant la perquisition, elle a trouvé un lecteur et enregistreur de cartes magnétiques, des pièces d'identité gouvernementales portant le nom de tierces personnes, des ordinateurs, des clés USB, des faux documents d'immigration et des armes à feu. L'appelant a été arrêté et accusé de 33 infractions

liées à la possession et à l'utilisation de cartes de crédit et de documents d'identification personnelle de tiers, ainsi qu'à la possession et à l'entreposage d'armes à feu.

[100] Avant le procès, l'appelant a demandé que soient écartés les éléments de preuve découverts grâce à l'utilisation par la police de ses adresses IP, alléguant que la police avait violé les droits que lui garantit l'art. 8 de la *Charte*. Il a produit le rapport de Matthew Musters, à qui la juge du procès a reconnu la qualité d'expert dans l'analyse criminalistique électronique ainsi que dans la nature et le fonctionnement des adresses IP. La Couronne a consenti à l'admission du rapport d'expertise de M. Musters et n'a pas cherché à contre-interroger ce dernier. Elle a également souscrit au contenu du rapport.

[101] Les parties pertinentes du rapport peuvent être résumées brièvement.

[102] Premièrement, le rapport explique qu'il existe deux types d'adresses IP : les externes et les internes. Le présent pourvoi ne concerne que des adresses IP externes. Une adresse IP externe est attribuée à un abonné par un fournisseur de services Internet (« FSI ») et est utilisée dans le transfert de l'information d'une source à une autre sur Internet. Sans adresse IP externe, un utilisateur ne peut envoyer ni recevoir de données. Chaque adresse IP externe est clairement associée à un abonné durant sa période de location. Le plus souvent, les abonnés résidentiels se voient attribuer des adresses IP externes dynamiques qu'un FSI peut changer à son gré et sans préavis. Chaque FSI tient un registre indiquant à quel abonné chaque adresse IP externe a été attribuée et pour quelle période.

[103] Ensuite, le rapport explique que dans une session de navigation Internet typique, l'adresse IP externe d'un utilisateur n'est connue que par le serveur de destination (à l'exclusion de tout saut effectué par celle-ci sur son passage). Le rapport décrit deux méthodes au moyen desquelles l'identité d'un utilisateur ou d'une utilisatrice peut être découverte à partir de son adresse IP externe. La première consiste à entrer l'adresse IP dans un site Web de recherche de FSI pour déterminer à quel FSI appartient l'adresse en question, et à obtenir par la suite du FSI les renseignements relatifs à l'abonné. L'autre repose sur l'hypothèse selon laquelle on peut avoir accès aux renseignements enregistrés par les sites Web de sociétés tierces. Les sites Web peuvent suivre l'adresse IP de chaque utilisateur qui les visite. Sur la base de ces renseignements, on pourrait essayer de déterminer l'identité d'une personne utilisant le service en ligne d'une société en examinant l'activité de cette utilisatrice sur le site Web en question.

III. Historique judiciaire

A. *Cour du Banc de la Reine de l'Alberta, 2020 ABQB 70, 10 Alta. L.R. (7th) 103 (la juge Ho)*

[104] Dans sa décision sur le voir-dire, la juge du procès a affirmé que la principale question à trancher en ce qui a trait à l'art. 8 de la *Charte* est de savoir si une personne a une attente raisonnable au respect de sa vie privée à l'égard d'une adresse IP. La Couronne a concédé que si l'appelant avait une attente raisonnable au respect de sa vie privée à l'égard des adresses IP, ses droits garantis par l'art. 8 avaient été violés.

Pour déterminer s'il existe une attente raisonnable au respect de la vie privée, la juge a appliqué le « test de l'ensemble des circonstances » énoncé par notre Cour dans l'arrêt *Spencer*.

[105] La juge du procès a conclu que la prétendue fouille avait pour objet les adresses IP. Tant à première vue qu'à la lumière de ce qui pouvait en être inféré, les adresses IP ne pouvaient fournir que des renseignements limités sur un internaute. Ce n'est qu'avec d'autres renseignements qu'une adresse IP pouvait mener à l'identification d'une personne en particulier. En l'espèce, la police « recherchait vraiment » les adresses IP elles-mêmes afin de découvrir le FSI de la personne soupçonnée de fraude et d'obtenir par la suite une ordonnance de communication visant à identifier cette dernière.

[106] La juge du procès a accepté que l'appelant avait un intérêt direct et une attente subjective au respect de sa vie privée à l'égard des adresses IP. Elle a toutefois conclu que cette attente n'était pas objectivement raisonnable. Contrairement à ce que faisait valoir l'appelant, la fouille avait eu lieu non pas chez lui, mais dans la base de données de l'entreprise de traitement des cartes de crédit. Constituant des ensembles de chiffres, les adresses IP ne communiquaient pas de renseignements personnels ni ne révélaient de détails intimes sur le mode de vie de l'appelant. Le FSI était en mesure de contrôler l'objet de la fouille grâce à sa capacité de changer les adresses IP de l'appelant, bien que ce ne fût pas un facteur déterminant.

[107] Prenant en considération l'ensemble des facteurs, la juge du procès a statué que l'appelant n'avait pas une attente raisonnable au respect de sa vie privée à l'égard des adresses IP. Par conséquent, la fouille n'avait pas mis en jeu ses droits garantis par l'art. 8. L'appelant a finalement été déclaré coupable de 14 des 33 infractions dont il avait été accusé.

B. *Cour d'appel de l'Alberta, 2022 ABCA 208, [2023] 5 W.W.R. 51*

(1) Juges majoritaires (les juges Schutz et Crighton)

[108] L'appelant a interjeté appel et a contesté la conclusion de la juge du procès portant que ses droits garantis par l'art. 8 n'avaient pas été violés. Les juges majoritaires de la Cour d'appel ont rejeté l'appel et ont statué, d'une part, que la juge du procès avait correctement interprété la portée de l'art. 8 et avait appliqué les bons principes, et, d'autre part, que ses conclusions de fait ne comportaient aucune erreur manifeste et dominante. La juge du procès a interprété l'objet de la fouille de manière fonctionnelle, comme elle était tenue de le faire. Elle a compris ce que la police « recherchait vraiment » : les adresses IP pour faire avancer l'enquête, dans l'espoir que le complément d'enquête autorisé révélerait les noms et adresses associés aux adresses IP. La juge du procès a conclu que les adresses IP ne révélaient aucun renseignement privé; l'appelant n'avait donc aucune attente raisonnable au respect de sa vie privée à leur égard. Les juges majoritaires ont donc souscrit à l'analyse et aux conclusions de la juge du procès.

