COUR SUPRÊME DU CANADA

RÉFÉRENCE : R. *c.* Spencer, 2014 CSC 43, [2014] 2 R.C.S. 212

DATE : 20140613
DOSSIER : 34644

ENTRE :

Matthew David Spencer
inAppelant
et
Sa Majesté la Reine
Intimée
et
Directeur des poursuites pénales,
procureur général de l'Ontario,
procureur général de l'Alberta,
commissaire à la protection de la vie privée du Canada,
Association canadienne des libertés civiles et
Criminal Lawyers' Association of Ontario
Intervenants

TRADUCTION FRANÇAISE OFFICIELLE

CORAM : La juge en chef McLachlin et les juges LeBel, Abella, Rothstein, Cromwell, Moldaver, Karakatsanis et Wagner

MOTIFS DE JUGEMENT : (par. 1 à 87)

Le juge Cromwell (avec l'accord de la juge en chef McLachlin et des juges LeBel, Abella, Rothstein, Moldaver, Karakatsanis et Wagner)

Matthew David Spencer *Appelant*

c.

Sa Majesté la Reine *Intimée*

et

Directeur des poursuites pénales,
procureur général de l'Ontario,
procureur général de l'Alberta,
commissaire à la protection de la vie privée du Canada,
Association canadienne des libertés civiles et
Criminal Lawyers' Association of Ontario *Intervenants*

Répertorié : R. *c.* Spencer

2014 CSC 43

N^{o} du greffe : 34644.

2013 : 9 décembre; 2014 : 13 juin[*].

Présents : La juge en chef McLachlin et les juges LeBel, Abella, Rothstein, Cromwell, Moldaver, Karakatsanis et Wagner.

EN APPEL DE LA COUR D'APPEL DE LA SASKATCHEWAN

---

[*] Une requête en modification des motifs a été accordée le 6 novembre 2014 modifiant le par. 12. Les modifications ont été incorporées dans les présents motifs.

Droit constitutionnel — Charte des droits — Fouilles, perquisitions et saisies — Protection des renseignements personnels — Police détenant des renseignements selon lesquels une adresse IP a été utilisée pour avoir accès à de la pornographie juvénile ou pour la télécharger — Demande de la police au fournisseur de services Internet de lui fournir volontairement le nom et l'adresse de l'abonnée à qui appartient l'adresse IP — Utilisation de ces renseignements par la police pour obtenir un mandat lui permettant de perquisitionner dans la résidence de l'accusé — La police a-t-elle effectué une fouille ou une perquisition inconstitutionnelle lorsqu'elle a obtenu les renseignements relatifs à l'abonnée à qui appartenait l'adresse IP? — La preuve ainsi obtenue devrait-elle être écartée? — L'élément de faute de l'infraction qui consiste à rendre accessible la pornographie juvénile exige-t-il la preuve d'un appui délibéré? — Code criminel, L.R.C. 1985, ch. C-46, art. 163.1(3), (4), 487.014(1) — Loi sur la protection des renseignements personnels et les documents électroniques, L.C. 2000, ch. 5, art. 7(3)c.1)(ii) — Charte canadienne des droits et libertés, art. 8.

La police a découvert l'adresse de protocole Internet (IP) de l'ordinateur qu'une personne avait utilisé pour accéder à de la pornographie juvénile et pour la stocker à l'aide d'un programme de partage de fichiers. Elle a ensuite obtenu auprès du fournisseur de services Internet (FSI), sans autorisation judiciaire préalable, les renseignements relatifs à l'abonnée à qui appartenait cette adresse IP. Il s'agit d'une demande qui aurait été fondée sur le sous-al. 7(3)*c.*1)(ii) de la *Loi sur la protection des renseignements personnels et les documents électroniques* (*LPRPDE*). Les

policiers ont ainsi découvert l'accusé. Celui-ci avait téléchargé de la pornographie juvénile à partir d'Internet avant de sauvegarder les fichiers en question dans un répertoire qui était accessible à d'autres internautes utilisateurs du même programme de partage de fichiers. L'accusé a été inculpé et déclaré coupable au procès de possession de pornographie juvénile, mais il a été acquitté de l'accusation de la rendre accessible. La Cour d'appel a confirmé la déclaration de culpabilité; elle a cependant annulé l'acquittement et ordonné la tenue d'un nouveau procès.

Arrêt : Le pourvoi est rejeté.

On détermine s'il existe une attente raisonnable en matière de respect de la vie privée, compte tenu de l'ensemble des circonstances, en examinant et en soupesant un grand nombre de facteurs interreliés. Dans la présente affaire, le litige porte principalement sur l'objet de la fouille ou de la perquisition et sur la question de savoir si l'attente subjective de l'accusé en matière de vie privée était raisonnable. Les deux éléments pertinents pour déterminer le caractère raisonnable de son attente au respect de sa vie privée sont, d'une part, la nature de l'intérêt en matière de vie privée qui est en jeu et, d'autre part, le cadre législatif et contractuel régissant la communication par le FSI des renseignements relatifs à l'abonnée.

Pour définir l'objet d'une fouille ou d'une perquisition, les tribunaux examinent non seulement la nature des renseignements précis recherchés, mais aussi la nature des renseignements qui sont ainsi révélés. En l'espèce, la fouille ou la perquisition n'avait pas simplement pour objet le nom et l'adresse d'une personne qui

était liée par contrat au FSI. Il s'agissait plutôt de l'identité d'une abonnée aux services Internet à qui correspondait une utilisation particulière de ces services.

La nature de l'intérêt en matière de vie privée visé par l'action de l'État tient au caractère privé du lieu ou de l'objet visé par la fouille ou la perquisition ainsi qu'aux conséquences de cette dernière pour la personne qui en fait l'objet, et non à la nature légale ou illégale de la chose recherchée. En l'espèce, on s'intéresse principalement au caractère privé des renseignements personnels. Cet aspect est souvent assimilé à la confidentialité. Il comprend également, en matière informationnelle, la notion connexe, mais plus large, de contrôle, d'accès et d'utilisation[1]. L'anonymat en tant que facette du droit à la vie privée revêt cependant une importance particulière dans le contexte de l'utilisation d'Internet. Il faut reconnaître que l'identité d'une personne liée à son utilisation d'Internet donne naissance à un intérêt en matière de vie privée qui a une portée plus grande que celui inhérent à son nom, à son adresse et à son numéro de téléphone qui figurent parmi les renseignements relatifs à l'abonné. En établissant un lien entre des renseignements particuliers et une personne identifiable, les renseignements relatifs à l'abonné peuvent compromettre les droits en matière de vie privée quant à l'identité d'une personne en tant que source, possesseur ou utilisateur des renseignements visés. Un certain degré d'anonymat est propre à beaucoup d'activités menées sur Internet et l'anonymat pourrait donc, compte tenu de l'ensemble des circonstances, servir de fondement au droit à la vie privée visé par la protection constitutionnelle contre les

[1] voir Erratum, [2018] 2 R.C.S. iv (à paraître)

fouilles, les perquisitions et les saisies abusives. En l'espèce, la demande de la police, dans le but d'établir un lien entre une adresse IP donnée et les renseignements relatifs à l'abonnée, visait en fait à établir un lien entre une personne précise et des activités en ligne précises. Ce genre de demande concerne, en ce qui a trait aux renseignements personnels, le droit à la vie privée relatif à l'anonymat puisqu'elle vise à établir un lien entre le suspect et des activités entreprises en ligne sous le couvert de l'anonymat, activités qui, comme on l'a reconnu dans d'autres circonstances, mettent en jeu d'importants droits en matière de vie privée.

Il ne fait aucun doute que les cadres législatif et contractuel peuvent aussi être pertinents, mais pas nécessairement déterminants, quant à la question de savoir s'il existe une attente raisonnable en matière de vie privée. En l'espèce, les cadres contractuel et législatif se chevauchent et les dispositions applicables ne sont guère utiles pour évaluer le caractère raisonnable de l'attente de l'accusé au respect de sa vie privée. Le sous-al. 7(3)*c.*1)(ii) de la *LPRPDE* ne peut être considéré comme un des facteurs défavorables à l'existence d'une attente raisonnable en matière de vie privée puisque l'interprétation juste de la disposition applicable dépend elle-même de l'existence d'une telle attente raisonnable en matière de vie privée. Il serait raisonnable que l'internaute s'attende à ce qu'une simple demande faite par la police n'entraîne pas l'obligation de communiquer les renseignements personnels en question ou n'écarte pas l'interdiction générale prévue par la *LPRPDE* quant à la communication de renseignements personnels sans le consentement de l'intéressé. Les dispositions du contrat en l'espèce justifient l'existence d'une attente raisonnable

en matière de vie privée. La demande de renseignements n'était pas étayée par la source de l'autorité légitime de la police, en ce sens que cette dernière pouvait formuler une demande, mais ne détenait pas l'autorité pour obliger le fournisseur à s'y conformer. Compte tenu de l'ensemble des circonstances de la présente affaire, il existe une attente raisonnable en matière de vie privée à l'égard des renseignements relatifs à l'abonnée. La demande faite par la police visant la communication volontaire par le FSI de renseignements de cette nature constitue donc une fouille.

La question de savoir si la fouille effectuée en l'espèce était légitime est subordonnée à celle de savoir si elle était autorisée par la loi. Ni le par. 487.014(1) du *Code criminel*, ni la *LPRPDE* n'ont pour effet de conférer à la police des pouvoirs en matière de fouilles, de perquisitions ou de saisies. Le paragraphe 487.014(1) est une disposition déclaratoire qui confirme les pouvoirs de common law permettant aux policiers de formuler des questions. La *LPRPDE* est une loi qui a pour objet d'accroître la protection des renseignements personnels. Puisque, en l'espèce, les policiers n'avaient pas le pouvoir d'effectuer une fouille ou une perquisition pour obtenir des renseignements relatifs à l'abonnée en l'absence de circonstances contraignantes ou d'une loi qui n'a rien d'abusif, ils ne peuvent obtenir un nouveau pouvoir en matière de fouille ou de perquisition par l'effet combiné d'une disposition déclaratoire et d'une disposition adoptée afin de favoriser la protection des renseignements personnels. L'exécution de la fouille ou de la perquisition en l'espèce violait donc la *Charte*. Si les renseignements relatifs à l'abonnée ne lui avaient pas été communiqués, la police n'aurait pas pu obtenir le mandat. Par

conséquent, si ces renseignements sont écartés (ce qui doit être le cas, parce qu'ils ont été obtenus d'une façon inconstitutionnelle), il n'y avait aucun motif valable justifiant la délivrance d'un mandat. La fouille ou la perquisition à la résidence était donc abusive et violait la *Charte*.

Les policiers se sont toutefois servi de ce qu'ils croyaient raisonnablement être des moyens légitimes pour poursuivre un objectif important visant l'application de la loi. Par sa nature, la conduite des policiers en l'espèce ne serait pas susceptible de déconsidérer l'administration de la justice. Bien que l'incidence de la conduite attentatoire sur les droits de l'accusé garantis par la *Charte* favorise l'exclusion de la preuve, les infractions reprochées en l'espèce sont graves. La société a un intérêt manifeste à ce que l'affaire soit jugée et à ce que le fonctionnement du système de justice demeure irréprochable au regard des individus accusés de ces infractions graves. Une mise en balance de ces trois facteurs permet de conclure que c'est l'exclusion de la preuve, et non son admission, qui serait susceptible de déconsidérer l'administration de la justice. L'admission de la preuve est donc confirmée.

Il n'est pas contesté que, dans le cadre d'une poursuite sous le régime du par. 163.1(3) du *Code criminel*, il faut prouver que l'accusé avait connaissance du fait que le matériel pornographique était rendu accessible à d'autres personnes. Il n'est toutefois pas nécessaire que l'accusé doive sciemment, par une certaine action délibérée, faciliter l'accessibilité au matériel. Les éléments de l'infraction sont tous

réunis lorsque l'accusé rend sciemment la pornographie accessible à d'autres personnes. Puisque l'aveuglement volontaire était une question en litige et que l'erreur du juge du procès — lorsqu'il a conclu qu'il était nécessaire d'accomplir une action délibérée pour satisfaire à l'exigence de la *mens rea* de l'infraction de rendre accessible — lui a fait omettre l'examen de cette question, il serait raisonnable de penser que cette erreur a eu une incidence sur le verdict d'acquittement. L'ordonnance prescrivant la tenue d'un nouveau procès est confirmée.

