Canadian Journal of Law and Technology

Volume 17 | Number 1 Article 1

6-1-2019

La saisie de données situées dans le nuage en droit criminel canadien

Laura Ellyson
PhD Candidate, Schulich School of Law, Dalhousie University

La saisie de données situées dans le *nuage* en droit criminel canadien

Laura Ellyson*

Résumé

L'article 8 de la Charte canadienne des droits et libertés prévoit que « chacun a droit à la protection contre les fouilles, les perquisitions ou les saisies abusives ». Cette disposition a fait couler beaucoup d'encre depuis son adoption, mais aussi plus récemment en raison de son application aux nouvelles technologies. En effet, dans les 20 dernières années, la Cour suprême du Canada a adapté les principes généraux découlant des fouilles, saisies et perquisitions aux réalités informatiques nouvelles, notamment l'ordinateur et le cellulaire.

Toutefois, l'émergence de nouvelles technologies est un phénomène qui ne cesse jamais. L'essor de l'infonuagique, ce modèle d'utilisation d'Internet qui permet l'accès à des services à distance, incluant notamment la sauvegarde de données sur des serveurs délocalisés, nous force à revoir la protection constitutionnelle qui peut être accordée aux données personnelles des individus. À travers l'étude des principes généraux applicables aux fouilles, saisies et perquisitions, nous expliquerons pourquoi les données délocalisées sauvegardées grâce à l'infonuagique peuvent être protégées par l'article 8 de la Charte. Nous analyserons également les différentes autorisations judiciaires permettant leur saisie, de même que certains autres principes connexes.

Abstract

Section 8 of the Canadian Charter of Rights and Freedoms provides that "everyone has the right to be secure against unreasonable search or seizure". This provision has been written about extensively since its adoption, but also more recently because of its application to new technologies. In fact, in the last 20 years, the Supreme Court of Canada has adapted the general principles arising from search and seizure law to new technological realities, including computers and cell phones.

However, the emergence of new technologies is a phenomenon that never stops. The rise of cloud computing, this model of Internet utilisation that allows access to remote services, including but not limited to data storage on delocalized servers, forces us to review the constitutional protection that can be granted to personal data. Through the study of the general principles applicable to search and seizure,

* L'auteure est candidate au doctorat à Dalhousie University, titulaire d'une maîtrise en droit de l'Université de Montréal et membre du Barreau du Québec. Elle coenseigne le cours *Cybercriminalité, enquête policière et droit*, à Polytechnique Montréal depuis 2016. Cet article est une version abrégée du troisième chapitre de son mémoire de maîtrise. L'auteure aimerait remercier particulièrement Professeurs Hugues Parent et Nicolas Vermeys pour leur aide dans la préparation de son mémoire.

we will explain why delocalized data saved using cloud computing can be protected under section 8 of the Charter. We will also analyze the various judicial authorizations available to obtain this data, as well as certain other related principles.

INTRODUCTION

« [. . .] nous devons toujours rester conscient du fait que les moyens modernes de surveillance électronique, s'ils ne sont pas contrôlés, sont susceptibles de supprimer toute vie privée ».[1]

L'article 8 de la *Charte canadienne des droits et libertés* (*Charte*) prévoit que « chacun a droit à la protection contre les fouilles, les perquisitions ou les saisies abusives ».[2] À travers les années d'existence de la *Charte*, cette disposition a été utilisée à maintes reprises afin d'examiner la légalité des intrusions de l'État dans la vie privée de ses citoyens dans le cadre d'enquêtes criminelles, qu'il s'agisse de perquisitions dans un domicile, de fouilles corporelles ou de saisie de documents. Par ailleurs, plus récemment, nous avons assisté à un réexamen de cette disposition, dans le cadre du développement de nouvelles technologies.

Dès 1990, la Cour suprême du Canada a commencé à se pencher sur le lien entre cette disposition et les nouvelles technologies utilisées par les policiers.[3] Toutefois, depuis 2010, nous assistons à une augmentation notable du nombre de décisions dans ce domaine, surtout en ce qui concerne les ordinateurs.[4] En effet, l'utilisation massive et répandue des ordinateurs a, en quelque sorte, enclenché cette étude de l'application de l'article 8 de la *Charte* aux nouvelles technologies. Il est maintenant rare qu'un individu ne possède aucun appareil électronique, qu'il s'agisse d'un ordinateur, d'une tablette, d'un téléphone intelligent ou encore d'une montre connectée. Tous ces appareils peuvent, le cas échéant, contenir des informations essentielles à une enquête criminelle.

Le recours croissant à l'Internet est également au cœur de ce débat. Peu de foyers canadiens sont maintenant hors ligne, c'est-à-dire qu'ils n'ont pas accès à l'Internet.[5] Ces considérations sont nécessairement au centre des enquêtes criminelles, que ce soient des enquêtes en matière de cybercriminalité[6] ou encore

---

1 *R* c *Wong*, [1990] 3 RCS 36 [*R c Wong*].

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

3 *R c Wong*, *supra* note 2; *R c Duarte*, [1990] 1 RCS 30.

4 Nous fixons le point de départ de cette vague à l'arrêt *R c Morelli*, [2010] 1 RCS 253.

5 Canadian Internet Registration Authority (CIRA), « Internet use in Canada » (2016), en ligne : *CIRA* <cira.ca/factbook/domain-industry-data-and-canadian-Internet-trends/internet-use-canada> (consulté le 20 octobre 2017).

6 L'étude approfondie de la cybercriminalité ne fait pas partie du cadre de cet article puisque la découverte de preuve électronique n'est pas pertinente uniquement dans les dossiers de cybercriminalité. Toutefois, cela sera bien souvent le cas, en raison de la

simplement des enquêtes où un élément de preuve peut se retrouver en format électronique.

La façon dont les Canadiens utilisent l'Internet et leurs ordinateurs est également en plein changement. En effet, de plus en plus de Canadiens utilisent des services d'infonuagique[7] (aussi connu sous le vocable anglophone de *cloud computing*[8]), c'est-à-dire qu'ils utilisent des services en ligne afin, notamment, de sauvegarder des données sur un serveur délocalisé, pouvant appartenant à un tiers, souvent une entreprise située à l'étranger. Les données ne se trouvent donc plus dans l'ordinateur du suspect ou de la personne sous enquête, mais bien sur un serveur qui peut être situé à n'importe quel endroit sur la planète. Ce serveur va souvent être désigné sous le vocable de *nuage* (ou *cloud* en anglais), puisque les données peuvent être accédées à partir de n'importe quel appareil électronique possédant une connexion Internet. Une importante proportion d'internautes utilise ce genre de service, parfois sans même le savoir.

Cette utilisation d'Internet soulève des questions importantes en matière de vie privée, mais également en matière d'enquêtes criminelles. En effet, il n'est pas intuitif de déterminer de quelle manière l'article 8 de la *Charte* s'applique à l'infonuagique et aux données situées sur le *nuage*. Par ailleurs, peu de décisions canadiennes en droit criminel ont été recensées à ce jour sur ce sujet, bien qu'il soit inévitable que des policiers se heurteront, tôt ou tard, à un problème d'accès au *nuage* d'un individu sous enquête, en raison de la prévalence de cette technologie. Par l'étude de la législation, de diverses décisions et de la doctrine, nous tenterons donc de déterminer comment le droit relatif aux fouilles, saisies et perquisitions peut s'adapter au *nuage* et aux données qui y sont sauvegardées.

---

nature même de ces infractions dites de cybercriminalité. Ainsi, il est utile de spécifier que la cybercriminalité inclut les crimes où l'ordinateur est l'objet même du crime (pensons ici aux infractions de méfait de données ou d'utilisation non-autorisée de services d'ordinateur, prévues au Code criminel, donc des infractions qui se déroule entièrement dans le monde virtuel, souvent désignées sous le vocal de piratage informatique), ou encore les crimes où l'ordinateur est l'outil du crime (des crimes où l'ordinateur facilite la commission de l'infraction ou encore des crimes traditionnels qui ont maintenant parfois une portée informatique). Voir par ex : Laura Ellyson et Annie Emond, « Cybercriminalité : développements jurisprudentiels et perquisitions informatiques » (2014) Repères, EYB2014REP1575.

7 Louis Columbus, « Roundup Of Cloud Computing Forecasts, 2017 » (2017), en ligne : Forbes < www.forbes.com/sites/louiscolumbus/2017/04/29/roundup-of-cloud-computing-forecasts-2017/#5d7958b731e8 > (consulté le 20 octobre 2017) [Columbus].

8 Office québécois de la langue française, « infonuagique », en ligne : < gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche = 26501384 > (consulté le 20 octobre 2017); Le terme anglophone *cloud computing* aurait été créé par Eric Schmidt, le PDG de l'entreprise Google, en 2006. Jacob M. Small, « Storing Documents in the Cloud: Toward an Evidentiary Privilege Protecting Papers and Effects Stored on the Internet », (2013) 23 Geo Mason U Civ Rts LJ 255 à la p 258.

SECTION 1 — PRINCIPES GÉNÉRAUX APPLICABLES À L'INFONUAGIQUE

La manière par laquelle nous sauvegardons nos données personnelles a connu de grands changements dans les dernières années. Auparavant, si un individu voulait enregistrer un fichier informatique quelconque, il devait le faire sur un support physique qui lui appartenait, comme une disquette, un CD, un DVD, une clé USB ou un disque dur. Depuis 2006, lorsque l'entreprise Amazon a commencé à offrir son service AWS,[9] cette réalité a bien changé.[10] Il est maintenant possible de sauvegarder nos données personnelles de manière délocalisée, c'est-à-dire sur des serveurs qui peuvent se trouver partout dans le monde, plutôt que dans nos propres appareils. Ce type de service—qui fait partir des diverses applications de l'infonuagique qui seront étudiées plus en détails ci-dessous—est de plus en plus populaire, notamment pour les entreprises.[11]

Avant de considérer plus amplement les impacts juridiques de l'infonuagique, nous allons d'abord examiner le fonctionnement de cette nouvelle technologie, ses différentes applications et les défis que son utilisation soulève pour les forces de l'ordre.

1.1 La définition de l'infonuagique et ses différentes utilisations

Selon le *National Institute of Standards and Technology*, une agence du Département du commerce américain :

> « Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. [. . .] »[12]

Le *nuage* est donc composé de ressources informatiques, accessibles par l'entremise d'un réseau, pouvant être employées pour plusieurs utilisations différentes, ou services différents. Certains auteurs accordent beaucoup d'importance à la distinction entre l'infonuagique (*cloud computing*) et les services offerts par l'entremise du *nuage* (*cloud services*).[13] Toutefois, dans le

---

9 AWS est un service d'infonuagique permettant notamment de sauvegarder des données à distance, sur un serveur appartenant à Amazon. Amazon, « What is AWS? - Amazon Web Services », en ligne : *Amazon Web Services* <aws.amazon.com/what-is-aws/> (consulté le 30 avril 2018).

10 L'infonuagique était appliquée avant cette date, mais le lancement du service d'Amazon nous permet de tracer une ligne à partir de laquelle l'utilisation de l'infonuagique a réellement pris de l'ampleur et où le terme a commencé à être plus répandu.

11 Backupify, « Bits & Bytes: A History of Data Storage », *Backupify,* en ligne : <www.backupify.com/history-of-data-storage/> (consulté le 30 avril 2018).

12 Peter Mell et Tim Grance, « The NIST Definition of Cloud Computing », en ligne : *Computer Security Resource Center* <csrc.nist.gov/publications/detail/sp/800-145/final> (consulté le 30 avril 2018).

cadre de saisies de nature criminelle, cette distinction est moins nécessaire.[14] Nous retiendrons donc que l'infonuagique se caractérise par le fait d'utiliser des applications et de sauvegarder des données sur un serveur distant, par l'entremise d'Internet, plutôt que sur nos propres appareils.[15] Les utilisateurs ne sont alors généralement pas propriétaires de la technologie qu'ils utilisent, mais plutôt locataires d'un espace virtuel fourni par une entreprise.[16] L'information ainsi sauvegardée sur le *nuage* peut être accédée à partir de n'importe quel appareil ayant une connexion Internet et les accès requis, à n'importe quel moment, à partir de n'importe quel endroit dans le monde.[17]

Il y a trois principaux modèles de services d'infonuagique[18] : le SaaS (*Software as a Service* ou « logiciel en tant que service »), le PaaS (*Platform as a Service* ou « plate-forme en tant que service ») et le IaaS (*Infrastructure as a Service* ou « infrastructure en tant que service »).[19] Le SaaS permet aux utilisateurs d'utiliser des applications à travers d'Internet, tel que des services de courriel en ligne.[20] Des exemples de ce modèle sont *Gmail* et *Hotmail*, de même que des logiciels de rédaction (*Office 365* et *Google Docs*), des logiciels de gestion des ventes (*Salesforce*) et des logiciels de gestion d'événements (*Planning Pod*).[21]

---

[13] Josiah Dykstra et Damien Riehl, « Forensic Collection of Electronic Evidence from Infrastructure-as-a-Service Cloud Computing » (2012) XIX-1 Rich JL & Tech 1-47 à la p 7 [Josiah Dykstra et Damien Riehl].