[109] Les juges majoritaires ont également convenu avec la juge du procès qu'il était possible d'établir une distinction avec l'affaire *Spencer* parce qu'en l'espèce, la police n'a pas obtenu les *données relatives à l'abonné* en plus des adresses IP elles-mêmes. Sans ces données, la police a simplement cru qu'un [TRADUCTION] « inconnu qui utilisait une adresse IP connue était en train de commettre une fraude à partir d'une adresse inconnue », ce qui n'était pas suffisant pour donner lieu à une attente raisonnable au respect de la vie privée (par. 17). De l'avis des juges majoritaires, une [TRADUCTION] « adresse IP est un numéro abstrait qui ne révèle aucun des renseignements biographiques qu'y rattache son émetteur. Prise isolément, elle ne révèle rien » (par. 21). C'est seulement de pair avec les renseignements relatifs à l'abonné qu'une adresse IP est susceptible de révéler des renseignements personnels, et ce n'est qu'en se conformant à l'arrêt *Spencer* que la police pouvait obtenir ces renseignements relatifs à l'abonné.

(2) Dissidence (la juge Veldhuis)

[110] La juge Veldhuis, dissidente, aurait conclu que l'appelant avait une attente raisonnable au respect de sa vie privée à l'égard des adresses IP parce que celles-ci étaient liées à une activité Internet particulière sous surveillance qui était susceptible de révéler des renseignements biographiques. Par conséquent, elle aurait conclu à la violation des droits que l'art. 8 garantit à l'appelant et elle aurait ordonné la tenue d'un nouveau procès.

[111] La juge Veldhuis était d'avis que la juge du procès n'avait pas appliqué l'approche normative aux attentes raisonnables au respect de la privée. À son avis, il n'était pas possible d'établir une distinction entre la présente espèce et l'affaire *Spencer*. Tant dans *Spencer* qu'en l'espèce, il était question d'une tentative de la police d'identifier un internaute particulier afin de pouvoir [TRADUCTION] « recueillir davantage de renseignements pour tirer des inférences quant aux détails intimes sur le mode de vie et les choix personnels de l'internaute » (par. 62).

[112] De l'avis de la juge Veldhuis, l'omission d'appliquer l'approche normative a amené la juge du procès à qualifier l'objet de la fouille de façon trop restrictive. La juge Veldhuis a souligné que la preuve d'expert indiquait comment une adresse IP pouvait être utilisée pour identifier un internaute à partir de sites Web de tiers, et que s'il n'y avait aucune attente raisonnable au respect de la vie privée, rien n'obligerait la police à obtenir un mandat avant de le faire. Pour la juge Veldhuis, le véritable objet de la fouille, et ce que la police recherchait vraiment, était [TRADUCTION] « l'identité d'un internaute qui correspond à une adresse IP particulière liée à une activité Internet particulière sous surveillance » (par. 77). Cet objet impliquait l'idée d'anonymat de la vie privée, ce qui est très important dans le contexte d'Internet.

[113] Selon la juge Veldhuis, l'erreur commise par la juge du procès en qualifiant l'objet de la fouille a amené celle-ci à commettre une autre erreur en concluant que l'attente subjective de l'appelant au respect de la vie privée n'était pas objectivement raisonnable. En ce qui concerne le lieu fouillé en tant que facteur dans l'appréciation

de ce caractère raisonnable, la juge Veldhuis a souligné que l'art. 8 [TRADUCTION] « protège les personnes et non les lieux », et a jugé qu'une personne s'attend à ce que les données de carte de crédit et l'adresse IP à partir de laquelle elles sont envoyées demeurent privées. En ce qui a trait au caractère privé de l'objet, elle a réitéré ses commentaires antérieurs sur la possibilité d'identifier un internaute en utilisant une adresse IP, ce qui fait intervenir des intérêts en matière de vie privée allant au-delà du nom et de l'adresse de l'utilisateur. Pour ce qui est du contrôle sur l'objet, la juge Veldhuis a statué que le contrôle n'est pas perdu simplement parce qu'une adresse IP est accessible à d'autres. Elle a affirmé que choisir entre ne pas du tout utiliser Internet et renoncer au contrôle sur son adresse IP ne constitue pas un véritable choix.

[114] La juge Veldhuis a conclu que l'appelant avait une attente raisonnable au respect de la vie privée à l'égard des adresses IP [TRADUCTION] « parce que celles-ci étaient liées à une activité Internet particulière sous surveillance qui était susceptible de révéler des renseignements biographiques » (par. 94).

[115] L'appelant se pourvoit maintenant devant notre Cour en se fondant sur la dissidence de la juge Veldhuis.

IV. Question en litige

[116] La seule question qui se pose en l'espèce est de savoir si une attente raisonnable au respect de la vie privée s'appliquait aux adresses IP. Si tel était le cas,

la Couronne concède que les droits que l'art. 8 de la *Charte* garantit à l'appelant ont été violés.

V. Analyse

[117] Le droit relatif aux attentes raisonnables au respect de la vie privée est bien établi. La présente affaire commande une simple application du droit à la situation où une entreprise de traitement de cartes de crédit en ligne fournit une adresse IP à la police.

[118] L'article 8 de la *Charte*, qui prévoit que « [c]hacun a droit à la protection contre les fouilles, les perquisitions ou les saisies abusives », vise à assurer une protection contre l'intrusion de l'État dans la vie privée d'une personne. Cependant, comme l'a fait observer notre Cour, « tout type d'enquête gouvernementale ne constituera pas forcément, sur le plan constitutionnel, une "fouille ou perquisition" » (*R. c. Evans*, [1996] 1 R.C.S. 8, par. 11). L'article 8 entre en jeu seulement « lorsque les attentes raisonnables d'une personne en matière de vie privée sont affectées d'une manière ou d'une autre par une technique d'enquête » (*ibid.*).

[119] Le test relatif à l'attente raisonnable au respect de la vie privée est tributaire des faits et contextuel. La question de savoir si une personne a une telle attente dépend de « l'ensemble des circonstances d'un cas particulier » (*R. c. Edwards*, [1996] 1 R.C.S. 128, par. 31). Notre Cour a établi une liste non exhaustive de facteurs à

considérer à cet égard. Les facteurs pertinents sont souvent commodément regroupés en quatre grandes catégories :

(1) Quel était l'objet de la prétendue fouille?

