Vol. 29, n° 2

Pirates, *hack*, messages textes et oubli : les décisions marquantes de 2016 en droit à la vie privée

Pierre-Luc Déziel*

* Professeur adjoint, Faculté de droit, Université Laval.

[Note de la rédaction : cet article a été soumis à une évaluation à double anonymat.]

INTRODUCTION

L'objectif de cet article est de présenter les cinq décisions canadiennes qui, à mon avis, ont été les plus importantes dans le domaine du droit à la vie privée en 2016. À cet effet, il convient de préciser le critère utilisé pour évaluer l'importance d'une décision. Une décision sera considérée comme importante dans la mesure où elle illustre un problème actuel dans le domaine de la protection de la vie privée, et permet de comprendre comment le droit s'est adapté pour offrir une solution à ce problème. À cet égard, il est peu surprenant que plusieurs de ces décisions, pour ne pas dire l'ensemble de ces décisions, portent sur la dimension « informationnelle »[1] de la vie privée, et sur les difficultés qu'engendre l'évolution rapide des technologies de l'information et des communications sur le plan de la protection du droit à la vie privée.

La décision qui coiffe ce « top-5 » est le Rapport de conclusions d'enquête en vertu de la LPRPDÉ nº 2016-005 produit par le Commissariat à la protection de la vie privée dans le cadre de l'affaire *Ashley Madison*, et qui aborde la question des mesures de sécurité que doit mettre en place une entreprise pour protéger les renseignements personnels qui sont sous son contrôle. Je me pencherai ensuite sur le nouveau *tort* de publication de faits intimes que la Cour supérieure de justice de l'Ontario a créé dans *Doe 464533* v *N.D.*, 2016 ONSC 541 pour faire remédier au phénomène du *revenge porn*. Troisièmement, je proposerai une analyse synchronique de deux décisions, *R* v *Craig*, 2016 BCCA 154 et *R* v *Marakah*, 2016 ONCA 542, qui portent toutes deux sur l'attente raisonnable qu'un individu peut revendiquer, ou non, à l'égard d'un message texte se trouvant dans l'objet connecté d'un tiers. La quatrième décision choisie est *R* v *Rogers Communications*, 2016 ONSC 70, jugement à l'occasion duquel la Cour supérieure

1. Rappelons que, dans *R* c *Dyment*, [1988] 2 RCS 417, le juge La Forest, aux para 19 et s, distingue trois dimensions de la vie privée : la dimension territoriale, qui touche à la protection de la vie privée dans les différents lieux, la dimension personnelle, qui porte sur la protection du corps et des substances corporelles de la personne, et la dimension informationnelle, qui porte sur la protection des renseignements.

de justice de l'Ontario a développé des lignes directrices pour encadrer la technique d'enquête de plus en plus courante qu'est le *tower dump*. Finalement, je tournerai mon attention vers la décision que la Commission d'accès à l'information du Québec a rendue à l'occasion de l'affaire *C.L.* c *BCF Avocats d'affaires*, 2016 QCCAI 114, une décision importante dans la mesure où elle nous permet de mettre en lumière certaines limites du droit canadien sur le plan de l'élaboration d'un « droit à l'oubli », tel que récemment consacré en Europe.

Pour chacune de ces décisions, que je présente par ailleurs en ordre décroissant d'importance, je m'affairerai d'abord à en présenter les faits, pour ensuite en donner une analyse descriptive, et finalement en expliquer la pertinence eu égard aux enjeux contemporains en matière de protection de la vie privée (dans sa dimension « informationnelle »). Je conclurai l'article en tentant d'identifier certains points de convergence et de recoupement entre les décisions présentées.

1. L'AFFAIRE *ASHLEY MADISON* : LE RAPPORT DE CONCLUSIONS D'ENQUÊTE EN VERTU DE LA LPRPDE N^{O} 2016-005

L'année 2016 fut le théâtre d'un nombre conséquent de cyberattaques ayant compromis la sécurité des renseignements personnels collectés par des entreprises privées. Au mois de septembre 2016, la compagnie Yahoo ! annonçait avoir été victime, en 2014, d'une attaque informatique par laquelle les renseignements personnels d'au moins 500 millions d'usagers de ses services lui furent dérobés[2]. Les renseignements volés comprenaient, notamment, le nom, l'adresse courriel et la date de naissance des usagers. Quelques semaines plus tard, soit au mois de décembre 2016, Yahoo ! annonçait avoir été victime d'une autre cyberattaque, remontant cette fois à 2013, et ayant permis le vol de renseignements personnels d'au moins un milliard de clients[3]. Toutefois, la cyberattaque ayant fort probablement fait le plus couler d'encre est celle qui a visé la compagnie Avid Life Media Inc (ALM), la compagnie qui exploite le site Ashley Madison, un site de rencontre dédié aux personnes désireuses d'entretenir une relation extra-conjugale.

2. Andy Greenberg, « Hack Brief: Yahoo Breach Hits Half a Billion Users », *Wired*, 22 septembre 2016, en ligne: <https://www.wired.com/2016/09/hack-brief-yahoo-looks-set-confirm-big-old-data-breach/>.
3. Lily Hay Newman, « Hack Brief: Hackers Breach a Billion Yahoo Accounts. A Billion », *Wired*, 14 décembre 2016, en ligne: <https://www.wired.com/2016/12/yahoo-hack-billion-users/>.

1.1 Les faits de l'affaire *Madison*

En juillet 2015, un groupe appelé « The Impact Team » a piraté le système informatique d'ALM. Le groupe a demandé à ALM de fermer deux de ses sites Internet, soit Ashley Madison et Established Men, ce dernier étant un autre site de rencontre, faute de quoi les renseignements personnels des utilisateurs du site Ashley Madison seraient publiés sur Internet. ALM a refusé la demande de The Impact Team et, en août 2015, les données personnelles de 36 millions d'utilisateurs du site Ashley Madison ont été rendues publiques. Le Commissaire à la protection de la vie privée du Canada (CPVP) a par conséquent ouvert une enquête sur les mesures qu'avait prises ALM afin d'assurer la sécurité des données personnelles qu'elle avait collectées auprès de ses clients. Il est important de mentionner qu'en raison de l'ampleur de l'atteinte à la sécurité des données[4], l'enquête fut menée de manière conjointe par le CPVP et le Commissariat à l'information de l'Australie. Toutefois, je me concentrerai ici uniquement sur le volet canadien du rapport.

En vertu de la *Loi sur la protection des renseignements personnels et les documents électroniques*[5], les compagnies canadiennes sont responsables des données qu'elles collectent et manipulent, en plus d'avoir l'obligation d'en assurer la sécurité. Ainsi, l'objet de l'enquête du CPVP était de déterminer si ALM avait respecté les obligations que lui impose la LRPDÉ en matière de sécurisation des données. Nous verrons que l'enquête aura révélé d'importants manquements d'ALM. Dans une certaine mesure, le rapport d'enquête du CPVP se présente comme un manuel à l'intention des entreprises qui collectent des renseignements personnels, puisqu'il vient préciser certaines des mesures que les entreprises devraient adopter pour atteindre les objectifs que leur fixe la LRPDÉ. À cet effet, il convient de mentionner que la LRPDÉ est une loi qui, en raison de l'intention du législateur à rester neutre sur le plan technologique, est relativement peu précise. Plusieurs obligations sont formulées de manière générale et, en ce sens, le rapport du CPVP dans l'affaire *Ashley Madison* vient apporter quelques précisions qui ne peuvent qu'être vues d'un bon œil par les entreprises canadiennes. Comme le mentionne le rapport, « [l]es conclusions énoncées dans le présent rapport comportent des leçons importantes pour d'autres organisations qui détiennent des renseignements personnels. »[6].

4. Rapport de conclusions d'enquête en vertu de la LPRPDÉ nº 2016-005 au para 3 [Rapport LPRPDÉ].
5. LC 2000, c 5 (LPRPDÉ).
6. Rapport LPRPDÉ, *supra* note 4, au para 9.

1.2 Le rapport de conclusions d'enquête

La première question à laquelle on se doit de répondre pour bien comprendre le rapport du CPVP est la suivante : quels sont les renseignements personnels qui furent dérobés à ALM ? Les renseignements volés peuvent être regroupés en trois catégories[7]. D'abord, on parle de renseignements « sur le profil » de l'utilisateur, c'est-à-dire des renseignements que l'utilisateur aura inscrits sur son profil afin de se décrire, mais aussi de partager le type de relation qu'il recherche. On parle donc du nom de l'utilisateur, de sa date de naissance, de son sexe, de sa silhouette, de sa taille et de son poids. On parle aussi de textes écrits par l'utilisateur où il précise quels sont ses désirs intimes, où il dépeint son partenaire idéal, où il parle de ses intérêts personnels et établit ses limites. La deuxième catégorie regroupe les renseignements sur la facturation : l'adresse de facturation de la personne et les quatre derniers chiffres de sa carte de crédit. Finalement, les pirates ont saisi des données sur le « compte » de l'utilisateur, c'est-à-dire les mots de passe, identifiants, adresses courriel, photos, et réponses aux questions de sécurité.

1.2.1 La sécurité des données (et l'importance de la composante organisationnelle)

On aura compris que les renseignements volés sont des renseignements hautement sensibles et personnels, des renseignements qui décrivent certaines des habitudes, croyances, préférences et intérêts les plus intimes d'une personne que l'on peut ici aisément identifier. La nature particulièrement sensible des données dérobées à ALM n'est pas, sur le plan juridique, sans incidence. En effet, en vertu du principe 4.7 de la LRPDÉ, les entreprises canadiennes ont l'obligation d'assurer la sécurité des données dont elles ont la responsabilité, et ce, « au moyen de mesures de sécurité correspondant à leur degré de sensibilité »[8]. Comme le degré de sensibilité des données dont il est ici question est particulièrement élevé, les moyens de sécurité adoptés par ALM auraient dû, eux aussi, être particulièrement élevés. Toutefois, l'enquête du CPVP tend à démontrer que les mesures de sécurité prises par ALM étaient nettement insuffisantes.

Les mesures de sécurité que doit prendre une entreprise peuvent être matérielles, technologiques et organisationnelles :

7. *Ibid*, au para 18.
8. LRPDÉ, *supra* note 5, annexe 1, principe 4.7.

- La *sécurité matérielle* se décline sous l'angle des mesures de sécurité physiques que prend une entreprise pour sécuriser ses données. Placer les serveurs dans une salle isolée et verrouillée, assurer la gestion de l'accès à cette salle par le biais de serrures biométriques, de cartes d'identification personnelle ou de code d'accès numérique sont des exemples de sécurité matérielle.
- La *sécurité technologique* renvoie à l'ensemble des mesures informatiques que prend une entreprise pour sécuriser ses serveurs et ses réseaux. On parle alors de pare-feu (*firewalls*), de segmentation du réseau, de logiciels antivirus, de serveurs privés et virtuels (*virtual private networks* ou *VPN*), de mots de passe et de codage de l'information. Sur le plan organisationnel, la sécurité se met en place par la formation du personnel, l'élaboration de politiques sur la vie privée et la sécurité de l'information, la gouvernance et la gestion du risque d'atteinte à la sécurité.
- Il serait facile de croire que la composante organisationnelle est, en quelque sorte, la moins importante des catégories de mesures de sécurité, mais il n'en est rien. Au contraire, c'est la *sécurité organisationnelle* qui fait en sorte que des personnes compétentes et bien formées sont chargées de mettre à jour les mesures techniques et de mettre en place des mesures physiques. En d'autres mots, les mesures de sécurité matérielles et technologiques dépendent en grande partie de l'efficacité de la sécurité organisationnelle.

