Chronique – Cybercriminalité : développements jurisprudentiels et perquisitions informatiques

Annie EMOND* et Laura ELLYSON*

EYB2014REP1575

EYB2014REP1575

Repères, Septembre 2014

Annie EMOND* et Laura ELLYSON*
Chronique – Cybercriminalité : développements jurisprudentiels et perquisitions informatiques

Indexation

PÉNAL ; QUESTIONS CONSTITUTIONNELLES ; *CHARTE CANADIENNE DES DROITS ET LIBERTÉS* ; PROTECTION CONTRE LES FOUILLES, LES PERQUISITIONS OU LES SAISIES ABUSIVES ; VIE, LIBERTÉ ET SÉCURITÉ DE LA PERSONNE ; PRIVILÈGE DE NON-INCRIMINATION ; COMMUNICATIONS ; TECHNOLOGIES DE L'INFORMATION

TABLE DES MATIÈRES

Résumé

Les auteures résument la jurisprudence applicable en matière de perquisitions informatiques et de cybercriminalité, plus particulièrement les décisions récentes de la Cour suprême du Canada en matière de respect de la vie privée en lien avec l'utilisation d'ordinateurs.

INTRODUCTION

Le développement accéléré des nouvelles technologies fait naître de nouveaux questionnements en matière de respect de la vie privée, que ce soit pour les usagers de ces technologies ou leur créateur. Alors que la majorité de ces problématiques seront réglées au niveau contractuel ou réglementaire (pensons notamment à la *Loi sur la protection des renseignements personnels et les documents électroniques*[1]), il n'en demeure pas moins que certains cas doivent être portés devant les tribunaux de juridiction criminelle, principalement dans des causes reliées à la cybercriminalité.

Alors que la cybercriminalité est généralement définie comme regroupant les infractions où l'ordinateur est l'outil du crime et les infractions où l'ordinateur est l'objet du crime[2], dans tous les cas où un ordinateur est impliqué dans la perpétration d'une infraction, celui-ci devient pertinent pour les policiers dans leur recherche de preuve. Il peut donc aussi bien s'agir d'infractions classiques, qui existent indépendamment de l'existence des ordinateurs et où l'ordinateur est utilisé pour faciliter la commission de l'infraction (distribution de pornographie juvénile par exemple, où l'ordinateur rend plus facile la distribution du matériel, sans toutefois qu'il soit impossible de commettre un tel crime sans posséder un ordinateur) ou encore d'infractions qui ne peuvent exister sans ordinateur (tous les crimes de piratage informatique, tels que le virus informatique ou les attaques par déni de service). Conséquemment, il existe une multitude de situations où les données contenues dans l'ordinateur seront essentielles à la preuve de la poursuite. Cela est d'autant plus vrai aujourd'hui alors que la plupart des gens possèdent plusieurs objets électroniques qui peuvent être considérés comme des ordinateurs (téléphones intelligents, tablettes, appareils MP3, etc.), plutôt qu'un seul ordinateur restant à la maison ou au bureau.

En plus de l'augmentation du nombre d'appareils pouvant être considérés comme des ordinateurs, notre relation à ces nouveaux appareils peut souvent nous mettre à risque de devenir victime de la cybercriminalité. Ces comportements à risque peuvent notamment inclure de ne pas avoir de logiciel antivirus sur nos appareils, partager sur les réseaux sociaux nos déplacements ou encore d'accéder à Internet sur des réseaux non sécurisés – le Palais de justice de Montréal s'est d'ailleurs, en juillet dernier, doté, après des années d'attente, d'un réseau sans fil ; malheureusement, ce dernier est, aussi surprenant que cela puisse paraître, non sécurisé, augmentant ainsi les risques d'infiltration dans les ordinateurs des avocats, des juges et du personnel de la cour. Toutes ces situations font en sorte que les tribunaux sont, et seront, de plus en plus sollicités par des cas de cybercriminalité, sans compter toutes les situations où l'utilisation de l'ordinateur devient pertinente en lien avec l'administration de la preuve[3]. Les tribunaux de juridiction criminelle doivent donc s'assurer que les règles classiques du droit criminel en matière de respect de la vie privée[4] sont respectées lorsqu'il est question de perquisitions d'ordinateurs, et plus spécifiquement de l'analyse des données qu'ils contiennent.