(2) Le demandeur avait-il un intérêt direct à l'égard de l'objet?

(3) Le demandeur avait-il une attente subjective au respect de sa vie privée relativement à l'objet?

(4) Dans l'affirmative, l'attente subjective du demandeur était-elle objectivement raisonnable?

[120] Comme on l'a souvent souligné, l'analyse est de nature normative, et non descriptive (*R. c. Tessling*, 2004 CSC 67, [2004] 3 R.C.S. 432, par. 42; *R. c. Reeves*, 2018 CSC 56, [2018] 3 R.C.S. 531, par. 28). L'objectif est de décider quel degré d'intimité une personne *devrait* avoir, et non pas quel degré d'intimité une personne a *effectivement*. Comme l'a affirmé le juge Binnie dans l'arrêt *Tessling* :

> À une époque où l'on peut facilement se procurer sur le marché des dispositifs de furetage de plus en plus diversifiés, le simple citoyen peut en venir à craindre (à tort ou à raison) que son téléphone soit placé sous écoute ou que son courrier personnel soit lu. [. . .] Il faut donc réfuter toute affirmation selon laquelle la diminution de l'attente *subjective* en matière de vie privée se traduira automatiquement par une diminution correspondante de la protection constitutionnelle. Affirmer qu'un particulier qui laisse ses ordures au ramassage n'a pas d'attente raisonnable en matière de vie privée à leur sujet est une chose. Mais c'en est une toute autre de dire qu'une personne qui craint que son téléphone soit sur écoute n'a plus d'attente *subjective* en matière de vie privée et qu'elle ne peut plus

> de ce fait revendiquer la protection de l'art. 8. [En italique dans l'original; par. 42.]

[121] Gardant à l'esprit cette approche normative, je me penche maintenant sur son application aux faits de l'espèce. À l'instar de la juge du procès, je reconnais que l'appelant avait un intérêt direct à l'égard des adresses IP, ainsi qu'une attente subjective au respect de sa vie privée relativement à leur contenu informationnel. Les principaux points de désaccord devant notre Cour ont trait aux première et quatrième parties de l'analyse : l'objet de la fouille et le caractère objectivement raisonnable de l'attente au respect de la vie privée, plus précisément en ce qui a trait au caractère privé de l'objet. Je les examine à tour de rôle.

A. *Objet de la fouille*

[122] Déterminer l'objet de la fouille est une question clé dans l'analyse de l'« ensemble des circonstances ». Notre Cour a adopté une « approche large et fonctionnelle » en la matière. L'objet de la fouille ne doit pas être défini suivant une approche [TRADUCTION] « restrictive portant sur les actes commis ou l'espace envahi, mais [. . .] plutôt [suivant] une approche qui tient compte de la nature des droits en matière de vie privée auxquels l'action de l'État pourrait porter atteinte » (*R. c. Marakah*, 2017 CSC 59, [2017] 2 R.C.S. 608, par. 15, citant *R. c. Ward*, 2012 ONCA 660, 112 O.R. (3d) 321, par. 65). Par conséquent, pour déterminer l'objet de la fouille, le tribunal doit se pencher sur le lien entre la technique d'enquête utilisée par la police et l'intérêt en matière de vie privée qui est en jeu (*Marakah*, par. 15). Il doit examiner

« non seulement la nature des renseignements précis recherchés, mais aussi la nature des renseignements qui sont ainsi révélés » (*Spencer*, par. 26).

[123] Lorsqu'il apprécie l'objet d'une prétendue fouille, le tribunal doit déterminer [TRADUCTION] « ce que la police recherchait vraiment » (*Marakah*, par. 15, citant *Ward*, par. 67). Cette question directrice fait ressortir le fait que l'objet de la fouille peut aller au-delà de l'objet ou des renseignements précis qu'obtient la police. Quand il se demande « ce que la police recherchait vraiment », le tribunal ne s'intéresse pas à l'objectif poursuivi par la police dans l'enquête criminelle (c.-à-d. à *la raison pour laquelle* la police recherchait les renseignements). Il ne s'intéresse pas non plus à ses intentions subjectives. Le tribunal se préoccupe plutôt de la capacité des renseignements précis recherchés de donner lieu à des inférences ou de révéler *d'autres* renseignements. Ces inférences et ces autres renseignements font partie du véritable objet de la fouille.

[124] L'arrêt *Spencer* illustre ces principes. Dans cette affaire, au cours d'une enquête en matière de pornographie juvénile, la police avait demandé au FSI à qui appartenait une adresse IP particulière les renseignements relatifs à l'abonnée (un nom et une adresse physique). La Cour s'est dite en désaccord avec la prétention suivant laquelle de tels renseignements constituaient en eux-mêmes le véritable objet de la fouille. Cette [TRADUCTION] « qualificatio[n] f[ait] abstraction de l'importance d'une adresse IP et des renseignements que cette adresse, une fois liée à une personne en particulier, peut révéler sur cette personne, notamment les activités en ligne que celle-ci

pratique dans sa résidence » (par. 32 (je souligne), citant *R. c. Trapp*, 2011 SKCA 143, 377 Sask. R. 246, par. 35). Notre Cour a plutôt conclu que la fouille avait pour objet « l'identité de l'abonnée dont la connexion à Internet correspondait à une activité informatique particulière sous surveillance » (par. 33). Les renseignements précis recherchés — les renseignements relatifs à l'abonnée — établissaient un lien entre une personne précise et l'activité en ligne particulière associée à une adresse IP anonyme. Tout cela constituait l'objet de la fouille.

[125] De même, dans l'arrêt *Marakah*, la juge en chef McLachlin a conclu que la fouille n'avait pas simplement pour objet le téléphone cellulaire qui avait été saisi par la police. Elle englobait plutôt les conversations par messagerie texte contenues dans le téléphone cellulaire ainsi que toute inférence sur les fréquentations et les activités « que l'on peut tirer [des] renseignements » échangés dans ces conversations (par. 20 (je souligne)).