Il semblerait que ce soit surtout sur le plan organisationnel que la sécurité d'ALM fut vulnérable. Une des lacunes principales identifiées par le CPVP est l'absence de politique générale de gestion et de sécurité des données. Une bonne politique de gestion des données est essentielle parce qu'elle établit clairement les pratiques à adopter et les procédures à suivre pour assurer la sécurité des données. Elle permet de gérer et de surveiller les accès aux réseaux, et identifie les mesures techniques qui doivent être mises en œuvre. Par conséquent, plusieurs des failles identifiées par le CPVP résultent directement de l'absence de cette politique générale de gestion de l'information. En ce sens, les auteurs du rapport du CPVP soulignent que :

> l'équipe d'enquête a relevé dans les mesures de sécurité de graves lacunes révélant l'absence de politiques et de pratiques appropriées. Par exemple, les politiques et procédures de sécurité devraient prévoir des mesures à la fois de prévention et de détection. Or, d'après l'information fournie, ALM n'avait pas mis en œuvre plusieurs contre-mesures de détection couram-

> ment utilisées qui pourraient aider à détecter les attaques ou à relever des anomalies indiquant des problèmes de sécurité. Ces systèmes n'auraient pas nécessairement permis de détecter des intrusions comme celle faite par le pirate, mais il s'agit d'importantes lignes de défense qui pourraient aider à limiter les répercussions des attaques.[9]

Dans le même ordre d'idée, ALM ne s'était pas dotée d'un système qui lui aurait permis de détecter des accès inusités à son système informatique ou des comportements inhabituels sur son réseau[10]. Cette lacune est particulièrement problématique, puisque, lors de l'enquête du CPVP, il fut possible de déterminer que le pirate avait eu accès au réseau d'ALM quelques semaines avant le vol, et qu'il avait utilisé des identifiants et des mots de passe valides. Le CPVP conclut ainsi que « ALM ne surveillait pas ses systèmes de façon adéquate pour déceler les indices d'intrusion ou d'autre activité non autorisée. »[11]. L'enquête du CPVP aura également permis d'établir que ALM ne s'était pas dotée de cadre de gestion des risques lui permettant d'évaluer périodiquement les menaces qui pèsent contre les données personnelles qui étaient sous son contrôle[12].

Les conclusions du rapport du CPVP en ce qui a trait à la sécurité des données sont claires. En n'adoptant pas de politique de gestion de la sécurité de l'information, ni de cadre de gestion du risque, ALM a contrevenu aux principes 4.1.4 et 4.7 de la LRPDÉ. La leçon du rapport du CPVP est, à mon sens, tout aussi claire : pour assurer la sécurité des renseignements personnels qui sont sous son contrôle, une entreprise doit, avant toute chose, se doter de fortes mesures de sécurité organisationnelles. Il s'agit là d'une condition première à la sécurisation efficace des renseignements personnels et du respect des obligations imposées par la LRPDÉ.

1.2.2 La conservation des données (et la question des frais de destruction)

Le rapport du CPVP met également en lumière des manquements de l'ALM en matière de conservation des données personnelles. Pour bien comprendre ce volet du rapport, il importe de préciser que certains des renseignements personnels volés par l'Impact Team portaient sur des profils de membres qui étaient depuis longtemps

9. Rapport LPRPDÉ, *supra* note 4, au para 67.
10. *Ibid*, au para 68.
11. *Ibid*, au para 68.
12. *Ibid*, au para 69.

inactifs sur le site, ou qui avaient décidé de fermer leur compte avec Ashley Madison. En vertu du principe 4.5 de la LRPDÉ, les entreprises ne doivent conserver les renseignements personnels sous leur contrôle que pour la durée de temps nécessaire à l'atteinte des fins visées par la collecte initiale[13]. À cet effet, les entreprises doivent clairement établir quelles sont les durées minimales et maximales de conservation des données. Elles doivent aussi mettre en place une procédure appropriée de destruction ou de minimisation des données qualifiées de désuètes. De plus, en vertu du principe 4.3 de la LRPDÉ, les entreprises sont tenues, en certains cas, de détruire les renseignements qu'elles possèdent à la demande de la personne qui en est la source. En ces cas, il s'agit d'un retrait du consentement de la personne.

Au moment de l'incident, ALM offrait deux options de désactivation des profils : une désactivation gratuite « de base », et une désactivation payante « complète ». Ainsi, une des principales questions d'intérêt de l'enquête du CPVP fut de déterminer s'il est acceptable pour une entreprise d'imposer des frais – dans ce cas 19 $ – pour détruire les renseignements qui sont sous son contrôle. L'imposition de ces frais n'était pas mentionnée dans la « Charte de confidentialité » du site Ashley Madison, ni dans les « Conditions générales d'utilisation » dudit site[14]. Je me concentrerai ici sur ce point, qui me semble d'intérêt tant pour les consommateurs canadiens que les entreprises qui manipulent des renseignements personnels. ALM justifie cette pratique par le fait que supprimer complètement un compte représente un travail long et coûteux. ALM précise que, lorsque l'on supprime un compte, on doit aussi effacer les messages que la personne a envoyés à d'autres membres et qui se trouvent dans les boîtes de messagerie de ces membres. Il y aurait là un important travail de traçage des messages.

Le principe 4.3.8 de la LRPDÉ établit qu'une personne « peut retirer son consentement en tout temps, sous réserve de restrictions prévues par une loi ou un contrat et d'un préavis raisonnable. » Dans ce cas, la loi n'établit pas de restrictions pour le retrait du consentement. De plus, tel qu'indiqué plus haut, ni la « Charte de confidentialité » ni les « Conditions d'utilisation » du site Ashley Madison ne prévoyaient ces frais. Ainsi, les restrictions évoquées par la LRPDÉ

13. Le principe 4.5 de la LRPDÉ spécifie que « [l]es renseignements personnels ne doivent pas être utilisés ou communiqués à des fins autres que celles auxquelles ils ont été recueillis à moins que la personne concernée n'y consente ou que la loi ne l'exige. On ne doit conserver les renseignements personnels qu'aussi longtemps que nécessaire pour la réalisation des fins déterminées. »
14. Rapport LPRPDÉ, *supra* note 4, au para 103.

ne peuvent être considérées comme émanant d'un contrat ou d'un préavis raisonnable. Par conséquent, cette pratique de facturation d'ALM contrevient au principe 4.3.8 de la LRPDÉ. Mentionnons aussi que le CPVP précise que, même si cette pratique avait été évoquée dans la « Charte de confidentialité » ou les « Conditions d'utilisation » il ne serait pas certain qu'elle aurait été pour autant qualifiée de raisonnable. En effet, comme le soulignent les auteurs du rapport, il aurait alors été nécessaire d'évaluer « le caractère raisonnable de cette pratique en fonction de facteurs tels que la pertinence et l'opportunité de l'avis, le coût réel pour l'organisation par rapport aux frais imposés et l'incidence probable des frais sur le droit d'un utilisateur de retirer son consentement. »[15].

1.2.3 L'exactitude des données

En vertu du principe 4.6 de la LRPDÉ, les entreprises doivent tenir des renseignements personnels qui sont exacts, complets et à jour. Dans la débâcle de l'affaire *Ashley Madison*, plusieurs adresses courriel furent publiées. Or, certaines de ces adresses courriel n'appartenaient pas à des personnes qui avaient utilisé le site de rencontre. L'explication réside dans le fait qu'au moment de l'inscription, il n'y avait pas de vérification automatique de l'exactitude de l'adresse courriel. Plus précisément, il n'y avait pas de processus de vérification que l'adresse courriel utilisée pour ouvrir le compte appartenait véritablement à la personne qui désirait ouvrir le compte. Pour assurer la vérification des adresses courriel, il aurait été nécessaire d'envoyer un courriel à l'adresse fournie par la personne. Celle-ci devra ensuite finaliser l'ouverture de compte à partir de cette adresse. Cette pratique permet de s'assurer que la personne a bel et bien accès à la boîte courriel qu'elle prétend utiliser. ALM défend sa position en affirmant qu'en vérifiant les adresses courriel, elle pourrait porter atteinte à la vie privée des abonnées et leur porter préjudice. En effet, une personne qui ouvre un compte sur un site de rencontres extra-conjugales ne souhaite peut-être pas recevoir un courriel qui confirme l'ouverture d'un tel compte…

Ainsi, certaines des adresses détenues par ALM n'étaient pas exactes. En ce sens, une des premières choses que doit faire le CPVP est de déterminer si une adresse courriel est un renseignement personnel au sens de la LRPDÉ. Sur ce point, les conclusions du CPVP sont éclairantes et répondent à une question qui, à ma connaissance, était encore sans réponse claire dans la jurisprudence canadienne. Un renseignement personnel est un renseignement qui concerne un

15. Rapport LPRPDÉ, *supra* note 4, au para 132.

individu identifiable. Certaines adresses courriel sont *directement* identifiables, par exemple, si elles contiennent le nom et prénom d'une personne. D'autres adresses, utilisant des pseudonymes ou des surnoms, ne permettent pas de directement identifier un individu. Toutefois, selon le CPVP, une adresse courriel est un renseignement personnel au sens de la LRPDÉ, même si elle ne permet pas une identification directe. La raison en est qu'une personne peut être indirectement identifiée au moyen d'une adresse courriel et d'autres renseignements :

> Certaines adresses de courriel permettent à elles seules d'identifier clairement une personne par son nom et d'autres données comme son lieu de travail. Par exemple l'information publiée en ligne contenait une adresse de courriel censée appartenir au premier ministre de la Nouvelle-Zélande, soit « john.key@pm.govt.nz ». Toutefois, une adresse de courriel ne permettant pas à elle seule d'identifier une personne peut permettre d'identifier une personne lorsqu'on la combine à d'autres données. Par exemple, il est possible de mener une recherche en ligne pour identifier le détenteur d'une adresse de courriel. Si cette recherche est possible, l'information associée à l'adresse de courriel constitue donc un renseignement personnel.

Ici, le raisonnement du CPVP explicite une tendance selon laquelle un renseignement peut être qualifié de « personnel » s'il permet une identification *indirecte* de la personne qui en est la source[16]. Comme ALM possédait des adresses courriel qui n'étaient pas exactes, et comme une adresse courriel est un renseignement personnel, ALM avait sous son contrôle des renseignements personnels qui n'étaient pas exacts. Par conséquent, la pratique de non-vérification d'ALM contrevenait au principe 4.6. de la LRPDÉ.

1.2.4 La transparence

La transparence est une composante de l'obligation d'obtenir un consentement valide. Le consommateur doit avoir en main des informations fiables et exactes quand il consent à la collecte et à l'utilisation de ses renseignements personnels. Ainsi, en vertu du principe 4.8 de la LRPDÉ, les entreprises doivent faire preuve de transparence avec leurs clients. Nous avons déjà vu qu'il y avait certains manquements en matière de désactivation et de suppression des comptes d'utilisateurs, alors qu'ALM n'avertissait pas les clients

16. Voir, par exemple, *Gordon* c *Canada (Santé)*, 2008 CF 258, et la *Loi de 2004 sur la protection des renseignements personnels sur la santé*, LO 2004, c 3.

potentiels que, pour détruire leurs renseignements personnels, ils devraient s'acquitter de frais de 19 $.