Jurisprudence

Arrêts mentionnés : *R. c. Ward*, 2012 ONCA 660, 112 O.R. (3d) 321; *Hunter c. Southam Inc.*, [1984] 2 R.C.S. 145; *R. c. Dyment*, [1988] 2 R.C.S. 417; *R. c. Plant*, [1993] 3 R.C.S. 281; *R. c. Tessling*, 2004 CSC 67, [2004] 3 R.C.S. 432; *Alberta (Information and Privacy Commissioner) c. Travailleurs et travailleuses unis de l'alimentation et du commerce, section locale 401*, 2013 CSC 62, [2013] 3 R.C.S. 733; *R. c. Patrick*, 2009 CSC 17, [2009] 1 R.C.S. 579; *R. c. Cole*, 2012 CSC 53, [2012] 3 R.C.S. 34; *R. c. Gomboc*, 2010 CSC 55, [2010] 3 R.C.S. 211; *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. A.M.*, 2008 CSC 19, [2008] 1 R.C.S. 569; *Dagg c. Canada (Ministre des Finances)*, [1997] 2 R.C.S. 403; *McInerney c. MacDonald*, [1992] 2 R.C.S. 138; *R. c. Duarte*, [1990] 1 R.C.S. 30; *R. c. Wise*, [1992] 1 R.C.S. 527; *R. c. Morelli*, 2010 CSC 8, [2010] 1 R.C.S. 253; *R. c. Vu*, 2013 CSC 60, [2013] 3 R.C.S. 657; *R. c. Collins*, [1987] 1 R.C.S. 265; *R. c. McNeice*, 2010 BCSC 1544 (CanLII); *R. c. Grant*, 2009

CSC 32, [2009] 2 R.C.S. 353; *R. c. Briscoe*, 2010 CSC 13, [2010] 1 R.C.S. 411; *R. c. Graveline*, 2006 CSC 16, [2006] 1 R.C.S. 609.

Lois et règlements cités

Charte canadienne des droits et libertés, art. 8, 24(2).

Code criminel, L.R.C. 1985, ch. C-46, art. 163.1(3), (4), 487.014.

Freedom of Information and Protection of Privacy Act, S.S. 1990-91, ch. F-22.01, art. 29(2)(g).

Loi sur la protection des renseignements personnels et les documents électroniques, L.C. 2000, ch. 5, art. 3, 5(3), 7, ann. 1, art. 4.3.

Doctrine et autres documents cités

Canada. Rapport du groupe d'étude établi conjointement par le ministère des Communications et le ministère de la Justice. *L'ordinateur et la vie privée*. Ottawa : Information Canada, 1972.

Gleicher, Nathaniel. « Neither a Customer Nor a Subscriber Be : Regulating the Release of User Information on the World Wide Web » (2009), 118 *Yale L.J.* 1945.

Gutterman, Melvin. « A Formulation of the Value and Means Models of the Fourth Amendment in the Age of Technologically Enhanced Surveillance » (1988), 39 *Syracuse L. Rev.* 647.

Hubbard, Robert W., Peter DeFreitas and Susan Magotiaux. « The Internet — Expectations of Privacy in a New Context » (2002), 45 *Crim. L.Q.* 170.

Hunt, Chris D. L. « Conceptualizing Privacy and Elucidating its Importance : Foundational Considerations for the Development of Canada's Fledgling Privacy Tort » (2011), 37 *Queen's L.J.* 167.

Paton-Simpson, Elizabeth. « Privacy and the Reasonable Paranoid : The Protection of Privacy in Public Places » (2000), 50 *U.T.L.J.* 305.

Slane, Andrea, and Lisa M. Austin. « What's In a Name? Privacy and Citizenship in the Voluntary Disclosure of Subscriber Information in Online Child Exploitation Investigations » (2011), 57 *Crim. L.Q.* 486.

Westin, Alan F. *Privacy and Freedom*. New York : Atheneum, 1970.

POURVOI contre un arrêt de la Cour d'appel de la Saskatchewan (les juges Cameron, Ottenbreit et Caldwell), 2011 SKCA 144, 377 Sask. R. 280, 528 W.A.C. 280, [2012] 4 W.W.R. 425, 283 C.C.C. (3d) 384, [2011] S.J. No. 729 (QL), 2011 CarswellSask 786, qui a confirmé la déclaration de culpabilité de l'accusé quant à l'infraction de possession de pornographie juvénile et annulé son acquittement quant à l'infraction de rendre accessible la pornographie juvénile prononcés par le juge Foley, 2009 SKQB 341, 361 Sask. R. 1, [2009] S.J. No. 798 (QL), 2009 CarswellSask 905, et ordonné la tenue d'un nouveau procès. Pourvoi rejeté.

Aaron A. Fox, c.r., et *Darren Kraushaar*, pour l'appelant.

Anthony B. Gerein, pour l'intimée.

Ronald C. Reimer et *David Schermbrucker*, pour l'intervenant le directeur des poursuites pénales.

Susan Magotiaux et *Allison Dellandrea*, pour l'intervenant le procureur général de l'Ontario.

Jolaine Antonio, pour l'intervenant le procureur général de l'Alberta.

Mahmud Jamal, *Patricia Kosseim*, *Daniel Caron* et *Sarah Speevak*, pour l'intervenant le commissaire à la protection de la vie privée du Canada.

Anil K. Kapoor et *Lindsay L. Daviau*, pour l'intervenante l'Association canadienne des libertés civiles.

Jonathan Dawe et *Jill R. Presser*, pour l'intervenante Criminal Lawyers' Association of Ontario.

Version française du jugement de la Cour rendu par

LE JUGE CROMWELL —

I. Introduction

[1] L'existence d'Internet remet en question la protection de la vie privée et soulève une multitude de questions inédites et épineuses à cet égard. Le présent pourvoi porte sur une de ces questions.

[2] La police a découvert l'adresse de protocole Internet (IP) de l'ordinateur qu'une personne avait utilisé pour accéder à de la pornographie juvénile et pour la stocker à l'aide d'un programme de partage de fichiers. Les policiers ont ensuite obtenu auprès du fournisseur de services Internet (FSI), sans autorisation judiciaire préalable, les renseignements relatifs à l'abonnée à qui appartenait cette adresse IP.

Ils ont ainsi découvert l'appelant, M. Spencer. Celui-ci avait téléchargé de la pornographie juvénile dans un répertoire qui était accessible à d'autres internautes utilisateurs du même programme de partage de fichiers. M. Spencer a été inculpé, puis, au procès, déclaré coupable de possession de pornographie juvénile et acquitté de l'infraction de rendre accessible de la pornographie juvénile.

[3] Au procès, M. Spencer a fait valoir que la police avait effectué une fouille ou une perquisition inconstitutionnelle lorsqu'elle a obtenu les renseignements relatifs à l'abonnée à qui appartenait l'adresse IP et que la preuve ainsi obtenue devait être écartée. Il a également déclaré dans son témoignage qu'il ignorait que d'autres personnes pouvaient avoir accès au répertoire partagé et qu'il n'a donc pas sciemment rendu les fichiers accessibles. Le juge du procès a conclu qu'il n'y avait pas eu de violation du droit de M. Spencer à la protection contre les fouilles, les perquisitions et les saisies abusives. Il a toutefois estimé que pour être déclaré coupable de l'infraction de « rendre accessible » il faut avoir donné un certain [TRADUCTION] « appui délibéré » à l'accès à la pornographie, ce que M. Spencer n'avait pas fait. Il a également jugé que la déposition de M. Spencer selon laquelle il ignorait que d'autres personnes pouvaient avoir accès à son répertoire était véridique, de sorte que l'élément de faute de cette infraction (*mens rea*) n'avait pas été établi. Le juge a donc déclaré M. Spencer coupable de l'infraction de possession, mais l'a acquitté de l'accusation de rendre accessible.

[4] La Cour d'appel a confirmé la déclaration de culpabilité pour possession

de pornographie juvénile, souscrivant à la conclusion du juge du procès selon laquelle le fait d'obtenir les renseignements relatifs à l'abonnée ne constituait pas une fouille ou une perquisition abusive et concluant que, même s'il y en avait eu une, elle aurait été raisonnable. La cour a cependant annulé l'acquittement quant à l'accusation de rendre accessible au motif que le juge du procès avait eu tort d'exiger la preuve d'un appui délibéré à l'accès aux fichiers par d'autres personnes et elle a ordonné la tenue d'un nouveau procès quant à ce chef d'accusation.

[5] Le présent pourvoi soulève quatre questions auxquelles je suis d'avis de répondre comme suit :

1. L'obtention par la police, auprès du FSI, des renseignements sur l'abonnée à qui appartenait l'adresse IP constitue-t-elle une fouille ou une perquisition?

Je suis d'avis que oui.

2. Si oui, la fouille ou la perquisition était-elle autorisée par la loi?

Je suis d'avis que non.

3. Sinon, la preuve ainsi obtenue devrait-elle être écartée?

J'estime que la preuve ne devrait pas être écartée.

4. Le juge du procès a-t-il commis une erreur relativement à l'élément de faute de l'infraction qui consiste à « rendre accessible »?

Le juge a effectivement commis une erreur et je suis d'avis de confirmer l'ordonnance de la Cour d'appel visant la tenue d'un nouveau procès.

II. Analyse

A. *L'obtention par la police, auprès du FSI, des renseignements sur l'abonnée à qui appartenait l'adresse IP constitue-t-elle une fouille ou une perquisition?*

[6] Monsieur Spencer soutient que la police effectuait une fouille ou une perquisition lorsqu'elle a obtenu, auprès du FSI, Shaw Communications Inc., les renseignements relatifs à l'abonnée à qui appartenait l'adresse IP en cause en l'espèce. Le ministère public intimé adopte le point de vue contraire. Je suis d'accord avec M. Spencer sur ce point. Je présenterai tout d'abord un résumé des faits pertinents; je procéderai ensuite à l'analyse juridique.

(1) Les faits et l'historique judiciaire

[7] Monsieur Spencer, qui habitait avec sa sœur, se connectait à Internet à partir d'un compte ouvert au nom de cette dernière. Il utilisait le programme de partage de fichiers LimeWire sur son ordinateur pour télécharger de la pornographie juvénile à partir d'Internet. LimeWire est un logiciel gratuit de partage de fichiers poste à poste que chacun pouvait télécharger à l'époque sur son ordinateur. Les

systèmes poste à poste, comme LimeWire, permettent aux utilisateurs de télécharger des fichiers directement à partir des ordinateurs d'autres utilisateurs. LimeWire ne comporte pas de base de données centrale. Il compte plutôt sur ses utilisateurs qui partagent directement leurs fichiers avec d'autres utilisateurs. Le logiciel est couramment utilisé pour télécharger de la musique et des films, mais il peut aussi servir à télécharger de la pornographie tant adulte que juvénile. C'est l'utilisation du programme de partage de fichiers par M. Spencer qui a retenu l'attention de la police et qui a finalement mené à la fouille ou à la perquisition qui fait l'objet du présent litige.

[8] À l'aide d'un logiciel accessible au public, l'agent Darren Parisien (nommé sergent-détective depuis), du Service de police de Saskatoon, a recherché des personnes qui partageaient des fichiers de pornographie juvénile. Il pouvait accéder au contenu des répertoires partagés appartenant à d'autres utilisateurs du logiciel. Autrement dit, il pouvait [TRADUCTION] « voir » ce que d'autres utilisateurs du programme de partage de fichiers pouvaient « voir ». Il pouvait également obtenir deux numéros associés à un utilisateur donné : l'adresse IP correspondant à la connexion Internet établie par un ordinateur et l'identificateur global unique (GUID), soit le numéro associé à chaque ordinateur qui utilise un logiciel donné. L'adresse IP de l'ordinateur à partir duquel on obtient des fichiers partagés est affichée dans le cadre du processus de partage de fichiers. Il y a peu de renseignements au dossier sur la nature des adresses IP en général ou des adresses IP que Shaw fournit à ses abonnés. Dans l'arrêt *R. c. Ward*, 2012 ONCA 660, 112 O.R. (3d) 321, par. 21-26, on

trouve une description de certaines des différences qui existent entre les adresses IP. Pour les besoins de l'espèce, une chose est certaine : l'adresse IP qu'a obtenue le sergent-détective Parisien correspondait aux activités informatiques qui se déroulaient au moment précis où il les observait.