I– PERQUISITIONS INFORMATIQUES ET RESPECT DE LA VIE PRIVÉE

La Cour suprême du Canada, dans le cadre de trois décisions en matière de cybercriminalité[5], s'est récemment positionnée en faveur de la protection des libertés fondamentales des individus et du respect de leur vie privée en matière informatique. Un peu à l'image de la maison comme « château fort » de la vie privée, le contenu de l'ordinateur est dorénavant protégé par une énorme expectative de vie privée dont jouit son propriétaire. L'honorable juge Fish avait d'ailleurs énoncé dès 2010 qu'« [il] est difficile d'imaginer une perquisition, une fouille et une saisie plus envahissantes, d'une plus grande ampleur ou plus attentatoires à la vie privée que celles d'un ordinateur personnel »[6].

Dans la décision *R.* c. *Société TELUS Communications*, précitée, se posait la question à savoir quel type d'autorisation judiciaire devait être utilisé par les policiers pour que TELUS puisse leur faire parvenir, sur une base quotidienne, les messages reçus et envoyés par deux de leurs abonnés. En fait, toutes les parties s'entendaient pour dire qu'une ordonnance d'autorisation d'écoute électronique[7] était normalement le véhicule approprié. La différence dans le cas de TELUS, contrairement aux autres fournisseurs de services cellulaires, résidait dans le fait qu'elle copie et stocke pendant un certain temps (30 jours) tous les messages envoyés et reçus par ses clients dans une banque. Les policiers, dans le cadre d'une enquête, avaient obtenu un mandat général, sous le régime de 487.01 C.cr., auprès d'un juge. TELUS avait alors refusé de fournir lesdits messages, alléguant que le mandat était invalide au motif que le mandat général ne peut être utilisé que lorsqu'aucun autre moyen n'est disponible. La Couronne, au contraire, plaidait qu'il ne s'agissait pas en l'espèce d'une interception de communication privée en raison de l'existence de ladite banque de données.

La Cour a tranché en décidant que la messagerie texte est essentiellement une conversation et qu'elle devait bénéficier de la même protection qu'une communication sous forme orale. La majorité, sous la plume de la juge Abella, énonçait : « À mon avis, les messages textes constituent des communications privées et, même s'ils sont stockés dans l'ordinateur d'un fournisseur de services, la communication prospective de futurs messages de cette nature doit être autorisée en vertu de la partie VI du *Code* »[8]. Le mandat général, ne pouvant être délivré que lorsqu'aucun autre moyen n'est disponible, ne pouvait donc pas être utilisé puisque l'ordonnance d'interception des communications privées était disponible. La Cour suprême reconnaissait du même coup que « [les] différences techniques intrinsèques des nouvelles technologies ne devraient pas déterminer l'étendue de la protection accordée aux communications privées »[9].

Dans le cas de *R.* c. *Vu*, précité, un mandat de perquisition en vertu de l'article 487 C.cr. avait été émis, autorisant les policiers à effectuer une perquisition chez l'appelant pour trouver des preuves de vol d'électricité, dans le contexte d'une accusation de production de marijuana. Bien que le mandat prévoyait que les policiers pouvaient saisir

des « notes générées par ordinateur », celui-ci ne prévoyait pas expressément la fouille du contenu desdits ordinateurs. Pendant la fouille de la maison, les policiers avaient saisi plusieurs ordinateurs qui contenaient une preuve de résidence de l'appelant. Ce dernier avait donc demandé à ce que ces éléments de preuve soient exclus, au motif que les policiers avaient outrepassé les limites du mandat de perquisition, violant son droit contre les fouilles, perquisitions ou saisies abusives. En examinant la différence entre les perquisitions traditionnelles et les perquisitions d'ordinateur, en lien avec l'application des règles traditionnelles de l'octroi des mandats et la transposition de celles-ci aux nouvelles technologies, le juge Cromwell, au nom de la Cour, énonça :