[14] Si le lecteur est particulièrement intéressé par le fonctionnement de l'infonuagique, ses différentes utilisations et modèles, nous l'invitons à consulter Nicolas Vermeys, Julie M. Gauthier et Sarit K. Mizrahi, « Étude sur les incidences juridiques de l'utilisation de l'infonuagique par le gouvernement du Québec », en ligne : < www.vermeys.com/publications/etude-sur-les-incidences-juridiques-de-lutilisation-de-linfonuagique-par-le-gouvernement-du-quebec/ > (consulté le 25 septembre 2018) [Nicolas Vermeys, Julie M. Gauthier et Sarit K. Mizrahi].

[15] William Jeremy Robison, « Free at What Cost?: Cloud Computing Privacy Under the Stored Communications Act » (2009) 98 Geo LJ 1195 à la p 1199; Matthew Nied, « Cloud Computing, the Internet, and the Charter Right to Privacy: The Effect of Terms of Service Agreements on Reasonable Expectations of Privacy » (2011) 69 Advocate 701 à la p 706 [Nied].

[16] Ilana R. Kattan, « Cloudy Privacy Protections: Why the Stored Communications Act Fails to Protect the Privacy of Communications Stored in the Cloud » (2011) 13 Van J Ent & Tech L 617 à la p 621.

[17] Laurie Buchan Serafino, « "I Know My Rights, So You Go'n Need A Warrant for That": The Fourth Amendment, Riley's Impact, And Warrantless Searches of Third-Party Clouds » (2014) 19 BJCL 154 à la p 161 [Buchan Serafino].

[18] D'autres modèles sont disponibles et utilisés par les entreprises, principalement dans le but de se distinguer de la compétition. Voir ex N. Vermeys, J. M. Gauthier et S. K. Mizrahi, *supra* note 15 à la p 43.

[19] David S. Barnhill, « Cloud Computing and Stored Communications: Another look at Quon v. Arch Wireless » (2010) 25 BTLJ aux pp 621-648 [Barnhill]; La traduction des termes est issue de Wikipedia, « Cloud computing », en ligne : *Wikipédia* < fr.wikipedia.org/w/index.php?title = Cloud_computing&oldid = 147706181 > (consulté le 30 avril 2018).

[20] Barnhill, *supra* note 20 à la p 639.

Le SaaS est également lié aux services de sauvegarde de données en ligne, tels que *Dropbox* ou *Microsoft OneDrive*.[22] L'utilisateur n'a pas le contrôle sur les applications utilisées et n'a pas à les télécharger ou à les tenir à jour; il ne fait qu'y accéder avec un nom d'utilisateur et un mot de passe.[23] Le SaaS est le type de *nuage* qui est le plus connu par les utilisateurs d'Internet,[24] ce qui le rendra souvent le plus pertinent dans une enquête criminelle. Par ailleurs, un auteur souligne que l'utilisation de ce type de service n'est pas sans risque puisque l'utilisateur ignore où se trouvent ses données, ce qui diminue son contrôle sur celles-ci.[25]

Le PaaS donne plus de possibilités aux usagers. Le fournisseur de ce type de service va créer une plateforme pour que les utilisateurs puissent créer leurs propres applications. Il va également fournir l'infrastructure de la plateforme, de sorte que les usagers n'aient pas à entretenir l'infrastructure (tels que les serveurs eux-mêmes ou encore le logiciel d'exploitation).[26] Il s'agit donc d'un modèle idéal pour les entreprises ou les particuliers qui développent des applications.[27] Ce modèle est facilement adaptable aux besoins grandissants d'une entreprise; il est facile d'augmenter la taille du *nuage* ou de modifier les paramètres de celui-ci au rythme de l'évolution de l'entreprise.[28] Toutefois, un risque est également présent puisque ce modèle cause une dépendance importante entre le client et le fournisseur de service. Ainsi, si le fournisseur décidait de changer ses paramètres ou s'il était contraint de fermer pour des motifs financiers, le client pourrait se trouver dans une situation fâcheuse.[29]

Finalement, avec le modèle IaaS, seule l'infrastructure est fournie. Le fournisseur de service s'occupe donc des installations physiques où se trouvent les serveurs, ainsi que l'accessibilité à ceux-ci.[30] L'utilisateur peut donc moduler comme bon lui semble l'infrastructure, en y installant tout ce qu'il désire.[31] Il s'agit surtout d'un modèle pertinent pour les entreprises.[32]

---

21 Gleb B., « Choosing the Right Cloud Service: IaaS, PaaS, or SaaS », en ligne : *Ruby Garage* < rubygarage.org/blog/iaas-vs-paas-vs-saas > (consulté le 30 avril 2018) [Gleb B.].

22 *Ibid.*

23 *Ibid.*

24 Barnhill, *supra* note 20 à la p 639.

25 Timothy D. Martin, « Hey! You! Get Off of My Cloud: Defining and Protecting the Metes and Bounds of Privacy, Security and Property in Cloud Computing », (2010) 92 JPTOS 283 à la p 289 [Martin].

26 Barnhill, *supra* note 20 aux pp 639-640.

27 Gleb B., *supra* note 22.

28 Martin, *supra* note 26 à la p 291.

29 *Ibid.*

30 Apprenda, « IaaS, PaaS, SaaS (Explained and Compared) », en ligne : *Apprenda* < apprenda.com/library/paas/iaas-paas-saas-explained-compared/ > (consulté le 30 avril 2018) [Apprenda].

31 Barnhill, *supra* note 20 à la p 640.

Bien qu'il soit possible pour une entreprise de créer ses propres installations d'infonuagique, évitant ainsi de passer par un fournisseur de service, cette façon de faire est assez rare considérant les ressources importantes nécessaires à un tel projet. En effet, l'entreprise serait alors responsable de l'entretien de l'infrastructure de son *nuage*, incluant le remplacement physique des serveurs, lorsque nécessaire.[33] Il existe toutefois une autre façon d'avoir un *nuage privé* (ou *private cloud* en anglais), sans avoir à investir dans l'infrastructure nécessaire à l'ouverture d'un centre de données privé. Certains fournisseurs de service d'infonuagique offrent la possibilité d'avoir un serveur dédié entièrement à un seul et unique client, créant donc l'équivalent d'un *nuage* qui serait situé sur les lieux d'affaires de l'entreprise.[34] Dans les deux cas, malgré des coûts plus importants, le *nuage privé* confère à l'entreprise une plus grande sécurité de ses données.[35]

Cependant, dans la majorité des cas, le *nuage* sera plutôt *public*, c'est-à-dire que l'infrastructure du *nuage* sera partagée par tous les utilisateurs, qui ne peuvent toutefois qu'accéder à leurs propres données.[36] Le *nuage public* a l'avantage d'être moins coûteux qu'un *nuage privé*, tout en fournissant une sécurité contre la perte de données puisque celles-ci peuvent être réparties sur plusieurs serveurs différents, plutôt que sur un seul.[37] Un service de *nuage hybride* peut également être utilisé, ce qui offre plus de possibilités aux entreprises choisissant cette option.[38]

1.2 La croissance de cette pratique dans le monde

Plusieurs avantages peuvent être reliés à l'infonuagique, expliquant sa croissance rapide. Tout d'abord, lorsqu'il est question de SaaS, l'un des avantages est que l'utilisateur n'a pas à télécharger ou mettre à jour ses applications, ce qui facilite l'utilisation et peut lui faire gagner du temps.[39] Par ailleurs, plusieurs applications utilisant les services d'infonuagique sont gratuites, facilement accessibles pour les usagers et permettent l'accès aux données à partir de n'importe quel appareil.[40] De plus, si l'appareil utilisé pour accéder au *nuage*

---

[32] Gleb B., *supra* note 22.

[33] John White, « Private vs. Public Cloud: What's the Difference? » (2014), en ligne : *Expedient* < www.expedient.com/blog/private-vs-public-cloud-whats-difference/ > (consulté le 30 avril 2018) [White].

[34] Microsoft, « Public Cloud vs Private Cloud vs Hybrid Cloud », en ligne : *Microsoft Azure* < azure.microsoft.com/en-gb/overview/what-are-private-public-hybrid-clouds/ > (consulté le 30 avril 2018) [Microsoft].

[35] White, *supra* note 34.

[36] Microsoft, *supra* note 35.

[37] *Ibid.*

[38] *Ibid.*

[39] Apprenda, *supra* note 31.

[40] Barnhill, *supra* note 20 à la p 641.

fait défaut, les données ne sont pas affectées et demeurent accessibles puisque celles-ci ne sont pas directement sur l'appareil, mais sur des serveurs distants.[41] En fait, les données sont habituellement situées sur plusieurs serveurs séparés, afin d'assurer l'accès aux données si un serveur faisait défaut.[42] La réduction des coûts de gestion est également un avantage important relié à l'utilisation de l'infonuagique pour les entreprises.[43] Le gouvernement américain, qui s'est doté d'une politique privilégiant l'utilisation du *nuage*,[44] reconnaît quatre avantages principaux reliés à l'utilisation du *nuage* :

> « (1) improving service delivery to internal and external customers; (2) introducing scalability, on demand provisioning, and resource pooling; (3) enhancing collaboration within each agency; and (4) replacing legacy IT infrastructure that is at the end of its lifespan. »[45]

De nombreux utilisateurs du *nuage* le font sans même le savoir.[46] En effet, l'interface de certains services fait en sorte que les usagers ne réalisent pas qu'ils utilisent l'infonuagique. On peut penser notamment à *Facebook* et à *LinkedIn*, deux sites de réseautage qui utilisent le *nuage* afin de sauvegarder les diverses informations qu'un usager partage sur sa page personnelle.[47]

L'infonuagique est théoriquement sans limites, au sens où tout ce qui peut être effectué de manière locale sur notre propre appareil peut également être exécuté de manière délocalisée sur le *nuage*.[48] Pour cette raison:

> « [. . .] users are switching to cloud computing because it provides the same traditional type of networking and file storage capacities for a fraction of the price. In fact, individuals and businesses alike are buying cheaper and less sophisticated machines because large hard drives are no longer necessary; users can stream programs such as word processing or online gaming, directly from the cloud ».[49]

---

41 IBM, « IaaS PaaS SaaS Cloud Service Models », en ligne : *IBM* < www.ibm.com/cloud/learn/iaas-paas-saas > (consulté le 30 avril 2018).

42 Sarit K. Mizrahi, « The Dangers of Sharing Cloud Storage: The Privacy Violations Suffered by Innocent Cloud Users during the Course of Criminal Investigations in Canada and the United States » (2017) 25 Tul J Intl & Comp L 303 à la p 308 [Mizrahi].

43 Barnhill, *supra* note 20 à la p. 641.

44 US Department of the Interior, « The Cloud First Strategy » (2017), en ligne : < www.doi.gov/cloud/strategy > (consulté le 10 mai 2018).

45 Dena G. McCorry, « With Cloud Technology, Who Owns Your Data? » (2014) 8 Fed Cts L Rev 125 à la p 130 [McCorry].

46 Quinn Hochhalter, « The Sky's the Limit: Twenty-First Century Searches of Hard-Drives, Smartphone Applications, & the Cloud » (2014) 90 NDL Rev 171 à la p 178 [Hochhalter].

47 McCorry, *supra* note 46 à la p 129.

48 Nicolette Lotrionte, « The Sky's the Limit - The Border Search Doctrine and Cloud Computing » (2013) 78 Brook L Rev 663 à la p 680 [Lotrionte].