[9] Le sergent-détective Parisien a dressé une liste des adresses IP correspondant aux ordinateurs qui avaient été utilisés pour le partage de ce qu'il estimait être de la pornographie juvénile. Il a ensuite comparé cette liste aux renseignements figurant dans une base de données qui permet d'associer des adresses IP à des emplacements approximatifs. Il a découvert qu'une des adresses IP semblait se trouver à Saskatoon et que Shaw était le FSI.

[10] Le sergent-détective Parisien a ensuite déterminé que l'ordinateur de M. Spencer était connecté à Internet ainsi qu'à LimeWire. Par conséquent, le sergent-détective (ainsi que tout autre utilisateur du logiciel LimeWire) pouvait parcourir le répertoire partagé du suspect. Il a vu une grande quantité de ce qu'il estimait être de la pornographie juvénile. Il ne connaissait cependant pas l'emplacement exact de l'ordinateur ni l'identité de son utilisateur.

[11] Pour établir un lien entre les activités informatiques en question et un emplacement précis, et potentiellement une personne, les enquêteurs ont présenté par écrit à Shaw une [TRADUCTION] « demande de la part des autorités d'application de la loi » en vue d'obtenir des renseignements relatifs à l'abonnée qui utilisait cette adresse IP, soit, notamment, son nom, son adresse et son numéro de téléphone. La

demande — qui aurait été fondée sur le sous-al. 7(3)*c.*1)(ii) de la *Loi sur la protection des renseignements personnels et les documents électroniques*, L.C. 2000, ch. 5 (*LPRPDE*) — indiquait que la police enquêtait sur une infraction prévue au *Code criminel*, L.R.C. 1985, ch. C-46, relative à la pornographie juvénile et à Internet et que les renseignements relatifs à l'abonnée étaient demandés aux fins d'une enquête qui était en cours. (Les dispositions législatives pertinentes sont reproduites en annexe.) Les enquêteurs n'avaient pas obtenu ni tenté d'obtenir une ordonnance de communication (c.-à-d. l'équivalent d'un mandat de perquisition dans ce contexte).

[12] Shaw a donné suite à la demande et a fourni le nom, l'adresse et le numéro de téléphone de la sœur de M. Spencer, la cliente à qui appartenait l'adresse IP. À l'aide de ces renseignements, la police a obtenu un mandat permettant de perquisitionner dans la résidence de M^{me} Spencer, où habitait M. Spencer, et de saisir l'ordinateur de celui-ci, ce que les policiers ont fait. La fouille de l'ordinateur de M. Spencer a permis de découvrir environ 50 images et deux vidéos de pornographie juvénile.

[13] Monsieur Spencer a été accusé de possession de pornographie juvénile, infraction décrite au par. 163.1(4) du *Code criminel*, et de rendre accessible de la pornographie juvénile sur Internet, en contravention du par. 163.1(3). Le fait que les images trouvées dans son répertoire partagé constituaient de la pornographie juvénile n'est pas contesté.

[14] Au procès, M. Spencer a tenté de faire écarter les éléments de preuve

découverts sur son ordinateur au motif que les mesures prises sans autorisation judiciaire préalable par les policiers, en vue d'obtenir son adresse auprès de Shaw, correspondaient à une fouille ou à une perquisition abusive et contrevenaient à l'art. 8 de la *Charte canadienne des droits et libertés*. Le juge du procès a rejeté cette prétention et déclaré M. Spencer coupable de l'infraction de possession. La Cour d'appel de la Saskatchewan a confirmé la décision du juge relativement à la question de la fouille ou de la perquisition.

(2) La demande adressée à Shaw constituait-elle une fouille ou une perquisition?

[15] Suivant l'article 8 de la *Charte*, « [c]hacun a droit à la protection contre les fouilles, les perquisitions ou les saisies abusives. » La Cour insiste depuis longtemps sur la nécessité d'adopter, à l'égard de l'art. 8, une approche téléologique axée principalement sur la protection de la vie privée considérée comme une condition préalable à la sécurité individuelle, à l'épanouissement personnel et à l'autonomie ainsi qu'au maintien d'une société démocratique prospère : *Hunter c. Southam Inc.*, [1984] 2 R.C.S. 145, p. 156-157; *R. c. Dyment*, [1988] 2 R.C.S. 417, p. 427-428; *R. c. Plant*, [1993] 3 R.C.S. 281, p. 292-293; *R. c. Tessling*, 2004 CSC 67, [2004] 3 R.C.S. 432, par. 12-16; *Alberta (Information and Privacy Commissioner) c. Travailleurs et travailleuses unis de l'alimentation et du commerce, section locale 401*, 2013 CSC 62, [2013] 3 R.C.S. 733, par. 22.

[16] En premier lieu, il s'agit de savoir si cette protection contre les fouilles,

les perquisitions et les saisies abusives s'applique en l'espèce. Pour le savoir, il faut déterminer si les mesures prises par la police en vue d'obtenir les renseignements sur l'abonnée à qui appartenait l'adresse IP constituaient une fouille, une perquisition ou une saisie au sens de l'art. 8 de la *Charte*. Pour ce faire, il faut déterminer si, compte tenu de l'ensemble des circonstances, M. Spencer s'attendait raisonnablement au respect du caractère privé des renseignements fournis par Shaw à la police. Si tel était le cas, l'obtention de ces renseignements constituait une fouille ou une perquisition.

[17] On détermine s'il existe une attente raisonnable en matière de respect de la vie privée, compte tenu de l'ensemble des circonstances, en examinant et en soupesant un grand nombre de facteurs interreliés qui comprennent à la fois des facteurs relatifs à la nature des droits en matière de vie privée visés par l'action de l'État et des facteurs qui ont trait plus directement à l'attente en matière de respect de la vie privée, considérée tant subjectivement qu'objectivement, par rapport à ces droits : voir, p. ex., *Tessling*, par. 38; *Ward*, par. 65. La nécessité d'examiner ces éléments compte tenu de « l'ensemble des circonstances » fait ressortir le fait qu'ils sont souvent interdépendants, qu'ils doivent être adaptés aux circonstances de chaque cas, et qu'ils doivent être considérés dans leur ensemble.

[18] La grande variété et le nombre important de facteurs pouvant être pris en considération pour évaluer les attentes raisonnables en matière de respect de la vie privée peuvent être regroupés, par souci de commodité, en quatre grandes catégories : (1) l'objet de la fouille ou de la perquisition contestée; (2) le droit du demandeur à

l'égard de l'objet; (3) l'attente subjective du demandeur en matière de respect de sa vie privée relativement à l'objet; et (4) la question de savoir si cette attente subjective en matière de respect de la vie privée était objectivement raisonnable, eu égard à l'ensemble des circonstances : *Tessling*, par. 32; *R. c. Patrick*, 2009 CSC 17, [2009] 1 R.C.S. 579, par. 27; *R. c. Cole*, 2012 CSC 53, [2012] 3 R.C.S. 34, par. 40. Il ne s'agit toutefois pas d'un examen purement factuel. L'attente raisonnable en matière de vie privée est de nature normative et non simplement descriptive : *Tessling*, par. 42. Ainsi, même si l'analyse du droit au respect de la vie privée tient compte du contexte factuel, elle « 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 privée » : *Patrick*, par. 14; voir aussi *R. c. Gomboc*, 2010 CSC 55, [2010] 3 R.C.S. 211, par. 34, et *Ward*, par. 81-85.

[19] Quelques brefs commentaires suffiront pour traiter deux aspects du pourvoi. Selon le juge du procès, il n'y avait pas d'attente subjective en matière de vie privée dans la présente affaire : 2009 SKQB 341, 361 Sask. R. 1, par. 18. Toutefois, comme je vais l'expliquer ultérieurement, la conclusion du juge du procès reposait sur une définition inexacte de l'objet de la fouille ou de la perquisition. Selon une interprétation juste de cet objet, l'attente subjective de M. Spencer au respect du caractère privé de ses activités en ligne peut aisément être déduite de son utilisation de la connexion réseau pour transmettre des renseignements sensibles : *Cole*, par. 43. L'intérêt direct de M. Spencer à l'égard de l'objet de la fouille ou de la perquisition

est également manifeste. Même s'il n'était pas personnellement parti au contrat conclu avec le FSI, il avait accès à Internet avec la permission de l'abonnée et il l'utilisait au moyen de son propre ordinateur, à son lieu de résidence.

[20] Dans la présente affaire, le litige porte donc principalement sur l'objet de la fouille ou de la perquisition et sur la question de savoir si l'attente subjective de M. Spencer en matière de vie privée était raisonnable. Les deux éléments pertinents pour déterminer le caractère raisonnable de son attente au respect de sa vie privée sont, d'une part, la nature de l'intérêt en matière de vie privée qui est en jeu et, d'autre part, le cadre législatif et contractuel régissant la communication par le FSI des renseignements relatifs à l'abonnée.

[21] En l'espèce, j'ai jugé utile d'examiner d'abord l'objet de la fouille ou de la perquisition, ensuite la nature des droits en matière de vie privée que mettent en jeu les actes de l'État et, enfin, le cadre législatif et contractuel applicable. Il s'agit manifestement d'éléments interreliés, mais l'analyse axée sur ces vastes catégories assure une certaine précision tout en permettant d'examiner de manière exhaustive « l'ensemble des circonstances ».

a) *L'objet de la fouille ou de la perquisition*

[22] Selon M. Spencer, c'est la demande faite à Shaw par la police qui constitue l'action de l'État correspondant à une fouille, à une perquisition ou à une saisie aux fins de l'application de l'art. 8 de la *Charte*. Nous devons donc examiner

l'objet de cette demande pour pouvoir déterminer quels étaient les droits en jeu en matière de vie privée.

[23] Dans bien des cas, il est facile de définir l'objet de l'action de la police qui, selon les allégations, constitue une fouille ou une perquisition. Ce n'est par contre pas toujours ainsi; et la présente espèce appartient à cette seconde catégorie. Les parties et les tribunaux de juridiction inférieure ont adopté des positions nettement divergentes sur cette question importante, situation qui se retrouve également dans la jurisprudence : voir, par exemple, les décisions mentionnées dans l'arrêt *Ward*, par. 3.

[24] Monsieur Spencer fait valoir que l'objet de la fouille ou de la perquisition contestée comportait des renseignements d'ordre biographique, soit des renseignements personnels et confidentiels sur les personnes habitant à l'adresse fournie par Shaw qui correspondait à l'adresse IP. Pour sa part, le ministère public soutient que la fouille ou la perquisition contestée visait plutôt simplement le nom, l'adresse et le numéro de téléphone correspondant à une adresse IP accessible au public.

[25] Les tribunaux de la Saskatchewan ont exprimé les mêmes opinions divergentes. Le juge du procès a adopté le point de vue du ministère public selon lequel la police n'avait recherché et obtenu que des renseignements d'ordre général qui ne correspondent pas à des données d'ordre biographique relatives à M. Spencer. Le juge Ottenbreit de la Cour d'appel a partagé en grande partie la même opinion. À

son avis, les renseignements recherchés par la police en l'espèce ne faisaient qu'établir l'identité de l'utilisateur de l'adresse IP qui était désigné dans le contrat. La possibilité que ces renseignements finissent par révéler plusieurs aspects des activités menées par des personnes identifiables sur Internet était [TRADUCTION] « sans importance » : 2011 SKCA 144, 377 Sask. R. 280, par. 110 (voir également *R. c. Trapp*, 2011 SKCA 143, 377 Sask. R. 246, par. 119-124 et 134). Par contre, selon le juge Caldwell (le juge Cameron a souscrit à son opinion à ce sujet), lorsqu'il s'agit de qualifier l'objet d'une fouille ou d'une perquisition contestée, il faut aller au-delà des renseignements [TRADUCTION] « banals » relatifs à l'abonné, tels son nom et son adresse (par. 22). Il faut aussi tenir compte de la possibilité que ces renseignements révèlent des détails intimes sur le mode de vie et les choix personnels de l'individu : voir également l'arrêt *Trapp*, le juge Cameron, par. 33-37.