[126] Enfin, et fait important, bien qu'il ne puisse pas être défini de façon trop restrictive, l'objet de la fouille doit tout de même être ancré dans ce qu'il est possible de tirer de la preuve elle-même. Plus précisément, la capacité des renseignements précis recherchés de donner lieu à des inférences ou de révéler d'autres renseignements doit être étayée par la preuve; elle ne peut reposer sur de simples conjectures ou hypothèses. On peut retrouver ce principe dans la jurisprudence de la Cour. Dans l'arrêt *R. c. Kang-Brown*, 2008 CSC 18, [2008] 1 R.C.S. 456, par exemple, la juge Deschamps, dissidente, mais non sur ce point, a expliqué que ce qui importe à propos de

l'intervention d'un chien renifleur pour vérifier le sac de l'accusé est que la police se fie aux chiens renifleurs avec un taux de réussite de plus de 92 p. 100 et que ces chiens ne font pas qu'identifier les odeurs qui émanent d'un sac, mais, ce faisant, ils déterminent effectivement le contenu de celui-ci (c.-à-d. une substance désignée) (par. 174). Dans cette affaire, l'intervention d'un chien renifleur a donc « immédiatement et directement permis aux policiers de faire une forte inférence » sur le contenu du sac de l'accusé, ce qui faisait vraiment l'objet de leurs recherches (par. 175). La capacité des renseignements précis recherchés — les odeurs détectées par le chien — de révéler d'autres renseignements était étayée par la preuve au dossier dans cette affaire.

[127] En revanche, dans l'arrêt *R. c. Gomboc,* 2010 CSC 55, [2010] 3 R.C.S. 211, la police soupçonnait l'accusé d'être impliqué dans la production de marijuana. Elle a demandé à une entreprise de services publics d'installer un appareil pour mesurer le courant électrique consommé par la résidence de l'accusé. Notre Cour s'est fondée sur le dossier de preuve pour déterminer ce que les renseignements précis recherchés (dans l'appareil) révèlent et quelles inférences ils appuient. La Cour d'appel avait conclu que certains éléments d'information à propos de ce qui se passe dans une habitation pouvaient être inférés de l'appareil. Plusieurs juges de notre Cour n'étaient pas de cet avis, car cette conclusion ne s'appuyait pas sur la preuve au dossier. Le dossier indiquait plutôt que l'appareil révèle seulement la consommation d'électricité; il ne révèle rien à propos des activités intimes ou des activités personnelles fondamentales

se déroulant à l'intérieur d'une maison (par. 14). Le dossier de preuve restreignait donc l'objet de la fouille.

[128] Dans les circonstances de l'espèce, l'objet de la fouille comprend les adresses IP et l'identité du FSI qui leur est associé. Bien que la police eût pour objectif ultime d'identifier la personne à qui une fraude était imputée, son objectif d'enquête n'est pas le point de mire de l'« approche large et fonctionnelle » permettant de déterminer l'objet de la fouille (*Spencer*, par. 26). L'objet doit plutôt refléter l'information révélée par les renseignements précis recherchés (*Spencer*, par. 26). Je ne suis pas d'accord avec la juge Veldhuis pour dire que la fouille avait pour objet [TRADUCTION] « l'identité d'un internaute qui correspond à une adresse IP particulière liée à une activité Internet particulière sous surveillance » (par. 77). Bien qu'il puisse s'être agi de l'objectif ultime de l'enquête, ce n'était pas des renseignements révélés par les adresses IP brutes elles-mêmes, de sorte qu'il ne s'agit pas de l'objet de la fouille.

[129] Je suis parfaitement consciente du fait que les chiffres constituant une adresse IP ne sont pas recherchés pour ces chiffres en eux-mêmes. Ils le sont en raison des renseignements qu'ils révèlent. Cependant, le dossier de preuve en l'espèce établit qu'une adresse IP, à elle seule, révèle seulement des renseignements limités. Elle ne révèle pas un « ensemble de renseignements biographiques d'ordre personnel que les particuliers pourraient, dans une société libre et démocratique, vouloir constituer et soustraire à la connaissance de l'État » (*R. c. Plant*, [1993] 3 R.C.S. 281, p. 293). À

elle seule, une adresse IP ne révèle même pas les habitudes de navigation. Ce qu'elle révèle, c'est le FSI d'un utilisateur — un élément d'information qui n'est guère plus privé que la consommation d'électricité (*Plant*) ou les émissions de chaleur (*Tessling*).

[130] Ce n'est que lorsqu'elle est combinée à d'autres renseignements qu'une adresse IP peut permettre de tirer des inférences sur l'identité d'un utilisateur, ce qui distingue fondamentalement la présente espèce de l'affaire *Spencer*. Dans *Spencer*, les renseignements relatifs à l'abonnée étaient la clé qui donnait accès à l'identité de la personne derrière une adresse IP et qui révélait ses activités en ligne. Une attente raisonnable au respect de la vie privée s'appliquait aux renseignements relatifs à l'abonnée parce que ceux-ci établissaient le lien entre l'activité Internet anonyme et une personne précise. Cependant, en l'espèce, il n'y avait pas un tel lien. La question est donc la suivante : Quels renseignements révèlent à elles seules des adresses IP, et quelles inférences ces adresses permettent-elles de tirer?

[131] Comme nous l'avons vu, la preuve d'expert non contestée présentée en l'espèce a établi qu'il existe deux méthodes permettant de découvrir l'identité d'un utilisateur ou d'une utilisatrice à partir de son adresse IP externe. La première méthode consiste à identifier le FSI à qui appartient une adresse IP en utilisant un [TRADUCTION] « site Web de recherche d'adresse IP » (d.a., p. 311). L'expert a expliqué [TRADUCTION] « [qu'u]ne fois que le FSI qui exerce un contrôle sur une adresse IP particulière a été identifié, il est possible de déterminer qui est l'abonné du compte en demandant au FSI en question ce renseignement » (d.a., p. 311). C'est ce qui s'est passé

dans *Spencer*. En réponse, notre Cour a jugé que des personnes ont une attente raisonnable au respect de leur vie privée à l'égard de ces renseignements relatifs à l'abonné. Compte tenu de l'arrêt *Spencer*, la police doit maintenant obtenir une ordonnance de communication pour obtenir cette information. Il importe de souligner qu'obtenir une telle ordonnance est exactement ce que la police a fait en l'espèce.

[132] Suivant le rapport d'expertise, la deuxième méthode par laquelle une adresse IP peut être utilisée pour déterminer l'identité d'une personne qui utilise Internet consiste à accéder [TRADUCTION] « aux renseignements enregistrés par le site Web d'une société tierce », lequel « peu[t] suivre l'adresse IP externe de chaque utilisateur qui visite » (d.a., p. 311). Selon l'expert, une adresse IP pourrait être fournie à une société comme Google, et Google pourrait utiliser cette adresse IP pour déterminer l'activité d'un utilisateur que cette société suit. Cela semble avoir été la principale préoccupation de la juge Veldhuis, et il semble que ma collègue la juge Karakatsanis ait la même préoccupation.