49 Sara J. Khols, « Searching the Clouds - Why Law Enforcement Officials Need to Get

Statistiquement parlant, la croissance du *nuage* n'est plus à prouver. Depuis 2009, les dépenses liées à l'infonuagique ont augmenté 4.5 fois plus rapidement que les dépenses générales en technologies de l'information.[50] Le nombre d'utilisateurs de l'infonuagique serait passé de 2.4 milliards en 2013 à 3.6 milliards en 2018.[51] Selon l'*Institut de la statistique* du Québec, le nombre d'entreprises branchées qui utilisent l'infonuagique au Québec a cru de manière appréciable entre 2012 et 2016.[52]

1.3 Les défis posés par l'infonuagique pour les forces de l'ordre

Dans la culture populaire, on entend souvent que le *nuage* n'existe pas réellement, qu'il ne s'agit que de l'ordinateur de quelqu'un d'autre.[53] Cette particularité du *nuage* est justement ce qui cause tant de fil à retordre aux forces de l'ordre. En effet, auparavant, si les policiers cherchaient de l'information concernant un suspect en particulier, ils pouvaient s'attendre à ce que les données contenues dans son ordinateur personnel soient pertinentes. Or, maintenant, les données pertinentes à une enquête criminelle peuvent se trouver partout dans le monde, sur des serveurs n'appartenant pas à l'individu sous enquête.[54] La multiplication des endroits où les policiers sont susceptibles de trouver de l'information pertinente à leur enquête complique bien évidemment celle-ci.

Pour aggraver davantage la situation, il arrivera souvent que les policiers ignorent si un suspect utilise des services d'infonuagique. Ils pourront parfois le découvrir lors d'une saisie visant l'ordinateur du suspect, mais cela ne sera pas toujours le cas. Des experts en informatique devront donc effectuer des recherches approfondies, par exemple en demandant à plusieurs fournisseurs de service s'ils hébergent des données liées à une adresse IP particulière.[55] Certaines traces laissées sur les appareils électroniques des usagers du *nuage* peuvent également permettre de déterminer quel fournisseur de service Internet

---

Their Heads Out of the Cloud and Obtain a Warrant Before Accessing a Cloud Network Account » (2012) 4 Case W Res L Rev 169 à la p 173 [Khols].

50 Columbus, *supra* note 8.

51 Statista, « Consumer cloud computing user worldwide 2018 », en ligne : *Statista* < www.statista.com/statistics/321215/global-consumer-cloud-computing-users/ > (consulté le 9 mai 2018).

52 Institut de la statistique du Québec, « Part des entreprises branchées qui utilisent l'infonuagique, Québec, 2012 et 2016 », en ligne : < www.stat.gouv.qc.ca/statistiques/science-technologie-innovation/utilisation-internet/entreprises/utilisation-infonuagique.html > (consulté le 9 mai 2018).

53 « *There is no cloud, it's just someone else's computer*. » Auteur inconnu.

54 Daniel M. Scanlan, « Issues in digital evidence and privacy: Enhanced expectations of privacy and appellate lag times » (2012) 16 Can Crim L Rev 301 à la p 311 [Scanlan].

55 Le fournisseur de service serait effectivement en mesure de retracer l'adresse IP utilisée afin de se connecter à ses services. Josiah Dykstra et Damien Riehl, *supra* note 14 à la p 22.

(FSI) est utilisé par un individu et où se trouvent les données de l'individu sur le *nuage* de l'entreprise en question.[56]

Qui plus est, même une fois les données recueillies par les policiers, leur analyse est susceptible d'être plus compliquée que si les données avaient été trouvées sur l'ordinateur physique du suspect. En effet, « by their nature, cloud-computing environments are more complex than a single computer or a server ».[57] Ainsi, un technicien spécialisé en informatique devra vraisemblablement passer plus de temps à analyser les données obtenues, afin de trouver celles qui sont pertinentes à l'enquête.

Bref, la mobilité des données des individus pose problème pour les forces de l'ordre qui veulent trouver des éléments de preuve sur des appareils électroniques.[58] Par ailleurs, comme il sera étudié plus amplement à la section 4 du présent texte, la question de la juridiction applicable est également susceptible de compliquer le travail des policiers.

SECTION 2 — L'ATTENTE DE VIE PRIVÉE ENVERS LES DONNÉES SAUVEGARDÉES DANS LE *NUAGE*

L'existence même d'une attente raisonnable de vie privée concernant les données sauvegardées dans le *nuage* se pose. En effet, les données sauvegardées par l'entremise de services d'infonuagique sont souvent partagées avec un tiers et elles se situent dans un endroit où l'accusé n'a pas de contrôle, ce qui peut influencer l'attente de vie privée.[59] Ce débat est très important aux États-Unis où plusieurs auteurs s'opposent à l'application de la *third-party doctrine*, qui nie l'existence d'une attente raisonnable de vie privée dès que les informations sont partagées avec un tiers.

Dans cette section, nous traiterons premièrement de cette approche américaine qui nie l'existence d'une attente raisonnable de vie privée envers les données délocalisées, qui sont sous le contrôle d'un tiers. Ultimement, nous démontrerons pourquoi celle-ci ne peut s'appliquer au Canada. Ensuite, nous examinerons certains facteurs pertinents dans la détermination d'une attente de vie privée, qui sont spécifiques aux données situées dans le *nuage*. Finalement, nous exposerons les motifs permettant de conclure qu'une telle attente de vie privée existe et que les données délocalisées sont donc protégées par l'article 8 de la *Charte*.

2.1 L'approche américaine

La *third-party doctrine* a été établie par les tribunaux américains dans un contexte de fouilles, saisies et perquisitions traditionnelles, c'est-à-dire qui ne

---

56 Mizrahi, *supra* note 43 à la p 312.

57 Josiah Dykstra et Damien Riehl, *supra* note 14 à la p 38.

58 Kohls, *supra* note 50 à la p 169.

59 *R c Edwards*, [1996] 1 RCS 128 au para 45.

portent pas sur du matériel informatique.[60] Selon cette doctrine, dès qu'un individu divulgue de l'information à une tierce partie, cette information ne peut plus faire l'objet d'une attente raisonnable de vie privée.[61] Donc, lorsque le tiers remet cette information aux forces de l'ordre, il ne s'agit pas d'une fouille, au sens de la célèbre décision *Katz*.[62] Cette négation du droit à la protection contre les fouilles, perquisitions ou saisies abusives serait justifiée par le risque que ce tiers divulgue l'information recueillie.[63]

Plus récemment, cette doctrine a été utilisée par les tribunaux américains afin de nier l'existence d'une attente raisonnable de vie privée envers des données informatiques détenues par des entreprises, portant sur leurs clients.[64] L'application de cette théorie aux nouvelles technologies est toutefois vivement critiquée par certains auteurs américains, qui militent plutôt pour la reconnaissance d'une attente raisonnable de vie privée visant les données personnelles, et ce, peu importe leur emplacement géographique.[65] Selon ceux-ci, dans un contexte d'infonuagique, la *third-party doctrine* ne devrait pas permettre aux forces de l'ordre d'obtenir lesdites données sans l'obtention préalable d'une autorisation judiciaire appropriée, puisque le fournisseur de service ne fait qu'emmagasiner les données d'un tiers.[66] En ce sens, les fournisseurs de service ne sont que des « mere custodians of the data, [. . .] ensuring that data is neither lost nor damaged ».[67] Ainsi, tout comme une conversation téléphonique est protégée bien qu'elle ait lieu sur le réseau d'une entreprise, le contenu du *nuage* devrait être protégé.[68] Ce raisonnement est toutefois sujet aux conditions de service imposées par les FSI qui peuvent prévoir un accès et une utilisation des données par ces derniers, ce qui sera étudié plus en détail ci-dessous.

---

60 *United States v Miller*, 423 US 435 à la p 443 (1976); *Smith v Maryland*, 422 US 735 aux pp 743-44 (1979); *Hoffa v United States*, 385 US 293 (1966); *Couch* v. *United States*, 409 US 322 (1973).

61 Hochhalter, *supra* note 47 à la p 180.

62 *Katz v United States*, 389 US 347 (1967).

63 Buchan Serafino, *supra* note 18 à la p 156.

64 *Ibid* à la p 168 citant les décisions *United States v Skinner*, 690 F.3d 772; *United States v Lifshitz*, 369 F.3d 173; *United States v Rigmaiden*, No. CR 08-814-PHX-DGC, 2013 QL 1932800; *United States v Wilson*, No. 1:11-CR-53-TCB-ECS-3, 2012 WL 1129199; *United States v Madison*, No. 11-60285-CR, 2012 WL 3095357; *In re Application of United States for Historical Cell Site Data*, 724 F.3d 600 (5th Cir. 2013); *United States v Graham*, 846 F. Supp. 2d 384, 389 (D. Md. 2012); *In re Application of the U.S. for an Order Pursuant to 18 U.S.C. s. 2703*, 830 F. Supp. 2d 114, 133 (E.D. Va. 2011).

65 La position inverse semble effectivement minoritaire. À ce sujet, voir notamment Orin S. Kerr, « The Case for the Third-Party Doctrine » (2009) 107 Mich L Rev 561.

66 Buchan Serafino, *supra* note 18 à la p 171.

67 Aaron J. Gold, « Obscured by Clouds: The Fourth Amendment and Searching Cloud Storage Accounts Through Locally Installed Software » (2015) 56 Wm & Mary L Rev 2321 à la p 2341 [Gold].

68 Lotrionte, *supra* note 49 à la p 687.

Selon ces auteurs, cette doctrine devrait également être écartée pour le motif que le fournisseur de service d'infonuagique n'a pas à consulter les données de ses clients afin d'effectuer la sauvegarde; le processus s'effectuant plutôt de manière automatisée, par un système informatique. Ainsi, en l'absence d'intervention humaine, on ne peut affirmer que l'attente de vie privée des gens est diminuée ou anéantie.[69] Les données ne seraient donc pas réellement divulguées à une tierce partie.[70] Toutefois, il importe de rappeler qu'il a été révélé par Edwards Snowden que plusieurs FSI accédaient aux données de leurs client et les communiquaient au gouvernement américain dans le cadre du programme PRISM.[71] Ainsi, cet argument peut sembler utopiste ou peut-être naïf. Par ailleurs, le fait que les usagers n'aient plus réellement le choix de recourir à l'infonuagique—en raison de la prévalence de cette technologie et du caractère désuet de ses alternatives—serait également un argument militant pour l'abolition de la *third-party doctrine* dans un contexte d'infonuagique,[72] de même que la constatation que les données situées dans le *nuage* sont de nature privée, non pas publique.[73] Selon Neil Richards, l'application de la *third-party doctrine* au *nuage* met tout simplement la protection constitutionnelle contre les fouilles, saisies et perquisitions abusives et le droit à la vie privée à risque.[74]

Au Canada, considérant la décision *Duarte* et le rejet de l'analyse fondée sur le risque,[75] ainsi que les nombreuses décisions où les informations détenues en mains tierces se sont vu accorder la protection de l'article 8 de la *Charte*,[76] il est clair que le partage des données avec un tiers ne peut justifier d'écarter complètement la protection constitutionnelle contre les fouilles, saisies et perquisitions abusives.[77] Cet élément a d'ailleurs été repris récemment dans la décision *Marakah*, où la majorité a rappelé que :

---

69 Orin S. Kerr, « Applying the Fourth Amendment to the Internet: A General Approach » (2009) 62 Stan L Rev 1005 à la p 1038; Andrew J. Pecoraro, « Drawing Lines in the Cloud: Implications of Extraterritorial Limits to the Stored Communications Act » (2017) 51 Creighton L Rev 75 à la p 103.

70 Wei Chen Lin, « Where Are Your Papers: The Fourth Amendment, the Stored Communications Act, the Third-Party Doctrine, the Cloud and Encryption » (2016) 65 DePaul L Rev 1093 à la p 1114 [Lin].

71 Lavanya Rathnam, « PRISM, Snowden and Government Surveillance: 6 Things You Need to Know » (2017), en ligne : *Cloudwards* < www.cloudwards.net/prism-snowden-and-government-surveillance/ > (consulté le 25 septembre 2018).

72 Buchan Serafino, *supra* note 18 à la p 172; Lin, *supra* note 71 à la p 1114.

73 Buchan Serafino, *supra* note 18 à la p 177.

74 Neil Richards, « The Third-Party Doctrine and the Future of the Cloud » (2017) 94 Wash L Rev 1441 à la p 1485.

75 *R c Duarte*, *supra* note 4.

76 Nous pensons notamment aux décisions *R c Spencer*, [2014] 2 RCS 212; *R c Société TELUS Communications*, [2013] 2 RCS 3.

77 *R. v. Craig*, 2016 BCCA 154 aux para 105 et suivants.