[26] Je souscris pour l'essentiel aux conclusions formulées sur ce point par les juges Caldwell et Cameron de la Cour d'appel. Dans bien des cas, la définition de l'objet de la fouille ou de la perquisition fait l'unanimité. Cependant, dans les cas qui posent davantage de difficultés à cet égard, la Cour a adopté dans le passé une approche large et fonctionnelle, 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. La Cour a examiné non seulement la nature des renseignements précis recherchés, mais aussi la nature des renseignements qui sont ainsi révélés.

[27] Plusieurs arrêts de la Cour reflètent cette approche. J'examinerai d'abord

l'arrêt *Plant*. Dans cette affaire concernant des aspects informationnels de la vie privée, la Cour a insisté sur le droit garanti au respect de la vie privée relativement à des 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 » : p. 293. Fait important, la Cour a ensuite précisé que la protection garantie par l'art. 8 vise non seulement les renseignements de cette nature, mais aussi les « renseignements tendant à révéler des détails intimes sur le mode de vie et les choix personnels de l'individu » : *ibid.* (je souligne).

[28] La Cour a suivi la même approche dans l'arrêt *Tessling*, mais elle a tiré une conclusion différente. Dans cette affaire, il a été conclu que l'objet de la perquisition contestée était la chaleur émanant de la surface d'un édifice. La technique d'imagerie FLIR (système infrarouge à vision frontale) a servi à évaluer les activités qu'il y avait à l'intérieur d'une résidence, mais les émanations de chaleur ne permettaient pas, à elles seules, de distinguer les sources de chaleur. Bref, les émanations de chaleur n'avaient, en elles-mêmes, aucune signification, parce qu'elles ne permettaient pas de déduire quelle activité précise produisait la chaleur : par. 35-36. La question cruciale portait sur la nature des activités que permettaient de déduire les images FLIR et qui se déroulaient à l'intérieur de la résidence — nous en conviendrons, un lieu de nature éminemment privée.

[29] Je passe maintenant à l'arrêt *R. c. Kang-Brown*, 2008 CSC 18, [2008] 1 R.C.S. 456, et au pourvoi connexe *R. c. A.M.*, 2008 CSC 19, [2008] 1 R.C.S. 569. La

Cour était divisée sur d'autres points, mais elle a conclu à l'unanimité que la vérification du sac de M. Kang-Brown à l'aide d'un chien renifleur constituait une fouille. Comme l'ont expliqué les juges Deschamps et Bastarache, en décelant ce qu'il y avait dans l'air à proximité du sac, le chien a servi d'outil d'enquête et son intervention a « immédiatement et directement permis [aux policiers] de faire une forte inférence » quant au contenu du sac : la juge Deschamps, par. 174-175; le juge Bastarache, par. 227. Ainsi, bien que les « informations » recueillies par le chien renifleur tenaient simplement de l'odeur qu'il y avait dans l'air à l'extérieur du sac, la réaction du chien a permis aux policiers de faire une forte inférence quant au contenu du sac. Comme l'a indiqué le juge Binnie dans l'arrêt *A.M.* (qui portait sur l'intervention d'un chien renifleur pour vérifier le sac à dos de l'accusé), « [e]n se servant du chien, le policier a pu "voir" à travers le tissu opaque du sac à dos » : par. 67.

[30] La façon de définir l'objet d'une fouille ou d'une perquisition contestée a été examinée pour la dernière fois par la Cour dans l'arrêt *Gomboc*. Bien qu'elle fût divisée sur d'autres questions, elle s'est prononcée à l'unanimité sur le cadre d'analyse à appliquer pour déterminer l'objet d'une « fouille ou [d'une] perquisition ». Dans cette affaire, la Cour a examiné la fiabilité des inférences qu'il est possible de tirer à partir des données enregistrées à l'aide d'un ampèremètre numérique muni d'un enregistreur (AN) au sujet d'activités données se déroulant à l'intérieur d'une résidence pour déterminer si l'utilisation de l'ampèremètre constituait une fouille ou une perquisition. La juge Abella (avec l'accord des juges

Binnie et LeBel) a tenu compte « de la solidité et de la fiabilité des inférences pouvant être tirées à partir des cycles de consommation d'électricité [. . .] relativement à la tenue d'une activité particulière à une adresse » : par. 81 (je souligne). La Juge en chef et le juge Fish ont affirmé que les données enregistrées par l'AN « éclairent sur les activités privées se déroulant à l'intérieur de la maison » : par. 119. La juge Deschamps (avec l'accord des juges Charron, Rothstein et Cromwell) s'est demandé dans quelle mesure les données enregistrées par l'AN révèlent les activités qui se déroulent à l'intérieur de la maison : par. 38.

[31] Ainsi, il est évident que, pour définir l'objet de la fouille ou de la perquisition, il faut tenir compte 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. La méthode qu'il convient d'adopter a été clairement résumée par le juge Doherty au par. 65 de l'arrêt *Ward*. Lorsqu'elle est appelée à identifier l'objet d'une fouille ou d'une perquisition contestée, une cour ne doit pas adopter une approche [TRADUCTION] « restrictive qui porte sur les actions commises ou sur l'espace envahi, mais plutôt une approche fondée sur la nature des droits en matière de vie privée auxquels l'action de l'État pourrait porter atteinte » : *ibid*.

[32] Si on applique cette méthode en l'espèce, je souscris pour l'essentiel à la conclusion tirée par le juge Cameron dans l'arrêt *Trapp* et adoptée par le juge Caldwell de la Cour d'appel dans la présente affaire. La fouille n'avait pas

simplement pour objet le nom et l'adresse d'une personne qui était liée par contrat à Shaw. Il s'agissait plutôt de l'identité d'une abonnée aux services Internet à qui correspondait une utilisation particulière de ces services. Comme l'a affirmé le juge Cameron au par. 35 de l'arrêt *Trapp* :

> [TRADUCTION] Qualifier de tels renseignements de simples « renseignements relatifs à l'abonné » ou de « renseignements sur le client » ou encore de rien d'autre que de « renseignements sur le nom, l'adresse et le numéro de téléphone » tend à occulter leur véritable nature. Je tiens à le préciser, parce que ces qualifications font 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.

[33] En l'espèce, la fouille avait pour objet l'identité de l'abonnée dont la connexion à Internet correspondait à une activité informatique particulière sous surveillance.

b) *La nature de l'intérêt en matière de vie privée auquel l'action de l'État pourrait porter atteinte*

[34] La nature de l'intérêt en matière de vie privée visé par l'action de l'État constitue un autre aspect de l'ensemble des circonstances et un facteur important pour apprécier le caractère raisonnable d'une attente en matière de vie privée. Dans le passé, la Cour a souligné l'importance, lorsqu'il est question de renseignements personnels, d'interpréter le droit à la vie privée de telle sorte qu'il protège tant la confidentialité que le contrôle des renseignements en question. À mon avis, il est

nécessaire en l'espèce d'élargir quelque peu cette interprétation de manière à tenir compte du rôle que joue l'anonymat dans la protection des droits en matière de vie privée sur Internet.

[35] Certes, la vie privée est « une notion générale quelque peu évanescente » : *Dagg c. Canada (Ministre des Finances)*, [1997] 2 R.C.S. 403, par. 67. Certains auteurs ont souligné la confusion à ce sujet, sur le plan théorique, et l'absence de consensus apparent quant à ses nature et limites : voir, p. ex., C. D. L. Hunt, « Conceptualizing Privacy and Elucidating its Importance : Foundational Considerations for the Development of Canada's Fledgling Privacy Tort » (2011), 37 *Queen's L.J.* 167, p. 176-177. Nonobstant ces enjeux, la Cour a décrit trois grandes catégories de droits en matière de vie privée, qui regroupent notamment les aspects qui ont trait aux lieux, à la personne et à l'information, et qui, malgré leur chevauchement fréquent, ont permis de préciser la nature des droits en matière de vie privée en jeu dans des situations particulières : voir, p. ex., *Dyment*, p. 428-429; *Tessling*, par. 21-24. Il s'agit d'outils d'analyse, et non de catégories strictes ou mutuellement exclusives.

[36] La nature de l'intérêt en matière de vie privée ne dépend pas de la question de savoir si, dans un cas particulier, le droit à la vie privée masque une activité légale ou une activité illégale. En effet, l'analyse porte sur le caractère privé du lieu ou de l'objet visé par la fouille ou la perquisition ainsi que sur les conséquences de cette dernière pour la personne qui en fait l'objet, et non sur la

nature légale ou illégale de la chose recherchée. Pour reprendre les propos du juge Binnie dans l'arrêt *Patrick*, il ne s'agit pas de savoir si l'appelant possédait un droit légitime au respect de la vie privée à l'égard de la dissimulation de son utilisation d'Internet dans le but d'accéder à de la pornographie juvénile, mais plutôt de savoir si, d'une manière générale, les citoyens ont droit au respect de leur vie privée à l'égard des renseignements concernant les abonnés de services Internet relativement aux ordinateurs qu'ils utilisent dans leur domicile à des fins privées : *Patrick*, par. 32.

[37] En l'espèce, nous nous intéressons principalement au caractère privé des renseignements personnels. En outre, puisque l'ordinateur repéré et, en quelque sorte, surveillé par la police se trouvait dans la résidence de M. Spencer, un aspect du droit à la vie privée lié aux lieux est aussi en jeu. Dans le présent contexte, le lieu de l'activité est toutefois accessoire à la nature de l'activité elle-même. En effet, les internautes ne s'attendent pas à perdre leur anonymat en ligne lorsqu'ils accèdent à Internet ailleurs que chez eux au moyen d'un téléphone intelligent ou d'un appareil portatif. En l'espèce, tout comme dans l'arrêt *Patrick*, par. 45, le fait qu'une résidence soit en cause ne constitue donc pas un facteur déterminant, mais fait néanmoins partie de l'ensemble des circonstances : voir, p. ex., *Ward*, par. 90.

[38] Pour revenir à la question du droit à la vie privée en ce qui a trait aux renseignements personnels, j'estime qu'il englobe au moins trois facettes qui se chevauchent, mais qui se distinguent sur le plan conceptuel. Il s'agit de la confidentialité, du contrôle et de l'anonymat.

[39] Le caractère privé des renseignements personnels est souvent assimilé à la confidentialité. Par exemple, le patient s'attend raisonnablement à ce que ses renseignements d'ordre médical demeurent confidentiels : voir, p. ex., *McInerney c. MacDonald*, [1992] 2 R.C.S. 138, p. 149.

[40] Or, le droit à la vie privée comprend également, en matière informationnelle, la notion connexe, mais plus large, de contrôle, d'accès et d'utilisation, c'est-à-dire [TRADUCTION] « le droit revendiqué par des particuliers, des groupes ou des institutions de déterminer eux-mêmes à quel moment les renseignements les concernant sont communiqués, de quelle manière et dans quelle mesure » : A. F. Westin, *Privacy and Freedom* (1970), p. 7, cité dans *Tessling*, par. 23[2]. Le juge La Forest a d'ailleurs souligné ce point dans l'arrêt *Dyment* en affirmant que la facette du droit à la vie privée en ce qui a trait aux renseignements personnels qui porte sur le contrôle « découle du postulat selon lequel l'information de caractère personnel est propre à l'intéressé, qui est libre de la communiquer ou de la taire comme il l'entend » (*Dyment*, p. 429, citant *L'ordinateur et la vie privée*, le Rapport du groupe d'étude établi conjointement par le ministère des Communications et le ministère de la Justice (1972), p. 13). Même si les renseignements seront divulgués et qu'ils ne peuvent être considérés comme confidentiels, « les cas abondent où on se doit de protéger les attentes raisonnables de l'individu que ces renseignements seront gardés confidentiellement par ceux à qui ils sont divulgués, et qu'ils ne seront utilisés que pour les fins pour lesquelles ils ont été divulgués » (p. 429-430); voir également

[2] voir Erratum, [2018] 2 R.C.S. iv (à paraître)

R. c. Duarte, [1990] 1 R.C.S. 30, p. 46.

[41] Il existe aussi une troisième conception de l'aspect informationnel du droit à la vie privée qui revêt une importance particulière dans le contexte de l'utilisation d'Internet. Il s'agit de l'anonymat. À mon avis, le droit à la vie privée que garantirait l'art. 8 doit inclure cette conception de la vie privée.

