

Université de Montréal

**La preuve civile et les interactions avec les assistants  
vocaux, un point de vue comparé**

par Nicolas Thiffault-Chouinard

Faculté de droit

Mémoire présenté

en vue de l'obtention du grade de maître en droit (LL. M.)  
en droit des technologies de l'information et de la communication

Décembre 2019

© Nicolas Thiffault-Chouinard, 2019

# Résumé

Les récents développements de l'intelligence artificielle, de l'Internet des objets et des outils de reconnaissance vocale, couplés à la démocratisation des appareils électroniques de grande consommation et à la couverture Internet étendue maintenant disponible dans plusieurs pays industrialisés, ont permis la mise en marché à grande échelle d'assistants vocaux personnels, qui consistent en des logiciels installés sur différents appareils tels que des téléphones cellulaires et des haut-parleurs connectés permettant aux utilisateurs de ces appareils d'interagir avec ceux-ci au moyen de commandes vocales.

L'adoption de technologies permettant aux utilisateurs d'interagir avec des objets connectés à l'Internet au moyen de leur voix connaît une forte croissance, et celles-ci constitueront bientôt l'un des modes d'interaction privilégiés pour utiliser l'Internet. Considérant la vaste nature des opérations réalisées au moyen de l'Internet en général et de l'Internet des objets en particulier, il convient de se questionner sur la manière de documenter les interactions entre un utilisateur et un assistant vocal.

Le présent mémoire adopte une approche comparant le cadre juridique québécois à différents cadres juridiques avec l'objectif de procéder à une qualification technique et juridique des assistants vocaux et des éléments de preuve en découlant. Dans un second temps, ce mémoire s'intéresse à la recevabilité et à la force probante de ces éléments de preuve dans le contexte du droit civil québécois. L'auteur se penche sur les conditions de recevabilité, discutant de la qualification du document technologique et de ses attributs, notamment ainsi qu'en premier lieu son authenticité et son intégrité et de la proportionnalité. L'auteur discute des exceptions à la recevabilité, soit spécifiquement l'atteinte aux droits fondamentaux et le respect du secret professionnel. Ensuite, l'auteur discute de la force probante de la preuve technologique en avançant que la compréhension de la technologie sous-jacente est l'élément clef dans l'évaluation de la force probante de tout élément de preuve technologique. L'auteur propose que l'intelligence artificielle relève d'une nouvelle catégorie de preuve qui commande peut-être des changements à la procédure et aux principes judiciaires québécois.

**Mots-clefs** : Preuve civile, Internet des objets, Intelligence artificielle, Assistants vocaux, Recevabilité, Qualification, Force probante, Alexa, Siri, Assistant Google

## **Abstract**

Recent developments in the fields of artificial intelligence, of the Internet of Things and of voice recognition, together with the accessibility to electronic devices and wide Internet connection in the industrialized countries, led to the introduction of virtual personal assistants. This software, installed on various devices such as mobile phones and smart speakers, allow their users to interact with these devices using their voice.

As these technologies allow their users to interact with connected devices through the Internet, they will most likely become the main gateway to the Internet in a near future. Considering the great variety of tasks performed with connected devices, the legal questions regarding evidence generated by and collected from their use must now be asked.

First, this master's thesis will compare the normative frameworks of both Quebec and other jurisdictions in order to define, technologically and legally, the virtual personal assistants and the evidence they generate.

In a second time, this thesis will focus on the admissibility and the probative value of the evidence garnered from virtual personal assistants, in the context of Quebec's civilist tradition. The author focuses on the conditions of admissibility and on the designation of technological documents and of their characteristics, analyzing first and foremost the criteria of authenticity and integrity and the questions of proportionality. The author discusses exceptions to admissibility, especially the violation of a fundamental right and privilege considerations. Furthermore, the author discusses the probative value of technological evidence, proposing that the understanding of the underlying technology is a key factor in the determination of the probative value of any technological evidence. Finally, the author suggests that artificial intelligence creates a new category of technological evidence that might be calling for changes in the judicial principles and procedures of the province of Quebec.

**Keywords:** Evidence law, Internet of Things, Artificial intelligence, Virtual personal assistant, Admissibility, Qualification, Probative value, Alexa, Siri, Google Assistant

# Table des matières

Résumé.....	i
Abstract.....	ii
Table des matières.....	iii
Liste des figures .....	v
Liste des sigles .....	vi
Liste des abréviations.....	vii
Remerciements.....	ix
Introduction.....	1
1. La nature technique et juridique des assistants vocaux .....	6
1.1 Une définition technique, juridique et historique de l'intelligence artificielle .....	11
1.1.1 Les algorithmes et l'intelligence artificielle .....	13
1.1.1.1 Une définition technique des algorithmes.....	15
1.1.1.2 Une définition juridique.....	18
1.1.2 La nature des bases de données .....	27
1.1.3 L'Internet des objets – The <i>Internet of Things</i> .....	34
1.1.4 Le traitement automatique des langues — <i>Natural Language Processing</i> .....	38
1.1.5 Compréhension des questions et recherche d'information .....	41
1.1.6 L'Internet comme canal unique de communication.....	46
1.1.6.1 Le rôle du fournisseur d'accès Internet.....	47
1.1.6.2 Le rôle des fabricants et fournisseurs de services.....	49
1.2 Qualification juridique des assistants vocaux et des éléments de preuve découlant de leur utilisation.....	53
1.2.1 L'information en contexte : questions et réponses .....	54
1.2.2 Sous quelle forme la preuve se présente-t-elle ?.....	55
1.2.2.1 Les historiques issus des applications elles-mêmes.....	56
1.2.2.2 Les autres sources d'information .....	64
1.2.3 La nature des moyens de preuve en présence .....	67
1.2.3.1 Une critique de l'approche fonctionnelle.....	72
1.2.3.2 L'approche fonctionnelle appliquée aux éléments de preuve issus de l'utilisation des assistants vocaux .....	74

2. Recevabilité et force probante .....	83
2.1 Conditions de recevabilité.....	85
2.1.1 Circonscrire l’information et son support.....	86
2.1.2 La pertinence de la preuve technologique .....	89
2.1.3 Authenticité et intégrité.....	90
2.1.3.1 Différentes approches relatives à l’intégrité .....	92
2.1.3.2 La documentation, une preuve à propos de la preuve.....	98
2.1.3.3 L’authenticité des éléments matériels de preuve dans le contexte des assistants vocaux.....	101
2.1.4 La proportionnalité.....	104
2.2 Exceptions à la recevabilité .....	111
2.2.1 Atteinte aux droits fondamentaux.....	111
2.2.2 Le secret professionnel .....	118
2.3 La force probante .....	121
2.3.1 La compréhension de la technologie.....	126
Conclusions.....	131
Table de la législation .....	138
Table de la jurisprudence .....	140
Bibliographie.....	143

## Liste des figures

Figure 1.	Interface d'accueil de l'historique de l'assistant vocal Alexa d'Amazon.....	58
Figure 2.	Entrées dans l'historique d'utilisation de l'assistant vocal Alexa d'Amazon....	58
Figure 3.	Accueil de l'historique d'utilisation de l'Assistant Google.....	59
Figure 4.	Détails d'un élément dans l'historique d'utilisation de l'Assistant Google .....	59
Figure 5.	Détails d'un élément dans l'historique d'utilisation de l'Assistant Google .....	60

## Liste des sigles

C.c.Q. : *Code civil du Québec*, L.Q. 1991, c. C-64.

ESI : Electronically Stored Information

FAI : Fournisseur d'accès Internet

IA : Intelligence artificielle

IoT : Internet des objets (*Internet of Things*)

LCCJTI. : *Loi concernant le cadre juridique des technologies de l'information*, RLRQ, c. C-1.1.

LPRPDE : *Loi sur la protection des renseignements personnels et les documents électroniques*, L.C. 2000, c. 5.

## Liste des abréviations

Charte canadienne : *Charte canadienne des droits et libertés*, Partie I de la *Loi constitutionnelle de 1982*, c. 11 (R-U).

Charte québécoise : *Charte des droits et libertés de la personne*, RLRQ, c. C-12

Quatrième amendement : Quatrième amendement de la Constitution des États-Unis d'Amérique (U.S. CONST. amend. IV.)



*À Yves et Pâquerette*

*À la mémoire de Rolland et Angèle*

*À Alexis*

# Remerciements

L'auteur tient à remercier tout particulièrement ses parents, madame Claudine Chouinard et monsieur Luc Thiffault, ainsi que toute sa famille pour leur support et leur aide précieuse tout au long du processus de recherche et de rédaction du présent mémoire.

L'auteur voudrait aussi remercier madame la vice-doyenne Catherine Piché pour sa rétroaction et son support inestimable. Bien avant la rédaction du présent mémoire, la professeure Piché a su insuffler à l'auteur, au cours de son baccalauréat, un intérêt certain pour le droit de la preuve. La professeure Piché a fait preuve de patience et de fermeté dans sa direction. Ses conseils avisés et sages ont rendu possible la présente recherche.

L'auteur désire aussi remercier le professeur Pierre-Claude Lafond. Le professeur Lafond a accepté de recommander la candidature de l'auteur en vue de son admission au programme de maîtrise en droit à l'Université de Montréal. Sans sa recommandation sincère, ces réflexions juridiques n'auraient pas vu le jour sous cette forme. À ce titre, l'auteur tient aussi à remercier le vice-doyen Nicolas Vermeys qui l'a aiguillé dans les premiers balbutiements de sa démarche. Les conseils du professeur Vermeys se sont avérés précieux.

L'auteur doit remercier deux amis qui lui ont offert leur aide en commentant de manière critique et constructive les ébauches de ce mémoire. Sans l'aide de Charles Laplante et Nicolas Pilon le présent mémoire ne serait que l'ombre de lui-même.

Enfin, l'auteur souhaite remercier des proches qui, tout au long de la recherche et de la rédaction, l'ont supporté dans ses efforts, à leur manière : Alexis Brazeau-Bergeron, Sylvie Bergeron, Claude Brazeau, Xavier Desrosiers, Marie-Christine Plouffe, Gabriel Marroco, Laurent Marois, Maxime Leboeuf et Sofia Panaccio.

« Savoir ce que tout le monde sait, c'est ne rien savoir. Le savoir commence là où commence ce que le monde ignore. La vraie science aussi est située au-delà de la science. »<sup>1</sup>

Rémy de Gourmont

---

<sup>1</sup> Rémy de GOURMONT, *Promenades philosophiques*, 10<sup>e</sup> éd., Paris, Mercure de France, 1925, p. 257.

# Introduction

La technologie semble toujours avoir un pas d'avance sur le droit. Dans son premier ouvrage sur le droit des technologies, Vincent Gautrais, professeur à l'Université de Montréal, citait à cet effet Cicéron : « le droit s'arrête là où commence la vérité »<sup>2</sup>. Cette vérité de La Palice est le motif principal soutenant le choix du sujet de ce mémoire : les assistants vocaux.

Les « assistants vocaux » peuvent s'entendre d'au moins deux différents concepts. D'abord, ce terme peut désigner les objets physiques avec lesquels l'utilisateur entre en relation au moyen de la voix. Pensons ici aux téléphones cellulaires, aux ordinateurs ou encore aux haut-parleurs connectés qui écoutent leur environnement en l'attente d'une commande qui déclenchera une action.

Sous une autre perspective, le terme « assistant vocal » peut désigner le programme informatique opérant sur l'ensemble de ces appareils, c'est-à-dire le logiciel lui-même. C'est ce programme d'ordinateur qui permet aux objets connectés de répondre, entre autres choses, à des commandes vocales.

Phénomène aujourd'hui bien réel, les objets parlants occupent une place importante dans notre imaginaire collectif tant par les œuvres de science-fiction que la littérature dystopique<sup>3</sup>. En 2018, il s'est vendu soixante-dix-huit millions de haut-parleurs connectés<sup>4</sup> dans le monde, un chiffre en hausse de 125 %<sup>5</sup> par rapport à l'année précédente. En 2019, selon certaines projections, il y

---

<sup>2</sup> Vincent GAUTRAIS, *Neutralité technologique. Rédaction et interprétation des lois face aux changements technologiques*, Montréal, Éditions Thémis, 2012, p. 2.

<sup>3</sup>Pensons ici à la voix de l'ordinateur embarqué sur le vaisseau *Enterprise* de la série télévisée *Star Trek* ainsi qu'à l'œuvre *1984* de George Orwell où les protagonistes interagissent avec une figure autoritaire au moyen de leurs téléviseurs. À ce sujet, Penelope GREEN, « “Alexa, Where Have You Been All My Life?” », *The New York Times*, sect. Style (20 janvier 2018), en ligne : <<https://www.nytimes.com/2017/07/11/style/alexa-amazon-echo.html>> ; George ORWELL, *1984*, traduit par Amélie AUDIBERTI, Paris, Gallimard, 1993.

<sup>4</sup> Ben STANTON, “Smart speaker market booms in 2018, driven by Google, Alibaba and Xiaomi”, *Canalys Newsroom*, en ligne: <<https://www.canalys.com/newsroom/smart-speaker-market-booms-in-2018-driven-by-google-alibaba-and-xiaomi>>.

<sup>5</sup> *Id.*

aura environ six millions de haut-parleurs connectés au Canada seulement<sup>6</sup>. Une étude de la banque d'investissement affiliée à la Banque Royale du Canada soulevait que 41 % des consommateurs américains possédaient, toujours en 2018, un haut-parleur connecté<sup>7</sup>. Tous les grands joueurs de l'industrie de l'électronique de grande consommation sont présentement engagés dans la course aux *voice tech*.

Si les grands leaders demeurent pour l'instant Amazon et Google, Apple tente de se tailler une place sur le marché avec son produit, le *HomePod*, disponible pour les consommateurs américains depuis 2018<sup>8</sup>. Or, le fabricant ayant connu la croissance la plus rapide en 2018 est Alibaba, le géant chinois de la vente en ligne, qui a lancé en 2017 son propre haut-parleur intelligent le *Tmall Genie*<sup>9</sup>.

Néanmoins, les haut-parleurs connectés ne sont qu'une composante des *voice techs*. Il ne faut pas négliger l'ensemble des autres objets connectés, au nombre desquels les téléphones cellulaires sont les plus nombreux. Au Canada seulement, 87,9 % des ménages ont un abonnement à un service de téléphonie mobile<sup>10</sup>, chaque ménage canadien possédant en moyenne 1,6 appareil mobile<sup>11</sup>. En conséquence, le contrôle des appareils connectés au moyen de la voix est un phénomène en réelle croissance que les juristes doivent considérer, notamment en ce qui a trait au droit de la preuve.