[133] Il y a deux réponses à cette préoccupation relative aux sites Web de tiers.

[134] Premièrement, eu égard aux faits de l'espèce, la police n'a tout simplement pas utilisé le suivi de l'appelant par un site Web de tiers pour identifier celui-ci. Comme l'a conclu la juge du procès, la police recherchait les adresses IP pour pousser l'enquête, et plus précisément pour découvrir le FSI qui y était associé. Le témoignage de l'enquêtrice principale allait dans ce sens. L'enquête qui a suivi a été réalisée avec une

ordonnance de communication, ce qui est conforme à l'arrêt rendu par notre Cour dans *Spencer*. Par conséquent, la préoccupation ne joue pas en l'espèce.

[135] Deuxièmement, comme l'a concédé la Couronne, un tel scénario (le recours à un site Web de tiers) semble ne pas pouvoir être distingué de celui de l'affaire *Spencer*. L'arrêt *Spencer* a établi qu'il peut exister une attente raisonnable au respect de la vie privée à l'égard du lien entre l'identité d'un utilisateur et une activité Internet précise. Que l'identité d'un internaute anonyme soit révélée par la combinaison de son adresse IP avec les renseignements relatifs à l'abonné détenus par un FSI, ou encore par la combinaison de son adresse IP avec d'autres renseignements détenus par des sites Web de tiers, le résultat est le même. L'intérêt en matière de vie privée de l'utilisateur à l'égard de l'anonymat est compromis. Par conséquent, comme le reconnaît la Couronne, l'arrêt *Spencer* oblige la police à obtenir une autorisation judiciaire avant de demander des données de cette nature — autrement dit, des données qui dévoilent l'identité d'une personne dont la connexion Internet est liée à une activité en ligne particulière sous surveillance. Je souligne en passant que, si le site Web d'un tiers fournissait spontanément des renseignements sans qu'on lui ait demandé de le faire, l'analyse de l'attente raisonnable au respect de la vie privée — qui est toujours guidée par « l'ensemble des circonstances » — pourrait fort bien être différente (*cf. Reeves*, par. 46). Il s'agit là, cependant, d'une question dont il convient de remettre l'examen à une autre occasion dans une affaire où la situation se présenterait effectivement.

[136] Enfin, l'appelant invoque l'arrêt *Reeves* pour soutenir que le simple fait que la police devait prendre d'autres mesures pour l'identifier et le relier à une activité Internet particulière ne signifie pas qu'il n'avait pas d'attente raisonnable au respect de sa vie privée à l'égard des adresses IP. À mon humble avis, c'est à tort qu'il invoque cet arrêt. Dans *Reeves*, la police avait, avec la permission de la conjointe de l'accusé, *saisi* un ordinateur que ce dernier partageait avec elle. La saisie de l'ordinateur impliquait nécessairement la saisie de ses données. Notre Cour a jugé que l'accusé avait une attente raisonnable au respect de sa vie privée à l'égard de l'ordinateur et de ses données. Un mandat était certes nécessaire pour fouiller l'ordinateur malgré la saisie (voir *R. c. Vu*, 2013 CSC 60, [2013] 3 R.C.S. 657, par. 49), mais la saisie elle-même a privé l'accusé de son contrôle à l'égard des données de nature privée contenues dans l'ordinateur (*Reeves*, par. 34). De plus, elle a mis la police en possession des données à l'égard desquelles l'accusé avait un intérêt. En l'espèce, cependant, les adresses IP à elles seules n'ont mis la police en possession d'aucun renseignement privé — immédiatement accessible ou non — concernant l'appelant. Ce n'est qu'en obtenant une ordonnance de communication intimant au FSI de fournir les renseignements relatifs à l'abonné que la police a découvert des renseignements constitutionnellement protégés, à savoir le lien entre l'identité de l'appelant et son activité Internet.

[137] La façon correcte de qualifier l'objet de la fouille consiste donc à décrire celui-ci comme les adresses IP et le FSI révélé par ces adresses. Une qualification de l'objet qui va bien au-delà de l'étendue des informations effectivement révélées par les renseignements précis recherchés par la police considère en fait un objectif important

de *nombreuses* enquêtes policières, c.-à-d. mener finalement à l'identification du suspect, comme concluant quant à l'objet de la fouille. Bien entendu, la police cherchait à identifier la personne qui avait utilisé les adresses IP lors de la perpétration des infractions, mais elle le faisait au moyen d'une série de mesures, et la mesure en cause en l'espèce a révélé uniquement le FSI de l'utilisateur.

[138] Ma collègue reconnaît à juste titre que les renseignements révélés par les adresses IP font partie de l'objet de la prétendue fouille. Cependant, elle inclut dans l'objet toute mesure menant à l'identification ultime du suspect, malgré le fait que de tels renseignements ne sont pas révélés par les adresses IP à elles seules, suivant la preuve au dossier. Avec égards, je crois qu'il s'agit là de la plus grande différence entre sa position et la mienne.

[139] J'ajoute en passant qu'il serait incompatible avec une définition fonctionnelle de l'objet de la fouille d'affirmer en fait que *toute* mesure prise dans une enquête met en jeu une attente raisonnable au respect de la vie privée. Une telle conclusion perturberait le juste équilibre que notre Cour a établi entre l'intérêt des Canadiens au respect effectif de leur vie privée et l'intérêt de ceux-ci à ce qu'il ne soit pas fait obstacle à l'application de la loi (voir, p. ex., *Tessling*, par. 17; *Kang-Brown*, par. 10; *Vu*, par. 21; *R. c. Stairs*, 2022 CSC 11). En rejetant une allégation selon laquelle il existait une attente raisonnable au respect de la vie privée à l'égard d'une conversation en ligne avec un policier qui se faisait passer pour une enfant, ma collègue l'a bien expliqué dans ses motifs concordants dans l'arrêt *R. c. Mills*, 2019 CSC 22,

[2019] 2 R.C.S. 320 : « L'autre conclusion aurait une incidence importante et négative sur les opérations policières d'infiltration, y compris celles menées électroniquement, [et elle] ne permet tout simplement pas d'établir un équilibre approprié entre la vie privée des individus et la sécurité de nos enfants » (par. 52). Je vois de la même façon les conséquences de la conclusion générale tirée par ma collègue en l'espèce.

[140] Je conclus donc que la présente fouille avait pour objet les adresses IP, c.-à-d. les ensembles de chiffres, et l'identité du FSI qui est révélée par celles-ci. La juge du procès et les juges majoritaires de la Cour d'appel ont statué correctement sur cette question.