[42] L'élément « anonymat » de la vie privée n'est pas nouveau. Il est présent dans un large éventail de contextes allant de sondages anonymes à la protection de l'identité des indicateurs de police. La personne qui répond à un sondage accepte volontiers de fournir ce qui peut fort bien être des renseignements de nature très personnelle. L'indicateur de police fournit des renseignements sur la perpétration d'un crime. Les renseignements en tant que tel ne sont pas privés — leur communication vise expressément la divulgation à d'autres personnes. Cela dit, cette communication tient compte du fait que l'identité de la personne qui fournit les renseignements demeurera confidentielle. Prenons, par exemple, des cas où la police veut obtenir la liste des noms correspondant aux numéros d'identification relativement aux résultats d'un sondage ou des cas où la partie défenderesse dans une affaire criminelle veut obtenir l'identité de l'indicateur ayant fourni les renseignements qui lui ont été communiqués. L'intérêt en matière de vie privée qui est en jeu dans ces exemples ne vise pas uniquement le nom d'une personne, mais aussi le lien entre la personne désignée et les renseignements personnels fournis de façon anonyme. Comme l'a fait valoir l'Association canadienne des libertés civiles,

intervenante en l'espèce, dans ses observations, [TRADUCTION] « le maintien de l'anonymat peut être essentiel pour garantir la protection de la vie privée » : mémoire, par. 7.

[43] Le professeur Westin présente l'anonymat comme une des facettes fondamentales de la vie privée. Selon lui, il permet aux personnes d'avoir des activités publiques tout en préservant la confidentialité de leur identité et en se protégeant contre la surveillance : p. 31-32; voir A. Slane et L. M. Austin, « What's In a Name? Privacy and Citizenship in the Voluntary Disclosure of Subscriber Information in Online Child Exploitation Investigations » (2011), 57 *Crim. L.Q.* 486, p. 501. L'arrêt *R. c. Wise*, [1992] 1 R.C.S. 527, donne un exemple du droit à la vie privée dans un endroit public. Dans cette affaire, la Cour a statué que la surveillance omniprésente des déplacements d'un véhicule sur la voie publique déjouait les attentes raisonnables du suspect en matière de vie privée. On aurait évidemment pu affirmer que le dispositif électronique ne constituait qu'un moyen pratique de suivre les déplacements en voiture du suspect, qu'il faisait d'ailleurs à la vue de tous. Mais la Cour n'a pas adopté cette approche.

[44] Le juge La Forest (qui, bien que dissident sur la question de l'exclusion de la preuve en application du par. 24(2), a souscrit à l'existence d'une attente raisonnable en matière du respect de la vie privée), a expliqué que, « [s]'il est normal, dans divers contextes publics, d'être observé fortuitement, nous aurions par contre toutes les raisons d'être choqués par des regards insistants. Dans ces activités

publiques, nous ne nous attendons pas à être identifiés personnellement et soumis à une surveillance intensive, mais nous cherchons plutôt à passer inaperçus » : p. 558 (je souligne), citant M. Gutterman, « A Formulation of the Value and Means Models of the Fourth Amendment in the Age of Technologically Enhanced Surveillance » (1988), 39 *Syracuse L. Rev.* 647, p. 706. Le simple fait qu'une personne quitte l'intimité de sa résidence et pénètre dans un lieu public ne signifie pas qu'elle renonce à tous ses droits en matière de vie privée, même si, en pratique, il se peut qu'elle ne soit pas en mesure d'exercer un contrôle à l'égard des personnes qui l'observent en public. Par conséquent, pour protéger les droits en matière de vie privée dans certains contextes, il nous faut reconnaître l'anonymat comme une des conceptions de la vie privée : voir E. Paton-Simpson, « Privacy and the Reasonable Paranoid : The Protection of Privacy in Public Places » (2000), 50 *U.T.L.J.* 305, p. 325-326; Westin, p. 32; Gutterman, p. 706.

[45] S'agissant de l'utilisation d'Internet, il me semble particulièrement important de reconnaître que l'anonymat s'inscrit parmi les conceptions de l'aspect informationnel du droit à la vie privée. Comme l'explique le professeur Westin, l'anonymat porte entre autres sur le droit revendiqué par une personne qui veut présenter publiquement ses idées sans être identifiée comme leur auteur : p. 32. Le professeur Westin, dont l'ouvrage a été publié en 1970, avait anticipé précisément une des caractéristiques déterminantes de certains types de communication par Internet. En effet, des millions de personnes peuvent avoir accès à une communication qui n'est toutefois pas associée à son auteur.

[46] De plus, Internet a augmenté de façon exponentielle la qualité et la quantité des renseignements stockés concernant les internautes. 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. Les fichiers témoins peuvent être utilisés pour suivre les habitudes de consommation et peuvent fournir des renseignements sur les options sélectionnées dans un site Web, sur les pages Web consultées avant et après avoir visité le site d'accueil et tout autre renseignement personnel fourni : voir N. Gleicher, « Neither a Customer Nor a Subscriber Be : Regulating the Release of User Information on the World Wide Web » (2009), 118 *Yale L.J.* 1945, p. 1948-1949; R. W. Hubbard, P. DeFreitas et S. Magotiaux, « The Internet — Expectations of Privacy in a New Context » (2002), 45 *Crim. L.Q.* 170, p. 189-191. L'utilisateur n'est pas en mesure d'exercer un contrôle total à l'égard de la personne qui peut observer le profil de ses activités en ligne et il n'est pas toujours informé de l'identité de celle-ci. Or, sous le couvert de l'anonymat — en protégeant le lien entre l'information et l'identité de la personne qu'elle concerne —, l'utilisateur peut en grande partie être assuré que ses activités demeurent confidentielles : voir Slane et Austin, p. 500-503.

[47] À mon avis, il faut reconnaître que l'identité d'une personne liée à son utilisation d'Internet donne naissance à un intérêt en matière de vie privée qui a une portée plus grande que celui inhérent à son nom, à son adresse et à son numéro de

téléphone qui figurent parmi les renseignements relatifs à l'abonné. Un chien renifleur fournit de l'information sur le contenu d'un sac et met donc en jeu des droits en matière de vie privée relativement à ce contenu. Les enregistrements de l'AN fournissent de l'information sur les activités qui se déroulent à l'intérieur d'une résidence et peuvent donc mettre en jeu des droits en matière de vie privée concernant ces activités. Dans le même ordre d'idées, en établissant un lien entre des renseignements particuliers et une personne identifiable, les renseignements relatifs à l'abonné peuvent compromettre les droits en matière de vie privée de cette personne non seulement parce qu'ils révèlent son nom et son adresse, mais aussi parce qu'ils l'identifient en tant que source, possesseur ou utilisateur des renseignements visés.

[48] Dans *Ward*, le juge Doherty, clair et lucide comme à son habitude, a fourni des explications semblables. [TRADUCTION] « Le droit à la vie privée », a-t-il écrit, « permet à une personne de fonctionner au quotidien dans la société tout en bénéficiant d'un certain degré d'anonymat indispensable à son épanouissement personnel ainsi qu'à l'épanouissement d'une société ouverte et démocratique » : par. 71. Il a conclu qu'un certain degré d'anonymat est propre à beaucoup d'activités exercées sur Internet et que, « [e]u égard à l'ensemble des circonstances, [. . .] l'anonymat peut bénéficier de la protection constitutionnelle prévue à l'art. 8 » : par. 75. Je suis d'accord. L'anonymat pourrait donc, compte tenu de l'ensemble des circonstances, servir de fondement au droit à la vie privée visé par la protection constitutionnelle contre les fouilles, les perquisitions et les saisies abusives.

[49] Le directeur des poursuites pénales, intervenant, a fait valoir que la reconnaissance du droit à l'anonymat en ligne transformerait Internet en un endroit favorable aux actes criminels en faisant obstacle aux enquêtes et aux poursuites efficaces des cybercrimes. Compte tenu de la gravité des actes criminels qui peuvent être perpétrés en ligne, cette préoccupation ne peut être prise à la légère. J'estime toutefois que la reconnaissance de la *possibilité* qu'il existe un intérêt en matière de vie privée à l'égard de l'anonymat, selon les circonstances, ne suffit pas pour reconnaître le « droit » à l'anonymat et n'a pas pour effet de menacer l'efficacité des autorités d'application de la loi relativement aux infractions commises sur Internet. En l'espèce, par exemple, il semble évident que la police disposait de renseignements détaillés permettant d'obtenir une ordonnance de communication enjoignant à Shaw de fournir les renseignements sur l'abonnée à qui appartenait l'adresse IP qu'elle avait obtenue.

[50] L'application de ce cadre d'analyse aux faits de la présente affaire est simple. Dans les circonstances de l'espèce, la demande de la police dans le but d'établir un lien entre une adresse IP donnée et les renseignements relatifs à l'abonnée visait en fait à établir un lien entre une personne précise (ou un nombre restreint de personnes dans le cas des services Internet partagés) et des activités en ligne précises. Ce genre de demande porte sur l'aspect informationnel du droit à la vie privée relatif à l'anonymat en cherchant à établir un lien entre le suspect et des activités entreprises en ligne, sous le couvert de l'anonymat, activités qui, comme la Cour l'a reconnu dans d'autres circonstances, mettent en jeu d'importants droits en

matière de vie privée : *R. c. Morelli*, 2010 CSC 8, [2010] 1 R.C.S. 253, par. 3; *Cole*, par. 47; *R. c. Vu*, 2013 CSC 60, [2013] 3 R.C.S. 657, par. 40-45.

[51] Par conséquent, je conclus que la demande de la police auprès de Shaw — visant à obtenir des renseignements relatifs à l'abonnée qui correspondaient à des activités entreprises sur Internet de façon anonyme et observées en particulier — fait intervenir, dans une grande mesure, l'aspect informationnel du droit à la vie privée. Je souscris à la conclusion du juge Caldwell sur ce point :

> [TRADUCTION] . . . une personne raisonnable et bien informée, qui se soucie de la protection de la vie privée, s'attendrait à ce que les activités qu'une personne effectue sur son propre ordinateur et dans son domicile soient confidentielles. [. . .] À mon avis, il n'importe nullement que les renseignements communiqués concernaient la sœur de M. Spencer parce que, en l'espèce, M. Spencer a, personnellement et directement, subi les conséquences des actes de la police. À première vue, ces actes font intervenir le droit de M. Spencer à la vie privée et, de ce fait, son intérêt en matière de vie privée relativement à la confidentialité des renseignements communiqués était direct et personnel. [par. 27]

c) *L'attente raisonnable en matière de respect de la vie privée*

[52] Il s'agit maintenant de savoir si l'attente de M. Spencer en matière de respect de sa vie privée était raisonnable. Selon le juge du procès, il ne pouvait pas y avoir d'attente raisonnable en matière de respect de la vie privée compte tenu des dispositions contractuelles et législatives applicables (par. 19), conclusion à laquelle le juge Caldwell a souscrit en appel : par. 42. Le juge Cameron a affirmé douter pour sa part que les dispositions du contrat et celles de la loi aient cet effet dans le contexte

de la présente affaire : par. 98.