---

<sup>6</sup> John STACKHOUSE, « Hey Alexa, What's Next for Voice Tech? Five Insights into a Voice-First World », *RBC Capital Markets* (2019), en ligne : <<https://bit.ly/2QuH1gP>>; Matthew BRAGA, « What Will the Year Hold for Alexa, Google, Siri and the Smart Speaker Vying for Space in Your Home? », *CBC News* (2019), en ligne : <<https://www.cbc.ca/news/technology/smart-speakers-voice-assistants-2019-google-amazon-apple-1.4966992>>; Jaimie CHUNG et Corey MCNAIR, « Global Smart Speaker Users 2019 », *eMarketer* (2019), en ligne : <<https://www.emarketer.com/content/global-smart-speaker-users-2019>>.

<sup>7</sup> J. STACKHOUSE, préc., note 6 ; RBC CAPITAL MARKETS et Marc HARRIS, *Imagine 2025 - Themes, Opportunities & « The Law of Accelerating Returns »*, Banque Royale du Canada, 2018, p. 19, en ligne : <<https://www.rbccm.com/imagine2025/ai-race.html>>.

<sup>8</sup> Chaim GARTENBERG, « Apple Announces Homepod Speaker to Take on Sonos », *The Verge* (5 juin 2017), en ligne : <<https://www.theverge.com/2017/6/5/15732144/apple-homepod-speaker-announced-siri-price-release-date-wwdc-2017>>; RADIO-CANADA, « Apple sort son enceinte HomePod avec un mois de retard », *Radio-Canada.ca* (24 janvier 2018), en ligne : <<https://ici.radio-canada.ca/nouvelle/1079995/apple-homepod-enceinte-haut-parleur-connecte-commande-vocale-lancement-prevente>>.

<sup>9</sup> Luna LIN, « Chinese Smart Speaker Apps Saw 822% Hike in Installations Last Year », *KrASIA* (6 mai 2019), en ligne : <<https://kr-asia.com/chinese-smart-speaker-apps-saw-822-hike-in-installations-last-year>>.

<sup>10</sup> CRTC, *Communications Monitoring Report 2018*, Ottawa, Conseil de la radiodiffusion et des télécommunications canadiennes, 2018, en ligne : <<https://crtc.gc.ca/eng/publications/reports/policymonitoring/2018/cmrl.htm>>.

<sup>11</sup> *Id.*

La preuve technologique<sup>12</sup> — ou électronique<sup>13</sup> — selon les vocables est un vaste pan du droit de la preuve. Dans le contexte québécois, la preuve technologique s'appuie depuis près de vingt ans sur la *Loi concernant le cadre juridique des technologies de l'information*<sup>14</sup>. Cette loi emprunte un langage dont l'origine est étrangère au droit, étant plutôt tirée du domaine de la bibliothéconomie. La LCCJTI est encore jeune souffre de l'absence d'interprétation jurisprudentielle sérieuse, sauf très récente<sup>15</sup>; moins d'une demi-douzaine d'auteurs se sont intéressés à cette loi depuis son entrée en vigueur<sup>16</sup>. L'approche du législateur québécois à l'égard de la preuve technologique se veut avant tout une mission d'adaptation et d'intégration des concepts issus des technologies de l'information aux règles générales de la preuve, le législateur ayant cherché à introduire la preuve technologique via des catégories existantes<sup>17</sup>. Cette vision est d'ailleurs partagée par le législateur fédéral canadien, qui a pour sa part introduit différentes dispositions dans la *Loi sur la preuve au Canada*<sup>18</sup> ainsi que dans la *Loi sur la protection des renseignements personnels et les documents électroniques*<sup>19</sup>.

Le Québec n'est toutefois pas la seule juridiction à s'être doté d'un cadre législatif en la matière. Dans plusieurs juridictions, notamment aux États-Unis, les législateurs ont légiféré pour soumettre la preuve technologique à un régime particulier<sup>20</sup>. L'exemple des États-Unis présente un intérêt certain dans le cadre d'une approche comparative, puisqu'il y existe des textes encadrant la preuve technologique, tant sur le plan fédéral que sur le plan étatique<sup>21</sup>.

---

<sup>12</sup> Vincent GAUTRAIS, *La preuve technologique*, 2<sup>e</sup> éd., Montréal, LexisNexis, 2018.

<sup>13</sup> Mark PHILLIPS, *La preuve électronique au Québec*, Montréal, LexisNexis, 2010.

<sup>14</sup> *Loi concernant le cadre juridique des technologies de l'information*, RLRQ, c. C -1. 1., ci-après la « LCCJTI »

<sup>15</sup> *Benisty c. Kloda*, 2018 QCCA 608.

<sup>16</sup> Voir entre autres : V. GAUTRAIS, préc., note 12 ; M. PHILLIPS, préc., note 13 ; Gilles DE SAINT-EXUPÉRY, *Le document technologique original dans le droit de la preuve au Québec*, coll. Thèses et mémoires électroniques de l'Université de Montréal, Montréal, Université de Montréal, 2012 ; Pierre TRUDEL, Daniel POULIN et F. ARBAN, *La loi en ligne. La Loi concernant le cadre juridique des technologies de l'information*, Québec, Secrétariat du Conseil du trésor du Québec, 2001, en ligne : <<https://www.tresor.gouv.qc.ca/ressources-informationnelles/cadre-normatif-de-gestion-des-ressources-informationnelles/loi-concernant-le-cadre-juridique-des-technologies-de-linformation/>>.

<sup>17</sup> *Loi sur la protection des renseignements personnels dans le secteur privé*, RLRQ, c. P -39.1.

<sup>18</sup> Voir notamment les articles 31 à 31,8 de la *Loi sur la preuve au Canada*, L.R.C. (1985), c. C -5.

<sup>19</sup> *Loi sur la protection des renseignements personnels et les documents électroniques*, L.C. 2000, c. 5., ci-après la « LPRPDE »

<sup>20</sup> OFFICE OF THE LAW REVISION COUNSEL, *Federal Rules of Evidence*, (2018) United States Code, en ligne: <<https://uscode.house.gov/view.xhtml?path=/prelim@title28/title28a/node218&edition=prelim>>.

<sup>21</sup> L'ensemble des États américains disposant de règles de preuve civile, ce ne sont pas toutes les législations qui adressent directement la preuve technologique.

Partant de ce constat technologique et du cadre juridique en place au Canada, le présent mémoire propose d'effectuer une description de la technologie soutenant les assistants vocaux, de la qualifier en droit, et d'en analyser la recevabilité et la force probante avec l'objectif de vérifier si et comment des informations recueillies par les assistants vocaux lors des interactions de leurs utilisateurs pourraient éventuellement être déposées et acceptées en preuve.

Il sera d'abord question de définir la nature des assistants vocaux, tant sur le plan technique que sur le plan juridique. Une description du fonctionnement des assistants vocaux sera suivie d'une tentative de les qualifier, à l'aune du droit québécois de la preuve civile. Nous nous pencherons sur le fonctionnement des assistants vocaux et les différents acteurs en présence, soit les utilisateurs, les fournisseurs de services et les intermédiaires unissant ces deux premiers, puis nous discuterons du cadre juridique entourant les composantes de l'écosystème dans lequel s'intègrent les assistants vocaux, soit nommément les algorithmes d'intelligence artificielle, les bases de données, l'Internet des objets et les oracles. Dans le cadre de notre tentative de qualification de l'objet juridique que sont les assistants vocaux, nous mettrons l'accent sur la comparaison entre le cadre juridique québécois et les autres cadres juridiques nord-américains et internationaux ainsi que sur l'adéquation entre les catégories juridiques existantes pour qualifier les éléments de preuves et les difficultés qu'apportent les assistants vocaux.

La seconde partie de ce mémoire se penchera sur la recevabilité et la force probante des éléments de preuve issus des interactions des utilisateurs avec les assistants vocaux dans le contexte du droit québécois, mais aussi à l'aune du droit d'autres juridictions. Il sera question des difficultés procédurales et techniques environnant le moment du dépôt en preuve de ce genre d'informations, ainsi que de la réelle signification que peuvent avoir ces éléments au moment d'analyser leur force probante au fond.

L'approche méthodologique ayant guidé la rédaction du présent mémoire est celle du droit comparé. Le droit comparé est « une discipline scientifique qui consiste dans l'étude de la comparaison des droits, c'est-à-dire tant des traditions juridiques [...] ou [des] règles juridiques

qui relèvent des cadres juridiques internes des États »<sup>22</sup>. Il s'agit d'une posture qui cherche à analyser les différences et les similarités entre deux ou plusieurs systèmes juridiques.

Dans le cas présent, nous avons principalement observé les cadres juridiques du droit de la preuve technologique québécois, canadien et américain, sans toutefois nous y limiter, puisque nous nous sommes permis des incursions au sein des cadres juridiques français et, de manière plus générale, européen.

Cette approche descriptive est évidemment empreinte de limites inhérentes à sa nature méthodologique. Elle ne saurait répondre à des questions d'ordre supérieur relativement au bien-fondé des différents systèmes analysés. Or, l'objectif premier de ce mémoire est avant tout de faire état du cadre normatif que les juristes québécois pourraient appliquer aux assistants vocaux dans le contexte de la preuve civile, tout en montrant comment les cadres normatifs étrangers pourraient être source d'inspiration pour traiter de ces questions, présentement inédites pour notre droit.

---

<sup>22</sup> Thierry RAMBAUD, « Introduction générale », dans *Introduction au droit comparé. Les grandes traditions juridiques dans le monde*, coll. Quadriga, Paris, Presses Universitaires de France, 2014, p. 1, par. 17, en ligne : <<https://www.cairn.info/introduction-au-droit-compare--9782130624554-p-1.htm>>.

# 1. La nature technique et juridique des assistants vocaux

Les assistants vocaux ne sont pas que des objets ; ils doivent aussi être compris comme étant des interfaces qui mettent en réseau plusieurs éléments, lesquelles permettent de contrôler l'ensemble des fonctions que l'on associe à un ordinateur. Les assistants vocaux permettent à l'utilisateur de réaliser des actions en effectuant lui-même peu ou pas de manipulations physiques au moyen d'appareils qui, de plus en plus, peuvent verbaliser avec leur utilisateur. Un assistant vocal, pour emprunter un vocabulaire propre au champ de l'intelligence artificielle, est un système multiagent au sein duquel plusieurs agents autonomes prennent des décisions et interagissent entre eux dans un complexe enchevêtrement.

La plupart des chefs de file du domaine des hautes technologies s'intéressent présentement à l'intelligence artificielle, qui peut avoir plusieurs applications. Il suffit ici de se référer à Watson, l'outil d'intelligence artificielle d'IBM<sup>23</sup>, ou encore à ROSS<sup>24</sup>, le robot juriste proposant de remplacer les recherchistes juridiques en effectuant des tâches généralement confiées à de jeunes avocats. Ces outils sont peut-être les plus connus des juristes, mais auprès du grand public, plusieurs autres outils ont été déployés, dont plusieurs assistants vocaux<sup>25</sup>. Le plus connu de ceux-ci est sans doute la personnalité virtuelle Siri, intégrée à l'iPhone depuis sa version 4S, mais auparavant disponible sous la forme d'une application<sup>26</sup>. Depuis 2014, Alexa habite les haut-parleurs connectés proposés par Amazon<sup>27</sup>. Pour sa part, l'assistant Google n'a pas de nom particulier. Microsoft n'est pas sans reste avec son assistant vocal, Cortana, dont l'utilisation se

---

<sup>23</sup> David FERRUCCI, Eric BROWN, Jennifer CHU-CARROLL, James FAN, David GONDEK, *et al.*, "Building Watson. An Overview of the DeepQA Project", (2010) 31-3 *AI Magazine* 59.

<sup>24</sup> Karen TURNER, "Meet 'ross,' the Newly Hired Legal Robot", *The Washington Post*, sect. Innovations (16 mai 2016), en ligne : <[https://www.washingtonpost.com/news/innovations/wp/2016/05/16/meet-ross-the-newly-hired-legal-robot/?noredirect=on&utm\\_term=.dd58a8d9bf5](https://www.washingtonpost.com/news/innovations/wp/2016/05/16/meet-ross-the-newly-hired-legal-robot/?noredirect=on&utm_term=.dd58a8d9bf5)>.

<sup>25</sup> Ava MUTCHLER, « A Timeline of Voice Assistant and Smart Speaker Technology From 1961 to Today », *Voicebot* (28 mars 2018), en ligne : <<https://voicebot.ai/2018/03/28/timeline-voice-assistant-smart-speaker-technology-1961-today/>>.

<sup>26</sup> Bianca BOSKER, « Siri Rising. The Inside Story of Siri's Origins And Why She Could Overshadow the iPhone », *The Huffington Post* (22 janvier 2013), en ligne : <[https://www.huffingtonpost.com/2013/01/22/siri-do-engine-apple-iphone\\_n\\_2499165.html](https://www.huffingtonpost.com/2013/01/22/siri-do-engine-apple-iphone_n_2499165.html)>; Jan L JACOBOWITZ et Justin ORTIZ, « Happy Birthday Siri! Dialing in Legal Ethics for Artificial Intelligence, Smartphones, and Real Time Lawyers », (2018) 4-5 *Texas A&M Journal of Property Law* 408.

<sup>27</sup> P. GREEN, préc., note 3.



fait au travers de l'interface du système d'exploitation Windows 10, ainsi que sur les différentes versions mobiles des appareils vendus par Microsoft, tels l'ordinateur portable Surface<sup>28</sup>.

Pour comprendre les assistants vocaux, il est important de s'attarder à l'écosystème sous-jacent puisqu'il revêt une importance capitale dans leur fonctionnement. En premier lieu, les assistants vocaux reposent sur un ensemble d'algorithmes qui permettent de fournir à l'utilisateur des réponses et déclencher des suites d'actions. Le développement des algorithmes fait appel à la recherche opérationnelle, une branche des mathématiques. Les assistants vocaux peuvent faire appel à plusieurs algorithmes, tant pour décoder la voix des personnes que pour répondre à leur demande en analysant leur question. Un algorithme fonctionne, comme nous le verrons, au moyen d'une base de données. Son action consiste essentiellement à tenter de faire des comparaisons entre l'interrogation de l'utilisateur et les éléments de sa base de données. Parmi ces algorithmes, certains ont une importance déterminante pour le fonctionnement des assistants vocaux ; ce sont ceux qui permettent à l'assistant de reconnaître la voix de l'utilisateur. Ces algorithmes permettent de transformer la voix — information sonore — en commande intelligible pour un ordinateur, c'est-à-dire en texte clair. Cette première étape fait appel à ce que l'on nomme le traitement automatique des langues, le *natural language processing*.