B. *Caractère objectivement raisonnable de l'attente au respect de la vie privée*

[141] Il faut alors se demander si l'attente subjective de l'appelant au respect de sa vie privée à l'égard de l'objet de la fouille était objectivement raisonnable. Je conclus qu'elle ne l'était pas.

[142] La question de savoir si une attente au respect de la vie privée est raisonnable dépend de plusieurs facteurs. Ils peuvent inclure le lieu fouillé, le contrôle sur l'objet de la fouille, le caractère privé de l'objet, si l'objet était à la vue du public, si l'objet a été abandonné, si des tiers possédaient déjà l'objet, si la méthode de fouille a porté atteinte à l'intérêt en matière de vie privée en cause, si la méthode de fouille était elle-même déraisonnable, et si la fouille a révélé des renseignements

biographiques (voir, p. ex., *Tessling*, par. 32). Cette liste n'est pas exhaustive. Aucun facteur à lui seul n'est déterminant.

[143] Les facteurs ne seront pas tous pertinents pour l'analyse dans un cas donné. Prendre en considération le type d'intérêt en matière de vie privée en cause peut parfois être utile lorsqu'il s'agit de déterminer quels facteurs sont pertinents.

[144] Les trois types d'intérêt en matière de vie privée qui ressortent de la jurisprudence sont d'ordre personnel, territorial et informationnel. C'est le dernier type d'intérêt qui est clairement en cause en l'espèce. L'intimité informationnelle peut être définie comme [TRADUCTION] « le droit revendiqué par des particuliers, des groupes ou des institutions de déterminer eux-mêmes le moment, la manière et la mesure dans lesquels des renseignements les concernant sont communiqués » (*Tessling*, par. 23, citant A. F. Westin, *Privacy and Freedom* (1970), p. 7).

[145] Compte tenu des faits de l'espèce et en particulier de l'intérêt en matière d'intimité informationnelle qui est en jeu, les facteurs pertinents pour l'analyse du caractère raisonnable sont le caractère privé de l'objet, le contrôle sur l'objet et le lieu fouillé (voir *Marakah*, par. 24). Il s'agit des facteurs sur lesquels les parties et les cours inférieures ont mis l'accent, et je vais les examiner à tour de rôle.

[146] Cependant, avant de ce faire, je souhaite examiner la décision de ma collègue de s'appuyer sur des décisions étrangères comme « décriv[ant] de façon convaincante l'interaction entre les adresses IP et l'approche normative que notre Cour

a systématiquement appliquée à l'art. 8 » (par. 83). Avec égards, j'estime que ces décisions ne sont pas pertinentes. Tout d'abord, elles portent sur des cadres législatifs différents de pays différents. L'arrêt *Breyer c. Bundesrepublik Deutschland*, C-582/14, EU:C:2016:779, traitait de la question de savoir si une personne était identifiable au moyen d'une adresse IP *par le site Web consulté*, et non par l'État en tant que tel. L'arrêt *Vidal-Hall c. Google Inc.*, [2015] EWCA Civ 311, [2016] Q.B. 1003, a simplement répondu à la question de savoir si la signification *ex juris* aurait dû être autorisée dans cette affaire, et la réponse affirmative donnée par la Cour d'appel s'apparentait au refus d'une demande visant à faire radier un acte de procédure au motif que celui-ci ne révèle aucune cause d'action raisonnable (*Altimo Holdings c. Kyrgyz Mobil Tel Ltd*, [2011] UKPC 7, [2012] 1 W.L.R. 1804, par. 84-86). Plus fondamentalement, toutefois, ces décisions traitaient de faits différents et de dossiers différents.

(1) Caractère privé de l'objet

[147] Le caractère privé de l'objet d'une prétendue fouille peut appuyer une conclusion suivant laquelle une attente au respect de la vie privée est raisonnable. C'est ce qui découle de l'objet de l'art. 8, à savoir protéger les gens « contre les intrusions injustifiées de l'État dans leur vie privée » (*Hunter c. Southam Inc.*, [1984] 2 R.C.S. 145, p. 160). Comme dans le cas de la détermination de l'objet, la question est de savoir non seulement si l'objet lui-même est privé, mais aussi s'il est susceptible de révéler d'autres renseignements privés essentiels, tels des renseignements biographiques

(*Gomboc*, par. 14). Ce facteur revêt une importance particulière en ce qui a trait aux intérêts en matière d'intimité informationnelle, comme celui en cause en l'espèce. Lorsque seule l'intimité informationnelle est en cause, il peut être presque essentiel que les renseignements eux-mêmes soient privés pour qu'il existe une attente raisonnable au respect de la vie privée.

[148] En l'espèce, les adresses IP n'étaient pas privées et, *eu égard aux faits*, ne révélaient pas de renseignements privés de quelque nature que ce soit, et encore moins des renseignements biographiques. Selon la preuve d'expert, ce n'est que lorsqu'une adresse IP est combinée à d'autres renseignements qu'elle peut tendre à révéler des renseignements intimes sur une personne. Comme je l'ai déjà démontré, rien dans la preuve ne suggère que la police peut obtenir quelque renseignement privé que ce soit sur une personne en ne disposant que d'une adresse IP. Sans plus, tout ce qu'une adresse IP révèle à la police est le FSI d'un utilisateur — ce qui ne constitue guère un élément de nature particulièrement privée, et encore moins des « renseignements biographiques ».

[149] Ma collègue conclut que des adresses IP, sans plus, révèlent des renseignements très sensibles et personnels, y compris l'identité de leur utilisateur. Bien que je sois consciente que l'approche normative applicable à l'analyse fondée sur l'art. 8 exige un certain degré de souplesse, j'estime que la présente affaire doit être jugée sur la base du dossier de preuve actuel et de rien d'autre. La preuve au dossier ne

doit pas être ignorée; elle a été soumise au juge du procès et vérifiée au moyen du processus contradictoire rigoureux.

[150] En outre, personne en l'espèce n'a soutenu qu'un simple achat constitue un renseignement privé, qu'il soit effectué en ligne ou autrement (par. 61-62). Personne n'a présenté un tel argument, probablement parce que sans identification de l'acheteur, le fait de l'achat ne veut rien dire.

[151] Tout cela milite fortement contre une conclusion selon laquelle toute attente au respect de la vie privée était raisonnable.