> « [l]a jurisprudence est claire : une personne ne perd pas le contrôle de renseignements pour l'application de l'art. 8 uniquement parce que quelqu'un d'autre les possède ou peut les consulter. Même lorsque "la réalité technologique" (*Cole*, par. 54) l'empêche d'exercer un contrôle exclusif sur ses renseignements personnels, une personne peut malgré tout s'attendre raisonnablement à ce que ces renseignements soient à l'abri du regard scrutateur de l'État. »[78]

Ce seul critère ne serait donc pas suffisant afin de nier l'existence d'une attente raisonnable de vie privée, puisqu'une analyse contextuelle doit être effectuée afin de déterminer s'il y a attente raisonnable de vie privée. La doctrine américaine sur la question demeure toutefois pertinente puisque l'analyse fondée sur le Quatrième amendement américain est très similaire à celle fondée sur l'article 8 de la *Charte* ; les deux s'appuyant sur l'existence d'une attente raisonnable de vie privée afin que la protection soit enclenchée. Il faudra donc considérer d'autres éléments, tels que les conditions de service imposées par les FSI, ainsi que les lois portant sur la protection des renseignements personnels, afin de déterminer si les données sauvegardées dans le *nuage* peuvent être protégées par l'article 8 de la *Charte*.

2.2 L'impact des conditions de service imposées par les FSI et des lois portant sur la protection des renseignements personnels

Le juge de première instance dans la décision *Spencer*—où il était question de la saisie de renseignements relatifs à l'abonné liés à une adresse IP précise—avait déterminé que l'attente de vie privée de l'accusé ne pouvait être considérée comme raisonnable en raison des dispositions contractuelles et législatives applicables, ce qui avait également été retenu en appel.[79] Toutefois, la Cour suprême en est plutôt arrivée à une conclusion différente. Selon la Cour, « les cadres législatifs et contractuels peuvent être pertinents, mais pas nécessairement déterminants, quant à la question de savoir s'il existe une attente raisonnable de vie privée ».[80] La Cour en est venue à cette conclusion en citant la décision *Gomboc*, où il avait été déterminé que le contrat entre un fournisseur de services et son client était d'une grande importance, mais qu'il n'était qu'un des facteurs pertinents à l'analyse.[81]

Aucune loi canadienne ne s'applique spécifiquement aux données situées dans le *nuage*. La *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) semble toutefois bel et bien s'appliquer en matière d'infonuagique.[82] Ainsi, les entreprises d'infonuagique devront

---

78 *R c Marakah*, [2017] 2 RCS 608 au para 41.

79 *R c Spencer*, *supra* note 77 au para 52; Pour un portrait de la situation sur cette question avant la décision de la Cour suprême dans *Spencer*, voir également Nied, *supra* note 16 à la p 702.

80 *R c Spencer*, *supra* note 77 au para 54.

81 *R c Gomboc*, [2010] 3 RCS 211 aux para 31-32.

normalement obtenir le consentement du client avant de divulguer des renseignements personnels,[83] sous réserve des conditions de services imposées par les FSI, ce qui sera examiné ci-après. Certaines exceptions existent, notamment dans le cadre d'enquêtes criminelles.[84] Toutefois, tel que noté dans la décision *Spencer*, « les dispositions de la LPRPDE ne sont pas très utiles pour déterminer s'il existe une attente raisonnable en matière de vie privée puisqu'après les avoir examinées, on se retrouve au point de départ ».[85] Ces dispositions sont donc d'un intérêt assez limité lorsque nous sommes à l'étape de déterminer s'il y a attente raisonnable de vie privée envers les données du *nuage*.

Aux États-Unis, les FSI ont une obligation de faire rapport aux autorités lorsqu'ils savent qu'un client a sauvegardé des fichiers de pornographie juvénile sur son *nuage*.[86] Une obligation similaire est prévue au Canada, en vertu de la *Loi concernant la déclaration obligatoire de la pornographie juvénile sur Internet par les personnes qui fournissent des services Internet*.[87] Afin de respecter cette obligation, plusieurs FSI, notamment *Microsoft*, *Facebook* et *Twitter*, ont mis sur place un programme permettant d'identifier de telles photos de manière automatique, dès que les photos sont sauvegardées sur le *nuage*.[88] Les FSI peuvent ensuite aviser les autorités pour que celles-ci obtiennent un mandat de perquisition visant les appareils électroniques du suspect. Lorsqu'une entreprise américaine identifie une adresse IP canadienne qui aurait été utilisée afin de sauvegarder de telles données dans le *nuage*, le FSI va contacter la *Gendarmerie Royale du Canada* (GRC) afin que l'enquête se poursuive de notre côté de la frontière.[89]

Dans la décision *Cusick*, les autorités canadiennes se sont basées sur un tel rapport fait par un FSI américain afin d'obtenir un mandat de perquisition visant un ordinateur situé au Canada.[90] Bien qu'ultimement un nouveau procès ait été ordonné, la Cour supérieure de l'Ontario a conclu que le rapport fourni par le FSI était une source crédible pouvant être utilisée par les autorités canadiennes afin d'obtenir un mandat de perquisition, sans que cette information n'ait besoin d'être autrement vérifiée.[91]

---

82 *Loi sur la protection des renseignements personnels et les documents électroniques*, LC 2000, c 5, art 4(1)(a).

83 *Ibid*, annexe 1, art 4.3.

84 *Loi sur la protection des renseignements personnels*, *supra* note 83 à l'art 7.

85 *R c Spencer*, *supra* note 77 au para 61.

86 *Victims of Child Abuse Act*, (1990), U.S. Code, Title 18 — Crimes and Criminal Procedure, Chapter 110.

87 *Loi concernant la déclaration obligatoire de la pornographie juvénile sur Internet par les personnes qui fournissent des services Internet*, LC 2011, c 4.

88 *R. v. Cusick*, 2015 ONSC 6739 au para 14.

89 *Ibid* au para 23.

90 *Ibid* au para 35.

91 *Ibid* au para 94.

Bien que démontrant que les FSI peuvent accéder aux données de leurs clients, nous pensons que ces obligations de divulgation ne font pas obstacle à la reconnaissance d'une attente raisonnable de vie privée envers les données du *nuage*. Comme la décision *Cusick* le démontre, les FSI vont principalement utiliser des logiciels automatisés afin d'identifier les fichiers de pornographie juvénile. Cela veut donc dire que les fichiers déposés sur le *nuage* ne sont pas examinés individuellement par un employé du FSI. Ainsi, les données demeurent pour la plupart confidentielles et non consultées par les FSI.

Outre les lois générales s'appliquant en matière de vie privée, la relation entre un FSI et un client est également régie par des conditions de service (*terms of service*) et par des politiques concernant la vie privée (*privacy policy*). Les conditions de service imposées[92] par un FSI peuvent varier grandement, notamment en ce qui concerne l'accès aux données des clients. Certaines entreprises, telles que *Mozy* et *SpiderOak*, prévoient dans leurs conditions de service qu'elles n'accéderont pas aux données sauvegardées sur le *nuage* de leurs clients.[93] Plus encore, ces entreprises ont mis en place des systèmes de cryptage sophistiqué qui font en sorte qu'elles ne sont même pas en mesure d'accéder aux données de leurs clients.[94] À l'autre extrémité du spectre, certains FSI indiquent dans leurs conditions qu'ils peuvent consulter les données de leurs clients à leur guise, sans aucun motif. C'est notamment le cas de *Apple*, de *Google* et de *DropBox*.[95] *Apple* spécifie toutefois dans ses politiques de confidentialité qu'elle ne fournira jamais aux forces de l'ordre les clés de cryptage des données utilisées par ses clients,[96] tandis que *DropBox* crypte ses données, mais ne mentionne pas si elle pourrait éventuellement remettre les clés de cryptage aux autorités.[97] Certains FSI, tel que *Microsoft*,[98] indiquent plutôt qu'ils n'accéderont pas aux

---

92 Les conditions de service sont effectivement non-négociables entre le FSI et le client et elles favorisent le FSI. Voir Jay P. Kesan, Carol M. Hayes et Masooda N. Bashir, « Information Privacy and Data Control in Cloud Computing: Consumers, Privacy Preferences, and Market Efficiency » (2013) 70 Wash L Rev 341 à la p 421.

93 Mozy, « Privacy Statement », en ligne : *Mozy* <mozy.com/about/legal/privacy> (consulté le 15 mai 2018); Spideroak, « Privacy Policy », en ligne : *Spideroak* <spideroak.com/privacy-policy/> (consulté le 15 mai 2018).

94 Mozy, « Online Backup Storage and Software for photos, music, and docs », en ligne : *Mozy* <mozy.com/product/mozy/personal> (consulté le 15 mai 2018); Spideroak, « No Knowledge, Secure-by-Default Products », en ligne : *Spideroak* <spideroak.com/no-knowledge/> (consulté le 15 mai 2018).

95 Google, « Terms of Service — Privacy & Terms », en ligne : *Google* <policies.google.com/terms> (consulté le 15 mai 2018); Apple, « iCloud Terms and Conditions », en ligne : *Apple Legal* <www.apple.com/legal/internet-services/icloud/en/terms.html> (consulté le 15 mai 2018); DropBox, « Terms », en ligne : *Dropbox* <www.dropbox.com/privacy> (consulté le 15 mai 2018).

96 Mizrahi, *supra* note 43 à la p 312.

97 *Ibid* à la p 311.

98 Microsoft, « Services Agreement », en ligne : *Microsoft* <www.microsoft.com/en-ca/servicesagreement/> (consulté le 15 mai 2018).

données de leurs clients, sauf dans le cadre d'une enquête interne sur la violation des conditions d'utilisation applicables. Pour sa part, *Amazon* indique qu'elle accédera aux données de ses clients seulement à la demande d'une autorité gouvernementale, ou afin d'exécuter sa prestation de services.[99] En ce qui concerne le partage des données avec les autorités, il y a également plusieurs différences dans les ententes de confidentialité applicables.[100]

Il est évident qu'une attente subjective de vie privée existe lorsque les usagers utilisent des services comme ceux de *Mozy* ou *SpiderOak*. Qu'en est-il cependant lorsque le FSI se réserve le droit d'accéder aux données à sa guise ou à la demande des autorités? Une première piste de solution provient peut-être du fait que la majorité des utilisateurs de services en ligne ne lisent pas les conditions d'utilisation. Certes, une personne qui accepte les conditions d'utilisation est présumée les avoir acceptées, mais il est indéniable que la majorité des consommateurs ne prennent pas le temps de s'enquérir des conditions d'utilisation des services qu'ils utilisent.[101]

Plusieurs auteurs soutiennent que l'attente de vie privée demeure valide, même lorsque les conditions de service indiquent que le FSI peut accéder aux données. Cela s'expliquerait notamment par le fait que les conditions de service sont modifiées très fréquemment et unilatéralement par les entreprises, que les lois applicables en matière de protection de la vie privée sont floues et qu'ultimement un utilisateur de services d'infonuagique confie ses données aux FSI pour qu'elles soient sauvegardées et conservées, non pas analysées.[102] Cette conclusion transparaît également de la décision *Spencer*, où une attente raisonnable de vie privée a été reconnue à l'accusé, malgré l'existence de dispositions contractuelles indiquant que le FSI avait le droit de communiquer certaines informations aux policiers.[103]

Ultimement, les dispositions contractuelles ou réglementaires sont moins susceptibles d'avoir un impact sur l'attente de vie privée lorsque l'information visée est intrinsèquement intime.[104] Ainsi, bien qu'utiles à l'analyse contextuelle

---

[99] Amazon, « AWS Customer Agreement », en ligne : *Amazon Web Services, Inc.* < aws.amazon.com/agreement/ > (consulté le 15 mai 2018); DropBox, préc., note 502.

[100] Mizrahi, *supra* note 43 aux pp 316-317.

[101] Selon une étude effectuée par une professeure à l'Université de New York, moins d'une personne sur 1000 clique sur les liens menant aux conditions de service en ligne (soit environ 0.11%). Voir Andy Greenberg, « Who Reads The Fine Print Online? Less Than One Person In 1000 », en ligne: *Forbes* < www.forbes.com/sites/firewall/2010/04/08/who-reads-the-fine-print-online-less-than-one-person-in-1000/ > (consulté le 15 mai 2018). Par ailleurs, la Cour supérieure et la Cour d'appel ont statué que les conditions d'utilisation imposées par les FSI étaient des contrats d'adhésion, faisant en sorte que les règles du Code civil à leur égard sont applicables. *Mofo Moko c Ebay Canada Ltd.* , 2013 QCCS 856, conf par 2013 QCCA 1912.

[102] Gold, *supra* note 68 aux pp 2341 et 2343; Khols, *supra* note 50 à la p 198.

