Compte-rendu d'un arrêt de jurisprudence

Dans le cadre du cours: Le droit de l'informatique

JUR6854

# PARTIE A: Le résumé

1. **Le nom des parties:**

M. Matthew David Spencer (**Appelant**) 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**)

2. **La citation précise ou référence**:

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

9 décembre 2013 au 13 juin 2014

Présents: La juge en chef McLachlin et les juges LeBel, Abella, Rothstein, Cromwell,

Moldaver, Karakatsanis et Wagner.

3. ***Les faits:***

3.1. ***Aspect matériel:***

L'appelant, M. Spencer a été reconnu coupable de possession de pornographie juvénile. A l'époque où les faits incriminés se sont produits, M. Spencer, se servant de la connexion internet de sa sœur, utilisait un logiciel de partage de fichiers poste à poste pour télécharger et stocker de la pornographie juvénile, infraction décrite au par. 163.1 (4) du code criminel et qui stipule notamment que:

« Quiconque a en sa possession de la pornographie juvénile 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.

c) passible d’un emprisonnement maximal de deux ans moins un jour, la peine minimale étant de six mois. »

La police, après avoir identifié une adresse IP liée à cette activité, a fait une demande auprès de Shaw, le fournisseur de services Internet (FSI), mais «sans autorisation judiciaire préalable» (par. 2), pour obtenir les renseignements relatifs à cette IP. A l’aide des ces renseignements, les policiers ont pu identifier M. Spencer.

Au procès, M. Spencer a été reconnu coupable de possession de pornographie juvénile mais a été acquitté du chef d’accusation de la « rendre accessible » à autrui. La cour d’appel a confirmé le premier jugement tout en prescrivant un nouveau procès quant au deuxième chef d’accusation. M. spencer a fait appel de cette décision. C’est ce pourvoi qui fait l’objet de ce présent jugement de la Cour Suprême du Canada.

3.2. ***Aspects procéduraux*** :

En première instance, le juge Foley a déclaré M. Spencer coupable d’un seul chef d’accusation, à savoir la possession de pornographie infantile. Quant à l’infraction de « rendre accessible », le juge a estimé que l’accusé n’avait pas donné accès à la pornographie juvénile de façon « délibérée » (par. 3) ; il n’était donc pas coupable de cette infraction.

Au procès, M. Spencer a, pour sa part, soutenu que la preuve ayant mené à son identification devait être écartée au motif que la police avait effectué une fouille ou perquisition inconstitutionnelle pour obtenir les renseignements relatifs à l'abonnée à qui appartenait l'adresse IP.

Le juge du procès n’était pas du même avis que M. Spencer, jugeant 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. » (par. 3)

Au procès en appel, la cour d'appel de la Saskatchewan, à l’unanimité, s'est alignée sur la décision du juge du procès concernant l'infraction de possession de pornographie juvénile. Le juge Caldwell, s’exprimant pour la majorité, se référant à l’arrêt *Trapp* déclare :

« (…) I would conclude the “search” was authorized by law, the law is reasonable and that the manner in which the search was conducted was reasonable » (par. 46).

La cour d’appel a cependant ordonné la tenue d'un nouveau procès quant au chef d'accusation de « rendre accessible ». Elle a en effet jugé que le juge du procès a commis une erreur en exigeant une action délibérée de la part de l’accusé quant à l’infraction de « rendre accessible ». Toujours selon le juge Caldwell :

« (...) the Crown did not have to prove actual knowledge as a basis for criminal liability, but the trial judge failed to turn his mind to whether the Crown had proven wilful blindness, a substitute for actual knowledge. This constituted a substantive error in law. » (par. 93)

M. Spencer a alors interjeté appel auprès de la cour suprême du Canada.

Le pourvoi a été rejeté.