Mais la réelle lacune, sur le plan de la transparence, se situe au niveau de la sécurité des données. Tel qu'exposé au point 1.2.1, la sécurité des données personnelles sous le contrôle d'ALM était largement déficiente. Néanmoins, sur la page d'*Ashley Madison* se trouvait un certain nombre de « logos » de marque de confiance laissant croire aux utilisateurs que le site offrait un niveau élevé de sécurité et de discrétion. Les logos prenaient la forme d'icône de cadenas et de médailles en or. Comme le mentionne le CPVP :

> À première vue, ces déclarations et marques de confiance semblaient donner aux personnes qui envisageaient d'utiliser les services d'ALM l'impression générale que le site était conforme à des normes élevées en matière de sécurité et de discrétion et qu'elles pouvaient se fier à ces affirmations. Par conséquent, la marque de confiance et le niveau de sécurité ont pu influencer leur décision d'utiliser ou non le site.[17]

Or, lors de l'enquête du CPVP, ALM a admis que ces logos et marque de confiance avaient été créés « de toutes pièces » par l'entreprise. Jamais ne s'était-elle vu attribuer cette certification – fictive – par une tierce partie compétente, objective et reconnue. Ces logos et marques de confiance étaient de pures créations d'ALM. Il s'agit là d'un comportement intentionnellement trompeur traduisant un manque flagrant de transparence. Par conséquent, ALM a enfreint le principe 4.8. de la LRPDÉ.

1.3 L'importance de l'affaire *Ashley Madison*

Le rapport des conclusions d'enquêtes du CPVP dans l'affaire *Ashley Madison* revêt une importance particulière à l'ère du numérique, et ce, pour plusieurs raisons. J'en retiendrai deux.

Dans un premier temps, le rapport du CPVP, discuté ici de manière relativement sommaire, est extrêmement détaillé et fouillé. Il renferme une quantité importante d'informations pouvant être particulièrement utiles pour les entreprises privées dans le cadre de leurs activités de sécurisation des données personnelles qui sont sous leur contrôle. Bien que la LRPDÉ établisse une obligation relative à la sécurité des données, la loi demeure sur la manière dont on s'attend à ce que les entreprises arrivent à respecter cette obligation.

17. Rapport LPRPDÉ, *supra* note 4, au para 51.

Qu'entend-on exactement par « sécurité des données » ? Comment arriver à un niveau de sécurité raisonnable qui permet de respecter les obligations légales ? À cet effet, le rapport du CPVP apporte de précieuses précisions qui, me semble-t-il, ne peuvent qu'être vues d'un bon œil par les entreprises.

Dans un deuxième temps, il me semble que l'affaire *Ashley Madison* aura produit des effets qui se font et se feront sentir bien au-delà du contexte purement juridique. Je crois qu'un des principaux effets de l'affaire *Ashley Madison* aura été de sensibiliser les entreprises privées, comme les citoyens d'ailleurs, à l'importance de la sécurité des données dans les environnements numériques. Il y a ici une double leçon à retenir. Assurer la sécurité des données n'est pas une mince affaire, ce n'est pas quelque chose à prendre à la légère. Il faut avoir une stratégie aboutie, une politique claire et un cadre de gestion des risques. La sécurité technologique n'est pas, à elle seule, suffisante. De même, partager ses renseignements personnels n'est pas une chose banale. Une attitude de « saine méfiance », si l'on peut dire, doit être adoptée par les usagers à l'égard des différents services qui leur sont disponibles en ligne.

2. LE CAS DU *REVENGE PORN* : *DOE 464533* V *N.D.*, 2016 ONSC 541

Le deuxième cas que j'ai retenu (l'affaire *Doe 464533*) touche à une problématique qui, malheureusement, s'impose à l'ère du numérique : le phénomène du *revenge porn*. Ce phénomène, par lequel des images ou vidéos de nature sexuelle et explicite sont publiés en ligne sans le consentement de toutes les parties[18], est de plus en plus répandu. Une étude, intitulée « Love, Relationships, and Technology » et publiée par la firme McAfee, révélait qu'une personne sur dix fut menacée par son ex-partenaire de publication d'images intimes en ligne. Dans 60 % des cas, ces menaces furent mises à exécution[19].

Depuis un certain nombre d'années, les législateurs provinciaux et fédéral ont adopté un certain nombre de lois s'attaquant au

18. Cette définition est une traduction libre de celle fournie par Michael Power, avocat et expert en droit à la vie privée. Voir *Revenge Porn and Canadian Law*, en ligne : <http://michaelpower.ca/2015/01/revenge-porn-canadian-law/> (dernière consultation, 11 février 2016).
19. *Lovers Beware: Scorned Exes May Share Intimate Data And Images Online*, Février 2013, McAfee, en ligne : <https://www.mcafee.com/us/about/news/2013/q1/20130204-01.aspx> (dernière consultation, 11 février 2016). L'étude fut trouvée dans l'article de Michael Power, *supra* note 18.

phénomène du *revenge porn*. En janvier 2016, la *Loi sur la protection des images intimes*[20] du Manitoba est entrée en vigueur et, en 2014, le législateur fédéral a adopté la *Loi sur la protection des Canadiens contre la cybercriminalité*[21] dont l'article 3 créait l'article 162.1 du *Code criminel*, article qui criminalise la publication non consensuelle d'une image intime. C'est dans ce contexte sociojuridique que la décision rendue par la Cour supérieure de justice de l'Ontario dans l'affaire *Doe 464533* doit être considérée. En effet, c'est à l'occasion de cette affaire que la Cour ontarienne aura créé un nouveau *tort*, le *tort* de publication de faits privés et embarrassants ou, en anglais, « public disclosure of embarrassing private facts »[22]. Il s'agit là du premier recours de droit civil canadien permettant à une victime de *revenge porn* d'obtenir des dommages-intérêts pour le préjudice causé par la publication non consensuelle d'images intimes.

2.1 Les faits de l'affaire *Doe 464533*

Les faits de l'affaire *Doe 464533* remontent au mois d'août 2011, alors que le défendeur a demandé à la plaignante d'enregistrer une vidéo érotique et de la lui envoyer. La plaignante a refusé à maintes reprises, mais a fini par accepter d'enregistrer la vidéo demandée. Avant d'envoyer la vidéo au défendeur, elle lui envoya un message texte lui faisant part de sa réticence. Le défendeur insista et, après avoir dit à la victime que personne d'autre que lui ne verrait la vidéo, il réussit finalement à convaincre la jeune femme de la lui envoyer. En décembre 2011, la plaignante apprit que la vidéo érotique qu'elle avait enregistrée avait été mise en ligne sur un site Internet pornographique. Il fut rapidement établi que la vidéo avait été téléversée par le défendeur. Les conséquences sur la santé psychologique de la victime furent particulièrement importantes. Elle subit les symptômes d'une grave dépression et dut, à un certain moment, être prise en charge par un centre d'intervention de crise. Les répercussions se firent également sentir dans sa vie sociale, puisque la plupart des membres de son entourage et de ses connaissances avaient vu la vidéo ou étaient au courant de son existence. Aux dires du juge Stinson, la jeune femme demeure, cinq ans plus tard, marquée par ces événements et profondément inquiète que la vidéo ne refasse surface un jour et porte atteinte à sa vie personnelle ou professionnelle[23].

20. LM 2015, c 42.
21. LC 2014, c 31.
22. *Doe 464533* v *N.D.*, 2016 ONSC 541 au para 36 [*Doe 464533*].
23. *Doe 464533*, *supra* note 22, aux para 11-15.

2.2 La décision

La décision du juge Stinson s'articule en deux temps. D'abord, la question de la responsabilité et, ensuite, les dommages-intérêts à accorder à la victime. Je traiterai ces deux volets séparément. Nous verrons que la création du *tort* de publication non consensuelle d'une image intime représente un élargissement du *tort* d'atteinte à la vie privée. À cet effet, il s'agit d'un deuxième *tort* d'atteinte à la vie privée, un *tort* qui vient s'ajouter à celui « d'intrusion dans la solitude »[24] consacré par la Cour d'appel de l'Ontario dans *Jones* v *Tisge*, 2012 ONCA 32.

2.2.1 La responsabilité

Sur la question de la responsabilité, le juge Stinson s'intéresse à trois *torts* : l'abus de confiance, la détresse émotionnelle infligée intentionnellement et l'atteinte à la vie privée. Bien que les trois *torts* soient pertinents et applicables en l'espèce, je me concentrerai sur celui d'atteinte à la vie privée. Dans *Jones* v *Tisge*, 2012 ONCA 32, la Cour d'appel de l'Ontario s'était inspirée d'un article de William L. Prosser[25] écrit en 1960 pour consacrer le *tort* d'intrusion dans la solitude. L'article de Prosser défend l'idée selon laquelle le *tort* d'atteinte à la vie privée est en dernière analyse composé de quatre *torts* différents. Un de ces *torts* est l'intrusion dans la solitude que la Cour d'appel aura alors intégré en droit canadien. Dans *Doe 464533*, la Cour supérieure de justice de l'Ontario reprend l'article de Prosser, mais se penche sur un autre *tort* qui, selon elle, correspond mieux aux faits de l'affaire : le *tort* de « public disclosure of embarrassing private facts », que nous traduisons ici librement comme le *tort* de publication de faits privés.

Le *tort* de publication de faits privés s'applique aux situations où un détail intime de la vie d'une personne est divulgué, sans le consentement de la personne, aux yeux du public, et ce d'une manière qu'une personne raisonnable considérerait comme offensante[26]. Selon le juge Stinson, l'adoption du *tort* de publication de faits privés répond à un besoin urgent à l'ère du numérique et d'Internet. Ne pas offrir de recours légal à une personne qui a vu des images intimes d'elle publiées sur Internet sans son consentement laisserait un vide juridique qui n'est pas souhaitable[27]. Ainsi, le juge Stinson adopte la

24. En Anglais : « intrusion upon seclusion ».
25. William L. Prosser, « Privacy », (1960) 48:3 *California Law Review* 383.
26. *Doe 464533*, *supra* note 22, au para 42.
27. *Ibid*, au para 45.

formulation de Prosser, avec un ajout mineur. Le *tort* de publication de faits privés se présente donc comme suit :

> One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of the other's privacy, if the matter publicized *or the act of the publication* (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public.[28] (Les italiques indiquent l'ajout du juge Stinson)

On remarque d'abord que la modification apportée par le juge Stinson vient préciser une chose qui est fondamentale dans le cas du *revenge porn*. En disant que le *tort* s'applique aux situations où l'image est offensante *ou* aux situations où c'est l'acte de publier un fait intime qui est offensant, le juge dit que ce n'est pas ici la vidéo qui est problématique, c'est le fait que le défendeur ait publié la vidéo qui l'est. En somme, ce n'est pas la victime qui a commis un acte offensant en créant la vidéo. Ce n'est pas le contenu de la vidéo qui est offensant. C'est le fait de rendre publique la vidéo intime qui est offensant. Il me semble que cette précision est la bienvenue, puisqu'on dit à la victime que ce n'est pas elle qui a quelque chose à se reprocher.

2.2.2 Les dommages-intérêts

L'analyse du juge menant à la détermination du montant de dommages-intérêts que le défendeur aura à verser à la victime revêt un intérêt particulier. Tel que mentionné plus haut, l'arrêt *Doe 464533* est le premier cas où une victime de *revenge porn* peut obtenir des dommages. Par conséquent, il n'existe aucun précédent sur lequel s'appuyer pour déterminer le montant auquel devraient s'élever les dommages-intérêts. L'avocate de la plaignante suggère au juge une analogie entre la présente affaire et les cas d'agression sexuelle. Selon elle, les effets psychologiques et émotionnels qui peuvent découler d'une agression sexuelle s'apparentent à ceux auxquels doit faire face la victime de *revenge porn*. Elle ajoute que, dans une certaine mesure, les cas de *revenge porn* sont, sur ce point, pires que les cas d'agression sexuelle, puisque la violation de la personne perdure dans le temps. En effet, la vidéo a peut-être été copiée, et continue peut-être d'être visionnée. De plus, puisque la vidéo a été vue par plusieurs membres de son entourage, la plaignante fut également victime d'une atteinte à la réputation[29]. Le juge considère qu'il existe en effet assez de similitudes entre les cas d'agression et le cas d'espèce pour que

28. *Ibid*, au para 46.
29. *Ibid*, au para 51.

cette analogie soit pertinente dans le processus de détermination du montant des dommages-intérêts.