(2) Contrôle sur l'objet

[152] Le contrôle sur l'objet de la fouille appuie généralement une conclusion selon laquelle il y avait une attente raisonnable au respect de la vie privée, alors que l'absence de contrôle peut militer contre une telle conclusion (*Marakah*, par. 38). L'idée est simple : lorsque nous contrôlons quelque chose, nous pouvons nous attendre à ce que les autres respectent notre intérêt à l'égard de cette chose — et jusqu'à un certain point l'exiger. Ce raisonnement ne rend pas le contrôle nécessaire à l'établissement d'une attente raisonnable au respect de la vie privée, mais son existence est un facteur qui peut étayer la conclusion qu'il existe une telle attente.

[153] À la lumière de la preuve d'expert, l'appelant semblait n'avoir guère de contrôle sur les adresses IP. Le FSI peut changer l'adresse IP d'un utilisateur à son gré

et sans préavis. C'est ce qui distingue nettement les adresses IP des messages textes, tels ceux dans *Marakah*, où les juges majoritaires de notre Cour ont affirmé que les gens « exercent un véritable contrôle sur l'information qu'ils envoient par message texte en décidant de la manière dont ils la divulguent ainsi que du moment où ils le font et à qui ils la divulguent » (par. 39).

[154] Au vu de la preuve, il semble que les adresses IP n'étaient visibles que pour les sites Web que l'appelant choisissait de visiter, ce qui constitue un contrôle limité. Cela dit, une comparaison utile peut être établie entre le fait de laisser des empreintes digitales sur les lieux d'un crime et celui de laisser une adresse IP à la vue d'un site Web. Un internaute qui laisse derrière lui des données relatives à une adresse IP perd complètement le contrôle de ce qui se passe avec ces chiffres, tout comme une personne perd le contrôle de ce qui se passe avec ses empreintes digitales après avoir touché quelque chose. On ne saurait sérieusement faire valoir qu'une enquête policière où des empreintes digitales sont relevées au moyen de poudres et conservées — sans plus — pourrait mettre en jeu une attente raisonnable au respect de la vie privée. Il en va de même — dans ce cas également, sans plus — de l'obtention d'une adresse IP.

[155] Le facteur du contrôle tend donc à exclure une conclusion selon laquelle l'attente de l'appelant au respect de sa vie privée était raisonnable.

(3) Lieu fouillé

[156] Le lieu fouillé joue sur le caractère raisonnable de toute attente au respect de la vie privée à l'égard de celui-ci. L'idée du lieu se rapporte essentiellement au concept d'intimité territoriale (*Tessling*, par. 22). Elle est donc quelque peu éloignée des faits de l'espèce, qui, rappelons-le, mettent en jeu l'intimité informationnelle, et elle prend nécessairement moins d'importance. La question qui se posait devant les cours inférieures, comme celle qui se pose devant la Cour, est celle de savoir si le lieu fouillé pourrait être qualifié comme étant le domicile de l'appelant, ainsi que ce dernier le soutient. Il est reconnu depuis longtemps qu'une personne a une attente accrue au respect de sa vie privée dans son domicile (voir, p. ex., *R. c. Feeney*, [1997] 2 R.C.S. 13, par. 78). Par conséquent, qualifier le lieu fouillé comme étant le domicile de l'appelant appuierait en quelque sorte son affirmation selon laquelle il avait une attente raisonnable au respect de sa vie privée.

[157] À mon avis, cependant, le lieu, lorsque correctement qualifié, est la base de données de l'entreprise de traitement des cartes de crédit. C'est à cet endroit que les adresses IP ont été stockées et que l'entreprise les a extraites afin de répondre à la demande de la police. Comme l'a reconnu à juste titre la juge du procès, la prétendue fouille n'a pas été effectuée au domicile de l'appelant, et le lieu où elle s'est déroulée n'accroît pas le caractère objectivement raisonnable de son attente subjective au respect de sa vie privée.

(4) Conclusion sur l'attente raisonnable au respect de la vie privée

[158] Considérant ces facteurs ensemble, je conclus que l'appelant n'avait pas une attente raisonnable au respect de sa vie privée à l'égard des adresses IP contenues sur les serveurs de l'entreprise de traitement des cartes de crédit, et du FSI qu'elles ont révélé. La police n'avait pas besoin d'une autorisation judiciaire avant de demander les adresses IP à l'entreprise afin de déterminer le FSI associé à celles-ci. La police a suivi à la lettre les enseignements de l'arrêt *Spencer*.

[159] Pour être claire, en concluant que l'appelant n'avait pas une attente raisonnable au respect de sa vie privée à l'égard des adresses IP dans les circonstances de l'espèce, je n'exclus pas du tout la possibilité qu'une personne puisse avoir une telle attente sur le fondement de faits différents. Il en est ainsi parce que, rappelons-le, « [l]'existence d'une attente raisonnable en matière de protection de la vie privée [. . .] exig[e] toujours une analyse contextuelle qui repose sur des faits » (*R. c. McNeil*, 2009 CSC 3, [2009] 1 R.C.S. 66, par. 12). En effet, l'analyse doit être effectuée eu égard à « l'ensemble des circonstances d'un cas particulier » (*Edwards*, par. 31 (je souligne)). Néanmoins, bien que la présente affaire porte sur l'infraction de fraude, il convient de noter que des enquêtes policières faisant intervenir des adresses IP ont également lieu dans le contexte d'autres infractions criminelles. De fait, la jurisprudence regorge d'exemples où la police fait enquête sur des infractions contre des enfants, y compris la pornographie juvénile et le leurre d'enfant, au moyen d'adresses IP (voir, p. ex., *R. c. O'Brien*, 2023 ONCA 197, 166 O.R. (3d) 114; *R. c. Ilia*, 2023 ONCA 75, 523 C.R.R. (2d) 128; *R. c. Allen*, 2020 ONCA 664, 396 C.C.C. (3d) 1; *R. c. West*, 2020 ONCA

473, 392 C.C.C. (3d) 271; *R. c. Caza*, 2015 BCCA 374, 376 B.C.A.C. 258; *Ward*; *Trapp*; *R. c. Smith*, 2005 BCCA 334, 199 C.C.C. (3d) 404).