4. ***La (Les) question(s) en litige:***

Les deux aspects de la question en litige dans cette affaire sont :

1. L’objet de la fouille ou de la perquisition. D’un côté, M. Spencer prétend que l’objet de la fouille 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. » (par. 24) De l’autre côté, pour le ministère public, les renseignements obtenus sont d’ordre général et ne correspondaient pas à « des données d’ordre biographique relatives à M. Spencer. » (par. 25)
2. L’existence d’une attente raisonnable en matière de respect de la vie privée. En particulier, il s’agit de « 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. » (par. 16)

5. ***Le jugé:***

Pourvoi rejeté. Confirmation de culpabilité relative au chef d’accusation de possession de pornographie juvénile. Confirmation de l’ordonnance de la cour d’appel pour la tenue d’un deuxième procès quant au chef d’accusation de « rendre accessible ».

6. ***Les motifs:***

Le juge Cromwell, s’exprimant pour la majorité, a commencé par reconnaître que l’action menée par la police représentait bel et bien une fouille ou une perquisition. (par. 6)

Le juge s’est ensuite attelé à définir l’objet de cette fouille ou perquisition. En se référant aux arrêts *Trapp*, *Plant*, *tessling*, *Kang-Brown* et *Gomboc* il est d’avis qu’on ne saurait circonscrire l’objet de la fouille aux seuls nom et adresse d’un abonné. Selon lui, il faut également tenir compte de la « possibilité que ces renseignements révèlent des détails intimes sur le mode de vie et les choix personnels de l’individu (…) » (par. 25)

Selon le juge, le cadre d’analyse à adopter pour la détermination de l’objet d’une fouille ou perquisition est celui proposé par la Cour dans les arrêts *Gomboc* et *Ward*, à savoir qu’il faut tenir compte des « inférences » au sujet d’autres renseignements privés que l’on peut tirer à partir des renseignements initiaux. En l’espèce, il s’est agi de renseignements relatifs à une abonnée qui ont mené à d’autres renseignements plus personnels. Et le juge Cromwell de conclure que :

« 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*. » (par. 32 ; C’est moi qui souligne)

Compte tenu de l’objet de la fouille, le juge Cromwell se propose ensuite de déterminer s’il y a attente raisonnable en matière de respect de la vie privée. Pour y arriver, il commence d’abord par élargir l’interprétation du droit à la vie privée pour y inclure la confidentialité, le contrôle, et surtout l’anonymat, point sur lequel il insiste vu le rôle que cette facette du droit privé joue dans « la protection des droits en matière de vie privé sur Internet. » (par. 34)

Selon le juge, l’élément « anonymat » fait intervenir l’aspect informationnel du droit à la vie privée, et de ce fait devrait tomber sous la protection de l’article 8 de la Charte, rejoignant en cela l’avis du juge Doherty dans l’arrêt *Ward*. (par. 48)

Appliquant ce raisonnement au présent pourvoi, il estime que la demande faite par la police auprès de Shaw pour l’obtention des renseignements relatifs à l’abonnée

«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* (…) » (par. 50 ; c’est moi qui souligne)

Passant en revue les dispositions du contrat liant Shaw à ses abonnés, le juge Cromwell conclut à la nécessité de se référer plutôt au cadre législatif pour répondre à la question de l’attente raisonnable, arguant que :

« 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.  » (par. 60)

Les dispositions de la LPRPDE, notamment à l’article 7, ne sont pas très utiles non plus, selon le juge, pour déterminer s’il existe une attente raisonnable du droit à la vie privée. (p. 61)

Selon le sous-alinéa 7(3)*c*.1(ii) invoqué par la police, toute demande faite par une institution gouvernementale doit être étayée par une « source de l’autorité légitime » qui, elle-même, dépend de l’existence d’une attente raisonnable en matière de droit à la vie privée. (par. 62) Or, en l’espèce, la demande de la police auprès de Shaw n’était pas étayée par une « source de l’autorité légitime », la police ne détenant pas l’autorité pour obliger un FSI à se conformer à sa demande de renseignements.