Sur ce point, la jurisprudence canadienne relative aux agressions sexuelles établit trois grands facteurs à prendre en considération :

- d'abord, les circonstances entourant l'agression, c'est-à-dire la fréquence, la violence, la nature dégradante ou attentatoire de celle-ci ;
- ensuite, les circonstances entourant la position de la victime. Est-ce une victime vulnérable en raison de son âge, qui avait confiance en son agresseur ? ;
- finalement, les conséquences que le comportement de l'agresseur aura engendrées sur la victime, y compris les blessures physiques et psychologiques.[30]

Pour chacun de ces facteurs, le juge considère que les actions du défendeur sont particulièrement graves. Fait particulier, le juge insiste sur le caractère particulièrement aggravant du *revenge porn* en soulignant que la publication de la vidéo équivaut à de multiples atteintes à la dignité de la victime. Son raisonnement s'appuie sur le fait que la vidéo peut être copiée, partagée, téléchargée et visionnée un nombre incalculable de fois :

> *The circumstances of the assaults including their number, frequency and how violent, invasive and degrading they were*. The wrongful act consisted of uploading to a pornographic website a video recording that displayed intimate images of the plaintiff. The defendant's actions were thus very invasive and degrading. The recording was available for viewing on the Internet for some three weeks. It is impossible to know how many times it was viewed, copied or downloaded, or how many copies still exist elsewhere, out of the defendant's (and the plaintiff's – and the Court's) control. As well, the defendant showed the video to his friends, who were also acquaintances of the plaintiff. Although there was no physical violence, in these circumstances, especially in light of the multiple times the video was viewed by others and, more importantly, the potential for the video still to be in circulation, it is appropriate to regard this as tantamount to multiple assaults on the plaintiff's dignity. (Les italiques sont nôtres)

30. *Ibid*, au para 53.

En raison de la gravité de la conduite du défendeur et du préjudice subi par la victime, le juge estime que le montant de dommages-intérêts approprié est celui qui, dans les circonstances, représente le montant maximum qu'il puisse allouer, soit 100 000 $. Le juge octroie donc des dommages généraux de 50 000 $, des dommages punitifs de 25 000 $ et des dommages majorés de 25 000 $. Le juge fixe l'indemnisation des dépens de la victime à 36 208,73 $.

2.3 L'importance de l'affaire *Doe 464533*

L'arrêt *Doe 464533* est un arrêt particulièrement important. Il démontre la volonté des tribunaux de sévir de manière conséquente contre la menace que représente le phénomène du *revenge porn*. Non seulement la Cour supérieure de justice de l'Ontario aura-t-elle créé un nouveau *tort*, mais elle aura aussi été, à mon avis, particulièrement lucide face aux particularités de ce phénomène, et sensible à l'éventail de blessures que subissent les victimes. Le dernier paragraphe de l'arrêt *Doe 464533* illustre bien la sensibilité du juge Stinson :

> Lastly, I wish to commend the plaintiff for her courage and resolve in pursuing the remedies to which she is entitled. She has experienced considerable psychological pain arising from the events in question, and has been called upon to relive and recount these events in the course of this litigation, thereby reviving painful memories. Given the lack of precedent in Canadian law for such a claim, she had no assurance of the outcome. Quite apart from the personal result for her, her efforts have established such a precedent that will enable others who endure the same experience to seek similar recourse.

On peut espérer que l'arrêt *Doe 464533* puisse permettre aux victimes de *revenge porn* d'obtenir une certaine forme de justice, mais qu'il puisse aussi servir de mise en garde aux potentiels agresseurs, et sensibiliser la population canadienne à la dure réalité de ce malheureux phénomène.

3. *R v CRAIG*, 2016 BCCA 154 ET *R v MARAKAH*, 2016 ONCA 542

Dans les affaires *Craig* et *Marakah*, les Cours d'appel de la Colombie-Britannique et de l'Ontario furent saisies d'une même question : peut-on revendiquer une attente raisonnable en matière de vie privée informationnelle à l'égard d'un message texte que l'on a envoyé, qui fut acheminé au destinataire, et qui est emmagasiné dans le téléphone de celui-ci (l'affaire *Marakah*) ou dans les serveurs

d'une entreprise privée de messagerie instantanée sociale (l'affaire *Craig*). Dans les deux cas, les messages révèlent des informations servant d'éléments de preuve mobilisés contre l'appelant. Dans les deux cas, il ne s'agit pas d'une *interception* de communication privée, puisque le message, tel que précisé plus haut, avait déjà rejoint son destinataire, mais bien d'une *saisie* de messages textes par des agents de police. Ainsi, dans *Craig* comme dans *Marakah*, ce n'est pas la partie VI du *Code criminel* qui s'applique, mais bien l'article 8 de la *Charte canadienne*.

Or, bien que les affaires *Craig* et *Marakah* comportent d'importantes similitudes sur les plans formel et factuel, les décisions rendues par les Cours d'appel de la Colombie-Britannique et de l'Ontario diffèrent largement sur le plan du contenu. En effet, si la Cour d'appel de la Colombie-Britannique a conclu dans *Craig* qu'une personne pouvait revendiquer une attente raisonnable à l'égard d'un message texte qu'il a envoyé et qui est emmagasiné dans un appareil qui n'est pas le sien, la Cour d'appel de l'Ontario a décidé dans *Marakah* qu'une telle attente n'était pas objectivement valide et ne pouvait exister. Ainsi, on est ici en présence de deux décisions qui traitent d'une question importante, mais qui arrivent à des conclusions (en apparence du moins) diamétralement opposées.

Nous verrons que ces résultats diffèrent principalement en raison du traitement que réserveront les Cours d'appel à *l'analyse fondée sur le risque* dans le contexte plus large de la détermination de l'existence, ou non, d'une attente raisonnable en matière de vie privée à l'égard des messages textes envoyés par une personne et emmagasinés sur l'appareil d'une autre. L'analyse fondée sur le risque affirme que, lorsqu'un tribunal doit déterminer si une attente raisonnable en matière de vie privée existe à l'égard d'un renseignement, le tribunal doit prendre en considération le risque que court consciemment la personne qui partage initialement ce renseignement à ce que ledit renseignement soit ensuite partagé avec d'autres personnes. En d'autres mots, le juge doit inclure dans son analyse le fait qu'une fois le message envoyé, une personne raisonnable doit s'attendre à ce que le message puisse être communiqué à d'autres, et ce, sans son consentement. Si ce risque est présent, on ne peut conclure que la personne pouvait raisonnablement s'attendre à ce que ledit message reste confidentiel. Par conséquent, on ne peut conclure que la personne puisse revendiquer une attente raisonnable *objective* en matière de vie privée à l'égard du message. Nous verrons plus loin que c'est en partie un tel raisonnement qui a amené la Cour d'appel de l'Ontario à conclure que l'appelant dans *Marakah* ne pouvait revendiquer d'attente raisonnable à l'égard d'un message texte qu'il avait envoyé

à un complice, et qui fut saisi par les policiers dans le téléphone de ce complice.

Il importe aussi de mentionner que l'analyse fondée sur le risque fut par ailleurs vigoureusement rejetée par la Cour suprême du Canada dans *R* c *Duarte*, [1990] 1 RCS 30 (*Duarte*) et *R* c *Wong*, [1990] 3 RCS 36 (*Wong*). Selon le plus haut tribunal du pays, une telle analyse est dangereuse et ne devrait pas être adoptée dans une société libre et démocratique. Nous y reviendrons. Pour le moment, il convient simplement de mentionner que la Cour d'appel de la Colombie-Britannique, à l'instar de la Cour suprême du Canada, a rejeté cette analyse fondée sur le risque. C'est, en partie, ce qui explique pourquoi, dans *Craig*, elle est arrivée à un résultat différent de celui auquel est arrivée la Cour d'appel de l'Ontario dans *Marakah*. Mentionnons que la dissidence du juge LaForme dans Marakah dénonce aussi cette analyse fondée sur le risque, et qu'il affirme l'existence d'une attente raisonnable à l'égard des messages textes qu'une personne envoie et qui sont emmagasinés dans le téléphone portable du destinataire.

3.1 Les faits des affaires *Craig* et *Marakah*

Dans *Craig*, l'appelant fait face à de nombreuses accusations d'infractions d'ordre sexuel perpétrées sur une personne âgée de moins de 16 ans. L'essentiel de la preuve présentée contre l'appelant est composé de messages qu'il a échangés avec la victime, E.V., sur le réseau social Nexopia, ainsi qu'avec certaines des amies de la victime. Ces messages étaient emmagasinés dans les serveurs de Nexopia, et furent saisis par les policiers à partir des profils Nexopia de E.V. et de ses amies. Certains des messages furent volontairement remis aux policiers par la victime, alors que d'autres furent saisis auprès de Nexopia à l'aide d'un mandat judiciaire. Au procès, l'accusé a contesté la validité du mandat judiciaire, un mandat qui avait été modifié par les policiers après son octroi et avant son exécution, et exécuté quelques jours après sa date d'expiration. Toutefois, le juge au procès a conclu que Craig ne pouvait revendiquer d'attente raisonnable à l'égard des messages saisis par les policiers, et n'était donc pas en position de contester la validité du mandat. Craig fut donc déclaré coupable des accusations pesant contre lui. Comme nous le verrons, la Cour d'appel de la Colombie-Britannique a conclu que Craig pouvait revendiquer une attente raisonnable à l'égard desdits messages, et qu'il pouvait contester la validité du mandat.

Dans *Marakah*, l'appelant est accusé de plusieurs infractions relatives à l'achat et au trafic d'armes à feu. Les principaux éléments de preuve sont le contenu de messages textes envoyés par Marakah

à son complice Andrew Winchester, et qui se trouvaient dans le téléphone de ce dernier quand il fut, lui aussi, arrêté. Les messages détaillaient les activités des complices en matière de trafic d'armes à feu. Lors d'une audience portant sur la capacité de l'appelant à contester la fouille du téléphone de son complice, le juge a conclu que celui-là ne pouvait revendiquer d'attente raisonnable à l'égard des messages extraits de la fouille du téléphone, et par conséquent, qu'il n'était pas en position de contester la validité de la fouille. La Cour d'appel de l'Ontario fut donc saisie pour déterminer si la conclusion du juge à l'audience préliminaire était valide. Comme nous le verrons, la Cour d'appel a confirmé la conclusion du juge à l'audience.

3.2 Les décisions

À mon avis, les décisions *Craig* et *Marakah* soulèvent trois grandes problématiques.

Dans un premier temps, est-ce que l'arrêt *R* c *Société Telus Communication*, [2013] 2 RCS 3 (*Telus*), qui porte sur l'interception de communications privées, et à l'occasion duquel la Cour suprême du Canada a conclu qu'un individu peut revendiquer une attente raisonnable à la vie privée à l'égard d'un message texte s'applique en l'espèce ?

Ensuite, quels sont les facteurs pertinents que l'on doit prendre en considération pour conduire une analyse de l'ensemble des circonstances menant à la détermination de l'existence ou non d'une telle attente raisonnable à l'endroit d'un message texte emmagasiné dans un serveur ou un téléphone que l'on ne possède pas ?

Finalement, quel rôle joue l'analyse fondée sur le risque dans ces affaires, et en quoi l'adoption d'une telle analyse influence-telle, ou non, les conclusions des Cours d'appel de la Colombie-Britannique et de l'Ontario ?