Une fois l'information rendue intelligible pour l'interface, celle-ci peut accomplir plusieurs tâches de nature très différentes, grâce à l'interconnexion d'une pluralité de services virtuels, la toile globale de ces échanges portant le nom « Internet des objets » ou *Internet of Things*<sup>29</sup>. L'IoT n'est toutefois pas un phénomène dépendant du développement des assistants vocaux ; les assistants peuvent supporter des applications qui n'entrent pas dans le giron de l'IoT, et l'IoT est à l'inverse partiellement constitué des échanges entre les logiciels respectifs d'un grand nombre d'objets connectés n'ayant aucun point en commun avec les Siri de ce monde. Ainsi, bien que l'IoT se développe de manière concurrente aux assistants vocaux, il s'agit d'une réalité

---

<sup>28</sup> Robert LANG et Lenore BENESSERE, “Alexa, Sirt, Btxby, Google’s Assistant, and Cortana Testifying in Court”, (2018) 74-1 *Journal of the Missouri Bar* 20.

<sup>29</sup> Ci-après « IoT »

plus large impliquant un grand nombre d'interactions entre machines<sup>30</sup> — désignées *machine-to-machine* ou *M2M* — qui échappent complètement aux utilisateurs, la plupart du temps<sup>31</sup>.

Toutefois, l'un des points communs entre les assistants vocaux et l'IoT en général est le fait qu'ils reposent tous deux sur une connexion Internet. Véritables réseaux à l'intérieur du grand réseau qu'est l'Internet<sup>32</sup>, les objets connectés communiquent entre eux et avec leurs utilisateurs au moyen d'un accès à l'Internet<sup>33</sup>. Encore, les objets connectés que l'on contrôle avec la voix communiquent avec des systèmes distants — sur lesquels fonctionnent le plus souvent leurs algorithmes — au moyen d'une connexion au Web.

Toute l'opération n'a donc pas lieu à l'intérieur du téléphone ou du haut-parleur connecté. En fait, à l'heure actuelle, la technologie est conçue de sorte que l'information recueillie par l'objet connecté voyage entre celui-ci et les serveurs du fournisseur de service. Dans le cas de Siri, l'assistant vocal développé et mis en marché par Apple, l'information est redirigée vers leurs serveurs :

« More specifically, Siri encodes your speech and transforms it into a compact digital form that is swiftly transmitted via cellular signals to Internet service providers who then send it to a cloud-based remote server. Once the encoded speech is on the server, the speech is analyzed and evaluated to determine the proper response to such a command. If the command cannot be 'handled on the phone ... [and] the server is needed it will compare your speech with a databased model to estimate what letters might constitute it. The server then uses the highest-probability estimate to proceed.' »<sup>34</sup>

(Références omises ; notre soulignement)

---

<sup>30</sup> Shin-Yeh TSAI et Sok-Ian SOU, "Effects of Data Aggregation in M2M Networks", dans *Internet of Things and M2M Communications*, Algade, River Publishers, 2013, p. 3.

<sup>31</sup> Margaret ROUSE, « What is Machine-to-Machine (M2M)? », *IoT Agenda* (août 2019), en ligne : <<https://internetofthingsagenda.techtarget.com/definition/machine-to-machine-M2M>>.

<sup>32</sup> Lu TAN et Neng WANG, *Future internet. The Internet of Things, 2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE)*, 2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), 5, août 2010, p. V5-376-V5-380.

<sup>33</sup> Qusay F. HASSAN, *Internet of Things A to Z. Technologies and Applications*, Hoboken, John Wiley & Sons, 2018, en ligne: <<https://onlinelibrary.wiley.com/doi/book/10.1002/9781119456735>>.

<sup>34</sup> Corinne MOINI, « Protecting Privacy in the Era of Smart Toys. Does Hello Barbie Have a Duty to Report? », (2017) 25-2 *Cath. U. J. L. & Tech* 281, 293.

C'est donc dire que le fournisseur d'accès Internet<sup>35</sup> ou encore le fournisseur de connexion cellulaire — celui qui fournit à l'utilisateur la connexion au Web — a techniquement connaissance de l'ensemble de ce qui circule sur son infrastructure ou, à tout le moins, du volume et de la fréquence de ces échanges.

La capacité du FAI à intercepter la substance de l'information qui voyage entre l'utilisateur et le fournisseur de services doit être nuancée, la plupart des données étant cryptées<sup>36</sup>, comme nous le rappellent l'auteure Moïni et les conditions d'utilisations de la plupart des services disponibles sur le marché<sup>37</sup>. Parmi ceux-ci figure notamment Siri de Apple, cette dernière se targuant d'assurer un cryptage bout-en-bout sur plusieurs de ses services<sup>38</sup>. Il faut donc dire qu'à défaut d'être présents dans la pièce, les FAI sont des témoins passifs privilégiés de certains aspects de nos interactions avec les assistants vocaux, au même titre que notre utilisation conventionnelle d'Internet.

Les assistants vocaux résultent de la mise en relation de plusieurs systèmes complexes. Ils se présentent néanmoins comme un tout ; une porte d'entrée universelle pour interagir avec tous nos objets connectés. Ils sont, tout à la fois, une nouvelle façon de naviguer sur Internet, une manière de contrôler différents objets de notre quotidien, une manière d'entrer en communication avec les autres et même, dans certains cas, l'outil par lequel certains contrats se forment.

---

<sup>35</sup> Ci-après « FAI ».

<sup>36</sup> C. MOINI, préc., note 34.

<sup>37</sup> Voir entre autres les conditions d'utilisation des services Alexa d'Amazon, à lire en conjonction avec les conditions d'utilisation générales et la déclaration de confidentialité d'Amazon ainsi que les conditions d'utilisation des produits Google, dont fait partie l'Assistant Google : AMAZON.COM, INC., « Alexa Terms of Use », *Amazon.com* (0614 2019), en ligne : <<https://www.amazon.com/gp/help/customer/display.html?nodeId=201809740>> ; AMAZON.COM, INC., « Privacy Notice », *Amazon.com* (29 août 2017), en ligne : <[https://www.amazon.com/gp/help/customer/display.html?nodeId=468496#GUID-1B2BDAD4-7ACF-4D7A-8608-CBA6EA897FD3\\_SECTION\\_277A1D99140544EE9259ACA749AE3C3D](https://www.amazon.com/gp/help/customer/display.html?nodeId=468496#GUID-1B2BDAD4-7ACF-4D7A-8608-CBA6EA897FD3_SECTION_277A1D99140544EE9259ACA749AE3C3D)> ; AMAZON.COM, INC., « Conditions of Use », *Amazon.com* (21 mai 2018), en ligne : <<https://www.amazon.com/gp/help/customer/display.html/?nodeId=508088>> ; GOOGLE, « Google Terms of Service », *Google Privacy & Terms* (25 octobre 2017), en ligne : <<https://policies.google.com/terms?hl=en-US>>.

<sup>38</sup> APPLE, « Présentation de la sécurité iCloud », *Apple Support* (3 juillet 2019), en ligne : <<https://support.apple.com/fr-ca/HT202303>>.

Leur utilisation a donc inévitablement des implications juridiques. Pour pouvoir les utiliser, il faut d'abord accepter les conditions imposées par leurs fabricants, ceux qui développent les différents services sous-jacents à l'ensemble des composantes en faisant partie. Le consentement donné au moment d'inviter ces objets dans nos demeures peut faire l'objet des mêmes critiques que l'on sert de manière générale au consentement donné pour les services en ligne. L'utilisateur qui le donne n'en comprend pas forcément toutes les nuances, puisque les contrats véhiculant ces conditions brillent d'inintelligibilité du fait de leur complexité et de leur longueur. Malgré que cela puisse constituer une source de vices au consentement, ce mémoire ne portera pas sur l'invalidité des « termes et conditions » entourant les assistants vocaux, puisque la jurisprudence et la doctrine à ce sujet tendent, pour l'instant, à en confirmer la validité<sup>39</sup>, sujet à ce qu'elles respectent d'autres formalités qui ne nous sont pas d'intérêt ici.

Ensuite, il faut considérer ce que l'on fait au moyen des assistants vocaux et les traces que nous laissons dans cet écosystème aux multiples facettes. Ces traces, en particulier, seront l'objet de nos discussions. L'information étant conservée par les différents fournisseurs de services pour l'amélioration continue de leurs produits, il convient de se demander si celle-ci serait accessible au justiciable souhaitant l'utiliser devant un tribunal. Nous nous pencherons sur la nature de cette information, sur la manière de l'extraire et sur les caractéristiques de son essence.

---

<sup>39</sup> *Dell Computer Corp. c. Union des consommateurs*, 2007 CSC 34.

## 1.1 Une définition technique, juridique et historique de l'intelligence artificielle

L'intelligence artificielle est un champ d'études qui existe depuis déjà un certain temps. Ce champ se trouve au carrefour des domaines de l'informatique, des mathématiques et des neurosciences, et est né de la jonction des percées scientifiques issues de ceux-ci. Depuis plus de trente ans déjà, on discute notamment de l'influence de l'intelligence artificielle sur le droit<sup>40</sup>. S'il apparaît conséquent de situer la naissance de l'intelligence artificielle au développement des premiers ordinateurs dans les années 1940<sup>41</sup>, la propension de l'être humain à vouloir créer des machines pensantes remonte sans doute à aussi loin que la fabrication d'automates par les horlogers et les joailliers du dix-huitième siècle<sup>42</sup>, le plus célèbre étant sans doute le Turc de Wolfgang von Kempelen<sup>43</sup> qui — ironiquement — dessinait déjà les limites de l'intelligence artificielle puisqu'il faisait appel à un être humain en chair et en os pour manipuler un mannequin jouant aux échecs. Il s'agissait d'une supercherie. La véritable confrontation entre l'homme et la machine, sur ce terrain, aura lieu plus tard, en 1996, lorsque l'ordinateur Deep Blue développé par IBM aura raison du champion d'échec de l'époque Garry Kasparov<sup>44</sup>.

---

<sup>40</sup> Voir à ce sujet l'excellent florilège de cinquante textes issus des treize premières conférences de l'*International Conference on AI and Law* : Trevor BENCH-CAPON, Michał ARASZKIEWICZ, Kevin ASHLEY, Katie ATKINSON, Floris BEX, *et al.*, « A History of Ai and Law in 50 Papers. 25 Years of the International Conference on Ai and Law », (2012) 20-3 *Artif Intell Law* 215.

<sup>41</sup> Bruce G. BUCHANAN, « A (Very) Brief History of Artificial Intelligence », (2005) 26-4 *AI Magazine* 53, 54.

<sup>42</sup> C'est d'ailleurs l'une des inspirations qu'évoque Adam Cheyer, l'un des créateurs de Siri dans un article de Danielle NEWNHAM, « The Story Behind Siri », *The Startup* (1<sup>er</sup> novembre 2015), en ligne : <<https://medium.com/swlh/the-story-behind-siri-fbeb109938b0>>.

<sup>43</sup> Jeff BARR et Luis Felipe CABRERA, « AI Gets a Brain », (2006) 4-4 *Queue* 24, 24 ; Mark SUSSMAN, « Performing the Intelligent Machine. Deception and Enchantment in the Life of the Automaton Chess Player », (1999) 43-3 *The Drama Review* 80, 83.

<sup>44</sup> Bruce PANDOLFINI, *Kasparov and Deep Blue. The Historic Chess Match Between Man and Machine*, New York, Simon and Schuster, 1997, p. 7 ; FENG-HSIUNG HSU, « IBM's Deep Blue Chess grandmaster chips », (1999) 19-2 *IEEE Micro* 70, 70.

Déjà, René Descartes<sup>45</sup>, dans son *Discours de la méthode*, posait une frontière au sein du vivant, entre les personnes et les animaux, considérant ces derniers comme des machines<sup>46</sup>. Cette théorie mécaniste, chez Descartes, souscrit à l'idée incidente supposant que les êtres humains ne sont pas des machines, car ils seraient doués d'une âme<sup>47</sup>. L'approche mécaniste sera par la suite reprise par La Mettrie<sup>48</sup> qui, rejetant le dualisme proposé par Descartes, avançait qu'il était possible de schématiser l'ensemble des pensées humaines et que l'homme n'était qu'un animal exceptionnellement intelligent.

Cette frontière imaginée par Descartes entre l'homme et l'animal, machine créée par Dieu, la science n'a cessé de vouloir la confondre. Les plus récents développements nous poussent à croire que l'intelligence artificielle pourrait bien *être* à force de *penser*. Toutefois, tant d'anthropomorphisme serait peut-être fallacieux, car si l'intelligence artificielle est le domaine de la science qui fait le plus parler actuellement, c'est parce qu'une conjoncture bien particulière se développe depuis une décennie.

Nous évoluons à l'ère des données<sup>49</sup>, laquelle se caractérise par la collecte et la classification informatisée systématique et à grande échelle d'informations, de telle manière qu'il est

---

<sup>45</sup>Buchanan évoque notamment Descartes brièvement dans son article : B. G. BUCHANAN, préc., note 41, 53.

<sup>46</sup> Descartes discute de ce sujet dans la cinquième partie de son ouvrage publié en 1637. La version consultée pour ce mémoire est celle proposée par le CÉGEP de Trois-Rivières, en accès libre : René DESCARTES, *Discours de la méthode*, Trois-Rivières, Les Échos du Maquis, 2011, p. 34 à 36, en ligne : <<https://philosophie.cegeptr.qc.ca/wp-content/documents/Discours-de-la-m%C3%A9thode.pdf>>.

<sup>47</sup> Une idée que Descartes explique dans le *Discours sur la méthode*, à la quatrième partie intitulée : « Preuves de l'existence de Dieu et de l'âme humaine ou Fondements de la métaphysique », voir à ce sujet : *Id.*, p. 22 et suivantes.

<sup>48</sup> La version en accès libre sur la plateforme Wikisource de l'ouvrage de La Mettrie a été consultée dans le cadre de la recherche liée à ce mémoire : Julien Offray de LA METTRIE, *L'homme machine*, Leyde, Elie Luzac fils, 1748, en ligne : <[https://fr.wikisource.org/wiki/L%E2%80%99Homme\\_Machine](https://fr.wikisource.org/wiki/L%E2%80%99Homme_Machine)>.