[103] *R c Spencer*, *supra* note 77 aux para 56 et suivants.

[104] Steven Penney, « The Digitization of Section 8 of the Charter: Reform or Revolution? » (2014) 67-2 SCLR 505 au para 35.

devant être effectuée afin de déterminer si une attente raisonnable de vie privée existe envers les données du *nuage*, ces éléments ne sont pas à eux seuls susceptibles de nier totalement la protection offerte par l'article 8 de la *Charte*.

2.3 L'existence d'une attente raisonnable de vie privée sur les données sauvegardées dans le nuage

Concrètement, l'infonuagique n'a fait que déplacer les données personnelles des individus de leur disque dur personnel au serveur d'une entreprise.[105] Est-ce que cette simple migration des données devrait justifier la négation de la protection offerte par l'article 8 de la *Charte* ? Nous ne le pensons pas.

Une analyse en quatre étapes est maintenant utilisée par les tribunaux afin de déterminer si une attente raisonnable de vie privée existe.[106] Nous allons donc reprendre ces quatre étapes afin d'en arriver à la conclusion que les données du *nuage* méritent la même protection que les données situées sur l'ordinateur d'un suspect.[107]

2.3.1 L'objet de la fouille

Les données qu'un individu désire sauvegarder sur le *nuage* peuvent être très variées. Il peut s'agir de données bancaires, de photos personnelles, de documents numérisés, de textes personnels, de conversations électroniques, de courriels, etc. Tout comme dans les décisions *Morelli*, *Vu* et *Cole*, l'objet de la fouille n'est ici pas le serveur en lui-même, mais bien les données qu'il contient.[108] Ces données peuvent évidemment révéler des détails intimes sur l'individu qui fait l'objet d'une enquête, puisque les ordinateurs « contiennent des renseignements qui sont significatifs, intimes et qui ont trait à l'ensemble des renseignements biographiques de l'utilisateur. »[109]

Selon l'auteur américain David S. Barnhill, une distinction devrait être faite entre les données personnelles qu'un individu a sauvegardées sur son *nuage* et celles que le FSI a créées lors de la sauvegarde des données, c'est-à-dire les métadonnées.[110] Alors que les premières seraient protégées par une attente raisonnable de vie privée, les secondes ne le seraient pas.[111] L'objet de la fouille

---

[105] Buchan Serafino, *supra* note 18 à la p 174; Khols, *supra* note 50 à la p 198.

[106] *R c Spencer*, *supra* note 77 au para 18; Voir aussi *R c Cole*, [2012] 3 RCS 34 au para 40.

[107] *R c Morelli*, *supra* note 5 au para 2.

[108] *R v Craig*, *supra* note 78 au para 136 citant; *R c Morelli*, *supra* note 5 au para 2; *R c Cole*, *supra* note 107; *R c Vu*, [2013] 3 RCS 657.

[109] *R c Cole*, *supra* note 107 au para 2. Voir également *R c Plant*, [1993] 3 RCS 281 à la p 293; *R c Vu*, *supra* note 109 aux para 41-44; *R c Spencer*, *supra* note 77 au para 27.

[110] Une métadonnée peut être définie comme « une donnée qui fournit de l'information sur une autre donnée ». Il s'agit par exemple de la date de création d'un fichier ou de son volume. Voir « Qu'est-ce qu'une "métadonnée" », en ligne: *Commissariat à la protection de la vie privée du Canada* < www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/technologie-et-vie-privee/md_info_201410/ > (consulté le 7 février 2019).

[111] Barnhill, *supra* note 20 aux pp 645-646; Voir également Kerr, *supra* note 70.

ne serait donc pas le même dans ces deux situations, ce qui justifierait un traitement différent ultimement en vertu de la *Charte*. Toutefois, certains auteurs prétendent le contraire et soutiennent que les données sauvegardées dans le *nuage* et les métadonnées devraient être protégées, puisque les métadonnées sont également susceptibles de révéler des détails intimes sur les individus.[112] En appliquant les enseignements de la Cour suprême dans l'arrêt *Spencer*, nous pensons, à l'instar de ces auteurs, que les métadonnées devraient être protégées, puisqu'elles ne servent pas seulement à identifier un individu, mais bien à identifier celui-ci par rapport à une utilisation particulière d'Internet.[113] Certes l'attente raisonnable de vie privée est peut-être moindre qu'envers les données personnelles elles-mêmes, mais il n'en demeure pas moins que l'attente existe.

2.3.2 Le droit du demandeur à l'égard de l'objet>

Malgré les divergences importantes recensées dans les conditions de service et les politiques concernant la vie privée, tous les FSI indiquent que les données demeurent la propriété du client.[114] Ainsi, bien que les données soient sauvegardées sur des serveurs appartenant généralement à un tiers, la propriété des données n'est pas transférée à celui-ci.

La propriété de l'appareil électronique utilisé pour accéder aux données n'est pas un élément pertinent à considérer puisque les données du *nuage* peuvent être accédées à partir de n'importe quel appareil avec une connexion Internet. Cette particularité du *nuage* avait d'ailleurs été soulignée dans la décision *Cole*, où la juge Abella, dans sa dissidence, avait indiqué que :

> « [. . .] comme plus de données sont stockées dans le nuage et qu'on y a accès tant sur l'ordinateur de travail que l'ordinateur personnel, la propriété de l'appareil ou des données, loin de constituer un critère déterminant de l'attente raisonnable en matière de protection de la vie privée, devient un repère de plus en plus inutile ».[115]

Lorsqu'il est question de données, le droit du demandeur à l'égard de celles-ci relève principalement du caractère privé des renseignements personnels qu'elles contiennent.[116] En l'espèce, il est indéniable que les données se trouvant dans le *nuage* peuvent « révéler des détails intimes sur le mode de vie et les choix personnels des individus ».[117] Par ailleurs, le droit à la vie privée inclut l'attente que les renseignements que nous divulguons de manière volontaire soient

---

[112] Michael W. Price, « Rethinking Privacy: Fourth Amendment "Papers" and the Third-Party Doctrine » (2016) 8 JNSLP 247 aux pp 250 et 285; Andrew Gray, « Cloud Atlas - A Map to Amending Metadata Privacy Law in the Modern Era » (2016) 52 Gonz L Rev 147.

[113] *R c Spencer*, *supra* note 77 au para 32.

[114] McCorry, *supra* note 46 à la p 143.

[115] *R c Cole*, *supra* note 107 au para 109.

[116] *R c Spencer*, *supra* note 77 au para 37.

[117] *R c Plant*, *supra* note 110 au para 293.

confidentiels et qu'ils ne soient utilisés que « pour les fins pour lesquelles ils ont été divulgués ».[118] S'ils sont utilisés dans un autre but, « la personne à laquelle se rapportent ces renseignements peut encore conserver une attente raisonnable en matière de protection de la vie privée à leur égard ».[119]

Autrement dit, les caractéristiques intrinsèques de l'infonuagique, soit le fait que les données peuvent être accédées à partir de n'importe quel appareil et qu'elles se trouvent sur des serveurs distants, ne doivent pas être utilisées afin de nier le droit du demandeur à l'égard de l'objet. Ainsi, « less emphasis is placed on factors which are of diminished relevance regarding digital privacy: the medium on which the data is stored and the physical location where storage takes place ».[120]

2.3.3 L'existence d'une attente subjective

Le contexte normatif peut être utilisé afin de déterminer si une attente raisonnable de vie privée existe envers un certain type d'information.[121] Dans le cas des données sauvegardées dans le *nuage*, nous pensons que ce contexte normatif milite pour la reconnaissance d'une attente raisonnable de vie privée. En effet, il existe une supposition sociale selon laquelle nos comptes en ligne font l'objet d'une certaine confidentialité ou d'une certaine vie privée.[122] En ce sens : « a cloud user has placed his files and media into the hands of the third-party cloud provider, and entrusts the third party will store and provide access to the files, but does not expect the provider to look at them ».[123]

Par ailleurs, l'interface utilisée afin d'accéder aux données situées sur le *nuage* ne permet pas toujours de savoir réellement où celles-ci se trouvent. En effet, les fichiers situés dans le *nuage* peuvent parfois être accédés de la même manière que les fichiers se trouvant directement sur le disque dur d'un individu.[124] Dans ces

---

[118] *R c Dyment*, [1988] 2 RCS 417 à la p 430.

[119] *R c Mills*, [1999] 3 RCS 668 au para 108.

[120] Scanlan, *supra* note 55 à la p 314.

[121] Selon Lisa M. Austin, « Is Consent the Foundation of Fair Information Practices? Canada's Experience under PIPEDA », (2006) 56 UTLJ 181, il importe de considérer le contexte normatif afin d'éviter de tomber dans une analyse purement descriptive des attentes des individus, par opposition à une analyse fondée sur la vie privée des gens. Voir également James A.Q. Stringham, « Reasonable Expectations Reconsidered: A Return to the Search for a Normative Core for Section 8? » (2005) 23 Criminal Reports 245; *R c Spencer*, *supra* note 77 au para 18; *R c Wong*, *supra* note 2 à la p 47; *R c Buhay*, *supra* note 51 au para 21; *R c Gomboc*, *supra* note 82 au para 34; *R c Wise*, [1992] 1 RCS 527 à la p 534; *R c Tessling*, [2004] 3 RCS 432 au para 42.

[122] Gold, *supra* note 68 aux pp 2332 et 2337; *R v Craig*, *supra* note 78 au para 121.

[123] Khols, *supra* note 50 au para 198.

[124] Nied, *supra* note 16 à la p 706; Hochhalter, *supra* note 47 à la p 178; Gold, *supra* note 68 à la p 2323; Par exemple, Google Drive peut être installé directement dans un Mac, faisant en sorte que les données sont accessibles de la même manière que celles qui se trouvent uniquement sur le disque dur de l'utilisateur. Voir Tom Nelson, « Setup and Price Guide to Google Drive for the Mac », en ligne: *Lifewire* < www.lifewire.com/how-to-set-up-and-use-google-drive-on-mac-2260845 > (consulté le 17 mai 2018).

cas, cette interface pourrait donc renforcer l'attente subjective d'un individu selon laquelle ses données sont protégées par la *Charte*. Le fait que les données du *nuage* soient habituellement protégées par mot de passe est également un indice qu'une attente subjective de vie privée est présente.[125] Il importe également de rappeler que l'existence d'une attente subjective de vie privée ne doit pas être un élément difficile à prouver pour un individu réclamant la protection offerte par l'article 9 de la *Charte*.[126]

2.3.4 Le caractère raisonnable de cette attente subjective, eu égard à l'ensemble des circonstances

Récemment, dans la décision *R.* v. *Craig*, la Cour d'appel de la Colombie-Britannique s'est penchée sur l'attente raisonnable de vie privée que prétendait avoir un accusé envers des données situées sur les serveurs d'une entreprise, donc des données situées dans le *nuage*.[127] Il s'agissait en l'espèce de conversations sur la plateforme *Nexopia*, un réseau social utilisé principalement par des adolescents.[128] La Cour, reprenant les enseignements de la Cour suprême dans la décision *Cole* selon lesquels il n'y a pas de liste de facteurs définitifs permettant d'analyser le caractère raisonnable d'une attente subjective de vie privée,[129] a retenu quatre critères principaux afin d'en arriver à la conclusion que l'attente subjective de l'accusé était objectivement raisonnable dans les circonstances.

Premièrement, concernant l'endroit de la fouille, la Cour a conclu que cet élément à lui seul n'appuyait pas l'existence d'une attente raisonnable de vie privée, puisque les données étaient situées sur les serveurs d'un tiers.[130] Toutefois, la Cour a souligné d'un même trait que, de nos jours, une importante partie de nos données ne se trouvent pas sur nos ordinateurs personnels, mais plutôt sur des serveurs. En ce sens, ce n'est pas l'endroit de la fouille qui justifie l'attente de vie privée,[131] mais plutôt le contenu des serveurs qui a été créé par l'accusé lui-même.[132] Deuxièmement, la Cour a observé que les messages n'étaient pas à la vue du public, étant protégés par un nom d'utilisateur et un mot de passe, ce qui suggère qu'il y a attente de vie privée.[133] Troisièmement, bien que les messages aient été partagés avec une tierce partie, cela ne rend pas l'attente de vie privée de

---

[125] Kerr, *supra* note 70 à la p 1021.

[126] Pierre Béliveau et Martin Vauclair, *Traité général de preuve et de procédure pénales*, 20e éd, Cowansville : Éditions Yvon Blais, 2013 au para 860.

