OJEN • ROEJ

Réseau ontarien d'éducation juridique

LES CINQ PRINCIPAUX ARRÊTS DE 2014

Chaque année, au cours de l'Institut estival de droit du ROEJ à Toronto, un juge de la Cour d'appel de l'Ontario choisit cinq causes d'importance sur le plan éducationnel. Le présent résumé, fondé sur ces commentaires et observations, est idéal pour lancer des discussions et des débats en salle de classe.

R c SPENCER, 2014 SCC 43.

Date du jugement : 13 juin 2014

https://scc-csc.lexum.com/scc-csc/scc-csc/fr/item/14233/index.do

Les faits

Matthew David Spencer, un homme de 18 ans de Saskatoon, a utilisé LimeWire, un logiciel gratuit de partage de fichiers poste-à-poste, pour télécharger et stocker de la pornographie juvénile. Il habitait avec sa sœur à ce moment-là et utilisait Internet au moyen de l'abonnement de sa sœur. Les systèmes de partage de fichiers poste-à-poste ne comportent pas une base de données centrale, mais permettent plutôt à leurs utilisateurs de partager des fichiers avec d'autres utilisateurs. De tels systèmes sont couramment utilisés pour télécharger de la musique et des films.

Un agent de la police de Saskatoon s'est inscrit à LimeWire afin de rechercher des utilisateurs qui partageaient des fichiers de pornographie juvénile. Lorsque l'ordinateur de Spencer était connecté à LimeWire, l'agent pouvait accéder au contenu de son « répertoire partagé », lequel était accessible à tous les utilisateurs de LimeWire. L'agent y a repéré ce qu'il croyait être de la pornographie juvénile. Après une enquête plus approfondie, la police a réussi à découvrir l'adresse de protocole Internet (IP) de l'ordinateur de Spencer.

Au moyen de cette adresse IP, la police pouvait seulement déterminer que l'adresse IP semblait se trouver à Saskatoon et que Shaw Communications Inc. (Shaw) était le fournisseur de services Internet (FSI).
La police a présenté à Shaw une « 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 était fondée sur le sous-al. 7(3)c.1)(ii) de la *Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE).*

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

7(3). […] l'organisation ne peut communiquer de renseignement personnel à l'insu de l'intéressé et sans son consentement que dans les cas suivants :

(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.

La demande indiquait que la police enquêtait sur une infraction relative à la pornographie juvénile et que les renseignements relatifs à l'abonnée étaient demandés aux fins d'une enquête en cours. La police n'avait pas obtenu ni tenté d'obtenir un mandat de perquisition. Shaw a donné suite à la demande et a fourni les coordonnées de la sœur de M. Spencer, la cliente à qui appartenait l'adresse IP. À l'aide de ces renseignements, M. Spencer a été identifié et accusé de possession de pornographie juvénile et de rendre accessible de la pornographie juvénile sur Internet, lesquelles sont des infractions aux termes du *Code criminel du Canada*.

Charte canadienne des droits et libertés

8. Chacun a droit à la protection contre les fouilles, les perquisitions ou les saisies abusives.

24(1). Toute personne, victime de violation ou de négation des droits ou libertés qui lui sont garantis par la présente *Charte*, peut s'adresser à un tribunal compétent pour obtenir la réparation que le tribunal estime convenable et juste eu égard aux circonstances.

(2). Lorsque, dans une instance visée au paragraphe (1), le tribunal a conclu que des éléments de preuve ont été obtenus dans des conditions qui portent atteinte aux droits ou libertés garantis par la présente *Charte*, ces éléments de preuve sont écartés s'il est établi, eu égard aux circonstances, que leur utilisation est susceptible de déconsidérer l'administration de la justice.

Historique des procédures

Lors du procès, Spencer a été déclaré coupable de possession de pornographie juvénile, mais il a été acquitté de l'accusation de la rendre accessible. La Cour d'appel de la Saskatchewan a confirmé la déclaration de culpabilité, mais elle a annulé l'acquittement relativement à l'accusation portée contre M. Spencer pour avoir rendu de la pornographie juvénile accessible et a ordonné la tenue d'un nouveau procès. M. Spencer a interjeté appel de la condamnation et du nouveau procès auprès de la Cour suprême du Canada (CSC).