<sup>49</sup> Au sujet du « Big Data Era », plusieurs sources révèlent, dès le début des années 2010, l'intérêt marqué des milieux d'affaires pour les potentiels de ces développements technologiques. Un des exemples les plus convaincants est celui de la vente de livres en ligne : « Once shopping moved online, though, the understanding of customers increased dramatically. Online retailers could track not only what customers bought, but also what else they looked at; how they navigated through the site; how much they were influenced by promotions, reviews, and page layouts; and similarities across individuals and groups. Before long, they developed algorithms to predict what books individual customers would like to read next—algorithms that performed better every time the customer responded to or ignored a recommendation » dans Andrew MCAFEE et Erik BRYNJOLFSSON, « Big Data. The Management Revolution », *Harvard Business Review* (1 octobre 2012), en ligne : <<https://hbr.org/2012/10/big-data-the-management-revolution>>; Viktor MAYER-SCHÖNBERGER et Kenneth CUKIER, *Big Data. A Revolution that Will Transform how We Live, Work, and Think*, New York, Houghton Mifflin Harcourt, 2013; Steve LOHR, « Big Data's Impact in the World », *The New York Times*, sect. Opinion (11 février 2012), en ligne : <<https://www.nytimes.com/2012/02/12/sunday-review/big-datas-impact-in-the-world.html>>.

aujourd'hui possible de « nourrir » les modèles mathématiques développés dans le domaine de l'intelligence artificielle ; c'est l'abondance de matériel informationnel qui permet le développement des applications pratiques comme les assistants vocaux. Nous sommes les témoins privilégiés d'un moment favorable dans l'histoire de la technique.

Pour comprendre les assistants vocaux, nous croyons justifié de traiter de l'intelligence artificielle dans son ensemble, en passant en revue quelques-unes de ses composantes primaires, c'est-à-dire les algorithmes, les bases de données, les oracles et dans le cas qui nous intéresse spécifiquement, le traitement automatique des langues.

### **1.1.1 Les algorithmes et l'intelligence artificielle**

Avant de tenter l'élaboration d'une définition technique et juridique de l'intelligence artificielle, expliquons brièvement ce qui se passe dans une enceinte connectée ou dans un téléphone muni d'un assistant comme Siri. Dans un tel appareil se trouvent des composantes physiques — le matériel informatique, ou *hardware*. Au sens du droit canadien, il s'agira là d'un ordinateur, lequel est défini de manière très large, notamment par le droit pénal<sup>50</sup>. Cet ordinateur est commandé par une multitude de logiciels, ou *software*. Le *software* commande les activités du *hardware*, instruisant à ses composantes la séquence suivant laquelle les tâches, constituées d'opérations mathématiques et logiques, doivent être effectuées.

---

<sup>50</sup> Le droit pénal canadien définit de manière très large l'ordinateur de sorte qu'à l'aune du droit pénal canadien, les enceintes connectées satisfont les critères suffisant pour être qualifiées, soit d'être un dispositif contenant un programme d'ordinateur et exécutant des fonctions logiques ou de commande conformément à ce programme. Voir à ce sujet : *Code criminel*, L.R.C. (1985), c. C -46, art. 342.1 (2), par. 8.

De l'extérieur, il peut être ardu de segmenter l'ensemble de ces étapes, mais l'agent de brevet Thierry Orlhac y est parvenu dans ce que nous considérons comme étant une description limpide, bien que datée :

« D'un point de vue pratique, un programme consiste généralement en une séquence d'instructions contrôlant l'opération d'un matériel d'informatique, telle qu'un ordinateur ou une machine équipée de circuits logiques, d'interfaces d'entrée et de sortie de données, de mémoire et d'un microprocesseur. Une telle séquence d'instructions, une fois "écrite", doit être "traduite" et enregistrée sur un support approprié pour que l'ordinateur ou la machine soit en mesure de l'interpréter.

Un logiciel peut ainsi être souvent représenté sous la forme d'un simple algorithme, ce mot se définissant dans le Petit Larousse comme une "suite finie d'opérations élémentaires constituant un schéma de calculs ou de résolutions d'un problème".

On peut immédiatement noter qu'il y a un problème ici. Si un logiciel consiste uniquement en une suite d'étapes effectuées dans un ordre donné pour résoudre un problème mathématique, cela équivaut à un calcul mathématique spécifiquement exclu de la brevetabilité selon l'article 27 (3) de la [*Loi sur les brevets*]. »<sup>51</sup>

(Références omises ; notre soulignement)

L'impossibilité que soulève l'auteur à ce moment de breveter — à première vue — les algorithmes est une position qu'il s'affaire à nuancer dans les pages suivant son introduction, à un article datant de 1995, dans lequel on trouve déjà toutes les questions auxquelles nous sommes confrontés aujourd'hui, non plus au sujet des logiciels, mais bien des algorithmes d'intelligence artificielle. Notons que depuis, la disposition de la *Loi sur les brevets* citée par

---

<sup>51</sup> On peut aussi considérer une récente définition de l'intelligence artificielle apportée par Gaon et Stedman : « What differentiates various conceptions of AI is the way in which particular systems are initially set up in order to go about accomplishing their 'cognitive' work. In most cases, current AI systems require human input for their creation. Once operational, however, they become capable of performing calculations and solving complex problems without necessary ongoing human supervision. ». Aviv GAON et Ian STEDMAN, « A Call to Action. Moving Forward with the Governance of Artificial Intelligence in Canada », (2019) 56-4 *Alta. L. Rev.* 1137, 3. Voir à ce sujet : Thierry ORLHAC, *La brevetabilité des logiciels*, Robic, agents de brevets et de marques de commerce, 1995, p. 3, en ligne : <<https://www.robic.ca/wp-content/uploads/2017/05/166-TOR.pdf>> ;



l'auteur a été remplacée<sup>52</sup> et il n'est plus aussi explicite que des algorithmes en soient exclus, même si c'est la posture généralement défendue<sup>53</sup>.

### 1.1.1.1 Une définition technique des algorithmes

Le présent mémoire ne saurait avoir la prétention d'expliquer les mathématiques et la science derrière les algorithmes d'intelligence artificielle, mais nous tentons néanmoins d'expliquer un tant soit peu leur fonctionnement<sup>54</sup>. L'Office québécois de la langue française définit l'algorithme comme une « séquence de règles opératoires exécutées sur des données et qui permettent l'obtention d'un résultat »<sup>55</sup>. Il s'agit donc ni plus ni moins d'un protocole que l'on applique à une matière — des données — afin d'en tirer des conclusions basées sur des tests mathématiques simples, comme la proximité avec la moyenne<sup>56</sup>. De cette manière, au moyen d'une grande base de données, les algorithmes peuvent répondre à certaines questions. Par exemple, ils peuvent classer des éléments dans une liste, créer des sous-groupes ou établir le degré de ressemblance entre un élément et les éléments d'une liste<sup>57</sup>.

---

<sup>52</sup> La référence spécifique aux calculs mathématiques a été remplacée par un énoncé général excluant la brevetabilité des « simples principes scientifiques ou conceptions théoriques », voir à ce sujet : *Loi sur les brevets*, L.R.C. (1985), c. P-4, art. 27 (8).

<sup>53</sup> Éric LAVALLÉE, « La propriété intellectuelle de l'intelligence artificielle », *Lavery* (5 octobre 2017), en ligne : <<https://www.lavery.ca/fr/publications/nos-publications/3037-la-propriete-intellectuelle-de-lintelligence-artificielle.html>>.

<sup>54</sup> Pour un ouvrage se penchant plus en profondeur sur l'intelligence artificielle et les algorithmes, nous suggérons de consulter l'ouvrage de Stuart J. RUSSELL et Peter NORVIG, *Intelligence artificielle*, 3e éd., Paris, Pearson Éducation, 2010 ; Nick BOSTROM, *Superintelligence. Paths, Dangers, Strategies*, Oxford, Oxford University Press, 2014 ; Nathan ENSMENGER, *The Computer Boys Take Over. Computers, Programmers, and the Politics of Technical Expertise*, coll. « History of Computing », Cambridge, MIT Press, 2010 ; Klaus SCHWAB, *The Fourth Industrial Revolution*, 1<sup>re</sup> éd., New York, Crown Business, 2016 ; Nils J. NILSSON, *The Quest for Artificial Intelligence. A History of Ideas and Achievements*, Cambridge, Cambridge University Press, 2010.

<sup>55</sup> OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE, *Grand dictionnaire terminologique*, Québec, Publications du Québec, 2018, v° « Algorithme », en ligne : <[http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id\\_Fiche=8367804](http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=8367804)>.

<sup>56</sup> Notamment la méthode des  $k$  plus proches voisins. Voir à ce sujet l'article : Naomi S. ALTMAN, « An Introduction to Kernel and Nearest Neighbor Nonparametric Regression », (1992) 46-3 *Am. Stat.* 175.

<sup>57</sup> Au sujet des applications de l'intelligence artificielle, voir notamment : Kevin WARWICK, *Artificial Intelligence. The Basics*, Londres, Routledge, 2013, en ligne : <<https://www.taylorfrancis.com/books/9780203802878>> ; G. M. P. O'HARE et N. R. JENNINGS, *Foundations of Distributed Artificial Intelligence*, John Wiley & Sons, 1996 ; Kazuo TANAKA, *An Introduction to Fuzzy Logic for Practical Applications*, New York, Springer, 1997.

Mis en relation avec des réseaux de neurones artificiels, les algorithmes peuvent se dire « d'apprentissage ». Un neurone artificiel consiste, pour sa part, en un modèle mathématique à l'image du neurone humain. Son rôle est de « convertir les signaux porteurs d'information [reçus] en un signal unique [transmis] à d'autres unités du réseau ou [dirigé] vers la sortie »<sup>58</sup>. Dans ce cas, le rôle de l'algorithme consiste à modifier le réseau de neurones afin d'améliorer ses performances, un phénomène que l'on décrit comme l'entraînement ou l'apprentissage. L'apprentissage peut être supervisé, semi-supervisé ou non supervisé<sup>59</sup>.

C'est la conjonction d'un réseau de neurones artificiels et d'un algorithme que l'on associe le plus souvent à « l'intelligence artificielle », dans le contexte actuel. Or, il existe d'autres approches pour schématiser la prise de décisions à partir de données. L'une d'entre elles, qui a grandement bénéficié des développements des mathématiques et de l'informatique, est l'arbre de décision<sup>60</sup>. Un arbre de décision se compose de nœuds qui interrogent les données entrantes pour les diriger vers une solution en les faisant passer à un nœud subséquent dans l'arbre en fonction de la réponse à un nombre limité de questions, par exemple « oui ou non »<sup>61</sup>.

---

<sup>58</sup> OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE, *Grand dictionnaire terminologique*, Québec, Publications du Québec, 2017, v<sup>o</sup> « Neurone artificiel », en ligne : <[http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id\\_Fiche=8385900](http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=8385900)> ; Ivan Nunes DA SILVA, Danilo Hernane SPATTI, Rogerio Andrade FLAUZINO, Luisa Helena BARTOCCI LIBONI et Silas Franco DOS REIS ALVES, *Artificial neural networks*, New York, Springer, 2016, en ligne : <<https://link.springer.com/content/pdf/10.1007/978-3-319-43162-8.pdf>> ; Marcel VAN GERVEN et Sander BOHTE, « Artificial Neural Networks as Models of Neural Information Processing », (2017) 11 *Front. Comput. Neurosci.* 114; XIN YAO, “Evolving Artificial Neural Networks”, (1999) 87-9 *Proceedings of the IEEE* 1423.

<sup>59</sup> On peut notamment consulter sur ce sujet : Zahangir ALOM, Tarek M. TAHA, Christopher YAKOPCIC, Stefan WESTBERG, Paheding SIDIKE, Shamima NASRIN, Brian C. VAN ESESN, Abdul A. S. AWWAL et Vijayan K. ASARI, « The History Began from AlexNet. A Comprehensive Survey on Deep Learning Approaches », *ArXiv* 2018.arXiv:1803.01164, en ligne : <<http://arxiv.org/abs/1803.01164>> ; Ethem ALPAYDIN, *Introduction to Machine Learning*, Cambridge, MIT Press, 2009; Yoshua BENGIO et Aaron COURVILLE, « Neural Network Architectures », dans Monica BIANCHINI et Marco MAGGINI, *Handbook on Neural Information Processing*, 1<sup>re</sup> éd., coll. « Intelligent Systems Reference Library », n° 49, New York, Springer, 2013, en ligne : <<https://link.springer.com/content/pdf/10.1007/978-3-642-36657-4.pdf>>; Yoshua BENGIO, “Learning Deep Architectures for AI”, (2009) 2-1 *Foundations and Trends in Machine Learning* 1; Sotiris KOTSIANTIS, « Supervised Machine Learning. A Review of Classification Techniques », dans I. MAGLOGIANNIS, *Emerging Artificial Intelligence Applications in Computer Engineering*, Amsterdam, IOS Press, 2007; Fabrizio SEBASTIANI, « Machine Learning in Automated Text Categorization », (2002) 34-1 *ACM Comput. Surv.* 1.

<sup>60</sup> J. R. QUINLAN, « Induction of Decision Trees », (1986) 1-1 *Mach. Learn* 81; Stéphane CARON, « Une introduction aux arbres de décision », *Stéphane Caron* (31 août 2011), en ligne : <<https://scaron.info/doc/intro-arbres-decision/intro.pdf>>.

<sup>61</sup> S. CARON, préc., note 60, p. 2 à 3.

Il est aussi possible de représenter un arbre de décision dans un algorithme mathématique et de l'automatiser de cette manière. Ces systèmes ont cependant davantage vocation à effectuer un classement des données qu'à répondre à des questions en tant que telles<sup>62</sup>. Mis en relation avec d'autres approches, comme la schématisation des neurones, l'arbre de décision permet la matérialisation des agents autonomes<sup>63</sup> que nous connaissons aujourd'hui.

Une fois entraîné, un algorithme peut permettre de répondre à des questions. Il peut, par exemple, établir le degré de ressemblance entre deux images numériques — elles-mêmes décomposables en pixels — et les associer à des catégories. Les applications pratiques de l'intelligence artificielle sont nombreuses, et celles-ci sont à la fois source de problèmes et de solutions dans plusieurs domaines, le droit n'étant que l'un d'entre eux<sup>64</sup>. Toutefois, l'entraînement peut aussi être continu et se poursuivre simultanément à la collecte de données et la production de résultats. Il s'agit alors d'un phénomène que l'on nomme l'« apprentissage automatique »<sup>65</sup>.