3.2.1 La pertinence de l'arrêt Telus *en l'espèce*

Dans l'arrêt *Telus*, la Cour suprême du Canada avait conclu que l'échange de messages textes représente, à notre époque, une forme de communication privée. Comme les communications privées jouissent d'une protection juridique élevée, et que l'on peut raisonnablement s'attendre à ce qu'elles demeurent « privées », il est possible, *a priori*, d'affirmer que les messages textes doivent eux aussi jouir d'une protection juridique élevée, et que l'on est en mesure de revendiquer une attente raisonnable en matière de vie privée à leur égard. Il n'est donc

pas surprenant que, dans *Marakah*, une des principales stratégies de l'appelant fut de s'en remettre à l'arrêt *Telus* pour affirmer l'existence d'une telle attente raisonnable à l'égard des messages textes contenus dans le téléphone de son complice. Toutefois, comme le souligne le juge MacPherson, bien que la thématique générale de la caractérisation des messages textes rapproche l'affaire *Marakah* de la décision *Telus*, d'importantes différences militent en faveur de leur différenciation.

Dans un premier temps, l'affaire *Telus* porte sur *l'interception* de messages textes, et sur la production *prospective* de messages textes. *Telus*, en d'autres termes, ne porte pas sur les messages textes envoyés et reçus, c'est-à-dire sur des messages textes *historiques*. Dans *Telus*, la Cour suprême du Canada devait déterminer si une interception de messages textes pouvait être conduite à l'aide d'un mandat général de fouille, ou si un mandat d'interception de communications privées devait plutôt servir d'autorisation juridique valide. C'est en ce sens que la Cour avait déterminé que l'échange de messages textes représente une forme de communications privées, et que seul un mandat d'interception obtenu en vertu de la partie VI du *Code criminel* pouvait autoriser une production prospective de messages textes. Tel que le mentionne le juge MacPherson, la juge Abella précise bien, dans *Telus*, que la décision de la Cour suprême du Canada ne s'intéresse pas à déterminer si la production de messages textes *historiques* nécessite un mandat d'interception[31].

Dans un deuxième temps, *Telus* n'est pas une décision où la Cour mène une analyse visant directement à déterminer l'existence ou non d'une attente raisonnable en matière de vie privée à l'égard des messages textes. *Telus* n'est pas un « standing case » où l'on entend déterminer si, dans un cas précis, une personne est en position de revendiquer une attente raisonnable à l'égard d'un objet, d'un renseignement ou d'un lieu. Pour le juge MacPherson, le fait d'interpréter *Telus* comme le suggère l'appelant – c'est-à-dire comme attribuant à tous les messages textes une attente raisonnable objective et élevée en matière de vie privée – reviendrait à créer une règle selon laquelle une personne peut *automatiquement* revendiquer une attente raisonnable à l'égard d'un message texte, peu importe où ce message se retrouve. Ce genre d'automatisme est contraire à la méthode déductive et contextuelle appliquée par les tribunaux canadiens. C'est pour ces raisons que le juge MacPherson écarte l'arrêt *Telus*. Mentionnons que l'arrêt *Telus* ne fut par ailleurs pas évoqué dans *Craig*.

31. *R* v *Marakah*, 2016 ONCA 542 au para 40 [*Marakah*].

3.2.2 Les questions relatives au contrôle, à l'accès et au contenu des messages textes

Contrairement à l'affaire *Telus*, les affaires *Craig* et *Marakah* sont des « standing cases », c'est-à-dire des cas où l'on doit déterminer si une personne est en position de contester la validité d'une fouille, d'une saisie ou d'une perquisition. Pour contester la validité d'une fouille, d'une saisie ou d'une perquisition et, par conséquent, invoquer la protection de l'article 8 de la *Charte canadienne*, une personne doit déterminer si elle possède une attente raisonnable en matière de vie privée à l'égard de l'objet, du lieu ou du renseignement qui fut saisi, fouillé ou perquisitionné. Pour déterminer si une personne peut revendiquer une telle attente, la Cour doit procéder, tel que prescrit dans *R* c *Edwards*, [1996] 1 RCS 28, à une analyse de l'ensemble des circonstances. Il n'existe cependant pas de liste exhaustive des critères pertinents et constituant cet « ensemble des circonstances ». Toutefois, dans le secteur informationnel, certains facteurs sont récurrents et souvent repris par les tribunaux : la nature de l'information, l'endroit où celle-ci se trouve, la capacité de la personne à contrôler l'accès à cet endroit, la possession par la personne de cet endroit, la capacité de l'information à révéler des détails intimes sur son mode de vie.

Dans *Craig* et dans *Marakah*, les Cours d'appel de la Colombie-Britannique et de l'Ontario se sont livrées à une analyse de l'ensemble des circonstances. De plus, elles reprirent essentiellement les mêmes critères. Toutefois, ce sera l'interprétation de ces critères et le poids qu'elles accorderont à chacun des facteurs choisis qui différeront et qui les mèneront à des conclusions largement différentes. Notons d'emblée que, pour le juge MacPherson de la Cour d'appel de l'Ontario, les critères du contrôle et de l'accès sont très importants. C'est l'accent mis sur ces facteurs qui, comme nous le verrons, entraînera le juge à mener une analyse fondée sur le risque. Le point 3.2.3, ci-dessous, portera plus précisément sur cette analyse et les risques qu'elle comporte.

3.2.2.1 Dans Marakah

Dans *Marakah*, l'analyse du juge MacPherson s'intéresse principalement aux facteurs que sont le contrôle et l'accès au téléphone du complice de Marakah où se trouvaient les messages. Selon lui, l'appelant n'était pas en mesure d'exercer quelque contrôle sur le téléphone de Winchester, et n'y avait aucunement accès. Par conséquent, il serait extrêmement difficile de reconnaître à Marakah une attente raisonnable en matière de vie privée qui soit objective à l'égard des messages que contient ce téléphone. Insistant sur la

notion de contrôle, le juge soutient que « [c]ontrol and access are fundamental to our understanding of informational privacy »[32]. À ce stade de son analyse, le juge fait intervenir, par le biais d'un extrait de la décision *R* c *Spencer*, [2014] 2 RCS 212, certaines des idées phares du théoricien Alan Westin. Il est important de mentionner que les idées de Westin inspirèrent certains des arrêts fondamentaux de la Cour suprême du Canada en matière de vie privée informationnelle comme, par exemple, *R* c *Dyment*, [1988] 2 RCS 417. Il est vrai que l'idée de contrôle occupe une place fondamentale dans la pensée de Westin et dans la jurisprudence canadienne relative à l'article 8 de la *Charte canadienne*. Elle joue aussi un rôle fondamental dans les lois fédérales et provinciales de protection des renseignements personnels. Mais, à mon avis, le rôle que joue la notion de contrôle, chez Westin comme dans nos lois et notre jurisprudence, est quelque peu différent du rôle que lui attribue le juge MacPherson.

Pour Alan Westin, la vie privée informationnelle se définit comme la capacité d'un individu à contrôler les modalités de diffusion et de circulation de ses renseignements personnels[33]. En somme, conférer à quelqu'un un droit à la vie privée, c'est lui donner le pouvoir et la liberté d'exercer un contrôle sur les renseignements dont il est la source. Cela ne revient pas à dire, comme semble le suggérer le juge MacPherson, qu'une personne qui n'exerce pas de contrôle sur un renseignement, ou sur un message texte, ne peut revendiquer de droit à la vie privée. Au contraire, cette absence de contrôle peut, dans une certaine mesure, traduire une *atteinte* à son droit à la vie privée. Il me semble donc que l'interprétation de la notion de contrôle chez Westin à laquelle se livre le juge est quelque peu hasardeuse.

Quoi qu'il en soit, pour le juge MacPherson, ce facteur de l'absence de contrôle et d'accès est un facteur déterminant et appuyant la conclusion selon laquelle l'appelant Marakah ne peut revendiquer d'attente raisonnable à l'égard des messages contenus dans le téléphone de son complice Winchester. Un autre facteur militant en faveur de cette conclusion, et qui différencie selon le juge MacPherson les affaires *Marakah* et *Craig*, est le fait que les messages ne contenaient pas d'information qui relevait du « cœur biographique » de l'accusé. Depuis *R* c *Plant*, [1993] 3 RCS 281 seuls les renseignements qui relèvent du cœur biographique de la personne, c'est-à-dire qui révèlent des détails intimes et relatifs au mode de vie de la personne, peuvent faire l'objet d'une attente raisonnable en matière de vie privée. Or, selon le juge, le contenu des messages textes soumis à l'examen ne

32. *Marakah*, *supra* note 31, au para 58.
33. Alan F. Westin, *Privacy and Freedom* (Londres, Bodley Head, 1970).

relève pas du cœur biographique de l'appelant et ne révèle pas des détails de nature intime. Par conséquent, le juge soutient que « [a]s such, control and access, as discussed above, are the primary considerations »[34].

Sur ce point, je dois avouer que je suis en désaccord avec le juge MacPherson. Les messages révélaient certaines des activités de l'appelant, nommément le fait qu'il participe au trafic d'armes à feu. Ces détails sont, à mon sens, révélateurs du mode de vie de la personne et de ses choix personnels. Si tel n'était pas le cas, les messages textes ne seraient d'aucune utilité pour les policiers ou pour la Couronne. Par conséquent, le contenu des messages relève du cœur biographique de la personne, et ce facteur devrait être pris en considération dans l'analyse de l'ensemble des circonstances. Précisons aussi que le fait que le mode de vie que met en lumière le contenu des messages textes puisse être qualifié de criminel, d'illégal, voire même d'immoral, n'a pas d'incidence sur les résultats de l'analyse en fonction de la doctrine du coeur biographique[35]. De même, la distinction que le juge établit entre les faits de l'affaire *Marakah* et ceux de l'affaire *Craig* ne me semble pas valide.

On aura donc compris que, dans *Marakah*, l'analyse de l'ensemble des circonstances est réduite à une analyse des facteurs que sont l'accès et le contrôle. Comme l'appelant n'est pas en contrôle du téléphone de son complice, et comme il n'a pas accès aux messages contenus dans ce téléphone, il ne peut revendiquer d'attente raisonnable en matière de vie privée à l'égard des messages soumis à l'examen. Ainsi, il n'est pas en mesure de contester la fouille du téléphone de son complice. La décision rendue en première instance est maintenue.

3.2.2.2 Dans Craig

L'analyse que mène la juge Bennett dans *Craig* diffère largement de celle menée par le juge MacPherson dans *Marakah*. Cette différence ne tient pas uniquement aux résultats auxquels arrivent les deux juges, mais au choix même des critères et facteurs à prendre en considération dans l'analyse de l'ensemble des circonstances. Dans *Craig*, la juge se penche sur quatre facteurs : le lieu de la fouille, la doctrine des objets bien en vue, les messages dans les mains de tierces parties et la nature de l'information. Les deux premiers points ne font

34. *Marakah*, *supra* note 31, au para 77.
35. Voir, sur ce point, *R* c *Morelli*, [2010] 1 RCS 253, *R* c *Cole*, [2012] 3 RCS 34 et, même, *R* v *Craig*, 2016 BCCA 154 [Craig].

pas l'objet d'un traitement particulièrement long. En ce qui a trait au lieu de la fouille, il s'agit du profil de la victime E.V. et, par extension, des serveurs de l'entreprise Nexopia. Comme le précise la juge, l'appelant Craig ne prétend pas revendiquer d'attente raisonnable à l'égard dudit profil ou desdits serveurs, mais bien à l'égard du *contenu* de certains des messages se trouvant dans ces « lieux », un contenu dont il est la source, le créateur. Un contenu, pour reprendre l'expression de la juge, qu'il a généré « [i]n this case, it is not ownership of the accounts which assist Mr. Craig. Rather, as I will discuss below, it is the fact that the accounts contained content *he generated* and were searched to obtain it. »[36].