Questions en litige

1. La police a-t-elle effectué une « fouille » ou une « perquisition » au sens de l'art. 8 de la *Charte* lorsqu'elle a obtenu les renseignements relatifs à l'abonnée à qui appartenait l'adresse IP?
2. Si oui, la fouille était-elle autorisée par la loi?
3. Si non, la preuve ainsi obtenue devrait-elle être écartée conformément à ce qui est prévu au par. 24(2) de la *Charte*?

Décision

La CSC a rejeté l'appel de façon unanime. Le juge Cromwell a, au nom de la Cour, statué que la demande présentée par la police en vue d'obtenir les renseignements constituait effectivement une « fouille » au sens de l'art. 8 de la *Charte*. De plus, la fouille n'a pas été effectuée de façon légale. Cependant, la CSC a au bout du compte décidé que la preuve obtenue au moyen de la fouille non autorisée ne serait pas écartée dans le nouveau procès.

Ratio decidendi

Pour déterminer si les mesures prises par la police sont considérées comme ou fouille ou une saisie au sens de l'art. 8 de la *Charte*, il faut déterminer si l'accusé s'attendait raisonnablement au respect du caractère privé des renseignements fournis. La Cour a statué qu'il existe une attente raisonnable en matière de vie privée à l'égard des renseignements relatifs à l'abonnée fournis par Shaw à la police. Dans bien des cas, la communication de ces renseignements permettra d'identifier l'utilisateur qui mène des activités intimes ou confidentielles en ligne en tenant normalement pour acquis que ces activités demeurent anonymes. Par conséquent, une demande faite par un policier pour demander au FSI de communiquer volontairement des renseignements de cette nature constitue une fouille.

Motifs du jugement

Lors du procès, Spencer a soutenu que la police avait porté atteinte au droit à la protection contre les fouilles, les perquisitions ou les saisies abusives qui lui est conféré par l'art. 8 de la *Charte*. La CSC devait tout d'abord déterminer si les mesures prises par la police constituaient effectivement une fouille. En examinant le lien entre la technique d'enquête utilisée par la police et l'intérêt en matière de vie privée qui était en cause, la CSC s'est penchée non seulement sur la nature des renseignements précis demandés, mais aussi sur la nature des renseignements qui ont ainsi été révélés. Le juge Cromwell a, au nom de la Cour, estimé que les renseignements de base liés à l'identité d'un abonné à un compte Internet (comme son nom et son adresse) correspondent à une activité informatique particulière sous surveillance et pourraient révéler des détails intimes sur le mode de vie et les choix personnels de la personne. Cela est important puisqu'un utilisateur Internet révèle seulement ces renseignements personnels intimes en tenant normalement pour acquis que ses activités demeureront anonymes.

La CSC a exploré la question de savoir si M. Spencer pouvait avoir des attentes raisonnables en matière de vie privée dans ce cas. Elle a examiné les conditions de service de Shaw puisqu'elles étaient pertinentes pour déterminer le caractère raisonnable des attentes d'un abonné quant au respect de sa vie privée. Les conditions de service de Shaw, dans leur ensemble,

n'étaient pas claires quant aux mesures que prendrait Shaw si la police lui adressait une demande de renseignements relatifs à un abonné. Puisque l'on ne pouvait se fonder sur les conditions de service pour justifier la communication des renseignements sur l'abonné, la CSC a statué que les attentes de Spencer en matière de respect de sa vie privée étaient effectivement raisonnables.

La prochaine question sur laquelle la CSC s'est penchée est de savoir si le sous-al. 7(3)c.1)(ii) de la *LPRPDE* autorise la communication de renseignements personnels. Cette disposition de la loi permet à un organisme de communiquer des renseignements personnels à la condition que la demande soit faite par une personne ayant « l'autorité légitime » de le faire. Pour que la police ait l'autorité légitime, elle a besoin soit d'un mandat ou d'une mesure législative (loi) qui l'autorise à agir.