---

<sup>62</sup> S. R. SAFAVIAN et D. LANDGREBE, « A Survey of Decision Tree Classifier Methodology », (1991) 21-3 *IEEE Transactions on Systems, Man, and Cybernetics* 660, 1 à 2.

<sup>63</sup> L'agent autonome est un agent, définit par l'OQLF comme une « entité physique ou virtuelle capable de percevoir son environnement et d'agir sur lui » qui est à même de « [déterminer] lui-même ses actions et son état interne, sans l'intervention d'un tiers », voir à cet effet : OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE, *Grand dictionnaire terminologique*, Québec, Publications du Québec, 2018, v° « Agent autonome », en ligne : <[http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id\\_Fiche=8395061](http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=8395061)> ; OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE, *Grand dictionnaire terminologique*, Québec, Publications du Québec, 2018, v° « Agent », en ligne : <[http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id\\_Fiche=8395061](http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=8395061)>.

<sup>64</sup> Le domaine où les applications pratiques de l'intelligence artificielle pourraient être les plus prometteuses est peut-être la médecine, mais l'intelligence artificielle peut aussi permettre d'améliorer, par exemple, l'occupation du territoire ou encore, dans le domaine financier, les fluctuations des marchés. Nous ne pouvons non plus passer sous silence les possibles applications militaires de l'intelligence artificielle. Pour poursuivre la réflexion relativement aux applications de l'intelligence artificielle : Fei JIANG, Yong JIANG et Hui ZHI, « Artificial Intelligence in Healthcare. Past, Present and Future », (2017) 2-4 *Stroke Vasc Neurol* 230 ; Ning WU et Elisabete A. SILVA, « Artificial Intelligence Solutions for Urban Land Dynamics. A Review », (2010) 24-3 *J. Plan. Lit* 246 ; Ilias G. MAGLOGIANNIS, *Emerging Artificial Intelligence Applications in Computer Engineering. Real Word AI Systems with Applications in EHealth, HCI, Information Retrieval and Pervasive Technologies*, Amsterdam, IOS Press, 2007 ; Paul J. SPRINGER, *Military Robots and Drones. A Reference Handbook*, Santa Barbara, ABC-CLIO, 2013.

<sup>65</sup> Voir à ce sujet : OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE, *Grand dictionnaire terminologique*, Québec, Publications du Québec, 2017, v° « Apprentissage automatique », en ligne : <[http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id\\_Fiche=8395061](http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=8395061)>.

### 1.1.1.2 Une définition juridique

Les algorithmes peuvent être compris comme des expressions mathématiques complexes et pourraient être considérés comme des œuvres au sens du droit de la propriété intellectuelle canadien<sup>66</sup>, s'ils offrent plus que l'expression d'une simple idée et constituent un réel programme d'ordinateur<sup>67</sup>. En effet, à l'image des logiciels, les algorithmes pourraient éventuellement être protégés en tant qu'œuvre littéraire<sup>68</sup>. Cette protection a été établie en droit canadien par l'arrêt de la Cour suprême *Apple Computer, Inc. c. Mackintosh Computers Ltd*<sup>69</sup>, à une époque où l'intelligence artificielle occupait toutefois une place moins prépondérante dans la société et le quotidien des utilisateurs.

Les algorithmes ne disposent cependant pas, sous le régime canadien, d'autres protections légales que celle, difficilement exécutoire, du droit d'auteur. Par exemple, ils sont difficilement brevetables dans le contexte nord-américain<sup>70</sup>, car ils ne constituent pas une invention en tant que telle, puisqu'ils se rapprochent de la recette ou du protocole plutôt que de l'objet fini. L'avocat Éric Lavallée écrivait en 2017, au sujet de la brevetabilité de l'intelligence artificielle :

« Au Canada, la jurisprudence n'a pas encore traité de cas spécifique aux systèmes d'intelligence artificielle. Par contre, nul doute que les principes dégagés par la Cour d'appel fédérale dans la décision *Schlumberger Canada Ltd. c. Commissaire des brevets* demeurent pertinents. Dans cette affaire, il a été décidé qu'un procédé permettant de recueillir, d'enregistrer et d'analyser des données à l'aide d'un ordinateur qui appliquait alors une formule mathématique ne pouvait faire l'objet d'un brevet. Par contre, dans une décision plus récente, la Cour en est venue à la conclusion qu'un procédé informatique pourrait être brevetable s'il "[...] ne constitue pas l'invention entière, mais seulement un

---

<sup>66</sup> La *Loi sur le droit d'auteur* canadienne prévoit explicitement que les « programmes d'ordinateur » sont assimilés à des œuvres littéraires, voir à cet effet : *Loi sur le droit d'auteur*, L.R.C. (1985), c. C-42, art. 2, al. 34.

<sup>67</sup> *Id.*, art. 2, al. 47.

<sup>68</sup> La protection de l'intelligence artificielle en tant qu'objet de droit d'auteur est l'avenue la plus sûre envisagée par l'avocat Éric Lavallée dans le contexte d'un billet de blogue publié sur le site web du cabinet montréalais Lavery lequel a développé une expertise en intelligence artificielle depuis 2017 avec le lancement d'un laboratoire juridique sur l'intelligence artificielle, L3IA. Voir à ce sujet : É. LAVALLÉE, préc., note 53.

<sup>69</sup> *Apple Computer, Inc. c. Mackintosh Computers Ltd.; Apple Computer, Inc. c. 115,778 Canada Inc.*, [1990] 2 RCS 209.

<sup>70</sup> *Alice Corp. v. CLS Bank Int'l*, [2014] 573 U.S. 208.

élément essentiel parmi d'autres dans une nouvelle combinaison.”<sup>71</sup> Il est donc à prévoir qu'un algorithme d'intelligence artificielle pris isolément ne pourra faire l'objet d'un brevet. »<sup>72</sup>

(Notre soulignement, références partiellement omises)

Lavallée expose par la suite que l'on peut aussi protéger l'intelligence artificielle au moyen du secret industriel et que de tels procédés peuvent faire l'objet d'ententes de confidentialité, mais que cette dernière avenue présente des risques, comme le fait que soient révélées par un employé malveillant certaines informations cruciales. Il expose que ce genre d'information appelle donc des mesures particulières de protection, comme la segmentation de l'information.

Ne perdons cependant pas de vue que l'intelligence artificielle est le résultat de l'interaction entre un algorithme et une base de données, elle-même une œuvre au sens des cadres juridiques nord-américains de la propriété intellectuelle<sup>73</sup>. Le droit d'auteur pourrait donc être une avenue intéressante pour définir juridiquement l'intelligence artificielle. Par exemple, dans le contexte où le produit de l'intelligence artificielle est aussi conservé dans une base de données, la question de savoir si cette nouvelle base de données se qualifie comme objet de droit d'auteur dépendra du fonctionnement de l'algorithme en question<sup>74</sup>.

S'il a été « entraîné » par un opérateur, il sera relativement vraisemblable de croire qu'il y aura là une part de « jugement et de talent »<sup>75</sup>, éléments nécessaires à la création d'une œuvre au sens du droit d'auteur canadien. Toutefois, si l'algorithme est dit « d'apprentissage automatique » et que les résultats qu'il produit sont strictement basés sur des tests statistiques, la qualification est incertaine puisqu'il n'y a peut-être pas d'originalité ni d'auteur<sup>76</sup>. Si le droit d'auteur continental

---

<sup>71</sup> La décision que Lavallée mentionne dans l'extrait cité est la suivante : *Canada (Procureur général) c. Amazon.com*, 2 RCF 459 (CAF).

<sup>72</sup> É. LAVALLÉE, préc., note 53, p. 1.

<sup>73</sup> *Loi sur le droit d'auteur*, préc., note 66, art. 2, al. 8.

<sup>74</sup> Dans un contexte canadien, cette nuance prend un sens particulier. Voir : É. LAVALLÉE, préc., note 53, p. 3.

<sup>75</sup> *CCH Canadienne Ltée c. Barreau du Haut-Canada*, 2004 CSC 13, par. 28.

<sup>76</sup> Rappelons que la doctrine de l'effort ou « sweat of the brow » n'est pas admise en droit canadien ni en droit américain. La complexité ayant mené au développement de l'algorithme ayant produit certains éléments susceptibles de protection ne serait donc pas pertinente dans l'analyse relative au droit d'auteur. Voir entre autres : *Feist Publications, Inc., v. Rural Telephone Service Co.*, [1991] 499 U.S. 340; *Tele-Direct (Publications) Inc. c. American Business Information*, [1998] 134 FTR 80 (CAF).

peut éprouver de la difficulté à considérer comme une œuvre l'objet résultant d'un algorithme d'intelligence artificielle, les différents régimes de « copyright » de tradition anglo-saxonne, comme celui ayant cours aux États-Unis, lesquels sont souvent fortement marqués par leur contractualisme, pourraient avoir la flexibilité nécessaire pour permettre la protection des produits de l'intelligence artificielle.

Dans le cas qui nous concerne, le questionnement relatif à la personne pouvant éventuellement tirer bénéfice de l'utilisation de l'algorithme en question, ou de l'outil d'intelligence artificielle qui en découle, le cas échéant, n'est pas superflu à nos yeux, car il permet d'identifier qui devrait être saisi des demandes éventuelles touchant des questions d'intégrité des données. En effet, sur le plan du droit de la preuve, un algorithme d'intelligence artificielle nourrissant lui-même la base de données au sein de laquelle il puise pour générer des réponses, sans intervention humaine, est susceptible de produire des résultats auxquels les créateurs de l'algorithme – ou de la base de données initiale – n'ont pas forcément pu penser.

En revanche, si l'on pose l'hypothèse qu'une base de données construite par des êtres humains est moins susceptible de faire en sorte que les algorithmes d'intelligence artificielle utilisant ces données produisent des résultats absolument inattendus<sup>77</sup>, une autre avenue devient alors possible. D'un point de vue strictement pragmatique, cette avenue offre la possibilité d'interroger une personne pour obtenir plus de précisions sur le fonctionnement de l'algorithme en question<sup>78</sup>. Dans ce scénario, une preuve testimoniale pourrait permettre la preuve de l'intégrité du fonctionnement d'un algorithme. Cette preuve pourrait être pertinente dans la mesure où, par exemple, on tentait de démontrer qu'un algorithme a « commis une erreur »,

---

<sup>77</sup> Ce qui est cependant une hypothèse fragile et facilement contredite. Il suffit de penser aux biais inhérents véhiculés par la science et le langage, sujets dont nous discuterons ci-après dans ce mémoire. Voir notamment : Fayyaz MINHAS, Amina ASIF et Asa BEN-HUR, « Ten Ways to Fool the Masses with Machine Learning », *ArXiv* 2019.arXiv:1901.01686, en ligne : <<http://arxiv.org/abs/1901.01686>>.

<sup>78</sup> Encore, ce genre de témoignage pourrait facilement susciter une certitude non fondée, même auprès d'experts. En effet, le champ de l'apprentissage machine traverse présentement une crise au niveau de la reproductibilité des expériences scientifiques et de l'utilisation de langage complexe dans la diffusion des recherches les plus récentes. Ce genre de failles peut donner l'impression que l'état de la science est plus avancé qu'il ne l'est réellement, tel que l'illustrent avec humour certains auteurs : *Id.*, 6 et 8.

c'est-à-dire qu'il a souffert d'un dysfonctionnement ayant altéré les résultats qu'il a proposés à son utilisateur<sup>79</sup>.

Dans un autre spectre d'idées, un riche débat a actuellement cours en ce qui a trait à la qualification de l'intelligence artificielle en tant qu'ensemble. Certains, en effet, vont jusqu'à proposer d'attribuer une personnalité juridique<sup>80</sup> à l'intelligence artificielle ; d'autres encore tentent de mettre en garde les juristes afin d'éviter que ceux-ci ne tombent dans le piège de l'anthropomorphisme<sup>81</sup>, c'est-à-dire l'association entre la machine et les caractéristiques de la personne humaine.

Si l'on propose que l'intelligence artificielle soit considérée comme une personne et dispose de ce fait de la personnalité juridique, certains demeurent farouchement opposés à cette idée<sup>82</sup>. Si celle-ci peut paraître à première vue des plus saugrenues, les juristes qui rejetteraient du revers de la main cette approche sans même y réfléchir ne feraient que briller par leur hypocrisie lorsque dans leur pratique ils accepteraient que par pure fiction des êtres humains aient pu

---

<sup>79</sup>Dans la mesure où le droit québécois prévoit certaines présomptions, il ne sera pas forcément nécessaire, pour la mise en preuve d'éléments issus d'un outil d'intelligence artificielle, de faire la preuve du bon fonctionnement de cet outil dans un contexte de transmission d'informations. Cela pourrait cependant présenter un certain intérêt pour contredire les présomptions en place et tenter de faire la preuve de l'absence d'intégrité. Cependant, le dysfonctionnement des algorithmes est absurdemment difficile à démontrer. Certains programmes pourraient éventuellement effectuer cette tâche, mais le réel risque pourrait se situer en amont, dans la qualité des données utilisées par l'algorithme. Voir notamment à ce sujet : Federico CABITZA, Davide CIUCCI et Raffaele RASOINI, « A Giant with Feet of Clay. On the Validity of the Data That Feed Machine Learning in Medicine », dans *Organizing for the Digital World*, New York, Springer, 2018, p. 121-136, en ligne : <[https://link.springer.com/content/pdf/10.1007%2F978-3-319-90503-7\\_10.pdf](https://link.springer.com/content/pdf/10.1007%2F978-3-319-90503-7_10.pdf)>; Vineeth KASHYAP, Jason RUCHTI, Lucja KOT, Emma TURETSKY, Rebecca SWORDS, Shih An PAN, Julien HENRY, David MELSKI et Eric SCHULTE, « Automated Customized Bug-Benchmark Generation », *ArXiv* 2019.arXiv:1901.02819, en ligne : <<http://arxiv.org/abs/1901.02819>>.

<sup>80</sup>Jiahong CHEN et Paul BURGESS, « The Boundaries of Legal Personhood. How Spontaneous Intelligence Can Problematiser Differences Between Humans, Artificial Intelligence, Companies and Animals », (2019) 27-1 *AI & L* 73-92; Ugo PAGALLO, « Vital, Sophia, and Co. The Quest for the Legal Personhood of Robots », (2018) 9-9 *Information* 230; Kamil MUZYKA, « The Outline of Personhood Law Regarding Artificial Intelligences and Emulated Human Entities », (2013) 4-3 *Journal of Artificial General Intelligence* 164.