Pour ce qui est de la doctrine des objets « bien en vue », il est important de remarquer que les messages n'étaient pas publics, qu'ils se trouvaient dans des profils ou serveurs protégés par des mots de passe et des identifiants, et qu'un mandat fut nécessaire pour saisir le contenu des messages. Ainsi, la doctrine ne s'applique pas[37].

C'est avec le troisième facteur que nous entrons dans le vif du sujet. Est-ce qu'en l'espèce, il serait raisonnable pour le citoyen ordinaire de s'attendre à ce que restent privés les messages qu'il envoie à une personne et qui sont emmagasinés dans le compte de cette personne[38] ? C'est à ce stade qu'entrent en jeu les notions de contrôle et d'accès, et qu'intervient l'analyse fondée sur le risque. Avant de porter notre attention sur cette analyse, annonçons d'emblée que la juge Bennett rejette cette approche fondée sur le risque, et soutient que le juge de première instance a accordé trop importance aux facteurs d'accès et de contrôle. Précisons aussi que le dernier facteur de l'analyse de la juge Bennett, soit la nature du contenu des messages saisis, lui aura permis de déterminer qu'il s'agissait de messages relevant du cœur biographique de l'individu. L'analyse de l'ensemble des circonstances menée par la juge Bennett l'amène à conclure que l'appelant peut revendiquer une attente raisonnable en matière de vie privée à l'égard du contenu des messages. Par conséquent, l'appelant est en mesure de contester la validité du mandat de fouille. Comme le mandat fut qualifié par la juge Bennett d'invalide, la fouille doit être qualifiée d'abusive et contraire à l'article 8 de la *Charte canadienne*. Toutefois, la juge n'a pas écarté les éléments de preuve que la fouille a permis de découvrir, soit les messages textes, et la déclaration de culpabilité prononcée en première instance fut maintenue.

36. *Craig*, *supra* note 35, au para 103.
37. *Ibid*, au para 104.
38. *Ibid*, au para 105.

3.2.3 La validité de l'analyse fondée sur le risque

Tel que mentionné plus haut, l'analyse fondée sur le risque affirme que l'un des facteurs qui doivent être pris en considération dans l'analyse de l'ensemble des circonstances est le risque qu'une personne court en divulguant des renseignements à quelqu'un et que cette personne partage lesdits renseignements avec d'autres personnes. En d'autres mots, il faudrait, en l'espèce, prendre en considération le risque conscient que prend une personne en envoyant un message texte que le destinataire partage ce message avec d'autres personnes. Ce risque encouru, cette « perte de contrôle » volontaire sur le contenu du message amoindrirait, voire même détruirait, l'attente raisonnable prétendue à l'égard dudit message. Ainsi, le facteur du contrôle, dans le contexte des affaires *Craig* et *Marakah*, et l'idée selon laquelle les deux appelants devaient savoir qu'ils couraient le risque que les messages envoyés soient partagés par leurs destinataires représenterait une réintroduction de l'analyse fondée sur le risque. Réintroduction parce que, dans *Duarte* et *Wong*, la Cour suprême du Canada avait critiqué de manière véhémente et rejeté cette analyse fondée sur le risque.

Dans *Duarte*, une décision portant sur l'écoute électronique et l'interception de communications privées, le juge La Forest avait établi une distinction claire entre le risque que la personne avec qui on communique divulgue le contenu de nos conversations à d'autres personnes, et le risque que l'État puisse saisir ou enregistrer ces conversations. Bien qu'il soit vrai qu'il existe une possibilité réelle que notre interlocuteur partage avec d'autres le contenu de la conversation que l'on a tenue avec lui, cette possibilité ne devrait pas servir de motif pour justifier l'écoute ou l'interception de ces communications par des représentants de l'État. Une société où les individus doivent se méfier de ce qu'ils disent aux autres de peur que leurs propos soient saisis par l'État ne peut être qualifiée de libre et démocratique. Selon le juge La Forest :

> Une société nous exposant, au gré de l'État, au risque qu'un enregistrement électronique permanent soit fait de nos propos chaque fois que nous ouvrons la bouche, disposerait peut-être d'excellents moyens de combattre le crime, mais serait une société où la notion de vie privée serait vide de sens.[39]

Dans le même ordre d'idée, la juge Bennett affirme dans *Craig* que :

39. *R* c *Duarte*, [1990] 1 RCS 30, à la p 44.

> In my view, this reasoning applies to the search of private online messages, recognizing that a permanent recording is, with certain exceptions, more insidious than sharing private email. […] The real risk to be concerned with is not that the other user in the "chat" will divulge it to the police. It is that the police can sift through the recipients' copy of private digital communications without the sender having the ability to challenge the search.[40]

La notion de risque ici évoquée se rapproche de la notion de contrôle. Lorsque l'on envoie un message, en d'autres mots, que l'on abandonne le contrôle que l'on peut exercer sur son contenu, on doit être conscient des risques que ce message se retrouve dans les mains d'autres personnes que son destinataire. Ce risque et cette perte de contrôle anéantiraient l'attente raisonnable que l'on peut revendiquer à l'égard dudit message. Par conséquent, les policiers pourraient s'en saisir sans que le rédacteur du message puisse revendiquer une attente raisonnable à son égard et donc bénéficier de la protection de l'article 8 de la *Charte canadienne*. À la lumière de ce raisonnement, fautif selon la juge Bennett, on comprend mieux les motifs à la fois du juge de première instance dans *Craig*, et ceux des juges de première instance et de la Cour d'appel dans *Marakah*. En effet, si, dans *Marakah*, le juge MacPherson insistait sur l'importance des facteurs que sont le contrôle et l'accès dans l'analyse de l'ensemble des circonstances, il se devait aussi de défendre cette analyse fondée sur le risque. L'appelant Marakah, dénonçant cette approche adoptée en première instance, fut donc débouté, sur ce point, par le juge MacPherson.

L'argument du juge de première instance, que validera le juge MacPherson, est articulé en fonction d'une différence de nature entre le risque dont il question dans *Duarte* et le risque dont il est question dans *Marakah*. Selon les juges, le risque dans *Duarte* porte sur l'interception de communications orales, et le risque dans *Marakah* porte sur le risque de fouille et de saisie de communications écrites et numériques. La différence tiendrait au fait que, dans le premier cas, les policiers créeraient un enregistrement permanent d'une conversation, un enregistrement qui n'existerait pas sans l'intervention des policiers, alors que dans le deuxième cas, il n'y a pas de création d'enregistrement ou de transformation de la conversation ; le message est déjà sur un support permanent et numérique. Ainsi, avec les messages textes, « the appelant himself chose to communicate by text message, using a medium that necessarily creates a permanent

40. *Craig*, *supra* note 35, au para 110.

record over which he had no control […] The risk in this case is of a different order than that in *Duarte*. »[41].

Cette distinction ne fut pas acceptée par le juge LaForme, dissident dans *Marakah*. Dans une opinion qui s'apparente à celle de la juge Bennett dans *Craig*, le juge LaForme dénonce l'approche de la Couronne endossée par le juge MacPherson. Dans un passage qu'il convient ici de reproduire en entier, le juge soutient que :

> The only difference between the text messages at issue here and the conversations at issue in *Duarte* is that in *Duarte* the state was creating records of the conversations whereas in this case the state is obtaining records created by the transmission process of text messaging.
>
> That distinction, in my view, is not enough to make *Duarte* inapplicable. In particular, I note that it makes no meaningful difference to the privacy interests implicated or the dynamics at issue. In both scenarios an individual is sharing potentially private information with another person and not with the general public or the state, the person revealing the information is abandoning control over the information by expressing it and no longer keeping it to herself, and the person sharing the information assumes the risk that the recipient may breach their confidence.[42]

Selon le juge LaForme, l'analyse par le risque doit être écartée, et la notion de contrôle ne devrait pas guider l'analyse de l'ensemble des circonstances. Le juge aurait donc attribué à l'appelant la capacité de remettre en question la validité de la fouille du téléphone de son complice. Qui plus est, s'appuyant sur *R* c *Fearon*, [2014] 3 RCS 621, qui porte sur les fouilles accessoires à une arrestation d'objets connectés, le juge aurait déclaré la fouille illégale. Il aurait également écarté les éléments de preuve.

3.3 L'importance des affaires *Craig* et *Marakah*

Les affaires *Craig* et *Marakah* posent des questions fondamentales à une époque où la grande partie de nos conversations se font par écrit sur format numérique. Devrait-on être en mesure de revendiquer une attente raisonnable en matière de vie privée à l'égard de messages que l'on envoie ? Perd-on toute attente raisonnable à l'endroit du contenu d'un message à partir du moment où l'on appuie

41. *Marakah*, *supra* note 31, au para 82.
42. *Ibid*, aux para 152 et 153.

sur « envoyer » ? Quels sont les dangers associés à une réintroduction de l'analyse fondée sur le risque au temps du numérique ? Il s'agit là de questions dont les réponses vont, à mon avis, tracer les grandes lignes de contour du droit à la vie privée informationnelle au Canada dans les années à venir. Je dis « vont définir » parce que les réponses apportées par les Cours d'appel de l'Ontario et de la Colombie-Britannique ne sont pas définitives. En effet, l'affaire *Marakah* fut portée devant la Cour suprême du Canada, et l'audience a eu lieu le 23 mars 2017. Il y a fort à parier qu'il s'agit d'une décision qui fera couler encore beaucoup d'encre. Un dossier important à suivre pour l'année 2017.

4. LA TECHNIQUE D'ENQUÊTE QUE REPRÉSENTE LE TOWER DUMP : *R* V *ROGERS COMMUNICATIONS*, 2016 ONSC 70

L'intérêt de l'affaire *Rogers* réside dans le fait qu'il s'agit, à ma connaissance, de la première fois qu'un juge canadien élabore des lignes directrices visant l'encadrement de la technique d'enquête policière que représente le *tower dump*. Cette technique, particulièrement attentatoire à la vie privée, consiste à obtenir une ordonnance de production de tous les renseignements portant sur le trafic d'appels téléphoniques traité par une tour de transmission donnée pour une période de temps déterminée. Ces renseignements comprennent les noms et adresses des abonnés au service de téléphonie, mais aussi des données comme le nom de la personne avec qui ils communiquèrent, leur géolocalisation, la durée des appels et, dans certains cas, le numéro de carte de crédit des abonnées. Comme le mentionne le juge Sproat, chaque année les renseignements personnels de milliers, sinon de millions d'usagers sont ainsi divulgués aux services de police[43].

Ces *tower dumps* sont utilisés par les agents de police afin d'identifier des criminels ayant potentiellement utilisé leur téléphone cellulaire pendant la perpétration de leurs crimes. Les agents peuvent croiser les données obtenues auprès des fournisseurs de télécommunication, en particulier l'emplacement géographique des personnes, avec d'autres données d'enquêtes, comme le ou les lieux où des infractions furent commises[44]. On aura compris qu'en obtenant l'ensemble des renseignements portant sur les communications ayant transité par une tour de télécommunication donnée, les policiers obtiennent une foule conséquente d'informations portant sur des personnes n'ayant

43. *R* v *Rogers Communications*, 2016 ONSC 70 au para 1 [*Rogers*].
44. Pour plus de détails sur le fonctionnement des *tower dumps* voir *Rogers*, *supra* note 43, aux para 4, 13-17.

rien à se reprocher[45]. C'est sur ce point que se concentrera le juge Sproat dans ses motifs.