[127] *R v Craig*, *supra* note 78.

[128] *Ibid* au para 3.

[129] *R c Cole*, *supra* note 107 au para 45.

[130] *R v Craig*, *supra* note 78 à la p 101.

[131] « The physical location of data has become an increasingly illogical basis for determining the protection to be afforded data from unreasonable search » Scanlan, *supra* note 55 à la p 313.

[132] *R v Craig*, *supra* note 78 au para 103.

[133] *Ibid* au para 104.

l'accusé déraisonnable, et ce, pour quatre raisons : le rejet de l'analyse fondée sur le risque dans *Duarte*, l'existence de normes sociales militant pour la reconnaissance d'une attente raisonnable de vie privée dans des messages privés, l'émergence de lois prouvant l'existence d'une attente raisonnable de vie privée envers des données partagées avec des tiers et l'émergence d'une jurisprudence au même effet.[134] Quatrièmement, la Cour a souligné que le contenu des messages envoyés par l'accusé soutient le caractère raisonnable de son attente subjective de vie privée, puisqu'ils contiennent des « intimates details of his lifestyle, personal choices, and private identifying information ».[135] Pour ces motifs, la Cour est arrivée à la conclusion que la protection de l'article 8 de la *Charte* est bel et bien applicable aux données de l'accusé qui se trouvaient sur le serveur de l'entreprise *Nexopia*.

Dans la décision *Marakah* la majorité de la Cour suprême a retenu trois critères afin de déterminer si l'attente subjective de l'accusé était raisonnable dans les circonstances : le lieu fouillé, le caractère privé de l'objet de la fouille et le contrôle de l'accusé sur l'objet de la fouille.[136] L'honorable juge McLachlin a alors mentionné qu'une « conversation électronique ne se déroule pas dans un lieu physique précis »,[137] ce qui est également pour les données situées dans le *nuage*. Cette constatation n'a toutefois pas empêché la reconnaissance du caractère raisonnable de l'attente de l'accusé dans les circonstances, principalement puisque la protection de l'article 8 de la *Charte* vise les personnes et non les lieux.[138] La majorité a également souligné que « l'absence de contrôle ne porte pas un coup fatal à la reconnaissance d'un intérêt en matière de vie privée »,[139] ce qui appuie d'autant plus la conclusion que les données dans le *nuage* sont protégées, malgré leur partage avec le FSI. Par ailleurs, comme la Cour suprême a adopté un principe de neutralité technologique dans son application de l'article 8 de la *Charte*,[140] il semble clair que les données personnelles des individus devraient recevoir la même protection et être accédées en vertu des mêmes standards de preuve, peu importe leur emplacement physique.[141]

Venant confirmer cette interprétation de l'arrêt *Marakah* quant aux données situées dans le *nuage*, la décision *R.* c. *Reeves* réitère qu'un contrôle partagé n'est pas fatal à la reconnaissance d'une attente raisonnable de vie privée.[142] Dans cette décision, l'ancienne conjointe de l'accusé avait consenti à la remise aux

---

134 *Ibid* aux para 105-131.

135 *Ibid* au para 132.

136 *R c Marakah*, *supra* note 79 au para 24.

137 *Ibid* au para 28.

138 *Hunter c Southam inc.*, [1984] 2 RCS 145 à la p 159.

139 *R c Marakah*, *supra* note 79 au para 38.

140 *R c Vu*, *supra* note 109 au para 38; *R c Fearon*, [2014] 3 RCS 621 au para 54.

141 Scanlan, *supra* note 55.

142 *R c Reeves*, 2018 CSC 56 aux para 33 et suivants.

policiers de l'ordinateur qu'ils utilisaient tous les deux puisqu'elle y avait découvert des fichiers de pornographie juvénile. La Cour est venue conclure que la saisie sans mandat de l'ordinateur, ainsi que la fouille subséquente du contenu de celui-ci, était illégale puisque l'accusé avait bel et bien une attente raisonnable de vie privée, bien qu'il n'exerçait pas un contrôle exclusif sur l'appareil.[143] Se basant notamment sur l'arrêt *Cole*, la Cour souligne encore une fois qu'un « contrôle partagé ne signifie pas une *absence* de contrôle »,[144] ce qui confirme notre conclusion voulant qu'un partage des données du *nuage* avec le FSI ne rende pas l'attente de vie privée déraisonnable pour autant.

Pour l'ensemble de ces raisons, il semble clair que les données situées dans le *nuage* pourront généralement faire l'objet d'une attente raisonnable de vie privée et ainsi bénéficier de la protection prévue à l'article 8 de la *Charte*.

SECTION 3 — LES AUTORISATIONS JUDICIAIRES APPLICABLES À LA SAISIE DES DONNÉES DU *NUAGE*

Plusieurs scénarios sont susceptibles de se présenter lorsque les policiers voudront accéder à des données situées sur le *nuage* d'un individu sous enquête. En effet, tel que mentionné, dans certains cas, les données seront accessibles directement sur l'ordinateur de l'individu, en raison d'une interface qui permet de consulter les données comme si elles étaient sauvegardées directement sur l'appareil. Ce principe est également applicable aux autres appareils électroniques, qui sont susceptibles d'avoir accès à l'ensemble des données délocalisées d'un individu. Au contraire, certains fournisseurs de services d'infonuagique n'offrent pas cette option et donc les données doivent être accédées par l'entremise d'un site web, à l'aide d'un nom d'utilisateur et d'un mot de passe. De plus, certains fournisseurs peuvent accéder aux données de leurs clients, alors que d'autres ont mis en place une structure sécurisée, ne leur permettant pas de consulter les données.

Nous allons donc poursuivre notre analyse en analysant les diverses autorisations judiciaires susceptibles d'être utilisées afin d'accéder aux données délocalisées se trouvant dans le *nuage*, selon les différents scénarios mentionnés ci-dessus. À ce propos, tel qu'il a été mentionné par un auteur canadien :

> « This dispersion of personal data into the "cloud" can work several different ways. Presuming grounds exist, police may use production orders to obtain data held by commercial entities and thereby not need to meet the higher standard necessary for a warrant to search a person's home. They may seek a warrant for a mobile device and use it to access the suspect's web services and home computer files available to it. They may seek a warrant for a home computer and use it to access any web-based or commercial services it has access to (data on the so-called "cloud"). »[145]

---

[143] *Ibid* au para 37.

[144] *Ibid*.

À cette étape, il est utile de souligner que, comme il y a attente raisonnable de vie privée dans les données du *nuage*, un FSI ne peut consentir à divulguer celles-ci aux forces de l'ordre. Tout comme dans la décision *Cole*, dans laquelle la Cour suprême a décidé qu'un employeur ne pouvait consentir à la saisie à la place de son employé titulaire de l'attente raisonnable de vie privée,[146] un FSI ne peut consentir à la remise des données plutôt que le propriétaire des données. Le FSI n'a pas contrôle direct sur les données et n'est pas le propriétaire conjoint de celles-ci avec l'utilisateur des services d'infonuagique.[147]

3.1 Le mandat de perquisition

Selon l'alinéa 487(2.1)a) C.cr., lorsqu'un mandat de perquisition est exécuté, toutes les données auxquelles l'ordinateur (ou un autre appareil électronique) donne accès peuvent être vérifiées. Cette disposition a été interprétée comme autorisant la fouille de données délocalisées, se trouvant sur d'autres ordinateurs accessibles par l'entremise d'un réseau.[148] Cette interprétation semble confirmer que le mandat de perquisition de l'article 487 C.cr. peut être utilisé afin d'accéder à des données situées dans le *nuage*, dans la mesure où ces données sont accessibles à partir de l'ordinateur visé par le mandat de perquisition.[149]

Toutefois, cette disposition a été adoptée alors que l'infonuagique n'était qu'à ses balbutiements. En effet, le paragraphe 487(2.1) C.cr. a été ajouté au *Code criminel* en 1997,[150] soit bien avant que l'infonuagique ne soit réellement utilisée à grande ampleur. Est-ce donc raisonnable de penser que le législateur canadien avait réellement anticipé qu'autant d'information privée serait accessible à partir d'un seul ordinateur? Probablement pas. Il est plus plausible que la situation anticipée à l'époque était celle des ordinateurs branchés en réseau local, comme dans une entreprise où les ordinateurs sont tous connectés ensemble. L'auteure Susan Magotiaux a noté les risques découlant de cette interprétation du paragraphe 487(2.1) C.cr. :

> « The search provisions in the Criminal Code have been updated to address the lack of tangibility and physical presence of digital data. In 1997, section 487 was amended to include provisions aimed directly at the problem of gathering digital "things". Section 487(2.1) and (2.2) provide that, in a regular search warrant under section 487, a police officer or a person at the search location may "use or cause to be used any computer system at the building or place to search any data

---

145 *Ibid* au para 311.

146 *R c Cole*, *supra* note 107 au para 77.

147 Khols, *supra* note 50 à la p 203.

148 Scanlan, *supra* note 55 à la p 303; *R. v. Edwards*, [1999] O.J. No. 3819 au para 89.

149 Dans la décision *R. v. Young*, 2012 ONCJ 716 aux para 18-19, la Cour mentionne que des données de l'accusé, en l'espèce des images de pornographie juvénile se trouvant dans le nuage, ont été accédées à l'aide d'un mandat de perquisition.

150 *Code criminel*, LRC 1985, c 18 (1997), art 41.

> contained in or available to the computer system". The scope of the subsection has not been widely considered. It is potentially boundless. If taking and examining the desktop box was deemed in R. v. Morelli to be the most intrusive, extensive, and invasive search imaginable, what about a search of all that is "accessible to" that box while its stands connected in a home or office? Depending on the configurations and active connections of a given device, there could be data accessible to the device from other people, other networks, other countries, or other businesses. The section 487 warrant looks for things in a place, yet the Court in Vu recognized that "a search of a computer connected to the Internet or a network gives access to information and documents that are not in any meaningful sense at the location for which the search is authorized". »[151]

Comment réconcilier cette disposition avec les développements jurisprudentiels subséquents en matière de nouvelles technologies? L'approche adoptée dans l'arrêt *Vu* serait probablement la meilleure option. Dans cette décision, la Cour suprême a décidé que les ordinateurs ne pouvaient être considérés comme de simples contenants, en raison des intérêts particuliers en matière de vie privée que leur utilisation implique.[152] Ceci a pour conséquence que les policiers doivent spécifiquement indiquer dans leur demande d'autorisation les motifs justifiant la fouille des appareils électroniques se trouvant sur les lieux d'une perquisition, à défaut de quoi ceux-ci ne pourront qu'être saisis—sans être fouillés—avant qu'un second mandat visant spécifiquement leur fouille ne soit obtenu.[153]

De la même manière, nous pensons que les policiers devraient indiquer dans leur demande d'autorisation les motifs pour lesquels ils désirent accéder au *nuage* d'un individu.[154] Si l'existence d'un *nuage* n'est découverte que lors de la fouille d'un appareil électronique validement saisi, les policiers devraient alors arrêter leurs recherches et obtenir un nouveau mandat avant d'accéder au *nuage*. Le juge émetteur serait alors en mesure d'évaluer les diverses implications en matière de vie privée et, dans certains cas, imposer des protocoles de saisie,[155] notamment lorsque les données du *nuage* sont également accessibles par des tiers innocents.

---

[151] Susan Magotiaux, « Out of Sync: Section 8 and Technologial Advancement in Supreme Court Jurisprudence » (2015) 71 SCLR 501 au para 26.

[152] *R c Vu*, *supra* note 109 au para 2.

[153] *Ibid* au para 3.

[154] Certains auteurs suggèrent qu'un mandat séparé doit être obtenu, voir Khols, *supra* note 50 à la p 201. Dans la mesure où les policiers indiquent spécifiquement dans leur demande d'autorisation les motifs expliquant la fouille du nuage, nous ne pensons pas que cette exigence soit nécessaire.

[155] Bien que la Cour suprême ait décidé dans la décision *Vu* que l'imposition d'un protocole de saisie ne sera généralement pas nécessaire, elle n'exclut pas la possibilité que cela soit le cas dans certaines situations précises, telle qu'une fouille d'ordinateur « concernant des droits de propriété intellectuelle confidentiels ou encore des renseignements susceptibles d'être protégés par un privilège » *R c Vu*, *supra* note 109 au para 62.

Par ailleurs, nous pensons que l'application de la doctrine des objets bien en vus ne pourrait ici permettre la fouille du *nuage* sans l'obtention d'une autorisation judiciaire séparée. Puisque le *nuage* peut être considéré comme un lieu distinct en matière de fouille, autant physiquement que virtuellement,[156] la première condition pour que la théorie s'applique, soit que « the seizing officer must be lawfully in the place of seizure »,[157] ne serait pas remplie.