<sup>81</sup>Andrew BURT, "Leave A.I. Alone", *The New York Times*, sect. Opinion (4 janvier 2018), en ligne : <<https://www.nytimes.com/2018/01/04/opinion/leave-artificial-intelligence.html>>.

<sup>82</sup>*Id.*; Matt SCHERER, « Is AI personhood already possible under U.S. LLC laws? », *Law and AI* (14 mai 2017), en ligne : <<http://www.lawandai.com/2017/05/14/is-ai-personhood-already-possible-under-current-u-s-laws-dont-count-on-it-part-one/>>.

accorder la personnalité juridique à la société par actions<sup>83</sup>. Ces propositions méritent donc que l'on s'y attarde afin de les évaluer au mérite.

Les propositions qui existent en ce moment ne sont pas à l'effet d'accorder une personnalité à l'égale de celle des êtres humains, ce qui ne serait pas forcément souhaitable par ailleurs, selon nous. En dehors du droit de la preuve, dans le champ du droit de la responsabilité civile, la chercheuse Iria Giuffrida<sup>84</sup> a d'ailleurs recensé quatre postures face à la question de la personnalité et de l'intelligence artificielle, soit la posture prônant l'octroi d'une forme de personnalité pour l'intelligence artificielle, la posture du « Leave AI Alone », la posture du « Robot Common Sense » et enfin la posture soutenant que les solutions reposent sur de nouvelles règles potentiellement en dehors du droit.

La posture du « Leave AI Alone » découle essentiellement de l'éditorial d'Andrew Burt, à l'effet que le droit a suffisamment d'outils pour adresser les problématiques naissant de l'intelligence artificielle. Burt soutient essentiellement que l'intelligence artificielle est difficile à définir et que la réglementer pourrait produire des effets néfastes :

« 'Artificial intelligence' is all too frequently used as a shorthand for software that simply does what humans used to do. But replacing human activity is precisely what new technologies accomplish—spears replaced clubs, wheels replaced feet, the printing press replaced scribes, and so on. What's new about AI is that this technology isn't simply replacing human activities, external to our bodies; it's also replacing human decision-making, inside our minds.

The challenges created by this novelty should not obscure the fact that AI itself is not one technology, or even one singular development. Regulating an assemblage of technology, we can't clearly define is a recipe for poor laws and even worse technology. »<sup>85</sup>

Les propos de Burt, alors ingénieur et *Chief Privacy Officer* pour une entreprise américaine œuvrant dans le domaine des technologies de l'information s'apparente, dans une certaine

---

<sup>83</sup> Voir entre autres à ce sujet le commentaire suivant de l'arrêt Elizabeth POLLMAN, « Reconceiving Corporate Personhood », *Utah L. Rev.* 2011.4.1629, 1636.

<sup>84</sup> Iria GIUFFRIDA, « Liability Risk for Artificial Intelligence Predictive Decision-Making », (2019) 88 — (Soumis pour publication) *Fordham L. Rev.*

<sup>85</sup> A. BURT, préc., note 81.



mesure, à la posture dite du « Robot Common Sense » où le droit actuel doit être réinterprété afin de permettre d'appliquer les règles existantes à de nouvelles situations<sup>86</sup>. Il y a ensuite la posture voulant que l'on attribue la personnalité à l'intelligence artificielle afin d'y appliquer l'ensemble des cadres juridiques existants. Certains d'ailleurs croient que c'est déjà une avenue possible à l'heure actuelle<sup>87</sup>. Enfin, il y a la posture prônant l'adoption de nouvelles règles conçues spécialement pour l'intelligence artificielle, retenant essentiellement la position de à l'égard des nouvelles technologies qui rappelle les propos de Lawrence Lessig<sup>88</sup>.

Néanmoins, rappelons que la personnalité juridique est un concept variable et modulable. Certains attributs de la personnalité pourraient en effet se retrouver chez certaines formes d'intelligence artificielle. Pensons par exemple à la créativité que l'on pourrait reconnaître chez certains agents autonomes, sous réserve de comprendre leur fonctionnement réel et accepter que le hasard puisse être source de créativité. Encore, l'habileté à « penser », comprise comme la capacité à mettre en relation de l'information<sup>89</sup> pourrait être considérée comme une caractéristique propre à une personne. Bref, se questionner sur les caractéristiques composant la personnalité peut faire l'objet d'un long débat qui n'est pas le but de l'exercice auquel nous voulons nous livrer ici.

Toutefois, l'attribution de la personnalité juridique à un assistant vocal — lui-même un agent autonome dont l'autonomie est assurée par une forme d'intelligence artificielle — n'est pas sans conséquence dans un contexte de preuve. Cela pourrait avoir deux effets particuliers, tant sur le plan de la qualification que sur le plan de la recevabilité — ce dont nous discuterons plus loin.

---

<sup>86</sup> Le concept est expliqué par Giuffrida : « With 'robot common sense' we refer not only to the legal system adapting concepts such as reasonableness and foreseeability to capture the nuances brought in by AI and new technologies, but also to our expectation that an AI system will 'update' its common sense by 'learning' from external input. » Voir I. GIUFFRIDA, préc., note 84, 11 citant ; Harry SURDEN et Mary-Anne WILLIAMS, "Technological Opacity, Predictability, and Self-Driving Cars", 38 *Cardozo L. Rev.* 62.

<sup>87</sup> Voir notamment les travaux du professeur Bayern qui défend dans un article que les lois de certains États américains sur la formation de *Limited Liability Company* sans membre (*zero-member LLC*) puissent permettre l'octroi du statut de *manager* à une intelligence artificielle. Shawn BAYERN, "Are Autonomous Entities Possible?", (2019) 114-23 *Northwestern University Law Review Online*, en ligne: <<https://papers.ssrn.com/abstract=3410395>> Voir aussi ; M. SCHERER, préc., note 82.

<sup>88</sup> Lawrence LESSIG, « The Law of the Horse. What Cyberlaw Might Teach », (1999) 113-2 *Harv. L. Rev.* 501 ; Voir aussi : Frank H. EASTERBROOK, "Cyberspace and the Law of the Horse", (1996) 166-1 *U. Chi. Legal F.* 207.

<sup>89</sup> *Le Petit Larousse illustré*, v<sup>o</sup> « Penser », en ligne : <<https://www.larousse.fr/dictionnaires/francais/penser/59268>>.

En premier lieu, cela pourrait modifier le type d'éléments de preuve avec lequel le juriste aurait à composer. Si l'intelligence artificielle n'est qu'un objet, nous ne sommes en présence ni plus ni moins que d'un microphone, dans le cas des assistants vocaux. S'il s'agit d'une personne au sens de la loi, le même élément de preuve pourrait alors devenir un témoignage<sup>90</sup>.

Il y a cependant un grand nombre de nuances à apporter ici. La preuve testimoniale d'une personne morale n'est pas directement assimilable au témoignage d'une personne physique. Encore, la personne morale, comme la conçoit actuellement le droit civil, est intimement liée à une ou plusieurs personnes physiques, les administrateurs. Ce sont d'ailleurs eux qui prennent la parole au nom de la personne morale dans une instance judiciaire au Québec<sup>91</sup>. Dans ce contexte, la possibilité d'octroyer une forme de personnalité juridique à l'intelligence artificielle semble moins pertinente, considérant que cela ne serait pas forcément d'un grand secours à l'étape de la qualification de la preuve. Parallèlement, dans ces circonstances, la protection de la vie privée poserait d'ailleurs d'importantes questions, lesquelles ont déjà fait couler beaucoup d'encre dans le contexte américain<sup>92</sup> où des règles concernant les garanties constitutionnelles protégeant les confidences faites à un proche n'ont pu être appliquées, puisqu'Alexa n'est dans les faits qu'un microphone qui répond à son utilisateur.

En second lieu, accorder la personnalité juridique à un agent autonome « mu » par l'intelligence artificielle constitue, pour certains, une dérive trouvant initialement son origine dans le langage. Il est vrai qu'il s'agit là d'une forme certaine d'anthropomorphisme qui consiste à utiliser des qualificatifs humanisants à l'endroit d'objets inanimés. Le mot « intelligence » ou encore

---

<sup>90</sup>L'article 2843 du C.c.Q. prévoyant explicitement que le témoignage émane d'une personne, il y a lieu de penser que certaines preuves ne se qualifiant pas comme telles pourraient être considérées comme des témoignages si la chose qui le produisait devenant éventuellement une personne. Cela ne signifie pas qu'accorder la personnalité juridique aux assistants vocaux ferait de l'ensemble de la preuve qu'ils peuvent produire des témoignages, surtout en considérant l'approche fonctionnelle dont nous discuterons plus loin dans le présent mémoire. Voir à ce sujet : *Code civil du Québec*, L. Q. 1991, c. C-64, art. 2843.

<sup>91</sup> Voir entre autres : *Code de procédure civile*, RLRQ, c. C -25.01, art. 224.

<sup>92</sup> Voir entre autres les récents articles suivants : Sarah AITCHISON, « Privacy in the Cloud. The Fourth Amendment Fog », (2018) 93 *Wash. L. Rev.* 1019; Susan ALLEN, « Privacy in the Twenty-First Century Smart Home », (2018) 19 *JHTL* 162 ; Allison S BOHM, Edward J GEORGE, Bennett CYPHERS et Shirley LU, « Privacy and Liberty in an Always-on, Always-Listening World », (2017) 19-1 *Colum. Sci. & Tech. L. Rev.* 1; Christopher BURKETT, « 'I Call Alexa to the Stand'. The Privacy Implications of Anthropomorphizing Virtual Assistants Accompanying Smart-Home Technology », (2018) 20 *Vand. J. Ent. & Tech. L.* 1181; Anne LOGSDON SMITH, « Alexa, Who Owns My Pillow Talk? Contracting, Collateralizing, and Monetizing Consumer Privacy Through Voice-Captured Personal Data », (2018) 27-1 *Cath. U. J. L. & Tech* 187.

« apprentissage » sont des caractéristiques que l'on associe généralement aux êtres humains ou — à tout le moins — aux êtres vivants.

L'anthropomorphisme en tant que tactique peut aussi prendre d'autres formes, par exemple dans le champ de la robotique où l'on remarque le développement de robots à l'apparence humaine — avec des yeux, des mains, des bras, une tête — afin de faciliter leurs interactions avec les utilisateurs<sup>93</sup>. Dans ce cas de figure, de la même manière qu'en présence d'un vocabulaire humanisant, les objectifs peuvent être louables — par exemple, faciliter les interactions entre l'utilisateur et le produit — toutefois, ils peuvent concurremment mener à un certain aveuglement.

Le fait d'utiliser des qualificatifs propres aux êtres humains en conjonction avec ce qui n'est fondamentalement qu'un programme d'ordinateur permettant à une expression mathématique complexe d'interagir avec une grande quantité de données organisées dans un ensemble donne à cet objet — l'intelligence artificielle — une apparence d'humanité. Cette apparence feinte ne doit pas nous détourner de la nature artificielle et purement matérielle de ces outils<sup>94</sup>.

Ce phénomène est particulièrement vrai en ce qui concerne les agents conversationnels, puisque ceux-ci sont l'une des matérialisations les plus près de l'être humain que peuvent être des agents autonomes. Rares sont ceux qui se méprennent à la vue d'un véhicule autonome ; il s'agit bel et bien d'une voiture. Cependant, au son de la voix d'Alexa ou de Siri, il y a là une résonance de plus en plus près de la nature humaine, ce qui peut pousser les gens à parler à ces objets comme ils parlent à des êtres humains — ce pour quoi ils sont d'ailleurs conçus.

Leurs noms, « assistants vocaux » ou « assistants virtuels » et le fait qu'on leur ait donné des noms propres — Alexa ou encore Siri — montrent à quel point le vocable que l'on utilise pour désigner quelque chose occupe une grande importance dans notre relation avec cet objet<sup>95</sup>.

---

<sup>93</sup> Brian R. DUFFY, "Anthropomorphism and the Social Robot", (2003) 42-3 *Robotics and Autonomous Systems* 177.

<sup>94</sup> Comme le faisait entendre la Cour suprême du Canada en 1990, à propos des composantes d'un ordinateur « [i]l faut plutôt [les] considérer [...] comme la réalisation d'un ensemble d'instructions en langage machine qui ont pour fonction de transmettre des données et d'accomplir d'autres opérations précises. », voir : *Apple Computer, Inc. c. Mackintosh Computers Ltd.; Apple Computer, Inc. c. 115 778 Canada Inc.*, préc., note 69.

<sup>95</sup> Voir à ce sujet le chapitre de l'ouvrage intitulé *On Naming Things* où l'auteure discute de la terminologie en archéologie et de son importance sur la perception de cette discipline : M. R. KLEINDIENST, "On Naming Things",

Là est le premier écueil, car en oubliant la réelle nature des assistants vocaux, l'utilisateur oublie souvent la relation de droit qui l'unit réellement à ces assistants vocaux et leurs fabricants, soit une relation où toute l'information qu'ils partagent — sans gêne, comme avec une véritable personne — est soumise à un enchevêtrement complexe de contrats d'adhésion auxquels on consent sans trop réfléchir et au risque, comme dans le contexte américain, de renoncer à certaines protections constitutionnelles<sup>96</sup>.

Le second écueil serait, selon nous, de nous méprendre sur le plan du droit de la preuve au sujet de la nature des données recueillies par ces objets. Le droit de la preuve ne peut souffrir de l'influence indue du langage lorsque vient le temps de qualifier juridiquement ce qu'on lui présente. Les historiques d'utilisation de ces appareils présentent, d'une part, de l'information recueillie par des capteurs et des micros et d'autre part ; les résultats de l'analyse statistique de données issues d'une base de données.

Il serait, à notre avis, dangereux d'y voir autre chose que les résultats d'interactions entre un être humain et une machine, en conservant en tête les limitations découlant de ce constat, soit que la machine est faillible, qu'elle peut reproduire des biais remontant à la période même de sa conception et qu'à l'instar de tout objet, elle ne peut pas être appelée à témoigner afin d'expliquer à la Cour sa version des faits.

---

dans Erella HOVERS et Steven L. KUHN (dir.), *Transitions Before the Transition. Evolution and Stability in the Middle Paleolithic and Middle Stone Age*, coll. « Interdisciplinary Contributions To Archaeology », Boston, Springer, 2006, p. 13.