> Les intérêts en matière de respect de la vie privée que met en jeu la fouille des ordinateurs diffèrent nettement de ceux en cause lors de la fouille de contenants tels des placards et des classeurs. En effet, les ordinateurs sont susceptibles de donner aux policiers accès à de vastes quantités de données sur lesquelles les utilisateurs n'ont aucune maîtrise, dont ils ne connaissent peut-être même pas l'existence ou dont ils peuvent avoir choisi de se départir, et qui d'ailleurs pourraient fort bien ne pas se trouver concrètement dans le lieu fouillé. Je suis d'avis que, considérés au regard des objectifs visés par l'art. 8 de la *Charte*, ces facteurs commandent l'obtention d'une autorisation expresse préalable. [10]

Bref, alors qu'un mandat de perquisition visant une résidence comprend nécessairement tous les « contenants » s'y trouvant (tiroirs, armoires, penderies, coffres, etc.), l'ordinateur ne saurait être assimilé à un simple contenant de la sorte. Ainsi, un mandat de perquisition ne mentionnant pas spécifiquement que le contenu des ordinateurs peut être examiné, n'autorise pas une telle fouille ; une autorisation expresse et spécifique préalable est nécessaire. L'ordinateur doit donc « être traité comme un lieu distinct » [11] lorsqu'il s'agit de perquisitions, un peu de la même manière qu'une remise attenante à une résidence doit être mentionnée au mandat pour pouvoir être fouillée. Par contre, en l'absence d'une telle autorisation, les policiers pourraient tout de même saisir les ordinateurs, s'il est raisonnable de croire qu'ils contiennent des éléments de preuve autorisés par le mandat bien évidemment, à condition de ne faire que des gestes de préservation de l'intégrité des données à leur égard. Ils pourraient ensuite obtenir un second mandat de perquisition pour en extraire et analyser le contenu. En l'espèce, bien qu'il y ait effectivement eu violation des droits de l'appelant, en raison de l'incertitude qui planait sur l'état du droit, la preuve recueillie en violation du mandat par les policiers n'avait pas été exclue sous l'article 24(2) de la Charte, en suivant les étapes prévues par l'arrêt *Grant* [12].

Dernièrement, une décision de la Cour du banc de la Reine de l'Alberta [13] a appliqué et combiné les principes dégagés par les arrêts *Vu* et *TELUS.* Dans cette décision, l'infraction alléguée était la tentative de meurtre. Par contre, lors de l'exécution de plusieurs mandats de perquisition, un ordinateur contenant ce qui semblait être de la pornographie juvénile fut saisi. Les policiers demandèrent donc un mandat général en vertu de l'article 487.01 C.cr. pour procéder à une fouille plus approfondie de l'appareil en question, puisque l'infraction de possession de pornographie juvénile n'était pas alléguée au premier mandat. Le juge refusa d'accorder un tel mandat au motif qu'un autre mandat était disponible, soit le mandat de perquisition prévu à 487 C.cr. La Cour, saisie d'une demande de *certiorari* avec *mandamus* ancillaire, à la suite du refus du juge émetteur de délivrer le mandat général, décida qu'un second mandat devait effectivement être obtenu, appliquant ainsi les principes de l'arrêt *R.* c. *Vu.* Ensuite, suivant le raisonnement du juge émetteur, la Cour rejeta le recours extraordinaire et décida que le mandat général de 487.01 C.cr. n'était effectivement pas l'autorisation appropriée, bien que les critères de 487.01 C.cr. soient plus exigeants que ceux du mandat de perquisition de 487 C.cr. Le juge détermina qu'un mandat de perquisition permettait bel et bien la fouille du contenu d'un ordinateur, empêchant ainsi l'utilisation du mandat général. Le juge Hugues réitéra le principe qu'un ordinateur doit être traité comme un lieu distinct :

> In conclusion, I find that on the facts before me, the police, by seeking a second warrant for a forensic examination, are seeking an authorization to search a place, that being the computer itself, and they are searching for things – data, images and video, on the computer which will afford evidence with respect to the commission of the offence of accessing and possession of child pornography. A search warrant allows the police to do all of these things. [14] (Nos soulignements)

Dans *R.* c. *Spencer*, précitée, la Cour suprême a statué qu'il existe une expectative raisonnable de vie privée sur les renseignements reliés à l'adresse IP [15] (nom et adresse de la personne liés à une adresse IP déterminée), donc qu'une autorisation judiciaire devait être préalablement obtenue pour qu'un corps de police obtienne d'un fournisseur de service Internet (FSI) ces renseignements. En l'espèce, les policiers avaient obtenu l'adresse IP de l'accusé en faisant des recherches sur un logiciel de partage pair à pair [16] et en voyant que l'accusé partageait certains fichiers de pornographie juvénile. Ils avaient ensuite fourni au FSI cette adresse IP et avaient demandé à celui-ci de leur fournir le nom et l'adresse de l'utilisateur de cette adresse. Le FSI avait obtempéré, malgré l'absence d'autorisation judiciaire, l'accusé Spencer avait donc pu être identifié. Au procès, Spencer demandait l'exclusion de la preuve obtenue au motif que l'obtention des informations relatives à l'adresse IP avait été faite illégalement.