Par conséquent, le juge Cromwell reconnaît l’existence d’une attente raisonnable en matière de droit à la privée dans cette affaire. (par. 66)

Enfin, bien que le juge reconnaisse que la fouille a été abusive, puisque elle a été effectuée sans mandat, il rejette néanmoins l’argument de M. Spencer selon lequel la preuve devrait être écartée. D’une part, le juge estime que les policiers avaient agi de bonne foi. (par. 77) D’autre part, au regard de la gravité des faits reprochés en l’espèce, l’exclusion de la preuve « serait susceptible de déconsidérer l’administration de la justice (…) » (par. 81)

**PARTIE B: Le commentaire**

Le présent arrêt pose le problème épineux de la conciliation entre la protection de la vie privée et la lutte contre la cybercriminalité, la cybercriminalité étant définie « comme regroupant les infractions où l'ordinateur est l'outil du crime et les infractions où l'ordinateur est l'objet du crime. » (Annie Emond et Laura Ellyson 2014 : 1)

L’usage quasi-généralisé de l’Internet depuis les deux dernières décennies dans toutes les sphères de la vie publique et privée pose de nouveaux défis pour le législateur et les forces de l’application de la loi, d’une part. D’autre part, l’utilisation d’Internet expose l’usager non-vigilant à des menaces variées qui vont du simple hameçonnage au vol d’identité.

Permettre aux autorités d’application de la loi de veiller à la sécurité des citoyens en ligne tout en respectant leur droit à une vie privée s’avère un exercice difficile. D’ailleurs, le juge Cromwell n’a pas manqué de rappeler les craintes que son jugement pourrait soulever pour les autorités d’application de la loi. (cf. par. 67)

Cependant, comme les révélations d’Edward Snowden l’ont montré, sans un encadrement juridique strict et un contrôle effectif des mesures de surveillance, l’état peut porter sérieusement atteinte à la vie privée des citoyens. Ces révélations ont montré que la surveillance massive est telle que « tout internaute a désormais connaissance de la possibilité – voire de la probabilité – d’être victime de surveillance, et donc des risques encourus lorsqu’il s’exprime ou s’informe sur la toile. » (Marine Farshian 2015 : 01)

La volonté du gouvernement à protéger les citoyens dans le cyberespace est réelle. Elle est surtout nécessaire à l’ère des réseaux sociaux et du tout-numérique. C’est la ligne de démarcation entre la protection et la surveillance qui constitue un défi. Cette tension entre la cybersécurité et la protection de la vie privée a été bien résumée dans un rapport du Commissariat à la protection de la vie privée du Canada (CPVPC):

« (…) certains efforts liés à la cybersécurité peuvent (…) constituer une menace pour la vie privée; la relation entre ces deux éléments n’est pas en totale harmonie. Les activités de cybersécurité peuvent exiger une surveillance constante des activités sur un réseau pour détecter les anomalies et les menaces, et parfois une surveillance de cette nature suppose la saisie et l’analyse de quantités énormes de renseignements personnels. » (CPVPC 2014 : 2)

Le gouvernement sera amené, dans l’avenir, à adapter son arsenal de lutte contre la cybercriminalité aux nouveaux défis que sont les nouvelles plateformes du cyberspace, notamment l’infonuage. Ce faisant, les risques d’intrusion dans la vie privée des citoyens se multiplieront. Je suis certain que la Cour Suprême du Canada ne manquera pas de le rappeler à l’ordre en cas d’intrusion, comme elle l’a si bien fait dans le présent arrêt.

**BIBLIOGRAPHIE**

Annie Emond et Laura Ellyson 2014  Chronique – Cybercriminalité : développements jurisprudentiels et perquisitions informatiques, in Repères, Septembre 2014

Marine Farshian, « Quand la réalité de la surveillance massive tend à dépasser la fiction orwellienne », La Revue des droits de l’homme [En ligne], Actualités Droits-Libertés, mis en ligne le 28 mai 2015, consulté le 01 octobre 2016. URL : http://revdh.revues.org/1300 ; DOI : 10.4000/revdh.1300

Commissariat à la protection de la vie privée du Canada, « Vie privée et cybersécurité. Mettre l’accent sur la protection de la vie privée dans les activités de cybersécurité»