<sup>96</sup> S. AITCHISON, préc., note 92 ; A. LOGSDON SMITH, préc., note 92 ; S. SICARI, A. RIZZARDI, L. A. GRIECO et A. COEN-PORISINI, « Security, Privacy and Trust in Internet of Things. The Road Ahead », (2015) 76 *Comput. Netw.* 146.

## 1.1.2 La nature des bases de données

Les bases de données consistent en de grands ensembles de données organisés et structurés<sup>97</sup>. Il ne s'agit donc pas ici d'informations éparses, recueillies sans précaution et de manière aléatoire, mais plutôt d'informations — de données — liées entre elles par un point commun. Par exemple, une base de données pourrait se composer d'images d'animaux, ou plus précisément d'images de chiens. La classification et l'étiquetage revêtent une grande importance dans la constitution d'une base de données, qu'elle soit informatique ou non. L'importance que l'on accorde à l'information n'aurait aucune valeur réelle s'il nous était impossible de donner une signification à cette information, comme l'expliquent Davison et ses coauteurs dans un ouvrage traitant de la protection juridique des bases de données :

« The economies of the First World are dominated by the creation, manipulation and use of information and the time it takes to do so. These economies do not suffer from a shortage of information; they suffer from the difficulties associated with collecting, organising, accessing, maintaining and presenting it. Databases are designed to help deal with these difficulties. They are collections of information arranged in such a way that one or more items of information within them may be retrieved by any person with access to the collection containing those items. »<sup>98</sup>

(Notre soulignement ; références omises)

Dans leur ouvrage paru il y a déjà une quinzaine d'années, les auteurs mettaient alors l'accent sur les différents aspects sociaux et économiques entourant le développement et l'accès aux bases de données, soulignant à grands traits que celles-ci ne soulèvent pas uniquement des interrogations sur le plan des affaires, mais aussi de la gouvernance et du droit<sup>99</sup>.

---

<sup>97</sup> OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE, *Grand dictionnaire terminologique*, Québec, Publications du Québec, 2005, v° « Base de données », en ligne : <[http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id\\_Fiche=8355656](http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=8355656)>.

<sup>98</sup> Mark J. DAVISON, W. R. CORNISH, François DESSEMONTET, Paul GOLDSTEIN et Robin JACOB, *The Legal Protection of Databases*, Cambridge, Cambridge University Press, 2003, p. 43.

<sup>99</sup> *Id.*, p. 3.

La notion d'assistant vocal est, pour sa part, relativement nouvelle en comparaison du concept de base de données. Pour assurer le fonctionnement des assistants vocaux — ou de toute autre technologie faisant appel au traitement automatique des langues — on peut imaginer que plusieurs bases de données sont convoquées.

D'abord, il y a une base de données composée de sons, d'extraits audio ou d'échantillons de voix, nécessaires aux algorithmes de traitement automatique des langues, mais aussi, concurremment, nécessaires aux agents conversationnels qui tenteront de s'exprimer verbalement à l'attention de l'utilisateur. Parallèlement, il y a aussi les bases de connaissances, un type particulier de base de données. Elles sont nécessaires pour répondre aux questions des utilisateurs<sup>100</sup> par le contenu informationnel duquel il s'enquiert.

Du point de vue juridique, les bases de données dont nous venons de discuter — et celles qui pourraient par la suite être interpellées par l'interaction entre les agents autonomes — peuvent constituer des œuvres au sens du droit d'auteur canadien dans une certaine mesure<sup>101</sup>. Ces œuvres sont protégées par le droit d'auteur au Canada et sont généralement la propriété de ceux qui les créent, et ce, même si l'information dont elles sont constituées est souvent le fruit de la divulgation des renseignements personnels des utilisateurs des outils d'intelligence artificielle, notamment les assistants vocaux. Ce paradoxe a poussé certains<sup>102</sup> à s'interroger sur la propriété des données dans le contexte de la collecte systématique des renseignements personnels.

Au regard du droit civil québécois, les banques de données sont assimilées à des documents, dans la mesure où leur structure permet de créer des documents en les interrogeant<sup>103</sup>. Une base

---

<sup>100</sup> Nous discuterons davantage des bases de connaissances au sein de la sous-section 1.1.5 « Compréhension des questions et recherche de l'information ».

<sup>101</sup> Entre autres choses, elles peuvent être considérées comme des compilations. Or, les bases de données, pour être des « œuvres », doivent aussi correspondre aux autres critères reconnus par le droit canadien, notamment l'originalité. Ainsi, il n'est pas certain que toutes les bases de données soient protégées par le droit d'auteur ou du moins que leur contenu le soit de manière aussi intégrale que pourrait l'être celui d'autres compilations, comme les recueils poétiques, par exemple. Voir à ce sujet : Normand TAMARO, *Loi sur le droit d'auteur, texte annoté*, 10<sup>e</sup> éd., Toronto, Carswell, 2015, sect. 2.

<sup>102</sup> Pierre TRUDEL, *Propriété ou liberté, La nécessité de faire revivre un débat initié il y a 30 ans*, Montréal, Centre de recherche en droit public, Entre propriété et liberté. 30 ans de protection des données personnelles, 6 novembre 2018, en ligne : <<https://www.youtube.com/watch?v=l70rPHvWdMo>>.

<sup>103</sup> *Loi concernant le cadre juridique des technologies de l'information*, préc., note 14, art. 3, al. 2.

de données sur un support faisant appel aux technologies de l'information<sup>104</sup> est donc, par conséquent, un document technologique<sup>105</sup>.

En droit européen, les bases de données sont notamment protégées par la Directive européenne de 1996 concernant à la protection juridique des bases de données<sup>106</sup>. Cette directive protège les bases de données en créant pour celles-ci un droit *sui generis* beaucoup plus étendu que la protection dont elles jouissaient auparavant<sup>107</sup> sous les différents régimes juridiques continentaux. La protection dont bénéficient les « fabricants »<sup>108</sup> des bases de données regroupe à la fois les critères de l'originalité et de l'effort<sup>109</sup>, conférant une protection qui n'a que peu de limites. La directive européenne propose que la base de données consiste en un :

« [R] ecueil d'œuvres, de données ou d'autres éléments indépendants, disposés de manière systématique ou méthodique et individuellement accessible par des moyens électroniques ou d'une autre manière »<sup>110</sup>

(Notre soulignement)

Tel que l'illustre le texte de cette directive qui s'applique sur le territoire européen, les bases de données n'ont pas forcément à être des œuvres, tant qu'elles se composent de données et que leur fabrication, pour reprendre le langage de la directive, a nécessité des ressources monétaires ou intellectuelles.

---

<sup>104</sup> *Id.*, art. 1 al. 1 par. 2 ainsi que l'art. 3 al. 4.

<sup>105</sup> *Id.*, art. 3.

<sup>106</sup> CE, *Directive 1996/9/CE du Parlement européen, du 11 mars 1996 concernant la protection juridique des bases de données*, JO, L 77/20.

<sup>107</sup> M. J. DAVISON, W. R. CORNISH, F. DESSEMONTET, P. GOLDSTEIN et R. JACOB, préc., note 98, p. 52.

<sup>108</sup> Un terme qui n'est pas défini dans la Directive, mais qui devrait selon Davison être distingué de celui « d'auteur ». Voir : M. J. DAVISON, W. R. CORNISH, F. DESSEMONTET, P. GOLDSTEIN et R. JACOB, préc., note 98.

<sup>109</sup> Davison résume : « What finally emerged in the Directive was a very different *sui generis* right. It can be categorised as a new form of copyright that applies to databases, covering both the sweat of the brow and creative aspects of making a database. », voir : *Id.*, p. 99.

<sup>110</sup> *Directive 1996/9/CE du Parlement européen, du 11 mars 1996 concernant la protection juridique des bases de données*, préc., note 106, art. 1, par. 2.

Parallèlement, du côté des États-Unis, le cadre juridique est différent. Sans être très strict, l'arrêt *Feist* de la Cour suprême des États-Unis que nous avons précédemment cité<sup>111</sup> requiert un certain niveau d'originalité en vertu duquel le simple effort n'est pas suffisant pour créer un droit d'auteur. Le sens qu'acquièrent les données en passant entre les mains expertes du fabricant de la base de données est potentiellement un travail original, mais les données elles-mêmes ne sont pas protégées en vertu du droit d'auteur américain.

Les données sont la matière première sur laquelle repose le fonctionnement des algorithmes et de l'intelligence artificielle. Elles sont inutiles si elles ne sont pas organisées. Seule l'organisation en base de données donne de la valeur — opérationnelle ou marchande — aux données, les décisions d'un algorithme d'intelligence artificielle reposant essentiellement sur la mise en relation des éléments d'une base de données.

Ainsi, afin de permettre le fonctionnement de ce que l'on désigne comme l'intelligence artificielle, il existe aussi un grand nombre de bases de données. Plusieurs d'entre elles ne sont pas la propriété de géants du Web et sont soumises à des ententes entre les fabricants des outils d'intelligence artificielle et des institutions qui collectent des données dans le cours de leurs activités. Les bases de données dans le domaine médical en sont de bons exemples. D'autres encore sont des bases de données qui n'appartiennent à personne et dont personne ne contrôle réellement la qualité. La base de connaissance Wikidata, dont nous discuterons plus amplement ultérieurement, en est un excellent exemple. Encore, il y a les données collectées via les réseaux sociaux, lesquelles sont servilement livrées par les utilisateurs de ces services. Enfin, on peut aussi penser aux données collectées par les outils d'intelligence artificielle eux-mêmes qui servent à améliorer les services de manière continue.

Il existe également un nombre important de bibliothèques de données rendues accessibles au public intéressé et compétent en programmation par les chercheurs qui les ont recueillies, colligées et étiquetées dans le but d'entraîner leurs algorithmes respectifs. Ces données, disponibles en quantités gargantuesques et dont les ensembles croissent en nombre et en taille à

---

<sup>111</sup> *Feist Publications, Inc., c. Rural Telephone Service Co.*, préc., note 76.



une vitesse exponentielle, servent aujourd'hui à l'entraînement d'algorithmes vierges<sup>112</sup>. De telles ressources existent également pour les fonctions de traitement algorithmique des données ; le praticien d'IA contemporain ne construit que rarement son algorithme à partir du néant, mais en construit plutôt le squelette en partant des fonctions de base disséminées sur le Web, qu'il agencera et améliorera et auxquelles il suppléera de ses propres fonctions pour former son propre algorithme complet et cohésif.

Le recours à toutes ces bases de données par des outils d'intelligence artificielle pourrait dans certains cas compromettre la vie privée des individus dont l'information — potentiellement de nature confidentielle — compose ces bases de données. Ce genre de situation est d'autant plus déplorable que les individus ignorent souvent l'existence même de l'étendue et de la complexité de l'information les concernant qui s'en trouve détenue par des tiers.

Dans un autre spectre d'idées, un autre aspect important à comprendre pour bien situer le rôle des bases de données dans le fonctionnement des assistants vocaux est le fait que la composition des bases de données — les données qu'elles contiennent — a des effets directs sur le comportement des algorithmes et, par extension, des agents autonomes qui en sont l'expression la plus aboutie. Le contrôle de la qualité des données, de leur organisation et de leur suffisance sur le plan tant quantitatif que sur le plan qualitatif est essentiel pour assurer le comportement anticipé de ces agents autonomes. Par exemple, cent photographies de chats prises de profil ne seraient pas suffisantes pour permettre à un algorithme de reconnaître à coup sûr n'importe quelle image d'un chat. Dans cet exemple simple, l'algorithme aurait de la difficulté à reconnaître un chat photographié de face.

Ces réflexions nous poussent à discuter d'un autre aspect incontournable de l'analyse juridique des bases de données : la sécurité des bases de données. La sécurité doit être abordée tant sur le plan de la contamination que sur le plan de la protection des données qu'elles contiennent. En premier lieu, contaminer un ensemble de données est une manière subtile, mais efficace d'influencer négativement un algorithme. Bien qu'il soit immensément improbable que les

---

<sup>112</sup> DATAFLAIR, « Python Libraries. Python Standard Library & List of Important Libraries », *DataFlair* (28 février 2018), en ligne : <<https://data-flair.training/blogs/python-libraries/>> ; DATAFLAIR, « Python Modules vs Packages. Differences Between Python Modules and Packages », *DataFlair* (27 février 2018), en ligne : <<https://data-flair.training/blogs/python-modules-vs-packages/>>.

bases de données soutenant le fonctionnement des assistants vocaux soient contaminées à dessein avec succès, celles-ci contenant une très grande quantité de données et étant physiquement situées dans des centres de données généralement hautement sécurisés, la protection des données demeure impérative. En effet, les stabilité, prévisibilité et constance de la performance des algorithmes dépendent de l'intégrité des bases sur lesquelles ils s'appuient pour leur fonctionnement. Ces immenses bases de données sont utiles, et inviolables sans un effort soutenu, du fait de leur taille et de leur architecture, mais cette taille est en elle-même un facteur de profonde complexité lorsque vient le temps d'assurer l'intégrité des données individuelles que contiennent les bases de données et, par extension, le bon fonctionnement des algorithmes qui s'alimentent de ces données.

Dans un second temps, la révélation malicieuse ou accidentelle d'une quantité massive de données pourrait malheureusement permettre, leur réorganisation de manière à les étiqueter dans le but de construire le profil des individus auxquels les données se rapportent. L'individualisation des données est donc un autre des risques liés à la collecte de celles-ci à grande échelle.

La réflexion sur la responsabilité des propriétaires des bases de données, dans le contexte de l'intelligence artificielle, est récente<sup>113</sup>. Dans la mesure où la collecte est effectuée par les mêmes personnes qui organisent l'information et développent les outils d'intelligence artificielle, la question de la responsabilité peut s'avérer plus simple ; cependant, telle n'est pas la réalité des assistants vocaux ni n'illustre la direction que suit l'évolution de l'écosystème virtuel. Or, lorsque les propriétaires n'ont pas de réel contrôle sur leur base de données, comme c'est le cas pour les bases de données ouvertes — Wikipédia est l'exemple le plus illustratif — la question de la responsabilité des propriétaires, ou du moins des responsables, s'avère épineuse.