4.1 Les faits de l'affaire *Rogers*

En avril 2011, dans le cadre d'une enquête sur une série de vols de bijoux, la *Peel Regional Police* a obtenu, en vertu de l'article 487.012 du *Code criminel*[46], une ordonnance demandant aux compagnies Rogers et Telus de produire des documents comprenant des informations portant sur tous les téléphones en activité et émettant ou recevant des données à partir d'un certain nombre de tours de télécommunication. L'ordonnance exigeait la production des noms, adresses et renseignements financiers des abonnés. Pour répondre aux demandes de production, la compagnie Telus estime qu'elle devra divulguer les renseignements de 9 000 individus. La compagnie Rogers, pour sa part, estime qu'elle devra conduire 378 recherches dans ses banques de données et produire 200 000 documents touchant plus de 34 000 abonnés. Les compagnies affirment aussi que, chaque année, elles doivent répondre à un nombre important de telles demandes des services de police. En 2013, Telus aurait reçu pas moins de 2 500 ordonnances de production. Toujours en 2013, Rogers aurait répondu à 13 800 demandes… Devant le nombre croissant de demandes, les deux compagnies ont saisi les tribunaux afin que ceux-ci établissent certaines lignes directrices clarifiant la manière dont les demandes de *tower dump* devaient être formulées. Elles ont fait valoir leurs obligations contractuelles en matière de protection de la vie privée de leurs abonnés, mais aussi le temps qu'elles doivent consacrer à la production des documents demandés.

4.2 La décision

La décision du juge Sproat se décline, pour nos fins, en trois temps. D'abord, on doit déterminer s'il existe une attente raisonnable en matière de vie privée à l'endroit des dossiers produits. Ensuite, on doit déterminer s'il y a eu violation de l'article 8 de la *Charte canadienne*. Finalement, on doit élaborer certaines lignes directrices que devront suivre les services de police dans la rédaction de demande d'ordonnance de production prenant la forme de *tower dumps*.

45. *Rogers*, *supra* note 43, au para 25.
46. L'article 487.012 du *Code criminel* fut remplacé par l'article 487.014 qui lui est presque identique.

4.2.1 L'attente raisonnable

Selon le juge, il ne fait aucun doute que les dossiers visés par les ordonnances de production jouissent d'une attente raisonnable en matière de vie privée. Les renseignements qu'ils contiennent peuvent comprendre des renseignements d'ordre biographique. Même si le contenu n'est pas révélé, les données de transmission, ou métadonnées, peuvent être particulièrement révélatrices. En effet, lorsque quelqu'un appelle un avocat spécialiste, ou une ligne de prévention du suicide, ou une clinique spécialisée, on peut déduire certaines informations sur son mode de vie et ses choix personnels. Il en va de même pour les données de géolocalisation : « [w]as the person at the Blue Jays game or at work? ».

De plus, l'argument selon lequel l'information ne se retrouve que dans les mains des services de police et que, par conséquent, elle ne sera pas divulguée au grand public n'est pas soutenable (ou suffisant). Évoquant le risque de piratage ou de divulgations accidentelles, le juge soutient que :

> One needs only read a daily newspaper to be aware of the fact that governments and large corporations […] are frequently "hacked" sculpting in confidential information being stolen and sometimes posted online. I appreciate that cell phone data is not right up there with Wikileaks and Ashley Madison in terms of information likely to be hacked and published. It remains that it is information Canadians certainly regard as private. The law supports this conclusion.[47]

Ce passage est pertinent pour deux raisons. D'abord, il évoque la prise en charge par les tribunaux du risque réel que représente le pirate informatique ou le *hacking*. On ne peut s'empêcher, ici, de faire le lien avec l'affaire *Ashley Madison*, par ailleurs ciblée par le juge Sproat, et que j'ai présentée plus haut dans cet article. Ensuite, il est intéressant de comparer la conclusion du juge à celle à laquelle en est arrivé le juge MacPherson dans *Marakah*, aussi analysée plus haut. Dans *Marakah*, le juge MacPherson avait conclu qu'une personne ne pouvait revendiquer d'attente raisonnable à l'égard d'un message texte se trouvant sur le téléphone du destinataire. Son raisonnement s'appuyait principalement sur le fait que la personne ne possédait pas ledit téléphone, qu'elle n'y avait pas accès, et qu'elle ne contrôlait pas le message. Ces mêmes composantes sont présentes ici. Les données ne sont pas accessibles à l'abonné, il ne contrôle pas les serveurs,

47. *Rogers*, *supra* note 43, au para 25.

et n'a pas accès à ceux-ci. De plus, il a volontairement divulgué ses renseignements personnels aux compagnies. Devrait-on conclure que le *risque* que ceux-ci soient divulgués à d'autres diminue ou anéantit l'attente raisonnable dont peuvent faire l'objet ces renseignements ? Il est vrai que les faits des deux affaires sont différents, et que dans *Rogers*, les informations ne sont pas intentionnellement générées par l'abonné, mais la comparaison semble à tout le moins intéressante.

4.2.2 Est-ce que les ordonnances sont contraires à l'article 8 de la Charte canadienne *?*

Un des principes phares de l'article 8 de la *Charte canadienne* est le principe de l'atteinte minimum. Le principe de l'atteinte minimum dicte que, lorsque l'État et ses représentants portent atteinte au droit à la vie privée garanti par l'article 8 de la *Charte*, cette atteinte doit être la plus petite possible. S'il est possible d'atteindre les buts visés par l'action étatique en portant moins atteinte au droit à la vie privée des personnes, l'action de l'État sera qualifiée d'abusive et contraire à la *Charte canadienne*. Ici, il ne fait aucun doute pour le juge Sproat que les ordonnances de *tower dump* sont abusives parce qu'elles exigent la production d'une somme exagérée de renseignements personnels. Tel que mentionné en introduction de cette partie, les renseignements portant sur *toutes* les communications ayant transigé par une tour de télécommunication donnée sont transmis. On demande le nom, l'adresse, les métadonnées de transmission, mais aussi les renseignements financiers des abonnées qui, aux dires du juge, ne sont pas particulièrement utiles pour localiser une personne[48]. En d'autres mots, bien trop d'information sur bien trop de personnes est produite. Pour respecter l'article 8 de la *Charte*, ces ordonnances devraient être rédigées de manière à mieux cibler les personnes et les informations pertinentes.

4.2.3 Les lignes directrices

Il ne me semble pas pertinent, pour les fins de cette contribution, de décrire chacune des sept lignes directrices tracées par le juge Sproat. Il suffit de mentionner que ces lignes sont élaborées pour aider les policiers à rédiger des demandes d'ordonnance qui respectent les valeurs de la *Charte canadienne*. À mon sens, les lignes directrices visent deux objectifs. D'abord, on demande aux policiers d'*expliquer* pourquoi les renseignements demandés sont nécessaires, et pourquoi ils visent certaines tours de transmission et certains moments dans

48. *Ibid*, aux para 42-43.

le temps précis. On veut que les policiers démontrent qu'il existe des motifs probables de croire que les renseignements recueillis permettront de collecter des éléments de preuve pour le crime sur lequel on enquête. Ensuite, on demande aux policiers de mieux *cibler* les renseignements considérés comme pertinents. On revient en quelque sorte à la notion d'explication. Est-ce que les numéros de carte de crédit sont nécessaires ? Pourquoi ? Est-ce que les renseignements de tous les abonnés sont utiles ? Pourquoi ? Serait-il possible de mieux circonscrire les paramètres de la recherche à effectuer, c'est-à-dire en précisant aux compagnies de télécommunication que l'on cherche des renseignements sur les abonnées qui étaient à une location précise à un moment donné et à une autre location précise à un autre moment donné ?

Le respect des lignes directrices du juge Sproat entraîne, selon moi, trois bénéfices. Dans un premier temps, on diminue le risque d'atteinte à la vie privée des personnes et on limite la divulgation inutile de renseignements personnels. Il importe de mentionner, toutefois, qu'en dépit de ces limites, les renseignements personnels de personnes qui n'ont rien à se reprocher seront tout de même divulgués à la police. Il y en aura certes moins de divulgation inutile et non consentie, mais il y en aura quand même. Dans un deuxième temps, on impose un fardeau moins lourd aux services de télécommunication en matière de production de documents. Dans un troisième temps, les policiers se retrouveront avec une quantité moindre de renseignements personnels, mais avec des renseignements de meilleure qualité. Ainsi, le temps de traitement des données par la police devrait prendre moins de temps et être plus efficace.

4.3 L'importance de la décision *Rogers*

La décision rendue par la Cour supérieure de justice de l'Ontario dans *Rogers* est importante parce qu'elle vient baliser une technique d'enquête policière qui, à mon avis, était, depuis trop longtemps déjà, excessivement attentatoire à la vie privée des citoyens et citoyennes canadiens. Les *tower dumps* sont un exemple flagrant de non-respect de principes phares du droit à la vie privée : le principe d'atteinte minimum, mais aussi de la limitation de la collecte aux renseignements qui seront *nécessaires* aux objectifs visés par celle-ci. Bien que les lignes directrices du juge Sproat ne soient pas contraignantes, elles amènent des balises qui, si elles sont respectées, pourront augmenter de manière significative le degré de protection de la vie privée informationnelle des Canadiens et des Canadiennes.

Reste à voir si ces lignes directrices seront respectées. Un autre dossier à suivre pour les années à venir.

5. *C.L.* c *BCF AVOCATS D'AFFAIRES*, 2016 QCCAI 114

L'affaire *BCF Avocats* touche à une thématique particulièrement actuelle : la thématique du droit à l'oubli. Au Canada, le droit à l'oubli suscite de nombreuses questions. À quoi renvoie ce droit ? Comment le définit-on ? Est-ce que le terme « oubli » est bien choisi ? Est-ce possible, voire souhaitable, d'élaborer un droit à l'oubli canadien ?

Les événements qui ont propulsé ces questionnements sont la décision rendue par la Cour de justice de l'Union européenne dans *Google Spain SL* c *Agencia Española de Protección de Datos (AEPD)*[49] et l'adoption, en 2016, d'un Règlement européen en matière de protection des données personnelles[50] qui codifie ce fameux droit à l'oubli. Il est important de préciser que, bien que l'article 16 du Règlement européen évoque le terme de droit à l'oubli, il cristallise en fait un *droit à l'effacement*. L'objet de ce texte n'est pas de définir le droit à l'effacement ou d'en fixer les limites. Mon objectif est plutôt de montrer que la problématique qu'incarne le droit à l'effacement est présente au Québec et au Canada. Pour le moment, acceptons simplement, en nous appuyant sur l'article 17 du Règlement européen, que le droit à l'effacement renvoie à l'idée selon laquelle une personne peut, *en certains cas*[51], demander à ce qu'une personne qui traite des renseignements dont il est la source efface ces renseignements. Le droit au *déréférencement*, qui peut être considéré comme une composante du droit à l'oubli, mais qui se distingue du droit à l'effacement, est ici aussi pertinent. Ce droit permet « de demander à un moteur de recherche de supprimer certains résultats de recherche associés à vos noms et prénoms »[52]. Toutefois, il convient de préciser que l'information ne sera pas supprimée du site Internet source. Le site n'apparaîtra simplement plus dans les résultats de recherches menées à l'aide du nom et du prénom d'une personne sur un moteur de recherche donné.

---

49. ECLI:EU:C:2014:317.
50. Règlement (UE) 2016/679 du parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)
51. Voir, par exemple, l'article 17.1. du Règlement (UE) 2016/679.
52. Site Internet de la Commission nationale de l'informatique et des libertés (CNIL), en ligne : <https://www.cnil.fr/fr/droit-au-dereferencement>.