Alors que la plupart des décisions de juridictions inférieures avaient conclu qu'il n'y avait pas d'expectative raisonnable de vie privée pour ces éléments, soit en raison d'une renonciation se trouvant dans le contrat conclu entre le FSI et l'abonné, soit puisque ces informations ne comportaient aucun élément biographique [17], la Cour suprême a plutôt conclu à l'inverse, en tenant compte des facteurs prévus par la jurisprudence antérieure pour déterminer si une expectative raisonnable de vie privée existait [18]. Ainsi, le juge Cromwell écrivait, sur l'objet même de la fouille survenue :

> 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* [note des auteures : *R.* v. *Trapp*, 2011 SKCA 143 (CanLII)] 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.
>
> 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. [19]
>
> Nos soulignements

Après avoir déterminé l'objet de la perquisition en question, la Cour a décidé que l'expectative de vie privée de l'accusé était raisonnable en l'espèce, et ce, malgré le cadre réglementaire et contractuel régissant la transmission de ces informations. La Cour souligna être en accord avec les propos du juge de la Cour d'appel selon lesquels une personne raisonnable et soucieuse du respect de la vie privée s'attendrait à ce que le contenu de son ordinateur personnel soit confidentiel [20]. La demande faite par les policiers au FSI constituait donc bel et bien une fouille, nécessitant du même coup une autorisation judiciaire. Par contre, en mettant en balance les critères de 24(2) de la Charte, la Cour a conclu que l'exclusion de la preuve déconsidérait davantage l'administration de la justice que son admission, notamment puisque les policiers croyaient de bonne foi qu'aucun mandat n'était nécessaire en raison des décisions contradictoires à cet effet [21].

II– PERQUISITIONS INFORMATIQUES ET DROIT CONTRE L'AUTO-INCRIMINATION

D'autres juridictions ont également clarifié certains autres aspects du respect à la vie privée des individus en lien avec l'utilisation d'un ordinateur et les perquisitions. C'est notamment le cas de la Cour d'appel du Québec dans la décision *R.* c. *Boudreau-Fontaine* [22]. Dans cette décision, l'accusé avait été intercepté par les policiers alors qu'il travaillait sur un ordinateur portable à partir de sa voiture stationnée. En procédant à des vérifications dans leur banque de données, les policiers avaient alors appris que l'accusé faisait l'objet d'une interdiction d'accéder à l'Internet. Ils avaient donc procédé à son arrestation, croyant qu'il accédait à l'Internet à partir de son ordinateur. De façon accessoire à l'arrestation, les policiers avaient saisi son ordinateur portable et avaient ensuite obtenu un mandat de perquisition pour procéder à l'analyse du contenu de l'ordinateur. Ce mandat contenait une clause particulière, obligeant l'accusé à leur fournir son mot de passe.

La Cour a d'abord conclu que la fouille et la perquisition de l'ordinateur étaient abusives puisque les policiers n'avaient pas de motifs raisonnables de croire que l'accusé accédait à l'Internet au moment de son arrestation. Ensuite, et de façon plus importante, la Cour a décidé que le mandat de perquisition ne pouvait sommer l'accusé de

fournir son mot de passe puisque cela allait à l'encontre des droits qui lui sont garantis par la Charte :