[160] Le résultat auquel arrive ma collègue selon lequel toutes les adresses IP, et non pas seulement certaines d'entre elles, créent une attente raisonnable au respect de la vie privée (voir les par. 12 et 87-88) compromettrait sérieusement la capacité de la police d'enquêter sur ces infractions graves contre des enfants. Étant « partie des membres les plus vulnérables de notre société » (*R. c. Friesen*, 2020 CSC 9, [2020] 1 R.C.S. 424, par. 1), les enfants doivent recevoir « une protection accrue afin [de ne pas être] victimes d'infractions sexuelles » (*Mills*, par. 23, le juge Brown). Comme l'a écrit ma collègue dans ses motifs concordants dans l'arrêt *Mills*, une affaire de leurre d'enfant, « au fur et à mesure qu'évolue la technologie, les moyens de commettre des crimes — et d'enquêter sur ceux-ci — évoluent également » (par. 39). Vu cette évolution de la cybercriminalité, exiger que la police demande l'autorisation d'obtenir une adresse IP dans tous les cas aurait pour effet d'exacerber les difficultés existantes auxquelles est confronté le système de justice pénale. À cet égard, je citerais les propos du juge Moldaver (dissident, bien que sur une question différente relative à l'art. 8) dans l'arrêt *Marakah*, par. 185, en ce qui a trait au fonctionnement du système de justice :

> La nécessité accrue d'obtenir cette autorisation judiciaire pourrait grever les ressources policières et judiciaires d'un système de justice pénale déjà surchargé. Les enquêtes seraient ralenties, il faudrait plus de fonctionnaires judiciaires et l'administration de la justice pénale tout entière en souffrira.

[161] Je souligne que, pour parvenir au même résultat que celui auquel arrive ma collègue en l'espèce, il me faudrait, d'une part, examiner différents scénarios factuels pour tirer de nouvelles conclusions sur les renseignements qu'une adresse IP est susceptible de révéler et, d'autre part, expliquer ce que des tiers pourraient faire volontairement avec les données qu'ils recueillent. Je ne le peux pas, parce cela reviendrait à ne tenir aucun compte des limites de la compétence de notre Cour, de la norme de contrôle applicable aux conclusions de fait, de la preuve particulière au dossier, et également de l'équité procédurale. Un tribunal doit examiner les faits tels qu'ils sont, et non tels qu'ils pourraient être, que ce soit en raison d'un changement technologique (*Tessling*, par. 28-29 et 55) ou d'un dossier de preuve différent. Si les faits sont changés, [TRADUCTION] « la cause est modifiée » pour reprendre les propos très anciens de Plowden. Mais ce ne serait pas la présente cause.

[162] Exposée brièvement, la compétence de notre Cour dans les appels en matière criminelle se limite aux questions de droit (*Code criminel*, L.R.C. 1985, c. C-46, art. 691 à 693; *Loi sur la Cour suprême*, L.R.C. 1985, c. S-26, par. 40(3)), ce qui signifie qu'annuler les conclusions de fait des cours inférieures ne constitue pas une option. Même s'il s'agissait d'une option, personne n'a suggéré que la norme de contrôle applicable pour annuler des conclusions de fait est respectée en l'espèce. Personne ne l'a fait parce qu'en première instance, les parties ont souscrit à la preuve de l'expert de la défense sur laquelle reposaient les conclusions de fait qui sous-tendent l'analyse fondée sur l'art. 8.

[163] Annuler les conclusions de fait des cours inférieures reviendrait aussi essentiellement à prendre connaissance d'office de divers faits contestables concernant les adresses IP et les renseignements qui peuvent en être dégagés, ce qui serait, à mon avis, incompatible avec la jurisprudence de notre Cour sur la connaissance d'office (*R. c. Find*, 2001 CSC 32, [2001] 1 R.C.S. 863, par. 48). Sur ce, j'aimerais également aborder le fait que l'une des parties intervenantes invoque dans son mémoire des documents gouvernementaux et autres documents (p. ex., Commissariat à la protection de la vie privée du Canada, *Ce qu'une adresse IP peut révéler à votre sujet : Rapport préparé par la Direction de l'analyse des technologies du Commissariat à la protection de la vie privée du Canada* (2013)). Bien que je convienne avec ma collègue que les intervenants jouent un rôle important, ce rôle est circonscrit. Des arrêts récents de la Cour ont indiqué clairement que des intervenants ne peuvent pas compléter le dossier de preuve en appel et ont expliqué pourquoi cette règle existe (*R. c. McGregor*, 2023 CSC 4, par. 24, citant *R. c. Sharma*, 2022 CSC 39, par. 75). Le point de vue général selon lequel il convient de recourir à une preuve vérifiée au moyen du processus contradictoire, plutôt qu'à la connaissance d'office, pour établir les faits en contexte constitutionnel est également bien établi (*R. c. Spence*, 2005 CSC 71, [2005] 3 R.C.S. 458, par. 68; *In re The Board of Commerce Act, 1919, and The Combines and Fair Prices Act, 1919*, [1922] 1 A.C. 191 (C.P.), p. 201).

[164] Avec le plus grand respect, j'estime que l'effet du raisonnement de ma collègue est de répondre à une question qui n'est pas posée, sur le fondement de scénarios factuels différents de celui en l'espèce, afin de régler un problème social qui

n’est pas en cause ici. Je ne dirai rien de plus sur le sujet, de manière à ne pas préjuger la question si jamais elle est soulevée.

VI. Conclusion

[165] Je conclus que les juges majoritaires de la Cour d’appel ont confirmé à juste titre la décision de la juge du procès selon laquelle l’appelant n’avait pas une attente raisonnable au respect de sa vie privée à l’égard des adresses IP dans les circonstances de l’espèce. Je suis donc d’avis de rejeter le pourvoi.

Pourvoi accueilli, le juge en chef WAGNER *et les juges* CÔTÉ, ROWE *et* O’BONSAWIN *sont dissidents.*

Procureurs de l’appelant : McKay Ferg, Calgary.

Procureur de l’intimé : Alberta Crown Prosecution Service, Calgary.

Procureur de l’intervenante la directrice des poursuites pénales : Service des poursuites pénales du Canada, Halifax.

Procureur de l’intervenant le procureur général de l’Ontario : Ministère du Procureur général de l’Ontario, Bureau des avocats de la Couronne — Droit criminel, Toronto.

Procureur de l'intervenant le procureur général de la Colombie-Britannique : Attorney General of British Columbia — Criminal Appeals and Special Prosecutions, Victoria.

Procureurs de l'intervenante l'Association canadienne des libertés civiles : Kapoor Barristers, Toronto.

Procureurs de l'intervenante British Columbia Civil Liberties Association : Pringle Chivers Sparks Teskey, Vancouver; British Columbia Civil Liberties Association, Vancouver.