5.1 Les faits de l'affaire *BCF Avocats*

Les faits de l'affaire *BCF Avocats* sont relativement simples. La demanderesse était adjointe juridique à l'emploi de BCF jusqu'en juillet 2013. À la suite de son départ, les renseignements personnels de la demanderesse qui apparaissaient sur le site Internet de BCF furent effacés. Toutefois, la recherche du nom de la demanderesse sur certains moteurs de recherche amène encore à la page Internet du bureau d'avocat. Selon la demanderesse, cet état de fait représente un problème pour elle. En effet, à son départ du bureau, on lui a fait comprendre qu'elle n'obtiendrait pas de bonnes références de BCF. Elle a par conséquent retiré cette ligne de son curriculum vitae. Toutefois, les employeurs potentiels, selon elle, font des recherches Internet et arrivent au résultat qu'elle aurait travaillé pour BCF. Cette discontinuité entraverait sa capacité à trouver un nouvel emploi. Elle demande donc que son ancien employeur retire complètement toutes les informations la concernant de son site Internet.

5.2 La décision

La preuve démontre qu'il n'y a plus de renseignements sur la demanderesse dans les serveurs ou sur le site Internet de BCF. Le problème, ici, se présente sur le plan du *référencement* sur les moteurs de recherche. Deux cas précis se présentent. D'abord, la recherche sur Google amène directement au site de BCF, même si ledit site ne contient pas d'information sur la demanderesse. Ensuite, la recherche sur Wayback Machine, un moteur qui « conserve des captures d'écran de site Web à différents moments dans le temps »[53], amène au site Internet de BCF tel qu'il existait à l'époque où la demanderesse y travaillait. Ses renseignements personnels se trouvent donc sur cette page.

Au Québec, le droit à la rectification – duquel on peut par ailleurs déduire une certaine forme de droit à l'effacement – est consacré par l'article 40 du *Code civil du Québec*, qui prévoit que :

> Toute personne peut faire corriger, dans un dossier qui la concerne, des renseignements inexacts, incomplets ou équivoques ; *elle peut aussi faire supprimer un renseignement périmé ou non justifié par l'objet du dossier*, ou formuler par écrit des commentaires et les verser au dossier. (Les italiques sont nôtres)

53. *C.L.* c *BCF Avocats d'affaires*, 2016 QCCAI 114, au para 58 [*BCF Avocats*].

La question qui se pose en l'espèce est de déterminer si BCF a respecté ce droit. En d'autres mots, a-t-elle bel et bien supprimé lesdits renseignements ? Selon la Commission d'accès à l'information du Québec, BCF s'est bel et bien acquitté de son obligation. Tel que mentionné plus haut, la preuve démontre que tous les renseignements sur la demanderesse furent supprimés du site de BCF. Le problème se situe sur le plan de l'indexation sur les moteurs de recherche, c'est-à-dire du lien de référencement que tissent ces moteurs entre le site de BCF et le nom de la demanderesse. Cette indexation est hors du contrôle de BCF. On arrive ici à une autre dimension du droit à l'oubli, que l'on nomme le droit au *déréférencement*. Et c'est particulièrement sur cette problématique que portait la décision rendue par la Cour de justice de l'Union européenne dans *Google Spain SL*. Peut-on ordonner à Google, ou à un autre moteur de recherche de déréférencer un nom et un site Internet ? Évidemment, Google déréférence souvent des sites, mais dans la plupart des cas, il le fait de son propre chef. Il ne s'agit pas, en d'autres mots, d'une ordonnance. La validité d'une telle ordonnance est, au Canada, une question encore en suspens. Quoi qu'il en soit, la Commission précise que le droit à la rectification que l'on trouve au Québec « n'est pas de l'ordre du « droit à l'oubli » qui vise à effacer des informations des espaces publics. D'ailleurs, il n'est pas certain que ce droit, reconnu en Europe, trouve application au Québec. »[54].

5.3 L'importance de la décision *BCF Avocats*

L'importance de la décision *BCF Avocats* réside dans le simple fait qu'elle met en lumière certaines des problématiques reliées à l'application du droit à l'oubli, dans ses volets d'effacement ou de déréférencement, au Canada. À cet effet, il convient de préciser que la question du référencement fait et continuera de faire l'objet d'un traitement par certaines des plus hautes instances judiciaires canadiennes. Mentionnons, par exemple, la récente décision de la Cour fédérale dans *A.T.* v *Globe24h.com*, 2017 FC 114, et la très attendue décision de la Cour suprême du Canada dans l'affaire *Equustek Solutions Inc* v *Google Inc*, une affaire portant sur la question du déréférencement qui fut entendue par la Cour en décembre 2016. Un dossier très important à suivre pour 2017.

54. *Ibid*, au para 65.

CONCLUSION

En conclusion, j'ai souhaité identifier trois grands thèmes qui traversent plusieurs des décisions présentées dans cet article. Ces thèmes touchent à certains des enjeux actuels les plus importants en matière de protection de la vie privée informationnelle. Ils nous permettent aussi d'avoir un portrait plus général du paysage juridique canadien et de situer les décisions présentées dans un contexte plus large. La première thématique que j'ai identifiée est celle relative aux risques associés au partage de renseignements personnels et aux divulgations non consenties de renseignements personnels.

La seconde est celle relative aux limites que viennent poser les tribunaux canadiens aux pouvoirs policiers en matière de collecte de renseignements personnels à l'ère du numérique. La troisième et dernière thématique que j'aimerais aborder est celle relative au caractère permanent des traces numériques et aux limites de l'oubli.

1. Les risques du partage de données personnelles

Je crois qu'une des choses les plus importantes que l'ensemble des décisions met en lumière est la notion de risque associé au partage de renseignements personnels. Plus précisément, je pense ici aux risques associés au fait que la personne ou l'entreprise à laquelle on confie nos données puisse, elle aussi, les partager avec d'autres personnes, et ce, sans notre consentement. Cette divulgation non consentie peut à la fois être intentionnelle ou involontaire, permise ou interdite par la loi. Quatre des décisions analysées dans cet article impliquent, sous une forme ou une autre, une divulgation non consentie de renseignements personnels. Dans *Ashley Madison*, il s'agit d'une divulgation non consentie involontaire, puisque résultant d'un piratage informatique. Toutefois, même involontaire, cette divulgation fut considérée par le Commissaire à la protection de la vie privée comme résultant, en partie, de manquement au respect des obligations relatives à la sécurisation des données personnelles qu'impose à *Avid Life Media Inc.* la LPRPDÉ. Dans *Doe 444533*, il s'agit d'une divulgation non consentie, intentionnelle et illégale d'une vidéo intime par un ancien compagnon. Dans *Rogers*, il s'agit d'une divulgation non consentie, intentionnelle et légale de renseignements personnels des abonnées par les compagnies de télécommunication. Dans *Marakah* et *Craig*, il y a aussi, dans une certaine mesure, divulgation non consentie de renseignements personnels. Dans *Marakah*, on pourrait dire qu'il s'agit d'une divulgation non consentie, involontaire, mais considérée légale par la Cour d'appel de l'Ontario, et dans *Craig* il

s'agit d'une divulgation non consentie, intentionnelle, mais illégale selon la Cour d'appel de la Colombie-Britannique.

Dans tous ces cas, que l'on considère la divulgation comme étant légale ou non, intentionnelle ou non, il n'en demeure pas moins qu'il s'agit d'une divulgation non consentie. De surcroît, dans *Ashley Madison*, dans *Craig*, dans *Marakah* et, surtout, dans *Doe 464533*, la divulgation aura eu des effets délétères sur la personne qui est à la source des renseignements. La chose à retenir, à mon avis, est qu'il y a souvent, pour ne pas dire toujours, des risques associés au partage de nos renseignements personnels les plus sensibles. Même si la personne ou l'entreprise à qui on confie ces renseignements n'a pas le droit de les divulguer sans notre consentement, rien ne garantit qu'il n'y aura pas de divulgation. Ceci étant dit, il me semble particulièrement important de mentionner que ce risque, bien qu'il doit être pris en compte par la personne qui divulgue ses renseignements personnels, ne devrait pas être retourné contre elle par la justice. Ce que je veux dire, c'est que l'omniprésence de ce risque ne devrait pas être utilisé par le droit pour justifier des atteintes à la vie privée de la personne. Ce n'est pas parce que ce risque est présent que l'on doit déduire qu'il ne peut y avoir une attente raisonnable réduite à l'égard des renseignements personnels que l'on partage avec les autres. À une époque où le risque de divulgation non consentie est omniprésent – et je crois que les décisions que j'ai choisies illustrent bien cette idée – cette déduction reviendrait à dire qu'aux yeux du droit canadien, on ne peut revendiquer d'attente raisonnable en matière de vie privée à l'égard de presque aucun renseignement. C'est en ce sens que l'analyse fondée sur le risque adoptée par la Cour d'appel de l'Ontario dans *Marakah* me semble particulièrement dangereuse aujourd'hui. On peut, par exemple, se demander quelle aurait été l'issue de l'affaire *Doe 464533* si le raisonnement du juge Stinson avait été guidé par une analyse fondée sur le risque…

2. La limitation des pouvoirs policiers à l'ère du numérique

Dans un deuxième temps, je crois que certaines des décisions choisies mettent en lumière une des tâches principales du droit à l'ère de la donnée numérique : redéfinir les limites du pouvoir policier en matière de surveillance et collecte de renseignements personnels. Je crois que cette redéfinition est inévitable et nécessaire. Le numérique aura profondément transformé la capacité de l'État à s'immiscer dans la vie privée des personnes. Il aura permis l'émergence de nouvelles formes de données, comme les messages textes des arrêts *Craig* et *Marakah*, de même que de nouvelles formes de surveillance ou de collecte de données, comme les *data dumps* de l'arrêt *Rogers*.

Au cours des dernières années, les tribunaux canadiens furent à maintes reprises invités à fixer les limites du pouvoir policier à l'ère des technologies de l'information. Dans *R* c *Vu*, [2013] 3 RCS 657, il fallait déterminer si un mandat de perquisition d'une résidence privée permettait la fouille des ordinateurs qui se trouvaient à l'intérieur de ladite résidence. Dans *R* c *Fearon*, [2014] 3 RCS 621, on se demandait si le pouvoir de fouille accessoire à une arrestation s'étendait à la fouille d'un téléphone portable trouvé sur l'accusé. Dans *R* c *Spencer*, [2014] 2 RCS 212 on se demandait si la divulgation aux services de police de renseignements personnels rattachés à une adresse IP était permise par la LPRPDÉ. Dans l'arrêt *Telus*, la Cour suprême devait déterminer si un mandat d'interception de communication privée est nécessaire pour autoriser la communication prospective de messages textes. À cet effet, les arrêts *Marakah*, *Craig* et *Rogers* me semblent continuer le travail entamé il y a de cela déjà quelques années.

3. Le caractère permanent de la trace numérique et l'oubli

Un des derniers points que je souhaite soulever est le caractère « permanent » de la donnée numérique et la problématique particulièrement saillante que cette qualité pose en matière de protection de la vie privée. À cet effet, les affaires *Ashley Madison* et *Doe 464533* sont particulièrement probantes. La publication en ligne de données personnelles peut entraîner des chaînes quasi infinies de partages, de duplications, de téléversements, de téléchargements ou d'indexation qui peuvent anéantir toute forme de contrôle qu'une personne peut exercer sur les modalités de circulation desdits renseignements. Dans un tel contexte, la protection de la vie privée représente un exercice difficile et complexe. Comme le démontre malheureusement si bien l'arrêt *Doe 464533*, une divulgation non consentie peut entraîner une répétition d'atteintes à la vie privée, à la réputation ou à la dignité de la personne. C'est en ce sens que les notions d'oubli et d'effacement évoquées par l'arrêt *BCF Avocats* revêtent un intérêt particulier. Toutefois, les réalités du monde numérique nous permettent de poser d'importantes questions quant à la portée ou l'étendue de ces notions. L'effacement de la trace numérique est-il réellement possible ? Internet peut-il véritablement oublier ? Selon moi, un des défis principaux du droit sera de fournir des réponses à ces questions fondamentales.