> Je rappelle qu'il ordonne à l'intimé de divulguer son ou ses mots de passe « *afin de démontrer que l'ordinateur a été connecté à Internet par M. Boudreau-Fontaine, contrevenant ainsi aux conditions de sa probation* ». En d'autres termes, le juge de paix sommait l'appelant de donner une information essentielle spécifiquement en vue de l'amener à s'incriminer. Je ne peux voir comment le d[r]oit criminel pourrait permettre une telle ordonnance. Il faut rappeler que l'intimé s'est conformé à l'ordonnance, mais qu'il ne l'aurait sûrement pas fait sans cet ordre, la preuve étant qu'il a refusé de parler aux policiers des événements du 19 septembre lors de son arrestation. Comme l'écrit l'intimé dans son exposé, cette ordonnance met en cause le droit au silence, le droit à la présomption d'innocence, le droit de ne pas être mobilisé contre soi-même et la protection contre l'auto incrimination. Contraint de participer à l'enquête policière et de donner une information cruciale, contrairement à ses droits constitutionnels, l'intimé a fait une déclaration (l'identification de son mot de passe) qui est irrecevable et qui rend abusive la saisie des données qui a suivi. Bref, même si cette saisie a été précédée d'une autorisation judiciaire, la loi ne permettait pas d'y adjoindre une ordonnance forçant l'intimé à s'incriminer.
>
> [...]
>
> Sans être nécessairement détenu, l'intimé était contraint de participer à sa propre incrimination et n'avait pas le choix : il devait aider les policiers à le faire condamner. Cette façon de faire ne peut être acceptée.[23] (Souligné dans l'original)

Un accusé ne peut donc être contraint de fournir son mot de passe, que ce soit par autorisation judiciaire ou non. De plus, le juge souligna que, dans le cas présent, un expert avait déterminé qu'il aurait été possible de décrypter le mot de passe de l'ordinateur de l'accusé. Alors que cet élément aurait pu favoriser l'admission de la preuve, en vertu du principe de la possibilité de découvrir la preuve, le juge a décidé qu'il n'avait aucune preuve que le mot de passe aurait effectivement été obtenu sans le concours de l'accusé ; l'information fournie par l'accusé était essentielle.[24] L'appel formulé par le ministère public fut donc rejeté et l'exclusion de la preuve prononcée par le juge de première instance fut maintenue.

CONCLUSION

Ces décisions démontrent bien l'importance qui devra être dorénavant accordée à la protection de la vie privée des individus, en lien avec l'usage d'Internet et d'un ordinateur. Bien que la preuve ait été admise dans certains de ces cas, par suite de l'analyse de 24(2) de la Charte, il n'en demeure pas moins que ces violations ne seront vraisemblablement plus tolérées à l'avenir, la société bénéficiant maintenant de jugements clairs et définitifs sur ces questions. D'ailleurs, malgré l'existence de ces jugements, il est clair que d'autres questions liées à la cybercriminalité seront amenées devant les tribunaux dans les années à venir. La difficulté de faire une preuve hors de tout doute raisonnable de l'identité d'un individu commettant des infractions en ligne ou encore le simple fait que ce type d'infractions peut maintenant être commis dans plusieurs circonscriptions territoriales à la fois compliquera assurément le travail des tribunaux et des avocats, autant de la poursuite que de la défense.

---

* M^e^ Annie Emond est avocate criminaliste à Montréal. Elle a, au cours de sa carrière, agi comme assistante temporaire au *Tribunal pénal international pour le Rwanda*, a plaidé devant la Cour suprême du Canada, la Cour d'appel du Québec, devant la Cour supérieure avec juge et jury et en première instance devant la Cour du Québec. Elle est récipiendaire de trois prix soulignant l'excellence de son parcours professionnel au cours de ses dix premières années comme membre du Barreau du Québec. Sa pratique professionnelle du droit tend aujourd'hui à se concentrer sur des mandats reliés aux crimes technologiques. M^e^ Laura Ellyson est une jeune avocate criminaliste pratiquant à Montréal depuis son assermentation en 2013. Sa carrière l'amène présentement à travailler majoritairement sur des dossiers de grande envergure, reliés notamment au crime organisé. Elle a été assistante de recherche lors de son baccalauréat à l'Université de Sherbrooke, travaillant principalement sur la récidive en droit criminel canadien. Elle a également été conférencière dans le cadre du *Congrès de l'Association du Jeune Barreau de Montréal.* Les auteures collaborent présentement à la rédaction d'un ouvrage sur la cybercriminalité intitulé *Cybercrimin@lité : L'ombre d'Internet*, à paraître prochainement aux Éditions Yvon Blais.