[53] Devant la Cour, M. Spencer a fait valoir que les dispositions du contrat et de la loi n'ont pas pour effet de compromettre une attente raisonnable en matière de vie privée relativement aux renseignements relatifs à l'abonné. Selon lui, les dispositions du contrat ne font rien d'autre qu'indiquer qu'il n'y aura pas de communication des renseignements à la police, à moins que cela ne soit requis par la loi, et que la *LPRPDE* — qui vise à protéger les droits en matière de vie privée — tend à confirmer plutôt qu'à nier le caractère raisonnable d'une attente en matière de vie privée en l'espèce. Le ministère public ne souscrit pas à cet argument et appuie la position adoptée sur ce point par le juge Caldwell de la Cour d'appel.

[54] Il ne fait aucun doute que les cadres législatif et contractuel peuvent être pertinents, mais pas nécessairement déterminants, quant à la question de savoir s'il existe une attente raisonnable en matière de vie privée. Dans l'arrêt *Gomboc*, par exemple, s'exprimant au nom de quatre juges de la Cour, la juge Deschamps a conclu que les dispositions régissant les rapports entre le fournisseur d'électricité et son client revêtent une « grande importance » quant à l'attente raisonnable de M. Gomboc en matière de vie privée, mais a considéré qu'il s'agissait d'« un des nombreux facteurs dont il faut tenir compte pour apprécier l'ensemble des circonstances » : par. 31-32. La juge Deschamps a également souligné que, dans le cadre de contrats d'adhésion qui régissent les relations avec les clients, « la prudence est évidemment de mise » lorsqu'il s'agit de juger des conséquences que peuvent avoir les

dispositions de ces contrats sur le caractère raisonnable d'une attente en matière de respect de la vie privée : par. 33. Dans leurs motifs dissidents, la Juge en chef et le juge Fish ont mis l'accent sur le besoin de faire preuve de prudence dans ce contexte : par. 138-142.

[55] En l'espèce, les cadres contractuel et législatif se chevauchent parce que les conditions de service de Shaw renvoient à la *LPRPDE* et que la portée de la communication autorisée de renseignements personnels sous le régime de la *LPRPDE* repose en partie sur la question de savoir si le client a donné son consentement à cet égard. Avant d'examiner les conséquences de ces régimes sur l'analyse relative aux attentes raisonnables en matière de vie privée, je dois en préciser les modalités. Lorsque je le fais, il devient clair que les dispositions applicables ne sont guère utiles pour évaluer le caractère raisonnable de l'attente de M. Spencer au respect de sa vie privée.

[56] Shaw fournit des services Internet à ses clients conformément à une entente type relative aux « Conditions de service » (« *Joint Terms of Service* »). Sa [TRADUCTION] « Politique relative à l'utilisation acceptable » (« *Acceptable Use Policy* ») et sa « Politique sur la protection de la vie privée » (« *Privacy Policy* ») prévoient des modalités et conditions supplémentaires. Les dispositions de ces ententes sont affichées en ligne sur le site Web de Shaw et font périodiquement l'objet de modifications. Les enquêteurs ont demandé à Shaw des renseignements sur l'abonnée à qui appartenait l'adresse IP utilisée le 31 août 2007.

[57] Monsieur Spencer n'était pas lui-même partie à ces ententes, puisqu'il avait accès à Internet au moyen de l'abonnement de sa sœur. Il est d'ailleurs très courant que plusieurs utilisateurs partagent une connexion Internet. L'usager raisonnable sait que l'utilisation du service Internet est régie par certaines modalités, qui étaient d'ailleurs facilement accessibles sur le site Web de Shaw. Nous n'avons toutefois pas à décider en l'espèce si M. Spencer était lié par les modalités du contrat avec Shaw. Cependant, indépendamment de la responsabilité contractuelle, les conditions auxquelles il a pu accéder à Internet sont pertinentes pour évaluer le caractère raisonnable de son attente quant au respect de sa vie privée. Il existe trois séries de dispositions applicables qui, dans leur ensemble, prêtent à confusion quant à la manière de Shaw de répondre à une demande de renseignements relatifs à un abonné adressée par la police. À première vue, les Conditions de service semblent conférer à Shaw un vaste pouvoir discrétionnaire parce qu'elles prévoient, entre autres, qu'[TRADUCTION] « [elle] peut communiquer les renseignements nécessaires pour [. . .] satisfaire à toute demande fondée sur une loi ou un règlement ou toute autre demande du gouvernement ». Il convient toutefois d'interpréter cette disposition générale en fonction de la disposition plus spécifique concernant la communication d'adresses IP et d'autres renseignements personnels dans le contexte d'enquêtes criminelles qui figure dans la Politique relative à l'utilisation acceptable qui, elle-même, est assujettie à la Politique sur la protection de la vie privée.

[58] Suivant la Politique relative à l'utilisation acceptable (dont la mise à jour la plus récente date du 18 juin 2007), Shaw est autorisée à collaborer avec les

autorités d'application de la loi dans le cadre d'enquêtes sur des infractions criminelles, notamment en fournissant des renseignements personnels sur un abonné, *conformément à sa Politique sur la protection de la vie privée*. Cette disposition est ainsi libellée :

> [TRADUCTION] Par la présente, vous autorisez Shaw à collaborer avec (i) les autorités d'application de la loi dans le cadre d'enquêtes sur des infractions criminelles présumées, et avec (ii) les administrateurs du système d'autres fournisseurs de services Internet ou d'autres réseaux ou installations informatiques afin de faire appliquer la présente entente. Cette collaboration peut comprendre la communication du nom d'utilisateur, de l'adresse IP ou d'autres renseignements personnels concernant un abonné, conformément aux lignes directrices énoncées dans sa Politique sur la protection de la vie privée. [Je souligne.]

[59] Suivant la Politique sur la protection de la vie privée qui figure au dossier (dont la mise à jour la plus récente date du 12 novembre 2008), Shaw s'engage à protéger les renseignements personnels, définis comme des renseignements concernant un individu identifiable. Un des dix principes énoncés dans la Politique sur la protection de la vie privée a pour effet de restreindre la communication de renseignements personnels (principe n^{o} 5). Cette politique limite les circonstances dans lesquelles les renseignements personnels seront communiqués à l'insu du client ou sans son consentement à des [TRADUCTION] « circonstances exceptionnelles, conformément à la loi ». Shaw peut communiquer des renseignements à ses partenaires afin de fournir ses services, et, dans de tels cas, ces renseignements sont régis par des « normes et politiques strictes en matière de confidentialité » pour assurer leur sécurité et pour veiller à ce qu'ils soient traités conformément à la

LPRPDE. La Politique sur la protection de la vie privée prévoit également que « Shaw peut communiquer des renseignements personnels concernant un client : [. . .] à une partie ou à plusieurs tierces parties lorsque le client visé a donné son consentement à cet égard ou lorsque la communication des renseignements est exigée par la loi, conformément à la *Loi sur la protection des renseignements personnels et les documents électroniques* » (je souligne).

[60] Ainsi, la réponse à la question de savoir si la communication des renseignements personnels par Shaw est « autorisée » ou « exigée par la loi » repose sur l'analyse du cadre législatif applicable. Les dispositions du contrat, lues conjointement, sont équivoques et prêtent à confusion quant à leurs conséquences sur l'attente raisonnable de l'utilisateur en matière de vie privée relativement aux demandes de la police visant à obtenir des renseignements relatifs à l'abonné. Le cadre législatif prévu par la *LPRPDE* ne permet pas d'en apprendre davantage.

[61] La collecte, l'utilisation et la communication par Shaw de renseignements personnels concernant ses abonnés sont assujetties à la *LPRPDE*, laquelle protège les renseignements personnels que possèdent les organisations qui exercent des activités commerciales contre leur communication à l'insu de l'intéressé et sans son consentement : ann. 1, art. 4.3. L'article 7 prévoit plusieurs exceptions à cette règle générale, permettant ainsi aux organisations de communiquer des renseignements personnels sans le consentement de l'intéressé. L'exception invoquée en l'espèce figure au sous-al. 7(3)*c*.1)(ii), qui autorise la communication de renseignements à une

institution gouvernementale qui a demandé à obtenir les renseignements visés aux fins du contrôle d'application du droit en mentionnant la « source de l'autorité légitime » étayant la demande. En l'espèce, les dispositions de la *LPRPDE* ne sont pas très utiles pour déterminer s'il existe une attente raisonnable en matière de vie privée puisqu'après les avoir examinées, on se retrouve au point de départ.

[62] Le sous-alinéa 7(3)*c*.1)(ii) autorise la communication de renseignements, sans le consentement de l'intéressé, faite à une institution gouvernementale lorsque cette dernière mentionne la *source de l'autorité légitime* étayant son droit à obtenir les renseignements demandés. Il s'agit toutefois de savoir s'il existe une telle source d'autorité légitime, question dont la réponse dépend, en partie, de l'existence d'une attente raisonnable en matière de vie privée à l'égard des renseignements concernant l'abonné. La *LPRPDE* ne peut donc être considérée comme un des facteurs défavorables à l'existence d'une attente raisonnable en matière de vie privée puisque l'interprétation juste de la disposition applicable dépend elle-même de l'existence d'une telle attente raisonnable en matière de vie privée. Puisque la *LPRPDE* a pour objet de fixer des règles régissant, entre autres, la communication de « renseignements personnels d'une manière qui tient compte du droit des individus à la vie privée à l'égard des renseignements personnels qui les concernent » (art. 3), il serait raisonnable que l'internaute s'attende à ce qu'une simple demande faite par la police n'entraîne pas l'obligation de communiquer les renseignements personnels en question ou qu'elle n'écarte pas l'interdiction générale prévue par la *LPRPDE* quant à la communication de renseignements personnels sans le consentement de l'intéressé.

[63] Certes, je suis arrivé à une conclusion différente que celle formulée, dans des circonstances semblables, dans l'arrêt *Ward*, où la Cour d'appel de l'Ontario a statué que les dispositions de la *LPRPDE* constituaient un facteur qui pesait contre la reconnaissance de l'existence d'une attente raisonnable en matière de vie privée à l'égard des renseignements concernant l'abonné. Cette conclusion reposait sur deux considérations principales. Premièrement, le fait que le FSI a un intérêt légitime à collaborer avec les autorités d'application de la loi relativement à des crimes commis lors de l'utilisation de ses services : par. 99. Deuxièmement, la gravité des infractions de pornographie juvénile, compte tenu de laquelle il était raisonnable de s'attendre à ce que le FSI collabore avec la police dans le cadre d'une enquête : par. 102-103. Bien qu'elles soient certainement pertinentes sur le plan des principes, ces considérations ne sauraient avoir priorité sur le libellé clair du sous-al. 7(3)*c.*1)(ii) de la *LPRPDE*, qui n'autorise la communication de renseignements que lorsqu'une institution gouvernementale mentionne la « source de l'autorité légitime » étayant sa demande. En effet, il est raisonnable de s'attendre à ce qu'une organisation assujettie à la *LPRPDE* respecte les obligations que celle-ci lui impose à l'égard des renseignements personnels. La Cour d'appel a statué dans l'arrêt *Ward* qu'il convient d'interpréter le sous-al. 7(3)*c.*1)(ii) en tenant compte du par. 5(3), suivant lequel « [l']organisation ne peut recueillir, utiliser ou communiquer des renseignements personnels qu'à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances ». Cette règle de la « communication raisonnable » a permis de prendre en considération, pour interpréter la *LPRPDE*, des facteurs comme l'autorisation des FSI à collaborer avec la police et la lutte contre les crimes graves. Le paragraphe 5(3)

énonce un principe directeur sur lequel repose l'interprétation des diverses dispositions de la *LPRPDE*. Il ne permet pas d'écarter l'exigence claire concernant la « source de l'autorité légitime » qui étaye la demande d'une institution gouvernementale et ne règle donc pas l'impasse que crée le sous-al. 7(3)*c*.1)(ii) pour juger de l'existence ou non d'une attente raisonnable en matière de vie privée.

[64] Je fais en outre remarquer, au sujet de l'intérêt légitime du FSI dans la lutte contre les crimes commis en utilisant ses services, que des considérations tout à fait différentes peuvent s'appliquer si le FSI détecte lui-même une activité illégale et, de sa propre initiative, souhaite la signaler à la police. Une telle situation tombe sous le coup d'une exemption distincte, plus large, prévue par la *LPRPDE*, à savoir celle énoncée à l'al. 7(3)*d*). En l'espèce, l'enquête a été commencée par la police et la communication des renseignements relatifs à l'abonnée a été faite par suite de la lettre de demande envoyée à Shaw par la police.