La CSC n'était pas convaincue que la police pouvait démontrer qu'elle avait l'autorité légitime nécessaire pour obtenir les renseignements sur l'abonnée sans avoir préalablement obtenu un mandat. D'autres dispositions de la *LPRPDE* exigent spécifiquement que les entreprises de télécommunications communiquent des renseignements personnels lorsque la police a un mandat. Pour cette raison, la CSC a déterminé que la *LPRPDE* créait effectivement un pouvoir d'enquête permettant à la police d'obtenir des renseignements pour lesquels elle aurait besoin d'obtenir un mandat en temps normal. La Cour a fait remarquer que, puisque la *LPRPDE* a en fait pour objet d'augmenter la protection de la vie privée, cela était incompatible avec l'intention de la loi. La *LPRPDE* ne pouvait servir d'autorité pour demander des renseignements – il faudrait promulguer une nouvelle loi à cette fin explicite. Sans l'autorité juridique appropriée, la communication des renseignements personnels constituait effectivement une violation du droit de M. Spencer à la protection de sa vie privée.

Le juge Cromwell a clarifié que l'illégalité des actes de M. Spencer n'annulait pas ses droits en matière de vie privée. Puisque M. Spencer participait à une activité en ligne pour laquelle il avait une attente raisonnable en matière de protection de sa vie privée et de son anonymat, la police n'avait pas l'autorité nécessaire pour forcer Shaw à fournir des renseignements permettant de l'identifier. Sans mandat, la police pouvait **demander** qu'on lui communique les renseignements, mais elle n'avait pas l'autorité requise pour **obliger** Shaw à donner suite à sa demande. En d'autres mots, en raison des droits en matière de vie privée, la police ne peut pas utiliser des adresses IP anonymes comme point de départ pour des « missions exploratoires » visant à identifier des suspects particuliers. Cependant, la CSC a clairement indiqué que, en général, un FSI a un intérêt légitime à lutter contre les crimes commis en utilisant ses services, et que des considérations tout à fait différentes peuvent donc s'appliquer si le FSI détecte lui-même une activité illégale et, de sa propre initiative, souhaite la signaler à la police.

Le paragraphe 24(2) de la *Charte* fournit aux tribunaux un critère qu'ils peuvent utiliser pour déterminer si la preuve relative à un crime qui a été recueillie en violant certains droits conférés par la *Charte* peut tout de même être présentée lors du procès. Les deux points clés pour ce critère sont : a) la police a t elle agi de bonne foi dans son enquête et; b) l'administration de la justice serait-elle déconsidérée davantage par l'exclusion de la preuve que par son admission. Bien que l'on ait violé le droit constitutionnel de M. Spencer de ne pas faire l'objet d'une fouille abusive, la CSC a conclu que la police s'est servie de ce qu'elle croyait raisonnablement être des moyens légitimes pour poursuivre un objectif important visant l'application de la loi. Selon la Cour, la nature des mesures prises par la police dans cette affaire n'était pas susceptible de déconsidérer l'administration de la justice. Au contraire, les infractions commises dans cette affaire sont graves et la société a un intérêt manifeste à ce que M. Spencer soit traduit en justice. Par conséquent, la CSC a statué que c'est l'exclusion de la preuve, et non son admission, qui serait susceptible de déconsidérer l'administration de la justice. La déclaration de culpabilité prononcée par le tribunal inférieur en ce qui concerne les accusations de possession de pornographie a été maintenue et la CSC a ordonné la tenue d'un nouveau procès pour l'accusation déposée contre M. Spencer pour avoir rendu disponible de la pornographie juvénile.

DISCUSSION

1. À quel point comprenez-vous la politique de votre FSI en matière de vie privée? Lorsque vous êtes en ligne, vous considérez-vous comme anonyme? Pourquoi?

2. Êtes-vous d'accord avec la Cour pour dire que la surveillance des activités en ligne d'une personne pourrait révéler des renseignements très personnels et privés? Cela pourrait-il révéler des renseignements qui sont délicats, mais pas illégaux?

3. Avant l'arrêt *Spencer*, il était devenu courant pour la police d'obtenir des renseignements d'identification sur des Canadiens et Canadiennes auprès de FSI. Que risque-t-on en permettant à la police de poursuivre cette pratique dans des cas tels que celui-ci?

4. Selon vous, les enquêtes policières sur des cas similaires seront-elles significativement retardées du fait que la police doit demander un mandat de perquisition?

5. La CSC s'est dite convaincue que la gravité de l'infraction était suffisante pour admettre la preuve au procès, même si elle a été obtenue de façon illégale. Selon vous, cela devrait-il être le cas pour d'autres cybercrimes anonymes, comme le harcèlement, le vol d'identité ou la fuite de documents classifiés? Expliquez votre réponse.