Les policiers peuvent parfois contourner l'exigence de l'obtention préalable d'un mandat en raison de l'urgence de la situation.[158] Certains pourraient prétendre que le risque de destruction des données dans le *nuage* constitue une situation urgente justifiant l'application de cette doctrine d'exception, puisque les données peuvent être détruites à partir d'un autre appareil ayant une connexion Internet. Or, le risque de perte des données est moins important que ce qui pourrait sembler. En effet:

> « [. . .] even after a user deletes his data or closes his account, many cloud storage providers will preserve data on their servers for a period of time. [. . .] Simply deleting data from a drive does not completely destroy the files hosted there, and "deleted" data is actually recoverable ».[159]

Par ailleurs, l'ordre et de l'ordonnance de préservation de données sont également accessibles aux policiers s'ils jugent qu'il y a un risque de destruction des données.

Somme toute, nous pensons que le paragraphe 487(2.1) C.cr. peut permettre la saisie des données situées dans le *nuage*, dans la mesure où le mandat de perquisition émis spécifie que cela est permis. Cela veut dire que dès que l'appareil électronique d'un suspect est validement saisi, l'entièreté de ses données délocalisées pourront être accédées et analysées par les forces de l'ordre. Cette autorisation judiciaire sera donc la plus pertinente dans le scénario où les données sont accessibles directement à partir de l'appareil électronique de l'individu ou lorsque les policiers ont accès aux mots de passe utilisés par le suspect afin de se connecter à ses services d'infonuagique par le biais d'Internet.[160] Si cela n'est pas le cas, l'ordonnance générale de communication sera probablement plus appropriée.

---

[156] Gold, *supra* note 68 à la p 2345.

[157] *R. v. Atkinson*, 2012 ONCA 380 au para 57.

[158] *R. v. Grant*, [1993] 3 RCS 223 aux pp 241-242; *R c Colarusso*, [1994] 1 RCS 20 à la p 53; *R c Kelsy*, 2011 ONCA 605 au para 25. Ce pouvoir ne peut toutefois être utilisé afin de pénétrer dans une maison d'habitation, voir *R c Silveira*, [1995] 2 RCS 297 aux para 50-52.

[159] Gold, *supra* note 68 à la p 2347.

[160] Concernant l'obtention de mots de passe, il est utile de rappeler que les policiers ne pourront forcer un individu à leur communiquer cette information. Voir *R c Boudreau-Fontaine*, 2010 QCCA 1108.

3.2 L'ordonnance générale de communication

Contrairement aux objets qui sont normalement visés par un mandat de perquisition ou aux données se trouvant dans l'ordinateur d'un suspect, les données du *nuage* sont très souvent accessibles par une tierce personne, soit le FSI. Cet accès supplémentaire simultané,[161] qui n'existe pas habituellement en matière de fouille, peut devenir un avantage intéressant pour les policiers qui pourront alors accéder aux données par l'entremise du FSI, sans que le suspect ne soit mis au courant immédiatement. Cela aurait également comme avantage de pouvoir contourner un mot de passe qui bloquerait l'accès aux données à partir de l'ordinateur de l'accusé.[162]

Dans le cas des données personnelles sauvegardées par l'individu sur un *nuage*, l'ordonnance générale de communication pourra être utilisée par les policiers afin de contraindre un FSI à divulguer celles-ci. Considérant que cette ordonnance peut être obtenue en respectant le même standard d'émission qu'un mandat de perquisition, soit l'existence de *motifs raisonnables de croire*, il semble que l'utilisation de cette technique d'enquête soit raisonnable, compte tenu du degré d'attente de vie privée élevé applicable à ces données.[163] Dans ce cas, le FSI deviendrait alors un agent de l'État en exécutant saisissant les données visées par l'ordonnance de communication.[164]

Par ailleurs, la décision *Jones* est venue confirmer qu'une ordonnance générale de communication est suffisante afin d'obtenir des messages textes arrivés à destination qui sont sauvegardés sur le serveur du FSI.[165] Selon la

---

[161] Scanlan, *supra* note 55 à la p 312.

[162] L'étude approfondie de la possibilité qu'ont les policiers d'obtenir le mot de passe d'un individu (par d'autres moyens que par l'accusé lui-même; par exemple en recourant à des logiciels particuliers, à des experts en informatique ou simplement en fonctionnant par essai-erreur) dépasse le cadre de cet article. Il est toutefois important de souligner que les mots de passe eux-mêmes peuvent être l'objet d'une attente raisonnable de vie privée. Voir Sarah Wilson, « Compelling Passwords from Third Parties: Why the Fourth and Fifth Amendments Do Not Adequately Protect Individuals When Third Parties Are Forced to Hand over Passwords » (2015) 30 BTLJ 1. Par ailleurs, la majorité des fabricants d'appareils électroniques ne conservent pas le mot de passe que l'usager utilise afin d'accéder à l'appareil. Ce ne seront donc que les mots de passe de comptes en ligne, tels que les comptes courriel ou des comptes de réseaux sociaux, qui pourront potentiellement être obtenus par ordonnance de communication.

[163] Le degré d'attente de vie privée d'un individu fait varier le degré de protection nécessaire. Ainsi, lorsqu'un individu a une attente dite « normale » de vie privée, le test des « motifs raisonnables de croire », établi à l'article 487 Ccr, sera la norme. Un degré d'attente plus faible pourrait se traduire par la norme des « motifs raisonnables de soupçonner », prévu notamment à l'article 487.018 Ccr, tandis qu'un degré plus fort se traduirait par des conditions additionnelles, comme il est le cas pour les ordonnances d'interception de communications privées ou pour les mandats relatifs aux analyses génétiques. Voir S. G. Coughlan, *Criminal procedure*, 3 éd, coll Essentials of Canadian law, Toronto: Irwin Law, 2016 à la p 142.

[164] Josiah Dykstra et Damien Rhiel, *supra* note 14 à la p 35.

[165] *R c Jones*, [2017] 2 RCS 696.

majorité, l'attente de vie privée de l'accusé envers ces communications privées était raisonnable, bien que les messages étaient également accessibles par le FSI.[166] Toutefois, comme les policiers avaient obtenu une ordonnance de communication,[167] la saisie des messages textes sur les serveurs du FSI n'a pas enfreint les droits de l'accusé. En effet, l'interprétation du terme « intercepter » ne permet pas de conclure qu'une autorisation d'interception de communications privées est nécessaire lorsque les communications sont arrivées à destination.[168] Pour cette raison, nous croyons que des courriels arrivés à destination, éléments se trouvant fréquemment sur le *nuage*, ou toute autre forme de communication virtuelle complétée, pourraient être validement saisis par l'entremise du FSI en utilisant l'ordonnance générale de communication.

Certains auteurs critiquent toutefois l'utilisation de telles ordonnances afin d'accéder aux données situées sur le *nuage*. Selon Christopher Soghoian, afin que la vie privée des usagers du *nuage* soit respectée, les données devraient être cryptées *de facto*, afin que les FSI ne puissent y avoir accès,[169] ce que les entreprises *SpiderOak* et *Mozy* font déjà. Selon lui, cette mesure aurait pour effet de rétablir l'équilibre entre le droit des individus au respect de leur vie privée et l'intérêt légitime de l'État à réprimer le crime. L'État pourrait alors utiliser d'autres méthodes d'enquête, en utilisant le mandat général de l'article 487.01 C.cr., afin d'accéder aux données non cryptées ou pour obtenir les mots de passe et clés de cryptage utilisés par le suspect.[170]

A contratrio, d'autres auteurs soulignent que le cryptage et les autres mesures de protection des données pourraient empêcher totalement les forces de l'ordre d'avoir accès aux données, ce qui ne serait pas souhaitable.[171] Dans certains cas, si les données du *nuage* sont protégées par mot de passe ou par cryptage, il sera en effet possible que les données soient complètement inaccessibles, malgré l'utilisation de logiciels tentant de déchiffrer les clés de cryptage utilisées. Cette situation s'est notamment présentée dans la décision *Pratchett*, dans laquelle un système d'infonuagique personnel (ou un *nuage privé*), constitué de quatre disques durs saisis sur les lieux de la perquisition, n'a pu être accédé en raison de la complexité du système de cryptage en place.[172]

---

[166] *Ibid* au para 41.

[167] Qui était alors en vertu de l'article 487.012 Ccr et qui correspond maintenant à l'article 487.014 Ccr.

[168] *R c Jones*, *supra* note 166 au para 77.

[169] Christopher Soghoian, « Caught in the Cloud: Privacy, Encryptions, and Government Back Doors in the Web 2.0 Era » (2010) 8 JTHTL 359 à la p 398 [Soghoian]. Voir également Lin, *supra* note 71.

[170] L'auteur mentionne notamment l'utilisation de la technique « black bag job », qui inclut des entrées subreptices ou l'utilisation de surveillance électronique. Soghoian, *supra* note 170 à la p 398.

[171] Susan W. Brenner, « Encryption, Smart Phones, and the Fifth Amendment » (2012) 33 Whittier L Rev 525 à la p 534.

[172] *R. v. Pratchett*, 2016 SKPC 19 aux para 74-78.

3.3 Le mandat général

Par ailleurs, qu'arrive-t-il si le FSI décide de ne pas collaborer et de ne pas respecter l'ordonnance de communication? Les policiers se trouveraient alors devant deux choix : saisir les serveurs du FSI, ce qui inclut l'accès à toutes les données s'y trouvant, y compris celles appartenant à des tiers innocents, ou encore d'utiliser des techniques d'accès à distance au *nuage*.[173] La première option semble à première vue laborieuse en raison de la quantité impressionnante de données que peuvent contenir de tels serveurs, mais elle n'est pas impossible même si les données sont situées à l'étranger tel que démontré par un renvoi de la Cour supérieure de l'Ontario où la *Loi sur l'entraide juridique en matière criminelle*[174] a été appliquée afin de saisir le contenu de serveurs se trouvant au Canada, dans le cadre d'une enquête menée par les Pays-Bas.[175] Concernant la seconde option, un tel accès à distance devrait selon toute vraisemblance être autorisé par l'entremise d'un mandat général de l'article 487.01 C.cr., puisqu'il s'agit d'une technique d'enquête inusitée équivalent à une entrée subreptice.[176]

Il est maintenant connu que les autorités ont la capacité technologique d'intercepter les données alors qu'elles sont en transit vers le *nuage*.[177] Cette technique a toutefois été vivement critiquée aux États-Unis puisqu'elle a été utilisée dans le cadre d'une opération de surveillance de masse par la *National Security Agency* (NSA), ce qui avait été révélé par le lanceur d'alerte Edward Snowden.[178] Cette technique devrait également être autorisée par mandat général au Canada, s'il s'avère que les autorités canadiennes ont également cette capacité technologique.

3.4 Les ordonnances de communication spécifiques

À la section 2.3.1, nous avons conclu que les métadonnées peuvent également être l'objet d'une attente raisonnable de vie privée. Une autorisation judiciaire est donc également nécessaire à leur saisie. Toutefois, certaines ordonnances de communication spécifiques sont susceptibles de s'appliquer, permettant plus facilement la saisie de ces données en raison du seuil plus bas nécessaire à leur obtention, soit celui des *motifs raisonnables de soupçonner*. Il s'agirait principalement de l'ordonnance de communication en vue de retracer des

---

[173] Mizrahi, *supra* note 43 à la p 321.

[174] *Loi sur l'entraide juridique en matière criminelle*, LRC 1985, c 30.

[175] *Mutual Legal Assistance in Criminal Matters Act (Re)*, 2016 ONSC 5699 aux para 10-11. Dans la décision, la Cour adresse également la problématique de l'accès aux données de tiers.

[176] Susan W. Brenner, « Law, Dissonance, and Remote Computer Searches » (2012) 24 JOTL 43 à la p 61.

[177] Joris V. J. Van Hoboken, « Privacy and Security in the Cloud: Some Realism about Technical Solutions to Transnational Surveillance in the Post-Snowden Era » (2014) 66 Me L Rev 487.