[65] De ces modalités se dégage l'impression générale que la communication faite à la demande de la police n'aurait lieu que lorsqu'elle est exigée ou autorisée par la loi. Or, la *LPRPDE* n'autorise une telle communication que suivant l'exception prévue à l'art. 7. Il faudrait donc que la police qui formule la demande de communication détienne « l'autorité légitime » à cet égard. Pour les motifs que j'énoncerai dans la prochaine partie, la demande en cause n'était pas étayée par la source de l'autorité légitime de la police, en ce sens que cette dernière pouvait formuler une demande, mais ne détenait pas l'autorité pour obliger le fournisseur à

s’y conformer. Je conclus que les dispositions du contrat en l’espèce justifient l’existence d’une attente raisonnable en matière de vie privée, si un quelconque effet doit être donné à ces termes en cette matière, puisque la Politique sur la protection de la vie privée a pour effet de limiter strictement le droit de Shaw de communiquer des renseignements personnels concernant ses abonnés.

[66] À mon avis, compte tenu de l’ensemble des circonstances de la présente affaire, il existe une attente raisonnable en matière de vie privée à l’égard des renseignements relatifs à l’abonnée. La communication de ces renseignements permettra souvent d’identifier l’utilisateur qui mène des activités intimes ou confidentielles en ligne en tenant normalement pour acquis que ces activités demeurent anonymes. La demande faite par un policier visant la communication volontaire par le FSI de renseignements de cette nature constitue donc une fouille.

[67] Le procureur général de l’Alberta, intervenant en l’espèce, a dit craindre que, si la police n’était pas autorisée à demander la communication de renseignements relatifs à un abonné donné, d’autres demandes courantes pouvant révéler des renseignements confidentiels sur un suspect risquent d’être également interdites, ce qui aurait pour effet d’entraver indûment l’enquête sur des crimes. Par exemple, lorsque les policiers interrogent la victime d’un crime, des renseignements biographiques d’ordre personnel concernant le mode de vie du suspect pourraient être révélés. Je ne suis pas d’accord pour dire que cette conclusion découle des principes énoncés dans les présents motifs. Pour déterminer si la demande faite par un policier

à un tiers de communiquer des renseignements concernant un suspect constitue une fouille ou une perquisition, il faut se demander si, compte tenu de l'ensemble des circonstances, le suspect a une attente raisonnable en matière de vie privée à l'égard de ces renseignements : *Plant*, p. 293; *Gomboc*, par. 27-30, la juge Deschamps. Dans l'arrêt *Duarte*, la Cour a établi une distinction entre une personne qui rapporte à la police une conversation avec un suspect et l'enregistrement par la police de la même conversation. Selon la Cour, il s'agit « non plus [du] risque que quelqu'un répète nos propos, mais [du] danger bien plus insidieux qu'il y a à permettre que l'État, à son entière discrétion, enregistre et transmette nos propos » : p. 43-44. De même, dans l'affaire qui nous occupe, la demande par la police que le FSI communique les renseignements relatifs à l'abonnée constituait en fait une demande d'établir un lien entre M. Spencer et des activités précises menées en ligne qui avaient été surveillées par police, et mettait donc en jeu un droit en matière de vie privée beaucoup plus important qu'une simple question formulée lors d'une enquête policière.

B. *La fouille était-elle légitime?*

[68] Une fouille sans mandat, comme celle qui a été effectuée en l'espèce, est présumée abusive : *R. c. Collins*, [1987] 1 R.C.S. 265. Il incombe au ministère public de réfuter cette présomption. Une fouille ne sera pas abusive si a) elle est autorisée par la loi, b) la loi elle-même n'a rien d'abusif, et c) la fouille n'a pas été effectuée d'une manière abusive : p. 278. M. Spencer ne conteste pas la constitutionnalité des lois qui auraient autorisé la fouille. Il a toutefois soulevé des objections quant à la

manière, qu'il estime abusive, dont a été effectuée la fouille. À mon avis, ces objections sont mal fondées. Il ne reste donc qu'à examiner si la fouille était autorisée par la loi.

[69] Le ministère public appuie les conclusions tirées par les juges Caldwell et Cameron de la Cour d'appel selon lesquelles la fouille était légitime, compte tenu de l'effet combiné de l'art. 487.014 du *Code criminel* et du sous-al. 7(3)*c.*1)(ii) de la *LPRPDE*. En toute déférence, je ne souscris pas à cette opinion.

[70] Suivant le par. 487.014(1) du *Code criminel*, une ordonnance de communication n'est pas nécessaire pour qu'un agent de la paix « demande à une personne de lui fournir volontairement des documents, données ou renseignements qu'aucune règle de droit n'interdit à celle-ci de communiquer ». La *LPRPDE* interdit la communication de renseignements à moins que les autorités d'application de la loi ne respectent les exigences les concernant, notamment l'exigence selon laquelle une institution gouvernementale doit mentionner la source de l'autorité légitime étayant son droit *d'obtenir* les renseignements, et non seulement de les demander : sous-al. 7(3)*c.*1)(ii). Selon l'interprétation que donne le ministère public de ces dispositions, une demande de renseignements personnels faite par la police rendrait pratiquement sans effet les protections prévues par la *LPRPDE* : l'exigence relative à la « source de l'autorité légitime » ne constitue qu'une simple demande sans aucun pouvoir de contrainte, mais, par suite d'une simple demande, la communication de renseignements par l'institution en question n'est plus prohibée par la loi.

[71] Il faut distinguer la « source de l'autorité légitime » à laquelle réfère le sous-al. 7(3)*c*.1)(ii) de la *LPRPDE* et l'al. 7(3)*c*), selon lequel la communication des renseignements personnels peut être faite sans le consentement de l'intéressé lorsqu'« elle est exigée par assignation, mandat ou ordonnance d'un tribunal, d'une personne ou d'un organisme ayant le pouvoir de contraindre à la production de renseignements ou exigée par des règles de procédure se rapportant à la production de documents ». Le renvoi à la « source de l'autorité légitime » au sous-al. 7(3)*c*.1)(ii) doit viser autre chose qu'une « assignation » ou un « mandat » de perquisition. La « source de l'autorité légitime » peut avoir plusieurs sens. Cette notion peut désigner le pouvoir conféré par la common law aux policiers de poser des questions portant sur des éléments qui ne font pas l'objet d'une attente raisonnable en matière de vie privée. Elle peut renvoyer au pouvoir de la police d'effectuer une fouille ou une perquisition sans mandat dans des circonstances contraignantes ou dans des cas où une loi qui n'a rien d'abusif le permet : *Collins*. Comme le fait valoir la commissaire à la protection de la vie privée du Canada, intervenante en l'espèce, si on tient pour acquis que la « source de l'autorité légitime » nécessite davantage qu'une simple demande faite par les autorités d'application de la loi, cette notion arrive à jouer un rôle significatif dans le contexte du par. 7(3), au détriment d'autres interprétations qui n'ont pas cet effet. Bref, je suis d'accord avec la Cour d'appel de l'Ontario dans l'arrêt *Ward* sur ce point, pour dire que ni le par. 487.014(1) du *Code criminel* ni la *LPRPDE* n'ont pour effet de conférer à la police des pouvoirs en matière de fouilles, de perquisitions ou de saisies : par. 46.

[72] Je reconnais que cette conclusion diffère de celle tirée par la Cour d'appel de la Saskatchewan dans *Trapp*, par. 66, et par la Cour suprême de la Colombie-Britannique dans *R. c. McNeice*, 2010 BCSC 1544 (CanLII), par. 43. Dans l'arrêt *Trapp*, la Cour d'appel a interprété le par. 487.014(1) de concert avec l'al. 29(2)(g) de la *Freedom of Information and Protection of Privacy Act*, S.S. 1990-91, ch. F-22.01, disposition analogue à celle énoncée au sous-al. 7(3)*c.*1)(ii) de la *LPRPDE*, même si l'exigence relative à la « source de l'autorité légitime » y est absente. La cour a affirmé que le par. 487.014(1) conférait aux policiers le pouvoir de faire toute demande qui n'était pas prohibée par la loi. La Cour suprême de la Colombie-Britannique a adopté la même approche dans l'affaire *McNeice*, même si celle-ci portait sur le sous-al. 7(3)*c.*1)(ii) de la *LPRPDE*, disposition qui est en cause dans le présent pourvoi.

[73] En toute déférence, je ne peux accepter que cette conclusion s'applique au sous-al. 7(3)*c.*1)(ii) de la *LPRPDE*. Le paragraphe 487.014(1) est une disposition déclaratoire qui confirme les pouvoirs de common law permettant aux policiers de formuler des questions, comme l'indique les premiers mots de son libellé en français « [i]l demeure entendu qu[e] » ou de son libellé en anglais « [f]or greater certainty » : voir *Ward*, par. 49. La *LPRPDE* est une loi qui a pour objet, comme il est indiqué à l'art. 3, d'accroître la protection des renseignements personnels. Puisque, en l'espèce, les policiers n'avaient pas le pouvoir d'effectuer une fouille ou une perquisition pour obtenir des renseignements relatifs à l'abonnée en l'absence de circonstances contraignantes ou d'une loi qui n'a rien d'abusif, je ne vois pas comment ils

pourraient obtenir un nouveau pouvoir en matière de fouille ou de perquisition par l'effet combiné d'une disposition déclaratoire et d'une disposition adoptée afin de favoriser la protection des renseignements personnels.

[74] La police a utilisé les renseignements relatifs à l'abonnée pour étayer la dénonciation qui a conduit à la délivrance d'un mandat l'autorisant à perquisitionner dans la résidence de M^{me} Spencer. En l'absence de ces renseignements, la police n'aurait pas pu obtenir le mandat. Par conséquent, si ces renseignements sont écartés (ce qui doit être le cas, parce qu'ils ont été obtenus d'une façon inconstitutionnelle), il n'y avait aucun motif valable justifiant la délivrance d'un mandat et la fouille ou la perquisition à la résidence était abusive. Je conclus donc que l'exécution de la fouille ou de la perquisition à la résidence de M^{me} Spencer violait la *Charte* : *Plant*, p. 296; *Hunter c. Southam*, p. 161. Rien dans les présents motifs ne porte sur les pouvoirs dont disposent les policiers pour obtenir des renseignements relatifs à un abonné dans des circonstances contraignantes, par exemple, lorsqu'il est nécessaire d'obtenir de tels renseignements pour prévenir un préjudice physique imminent, ce qui n'était pas le cas en l'espèce. Rien non plus, dans les présents motifs, ne restreint ces pouvoirs.

C. *La preuve aurait-elle dû être écartée?*

[75] Ni le juge du procès ni la Cour d'appel n'ont conclu qu'il y avait violation de l'art. 8 en l'espèce. Ils n'avaient donc pas à se demander si les éléments de preuve obtenus d'une façon qui portait atteinte aux droits de M. Spencer garantis par la *Charte* devraient être écartés en application du par. 24(2) de la même *Charte*. Il

s’agit de savoir si l’admission de la preuve serait susceptible de déconsidérer l’administration de la justice. J’admets, comme M. Spencer et le ministère public intimé en conviennent, que nous pouvons trancher cette question sur la foi du dossier dont nous sommes saisis. Toutefois, je ne souscris pas à l’argument de M. Spencer selon lequel la preuve devrait être écartée. En effet, j’estime qu’il n’y a pas lieu qu’elle le soit.

[76] Le critère relatif à l’application du par. 24(2) est énoncé dans l’arrêt *R. c. Grant*, 2009 CSC 32, [2009] 2 R.C.S. 353. Le tribunal doit « évaluer et mettre en balance l’effet que l’utilisation des éléments de preuve aurait sur la confiance de la société envers le système de justice en tenant compte de : (1) la gravité de la conduite attentatoire de l’État [. . .], (2) l’incidence de la violation sur les droits de l’accusé garantis par la *Charte* [. . .] et (3) l’intérêt de la société à ce que l’affaire soit jugée au fond » : par. 71.