1. L.C. 2000, ch. 5.

2. Voir notamment : Robert W.K. Davis et Scott C. Hutchison, *Computer crime in Canada – An Introduction to Technological Crime and Legal Issues*, Scarborough, Carswell, 1997, 313 p. ; Frédéric-Jérôme Pansier et Emmanuel Jez, *La criminalité sur l'Internet*, Paris, Presses universitaires de France, 2001, 127 p. ; Daniel Martin et Frédéric-Paul Martin, *Cybercrime – Menaces, vulnérabilités, ripostes*, Paris, Presses universitaires de France, 2001, 290 p., ainsi que Gouvernement du Canada, Centre canadien de la statistique juridique, Statistique Canada, *Cybercriminalité : enjeux, sources de données et faisabilité de recueillir des données auprès de la police*, n^o^ 85-558-XIF au catalogue de Statistique Canada, Ottawa, 2002, p. 6 (citant le *Collège canadien de police*).

3. Voir notamment les dispositions à ce sujet de la *Loi sur la preuve au Canada*, L.R.C. (1985), ch. C-5.

4. *Charte canadienne des droits et libertés*, partie I de la *Loi constitutionnelle de 1982*, constituant l'annexe B de la *Loi de 1982 sur le Canada* (R.-U.), 1982, c. 11, art. 7 et 8.

5. *R.* c. *Société TELUS Communications*, [2013] 2 R.C.S. 3, EYB 2013-219905 ; *R.* c. *Vu*, [2013] 3 R.C.S. 657, EYB 2013-228909 et *R.* c. *Spencer*, 2014 CSC 43, EYB 2014-238452.

6. *R.* c. *Morelli*, [2010] 1 R.C.S. 253, EYB 2010-171050, par. 2.

7. *Code criminel*, L.R.C. (1985), ch. C-46, partie VI.

8. *R.* c. *Société TELUS Communications*, préc., note 5, par. 12.

9. *Id.*, par. 5.

10. *R.* c. *Vu*, préc., note 5, par. 24.

11. *Id.*, par. 51.

12. *R.* c. *Grant*, [2009] 2 R.C.S. 353, EYB 2009-161617.

13. *R.* v. *K.Z.*, 2014 ABQB 235.

14. *Id.*, par. 47.

15. L'adresse IP est un numéro d'identification attitré à tout appareil qui est relié à l'Internet. Par exemple, un ordinateur portable qui se connecte à partir de plusieurs endroits se verra attitrer une nouvelle adresse IP à chaque connexion alors qu'un réseau fixe aura toujours la même adresse IP.

16. Logiciel permettant aux usagers de rendre accessibles au téléchargement par d'autres usagers certains fichiers qu'ils ont sur leur propre ordinateur par Internet.

17. Voir notamment : *R.* v. *Vasic*, 2009 CanLII 6842 (ON SC) ; *R.* c. *Wilson*, [2009] O.J. No. 1067 (S.C.J.) ; *R.* v. *McNeice*, 2010 BCSC 1544 (CanLII) ; *R.* v. *Brousseau*, 2010 ONSC 6753 (CanLII) ; *R.* v. *Lo*, 2011 ONSC 6527 (CanLII) ; *R.* v. *Spencer*, 2011 SKCA 144 (CanLII) ; *R.* v. *Cuttell,* 2012 ONCA 661 (CanLII) ; *R.* v. *Ward*, 2012 ONCA 660 ; *R. v. Caza*, 2012 BCSC 525 (CanLII) et *R.* v. *Thomas*, 2013 ABQB 223 (CanLII).

18. *R.* c. *Tessling*, [2004] 3 R.C.S. 432, REJB 2004-72161, par. 32 ; *R.* c. *Patrick*, [2009] 1 R.C.S. 579, EYB 2009-157141, par. 27 et *R.* c. *Cole*, [2012] 3 R.C.S. 34, EYB 2012-212617, par. 40.

19. *R.* c. *Spencer*, préc., note 5, par. 32-33.

20. *Id.*, par. 51.

21. *Id.*, par. 81.

22. *R.* c. *Boudreau-Fontaine*, 2010 QCCA 1108 (CanLII), EYB 2010-175094.

23. *Id.*, par. 39 et 41.

24. *Id.*, par. 42.

Date de dépôt : 3 septembre 2014