[178] *Ibid.*

communications données (487.015 C.cr.) et de l'ordonnance de communication — données de transmission (487.016 C.cr.). Ces ordonnances pourraient par exemple être utilisées afin d'identifier un ordinateur accédant au *nuage*, par l'entremise d'une adresse IP particulière, ou encore afin d'obtenir le registre des connexions au *nuage*, avec la date, l'heure et l'appareil ayant été utilisé afin de se connecter.[179]

3.5 Conclusion sur les ordonnances judiciaires applicables

Somme toute, selon la stratégie policière mise de l'avant, les forces de l'ordre sont susceptibles de recourir à diverses autorisations judiciaires, que ce soit séparément ou ensemble. Il se pourrait effectivement que plusieurs autorisations soient nécessaires et pertinentes, par exemple dans le cas où certaines données sont protégées par mot de passe et d'autres non. Malgré tout cela, une constante demeure pour les autorités : l'obligation d'obtenir une autorisation judiciaire préalable, en raison de l'existence d'une attente raisonnable de vie privée visant les données du *nuage* et les métadonnées y étant rattachées.

Devant la multiplication des données se trouvant dans le *nuage*, il est clair que les FSI seront de plus en plus sollicités par l'entremise d'ordonnances de communication diverses. À ce sujet, il est intéressant de noter que l'individu ou l'entreprise qui obtempère à une telle ordonnance ne peut se faire dédommager pour les frais encourus afin de respecter celle-ci.[180]

SECTION 4 — SURVOL DES CONSIDÉRATIONS DE JURIDICTION

Une controverse jurisprudentielle et doctrinale existe actuellement sur l'application extraterritoriale des ordonnances de communication prévues au *Code criminel*. En effet, certains croient que les ordonnances de communication peuvent avoir une portée extraterritoriale, tandis que d'autres prétendent que la communication de telles données doit se faire selon les règles applicables du pays où sont situés les serveurs.

La Cour d'appel de la Colombie-Britannique a jugé qu'une ordonnance générale de communication pouvait être utilisée afin d'obtenir la communication de données détenues par une entreprise américaine n'ayant qu'une présence virtuelle au Canada.[181] Ainsi, l'entreprise américaine *Craigslist* a dû remettre des documents aux autorités canadiennes, en vertu d'une ordonnance générale de communication, bien que l'entreprise ait son siège social en Californie et que l'emplacement géographique exact des données recherchées était inconnu.[182] À l'appui de sa décision, la Cour souligne notamment que le résumé législatif du projet de loi C-13 indique que les diverses ordonnances de communication

---

[179] Josiah Dykstra et Damien Riehl, *supra* note 14 à la p 22.

[180] *Société Télé-Mobile c Ontario*, [2008] 1 RCS 305.

[181] *British Columbia (Attorney General) v Brecknell*, 2018 BCCA 5.

[182] *Ibid* au para 14.

peuvent effectivement être utilisées afin d'obtenir des documents se trouvant dans un autre pays.[183] La Cour retient également que la distinction entre présence physique et présence virtuelle est maintenant illusoire.[184]

Tandis que la Cour d'appel de la Colombie-Britannique a appuyé son raisonnement sur la présence virtuelle du FSI au Canada, une interprétation qui semble être partagée par les auteurs Fontana et Keeshan,[185] le paragraphe 487(2.1) C.cr. a également été interprété comme autorisant des saisies à distance, sur des serveurs se trouvant de l'autre côté de la frontière.[186]
Parallèlement, la Cour fédérale a conclu que des documents accessibles au Canada, mais qui se trouvent dans un autre pays, peuvent être visés par une demande de communication en vertu de la *Loi de l'impôt sur le revenu*.[187] Selon la Cour :

> « [. . .] On ne peut pas vraiment prétendre que ces renseignements "résident" en seul endroit ou qu'ils "appartiennent" à une seule personne. La réalité est que les renseignements peuvent être obtenus facilement et instantanément par les personnes qui font partie du groupe des entités de eBay dans divers endroits. Il importe peu de savoir où se trouvent les renseignements conservés électroniquement et de savoir quelle entité, le cas échéant, par entente ou autrement, revendique la "propriété" de ces renseignements. Ils se "situe[nt] à la fois ici et à l'autre endroit" pour reprendre les mots du juge Binnie au paragraphe 59 de l'arrêt *Société canadienne des auteurs, compositeurs et éditeurs de musique c. Association canadienne des fournisseurs Internet*, [2004] 2 R.C.S. 427. [. . .] »[188]

Cette décision a été confirmée par la Cour d'appel fédérale, qui se demande « [q]ui, après tout, se rend à l'emplacement des serveurs pour lire les renseignements qui y sont stockés ».[189] Les auteurs Halladay et Chad prétendent toutefois que les conclusions de la Cour fédérale et de la Cour d'appel fédérale dans ce dossier ne s'appliquent qu'aux données qui sont utilisées de manière fréquente et usuelle par les employés d'une entreprise, non pas à toutes les données auxquelles ces individus ont accès.[190]

De son côté, la Cour provinciale de Terre-Neuve et Labrador a plutôt conclu que l'ordonnance générale de communication ne pouvait être utilisée pour obtenir les données se trouvant physiquement hors du Canada.[191] Bien que jugeant valides les préoccupations soulevées par les juges de la Colombie-Britannique en ce qui concerne les difficultés d'enquêter sur des crimes ayant une portée extraterritoriale, le juge Gorman a conclu que la disposition ne peut avoir une portée extraterritoriale, en appliquant les enseignements de l'arrêt *Hape*.[192] Selon la Cour, le Parlement aurait dû mentionner expressément que la disposition peut avoir une portée extraterritoriale, si tel était son intention.[193] La Cour semble donc conclure que le recours à la *Loi sur l'entraide juridique en*

---

[183] Julia Nicol et Dominique Valiquet, « Résumé législatif du projet de loi C-13 <

matière criminelle est nécessaire, malgré les problèmes que pose son application.[194]

De la même manière, aux États-Unis, un tribunal a conclu que la communication de données situées sur un serveur en Irlande ne pouvait être autorisée en vertu des lois américaines. Bien que le juge émetteur eût autorisé la communication des données situées en Irlande, au motif que l'entreprise avait contrôle sur les données à partir des États-Unis, ce qui était suffisant afin d'en autoriser la communication en vertu des lois américaines, et non irlandaises,[195] la Cour siégeant en révision a plutôt conclu à l'inverse.[196] Toutefois, une nouvelle loi a depuis été adoptée aux États-Unis, rendant la décision de la Cour siégeant en révision sans objet. En effet, le *Clarifying Lawful Overseas Use of Data Act* (CLOUD Act) prévoit maintenant que les ordonnances judiciaires américaines peuvent être utilisées afin d'obtenir ou de saisir des données situées à l'étranger.[197] Il est intéressant de souligner que plusieurs FSI se sont réjouis de l'adoption de cette loi, tandis que la majorité des groupes de défense des droits des usagers d'Internet se sont plutôt prononcés contre son adoption.[198]

Dans tous les cas, ces questions risquent d'être analysées tôt ou tard par la Cour suprême, ou alors par le législateur canadien, considérant leur importance et le fait que la majorité des grands sites web ne sont pas administrés par des entreprises canadiennes. Les notions de présence virtuelle, de contrôle et d'accès risquent donc d'être importantes dans cette analyse.

CONCLUSION

À travers les années, la Cour suprême a tenté d'adapter les principes généraux applicables aux fouilles, saisies et perquisitions aux réalités contemporaines soulevées par l'arrivée de nouvelles technologies. Toutefois, il semble que cette adaptation ne soit pas entièrement cohérente à certains égards. Il nous semble en effet contradictoire que la Cour suprême reconnaisse d'emblée que les fouilles d'ordinateur soient envahissantes et attentatoires à la vie privée,[199] tandis que les téléphones reçoivent une protection moindre dans le cas

---

[194] *Loi sur l'entraide juridique en matière criminelle*, *supra* note 175.

[195] *In re Warrant to Search a Certain E-mail Account Controlled & Maintained by Microsoft Corp.*, 15 F. Supp. 3d 466 (SDNY 2014).

[196] *In re Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corp.*, 829 F. 3d. 197, 200-01 (2nd Cir. 2016).

[197] *Clarifying Lawful Overseas Use of Data (CLOUD) Act*, H.R. 4943, 115th Cong. (2018).

[198] Aaron Mak, « Congress Put the Controversial CLOUD Act in Its Spending Bill. What Does That Mean For Data Privacy? », *Slate Magazine* (2018), en ligne : *Slate* <slate.com/technology/2018/03/cloud-act-microsoft-justice-department-omnibus-spending-bill.html> (consulté le 20 mai 2018); Mary Jo Foley, « Microsoft bullish on Congress' inclusion of CLOUD Act in funding bill », en ligne: *ZDNet* <www.zdnet.-com/article/microsoft-bullish-on-congress-inclusion-of-cloud-act-in-funding-bill/> (consulté le 20 mai 2018).

[199] *R c Morelli*, *supra* note 5 au para 2.

d'une arrestation, malgré la quantité importante de données auxquelles ils peuvent donner accès.[200] En ce sens, la dissidence de *Fearon*, signée par la juge Karakatsanis, nous semble cadrer davantage avec les décisions précédentes de la Cour suprême lorsqu'il s'agit « de réaliser une mise en équilibre effective et impartiale des objectifs de l'État en matière d'application de la loi et des intérêts des gens au respect de leur vie privée en ce qui concerne leurs ordinateurs personnels ».[201] Malgré cela, les développements récents en cette matière constituent néanmoins un pas dans la bonne direction lorsqu'il s'agit de reconnaître un droit à la vie privée pour les usagers des nouvelles technologies.

Le rejet de l'approche fondée sur le risque par la Cour suprême dans l'arrêt *Duarte* semble au cœur de cette adaptation des anciens principes découlant de l'application de l'article 8 de la *Charte* aux nouvelles réalités du monde virtuel. En effet, cette décision a récemment retrouvé son importance dans l'arrêt *Marakah*, où la majorité a réitéré le fait que le risque qu'un tiers divulgue notre information à l'État n'est pas un élément suffisant afin de nier la protection constitutionnelle contre les fouilles, perquisitions ou saisies abusives.[202] De plus, comme nous l'avons vu, l'arrêt *Duarte* est également central à la reconnaissance d'une attente raisonnable de vie privée envers les données du *nuage*.

Malgré la reconnaissance d'une attente raisonnable de vie privée envers les données situées dans le *nuage*, la protection réelle de ces données est quelque peu amenuisée par les multiples ordonnances judiciaires pouvant être utilisées afin de procéder à leur saisie. En effet, tandis que les données situées dans un ordinateur ne peuvent être obtenues que par mandat de perquisition, les données situées dans le *nuage* peuvent également être obtenues avec des ordonnances de communication, par l'entremise du FSI. Bien que pouvant être décriée, cette multiplication des ordonnances applicables peut également être perçue comme une manière de rétablir la capacité de l'État d'enquêter et d'obtenir de telles données informatiques ; un procédé qui n'est pas sans heurt. En effet, la saisie des données situées dans le nuage est confrontée à plusieurs complications qui n'existent pas dans le monde réel. Mots de passe, cryptage, serveurs situés dans le monde entier. . . tous des éléments qui peuvent ralentir le travail des autorités dans des dossiers déjà complexes. La possibilité de recourir à diverses autorisations judiciaires serait alors une manière de rétablir le droit de l'État de lutter contre la criminalité.

De plus, une fois les données saisies et analysées, les problèmes ne sont pas nécessairement terminés. L'admissibilité en preuve des données du *nuage* n'est pas bien définie à l'heure actuelle.[202] D'abord, l'authenticité de ces données peut être difficile à établir, puisque plusieurs personnes peuvent y accéder, souvent en

---

[200] *R c Fearon*, *supra* note 141.

[201] *Ibid* au para 105, dans la dissidence de la juge Karakatsanis.

[202] *R c Marakah*, *supra* note 79 au para 40.

[202] Voir notamment Kenneth N. Rashbaum, Bennett Borden et Theresa H. Beaumont, « Outrun the Lions: A Practical Framework for Analysis of Legal Issues in the Evolution of Cloud Computing » (2014) 12 Ave Maria L Rev 71 aux pp 98 et suivantes.

simultané. De plus, le *nuage* est un environnement numérique complexe dont l'analyse ne fait pas consensus à travers les différents spécialistes[203]. Pour cette raison et puisqu'il s'agit d'une technologie qui est en constante évolution, la fiabilité du *nuage* peut être sujette à discussion devant les tribunaux.[204]

---

[203] Josiah Dykstra et Damien Riehl, *supra* note 13 aux pp 38 et 43.

[204] Au sujet de la fiabilité des sciences nouvelles, voir *R c J.-L.J.* , [2000] 2 RCS 600; *R c Trochym*, [2007] 1 RCS 239.