[77] En ce qui concerne la gravité de la conduite de l’État, j’estime qu’il n’y a pas lieu de qualifier cette dernière de « non-respect délibéré ou manifeste de la *Charte* » : *Grant*, par. 75. Le sergent-détective Parisien a déclaré qu’il croyait que la demande adressée à Shaw était autorisée par la loi et que Shaw consentirait à lui fournir l’information. Il a toutefois ajouté qu’il connaissait l’existence de décisions contradictoires quant à la question de savoir si cette pratique était légale. Bien que je ne voudrais pas qu’on comprenne des présents motifs que j’encourage les policiers à agir sans mandat dans les « zones grises », vu que le juge du procès et les trois juges

de la Cour d'appel ont conclu que le sergent-détective Parisien avait agi légalement, sa conviction était manifestement raisonnable. Bref, les policiers se sont servi de ce qu'ils croyaient raisonnablement être des moyens légitimes pour poursuivre un objectif important visant l'application de la loi. Les autres aspects relatifs à la dénonciation justifiant l'obtention du mandat de perquisition ne sont pas contestés. Par sa nature, la conduite des policiers en l'espèce ne serait pas susceptible de déconsidérer l'administration de la justice.

[78] Le deuxième facteur énoncé dans l'arrêt *Grant* porte sur l'incidence de la conduite attentatoire sur les droits de M. Spencer garantis par la *Charte*. L'incidence était très grave en l'espèce. Rappelons que l'anonymat constitue une protection importante des droits en matière de vie privée à l'égard des activités en ligne. La violation de l'anonymat a exposé les choix personnels de M. Spencer et les a soumis à l'examen de la police. Ce facteur favorise l'exclusion de la preuve.

[79] Je passe maintenant au dernier facteur, à savoir l'intérêt de la société à ce que l'affaire soit jugée au fond. Comme il est expliqué dans l'arrêt *Grant*,

> si la gravité d'une infraction accroît l'intérêt du public à ce qu'il y ait un jugement au fond, l'intérêt du public en l'irréprochabilité du système de justice n'est pas moins vital, particulièrement lorsque l'accusé encourt de lourdes conséquences pénales. [par. 84]

[80] Les infractions reprochées en l'espèce sont graves et sont punissables de peines minimales d'emprisonnement. La société a un intérêt manifeste à la fois à ce

que l'affaire soit jugée et à ce que le fonctionnement du système de justice demeure irréprochable au regard des individus accusés de ces infractions graves. Si la preuve est écartée, le ministère public n'aura effectivement aucun recours à faire valoir. Les éléments de preuve contestés (les fichiers électroniques contenant de la pornographie juvénile) sont fiables et la défense a admis lors du procès qu'ils constituaient de la pornographie juvénile. La société a sans doute un intérêt à ce que l'affaire soit jugée dans le cadre d'un procès juste et équitable, fondé sur une preuve fiable, et encore plus dans le cas d'un crime qui vise la sécurité des enfants.

[81] Après avoir mis en balance les trois facteurs, j'estime que c'est l'exclusion de la preuve, et non son admission, qui serait susceptible de déconsidérer l'administration de la justice et je suis d'avis de confirmer l'admission de cette preuve.

D. *L'élément de faute de l'infraction de « rendre accessible »*

[82] La Cour d'appel a ordonné la tenue d'un nouveau procès sur le chef d'accusation de « rendre accessible », au motif que le juge du procès avait commis une erreur dans son analyse relative à l'exigence de faute de l'infraction. Selon la Cour, le juge du procès a commis une erreur en concluant que l'infraction de rendre accessible exigeait que M. Spencer ait connaissance que certaines de ses actions délibérées avaient facilité l'accès d'autres personnes à la pornographie. De l'avis de la Cour, le juge a ainsi omis de se demander si M. Spencer avait fait preuve d'aveuglement volontaire quant à l'accessibilité de la pornographie à d'autres

personnes au moyen du répertoire partagé. Je souscris à l'opinion de la Cour d'appel sur ces deux points et je suis d'avis de confirmer l'ordonnance prescrivant la tenue d'un nouveau procès.

[83] Il n'est pas contesté que, dans le cadre d'une poursuite sous le régime du par. 163.1(3) du *Code criminel*, il faut prouver que l'accusé avait connaissance du fait que le matériel pornographique était rendu accessible à d'autres personnes. Il n'est toutefois pas nécessaire, comme l'a suggéré le juge du procès, que l'accusé doive sciemment, par une certaine action concrète, faciliter l'accès au matériel. J'accepte la conclusion du juge Caldwell selon laquelle les éléments de l'infraction sont tous réunis lorsque l'accusé rend sciemment accessible la pornographie à d'autres personnes. Selon le juge :

> [TRADUCTION] S'agissant d'un programme de partage de fichiers, l'élément de *mens rea* relatif à l'infraction de rendre accessible de la pornographie juvénile prévue au par. 163.1(3) exige une preuve de l'intention de rendre les fichiers informatiques contenant de la pornographie juvénile accessibles à d'autres personnes en utilisant ce logiciel ou une connaissance réelle que le programme de partage de fichiers rend les fichiers accessibles à d'autres personnes. [par. 87]

Bien que les motifs formulés par le juge du procès se prêtent probablement à plusieurs interprétations sur ce point, compte tenu de leur ensemble, je partage également l'avis du juge Caldwell selon lequel le juge du procès a commis une erreur en décidant que la *mens rea* de l'infraction de rendre accessible exigeait l'accomplissement d'un geste délibéré : par. 81.

[84] À l'instar du juge Caldwell, j'estime aussi que l'aveuglement volontaire était une question en litige compte tenu de la preuve et qu'en raison de son erreur relative au geste délibéré le juge du procès ne s'est pas penché sur les éléments de preuve susceptibles d'étayer une conclusion d'aveuglement volontaire. L'aveuglement volontaire remplace la connaissance. Comme l'a expliqué la juge Charron dans l'arrêt *R. c. Briscoe*, 2010 CSC 13, [2010] 1 R.C.S. 411, par. 21 :

> L'ignorance volontaire ne définit pas la *mens rea* requise d'infractions particulières. Au contraire, elle peut remplacer la connaissance réelle chaque fois que la connaissance est un élément de la *mens rea*. La doctrine de l'ignorance volontaire impute une connaissance à l'accusé qui a des doutes au point de vouloir se renseigner davantage, mais qui choisit délibérément de ne pas le faire. Voir *Sansregret c. La Reine*, [1985] 1 R.C.S. 570, et *R. c. Jorgensen*, [1995] 4 R.C.S. 55. Comme l'a dit succinctement le juge Sopinka dans *Jorgensen* (par. 103), « [p]our conclure à l'ignorance volontaire, il faut répondre par l'affirmative à la question suivante : L'accusé a-t-il fermé les yeux parce qu'il savait ou soupçonnait fortement que s'il regardait, il saurait? » [Je souligne.]

[85] Parmi les éléments de preuve commandant l'examen de la question de l'aveuglement volontaire, mentionnons entre autres le fait que M. Spencer a reconnu dans sa déclaration à la police ceci : que LimeWire est un programme de partage de fichiers; qu'il avait modifié au moins un réglage par défaut de ce logiciel; que, lorsqu'il est installé la première fois sur un ordinateur, LimeWire affiche un message d'avertissement pour aviser l'utilisateur qu'il s'agit d'un programme de partage de fichiers; que, au début de chaque session, LimeWire avise l'utilisateur que c'est un programme de partage de fichiers et le met en garde contre les répercussions du partage de fichiers; que LimeWire contient des indicateurs visuels qui montrent la

progression du téléchargement des fichiers par d'autres personnes à partir de l'ordinateur de l'utilisateur : par. 88-89.

[86] Puisque l'aveuglement volontaire était une question en litige et que l'erreur du juge du procès — lorsqu'il a conclu qu'un geste délibéré était nécessaire pour satisfaire à l'exigence de la *mens rea* de l'infraction de rendre accessible — lui a fait omettre l'examen de cette question, je conviens avec le juge Caldwell qu'il serait raisonnable de penser que cette erreur a eu une incidence sur le verdict d'acquittement : par. 93; *R. c. Graveline*, 2006 CSC 16, [2006] 1 R.C.S. 609, par. 14.

III. Dispositif

[87] Je suis d'avis de rejeter le pourvoi, de confirmer la déclaration de culpabilité relative au chef d'accusation de possession ainsi que l'ordonnance de Cour d'appel enjoignant la tenue d'un nouveau procès sur le chef d'accusation de rendre accessible.

ANNEXE

Loi sur la protection des renseignements personnels et les documents électroniques, L.C. 2000, ch. 5

7. . . .

(3) [Communication à l'insu de l'intéressé et sans son consentement] Pour l'application de l'article 4.3 de l'annexe 1 et malgré la note afférente, l'organisation ne peut communiquer de renseignement personnel à l'insu de

l'intéressé et sans son consentement que dans les cas suivants :

. . .

c) elle est exigée par assignation, mandat ou ordonnance d'un tribunal, d'une personne ou d'un organisme ayant le pouvoir de contraindre à la production de renseignements ou exigée par des règles de procédure se rapportant à la production de documents;

c.1) elle est faite à une institution gouvernementale — ou à une subdivision d'une telle institution — qui a demandé à obtenir le renseignement en mentionnant la source de l'autorité légitime étayant son droit de l'obtenir et le fait, selon le cas :

. . .

(ii) que la communication est demandée aux fins du contrôle d'application du droit canadien, provincial ou étranger, de la tenue d'enquêtes liées à ce contrôle d'application ou de la collecte de renseignements en matière de sécurité en vue de ce contrôle d'application,

. . .

d) elle est faite, à l'initiative de l'organisation, à un organisme d'enquête, une institution gouvernementale ou une subdivision d'une telle institution et l'organisation, selon le cas, a des motifs raisonnables de croire que le renseignement est afférent à la violation d'un accord ou à une contravention au droit fédéral, provincial ou étranger qui a été commise ou est en train ou sur le point de l'être ou soupçonne que le renseignement est afférent à la sécurité nationale, à la défense du Canada ou à la conduite des affaires internationales;

. . .

Code criminel, L.R.C. 1985, ch. C-46

163.1 . . .

(3) [Distribution de pornographie juvénile] Quiconque transmet, rend accessible, distribue, vend, importe ou exporte de la pornographie juvénile ou en fait la publicité, ou en a en sa possession en vue de la transmettre, de la rendre accessible, de la distribuer, de la vendre, de l'exporter ou d'en faire la publicité, est coupable :

a) soit d'un acte criminel passible d'un emprisonnement maximal de dix ans, la peine minimale étant de un an;

b) soit d'une infraction punissable sur déclaration de culpabilité par procédure sommaire et passible d'un emprisonnement maximal de deux ans moins un jour, la peine minimale étant de six mois.

. . .

487.014 (1) [Pouvoir de l'agent de la paix] Il demeure entendu qu'une ordonnance de communication n'est pas nécessaire pour qu'un agent de la paix ou un fonctionnaire public chargé de l'application ou de l'exécution de la présente loi ou de toute autre loi fédérale demande à une personne de lui fournir volontairement des documents, données ou renseignements qu'aucune règle de droit n'interdit à celle-ci de communiquer.

Pourvoi rejeté.

Procureurs de l'appelant : McDougall Gauley, Regina.

Procureur de l'intimée : Procureur général de la Saskatchewan, Regina.

Procureur de l'intervenant le directeur des poursuites pénales : Service des poursuites pénales du Canada, Edmonton et Halifax.

Procureur de l'intervenant le procureur général de l'Ontario : Procureur général de l'Ontario, Toronto.

Procureur de l'intervenant le procureur général de l'Alberta : Procureur général de l'Alberta, Calgary.

Procureurs de l'intervenant le commissaire à la protection de la vie privée du Canada : Osler, Hoskin & Harcourt, Toronto.

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

Procureurs de l'intervenante Criminal Lawyers' Association of Ontario : Dawe & Dineen, Toronto; Schreck Presser, Toronto.