Dans le contexte de l'utilisation des assistants vocaux, les outils de reconnaissance vocale convoquent en cascade plusieurs agents autonomes. Ces agents autonomes sont eux-mêmes soutenus par différents algorithmes d'intelligence artificielle faisant appel à un grand nombre de bases de données. Cette interdépendance entre plusieurs outils différents pose problème sur le plan de la preuve. On ne peut par exemple pas réellement savoir de quel endroit a été tirée

---

<sup>113</sup> I. GIUFFRIDA, préc., note 84.

l'information ayant permis à l'outil de reconnaissance vocale de transformer la voix d'un utilisateur en texte clair. Il peut donc s'avérer difficile de vérifier si l'ensemble des processus ayant mené à la compréhension de l'individu par la machine, la réponse à sa demande ou la formulation de cette réponse se sont déroulés normalement. Cela crée un contexte clair-obscur, en ce sens où l'utilisateur ignore quelles données sont convoquées par quel algorithme et avec quelle intensité ceux-ci puisent parmi elles.

Ainsi, la relation entre les algorithmes et les données se compare, du point de vue de l'utilisateur individuel, en quelque sorte à une « boîte noire » puisqu'il ne connaît qu'une partie des intrants et des extrants, les rouages du système lui étant cachés. Nous verrons ci-après que les plus récentes recherches relativement au développement de l'intelligence artificielle tendent toutefois à remettre en question la compréhension répandue à l'effet que le fonctionnement de l'intelligence artificielle est opaque<sup>114</sup>, puisque certaines percées techniques permettent notamment à l'algorithme qui en est doté, d'expliquer le procédé qu'il suit au fur et à mesure de son fonctionnement. Toute cette activité est sous-jacente aux assistants vocaux qui se manifestent généralement à leurs utilisateurs sous la forme d'objets physiques, comme des enceintes connectées, des téléphones ou des montres, dont l'ensemble forme l'écosystème désigné « Internet des objets ».

---

<sup>114</sup> Voir à cet effet la section 1.2 « Qualification juridique des assistants vocaux et des éléments de preuve en découlant ».

### 1.1.3 L'Internet des objets – The *Internet of Things*

Dans le contexte descriptif de ce mémoire, nous croyons pertinent d'expliquer ici ce qui compose l'Internet des objets ou « Internet of Things ». Nous tenterons aussi d'expliquer comment cette notion intervient en lien avec les assistants vocaux et, de manière incidente, les considérations relatives au droit de la preuve. L'IoT prend la forme d'une constellation d'objets connectés entre eux au moyen d'Internet, comme le décrivent certains auteurs :

«IoT refers to the networked interconnection of everyday objects, which are often equipped with ubiquitous intelligence. IoT will increase the ubiquity of the Internet by integrating every object for interaction via embedded systems, which leads to a highly distributed network of devices communicating with human beings as well as other devices.»<sup>115</sup>

Ceux-ci, dans les scénarios les plus complexes, peuvent être commandés par des agents autonomes. Dans le contexte de l'IoT, la communication ne se fait pas seulement entre les utilisateurs et leurs objets connectés, desquels font partie les assistants vocaux ; mais aussi entre les objets eux-mêmes, ce que l'on nomme la communication « dispositif à dispositif » ou « *machine-to-machine* », communément simplifié « M2M » comme nous en avons précédemment discuté<sup>116</sup>.

Cette dernière catégorie de communications est celle qui représente la plus grande part des interactions dans l'environnement de l'IoT. L'ensemble des flux d'information de la communication directe entre les dispositifs échappe la plupart du temps aux utilisateurs<sup>117</sup>, mais peut constituer une source d'information importante pouvant révéler la nature d'une situation à

---

<sup>115</sup> Feng XIA, Laurence T YANG, Lizhe WANG et Alexey VINEL, « Internet of Things », *Int. J. Commun. Syst.* 2012.25.1101.

<sup>116</sup> M. ROUSE, préc., note 31 ; S.-Y. TSAI et S.-I. SOU, préc., note 30 ; Fabrice THEOLEYRE et Ai-Chun PANG, *Internet of Things and M2M Communications*, Algade, River Publishers, 2013.

<sup>117</sup> Jayavardhana GUBBIA, Rajkumar BUYYAB, Marimuthu PALANISWAMIA et Slaven MARUSICA, « Internet of Things (iot). a Vision, Architectural Elements, and Future Directions », (2013) 29-7 *Future Generation Computer Systems* 1645, 10.

partir de plusieurs angles d'observation, pourtant, c'est la plus abstraite de la question. Il s'agit aussi sans doute de l'aspect que le droit de la preuve aura sans doute le plus de difficulté à aborder puisque les tribunaux devront systématiquement s'en remettre à des experts, un état de fait engendrant plusieurs conséquences dont nous discuterons plus loin dans ce mémoire<sup>118</sup>.

Malgré ces difficultés, le droit de la preuve, selon le professeur Michael Legg de l'Université de Nouvelle-Galles-du-Sud, doit s'intéresser à l'IoT<sup>119</sup>. L'argument du professeur Legg est que cet écosystème d'objets, déployés dans un environnement en particulier — un domicile par exemple — ou encore dans un contexte plus large — le domicile, le lieu de travail et l'interaction entre ces deux milieux — est susceptible de révéler de l'information qui, avant le déploiement à grande échelle de cette technologie, n'aurait pas été accessible, sinon par le biais des sens humains ou d'instruments de mesure conventionnels. La plus grande nouveauté de l'IoT, toutefois, consiste en ce qu'un essaim d'objets anodins interconnectés dispose maintenant de la capacité de gérer, de choisir et d'agir sans intervention humaine directe, ce qui sur le plan juridique s'avère porteur d'épineuses questions en matière de responsabilité extracontractuelle, et accessoirement en droit de la preuve dans la démonstration de ladite responsabilité.

Un certain nombre d'affaires impliquant l'Internet des objets ont déjà été portées devant les tribunaux, dans différentes juridictions et différents contextes<sup>120</sup>. La plus pertinente dans le cas qui nous concerne est sans doute l'affaire *Bates*<sup>121</sup>, un cas d'homicide, dont nous discuterons davantage ultérieurement. Notons que certains éléments issus de l'Internet des objets ont aussi

---

<sup>118</sup> Voir la partie 2.3.1 et suivantes sur la compréhension de la technologie.

<sup>119</sup> Michael LEGG et Claire GOULDING, « Technology. How the Internet of Things Will Affect the Future of Litigation », *Univ. of NSWLJ* 2016.28.88; Erica VOWLES et Jeremy STORY CARTER, *Your Smart Device Could Be Used Against You in Court*, *The Law Report*, ABC News, 9 mars 2018, en ligne: <<https://www.abc.net.au/news/2018-03-09/your-google-home-or-fit-bit-could-be-used-against-you-in-court/9510368>>.

<sup>120</sup> Clifford J. ZATZ, Joe MEADOWS, Paul MATHIS et Laura ARADI, « Recent IoT Device Cases », *Data Law Insights* (10 juillet 2017), en ligne : <<https://www.crowelldatalaw.com/2017/07/recent-iot-device-cases/>>.

<sup>121</sup> *State of Arkansas v. James A. Bates*, 2016 Ark. Cir.

été impliqués dans au moins une autre affaire d’homicide aux États-Unis<sup>122</sup>, dans un cas de fraude aux assurances<sup>123</sup>, ainsi dans certaines affaires d’invalidité<sup>124</sup>.

La température dans une pièce à un moment précis de la journée, la quantité d’œufs dans un réfrigérateur, le niveau de carburant dans un véhicule, le nombre de pas effectués par une personne sont autant d’informations pouvant se révéler pertinentes dans le contexte d’un litige. Lorsque l’ensemble de ces objets — le thermostat, le réfrigérateur, le véhicule et le bracelet connecté — sont reliés à l’Internet et communiquent entre eux pour déclencher des actions de manière autonome, ils laissent des traces. Ces traces constituent une manière de faire la preuve d’évènements, c’est-à-dire de faits matériels et peut-être même d’actes juridiques, jusqu’à un certain point et sujet au respect du formalisme requis pour la conclusion de certains d’entre eux.

Les assistants vocaux gagnent de l’importance au sein de l’IoT. Leur nombre est en constante augmentation, mais l’intensité et l’univers des interactions possibles qu’ils permettent en font aussi des éléments très actifs de cet écosystème. Les assistants vocaux s’intègrent à ces réseaux sous-jacents permettant le contrôle de plusieurs éléments avec la voix, comme les téléviseurs connectés ou l’éclairage d’une pièce. À l’heure actuelle, nos relations avec les assistants vocaux laissent des traces de plusieurs manières, notamment via des enregistrements audios, des informations relatives à notre géolocalisation, et des données biométriques. En somme, une grande quantité d’information à caractère personnel transite entre les mains des fabricants, des FAI et d’autres tiers intermédiaires.

---

<sup>122</sup> Le bracelet connecté d’une victime de meurtre a révélé aux forces de l’ordre que l’alibi de l’époux de la victime manquait de crédibilité. Voir à ce sujet : Christine HAUSER, “In Connecticut Murder Case, a Fitbit Is a Silent Witness”, *The New York Times*, sect. New York (22 décembre 2017), en ligne : <<https://www.nytimes.com/2017/04/27/nyregion/in-connecticut-murder-case-a-fitbit-is-a-silent-witness.html>>.

<sup>123</sup> Lors d’un incendie en 2016, le défibrillateur cardiaque connecté implanté chez un homme de l’Ohio a permis aux forces de l’ordre de constater que le rythme cardiaque de celui-ci n’avait subi aucune variation pendant un incendie pour lequel l’homme avait par la suite présenté une réclamation d’assurance très élevée. Des investigations plus approfondies ont montré que l’incendie avait été déclenché par le réclamant. Voir à ce sujet :

Debra CASSENS WEISS, « Data on Man’s Pacemaker Led to His Arrest on Arson Charges », *ABA Journal* (6 février 2017), en ligne : <[http://www.abajournal.com/news/article/data\\_on\\_mans\\_pacemaker\\_led\\_to\\_his\\_arrest\\_on\\_arson\\_charges/](http://www.abajournal.com/news/article/data_on_mans_pacemaker_led_to_his_arrest_on_arson_charges/)> ; John GREGORY, “Devices Gone Wild”, *Slaw Canada’s Online Legal Magazine* (3 mai 2018), en ligne : <<http://www.slaw.ca/2018/05/03/devices-gone-wild/>>.

<sup>124</sup> Dans certains cas, le bracelet connecté a permis au requérant de faire une démonstration relativement à leur niveau d’activité physique avant et après un accident. Voir : *A1702178 (Re)*, CanLII 95902 (BC WCAT) ; *Ainger v. Posendorf*, ONSC 2220.

Néanmoins, il ne faut pas négliger les traces laissées par l'interaction des objets eux-mêmes, entre eux, et des protocoles déclenchés par certains capteurs. La preuve d'une telle interaction peut nous en apprendre énormément sur la situation en général. Le fonctionnement coordonné de machines n'étant pas influencées par la main de leur utilisateur peut nous permettre de brosser un portrait presque exact d'un moment précis. Un tel portrait — purement « mécanique » — est d'un intérêt certain, considérant sa précision et l'absence d'interactions pouvant le biaiser.

L'affaire *Bates*<sup>125</sup> est un exemple intéressant de l'importance de ces interactions sur le plan de la preuve. Dans cette affaire, les autorités cherchaient à obtenir les informations en possession d'Amazon, car la maison du suspect, dans cette affaire de meurtre, était à la fine pointe de la technologie. En demandant à Amazon de fournir l'information captée par « Echo », l'enceinte connectée, les enquêteurs cherchaient à vérifier si l'un des instruments installés sur le lieu du crime aurait pu enregistrer quelque chose en lien avec les événements. Nous discuterons plus loin des raisons invoquées par Amazon pour refuser l'accès aux forces de l'ordre à cette information, mais soulignons ici que c'est en montrant que son téléphone n'avait enregistré aucun pas avant l'heure du meurtre que Bates a pu préparer sa défense<sup>126</sup>.

Cela étant dit, à l'heure actuelle et sur le marché nord-américain, les différents acteurs en présence proposent des assistants vocaux se voulant être la porte d'entrée unique à l'immense champ des possibles que représente l'IoT. En effet, même si une ampoule connectée est fabriquée par une entreprise tierce, elle pourrait malgré tout être compatible avec les produits de Google ou d'Amazon. C'est le cas des ampoules Philips Hue fabriquées par la compagnie Signify, que l'on peut synchroniser avec Alexa et l'Assistant Google<sup>127</sup>. Encore, l'entreprise Google est sans doute celle qui va actuellement le plus loin en tentant d'intégrer horizontalement l'ensemble des produits de domotique connectés, Google étant propriétaire, depuis 2014<sup>128</sup>, de

---

<sup>125</sup> *State of Arkansas v. James A. Bates*, préc., note 121.

<sup>126</sup> E. VOWLES et J. STORY CARTER, préc., note 119.

<sup>127</sup> SIGNIFY HOLDING, « Configuration de Hue à Google », *Philips Hue* (2018), en ligne : <<https://www2.meethue.com/fr-ca/friends-of-hue/google-home-products>>.

<sup>128</sup> Matthew PANZARINO, « Google Is Buying Connected Device Company Nest For \$3.2B In Cash », *TechCrunch* (13 janvier 2014), en ligne : <<http://social.techcrunch.com/2014/01/13/google-just-bought-connected-device-company-nest-for-3-2b-in-cash/>> ; Nicolas RAULINE et Solveig GODELUCK, « Google fait son nid dans la maison intelligente », *Les Echos* (13 janvier 2014), en ligne : <<https://www.lesechos.fr/2014/01/google-fait-son-nid-dans-la-maison-intelligente-287819>> ; Greg KUMPARAK, « Nest Is Being Rolled into Google's Hardware Team »,

l'entreprise Nest, un fabricant et fournisseur d'objets connectés au nombre desquels on compte des thermostats, des caméras ou encore des sonnettes de porte d'entrée.

Dans ce contexte d'intégration — vers lequel tend l'ensemble des joueurs de l'industrie — les assistants vocaux sont la porte d'entrée vers l'IoT et leur qualification sur le plan juridique devient nécessaire pour faciliter l'analyse de l'information que nous pouvons extraire des outils à la disposition du justiciable, considérant que toute l'information existe sans doute, mais sera très probablement jalousement gardée<sup>129</sup> par ceux à qui nous l'aurons, peut-être trop aveuglément, confiée, soit les Google, Amazon et Apple de ce monde. Avant d'arriver à cette étape, poursuivons d'abord la discussion relativement aux assistants vocaux en nous penchant sur un autre élément clef de leur fonctionnement, le traitement automatique des langues.

### 1.1.4 Le traitement automatique des langues — *Natural Language*

#### *Processing*

Le traitement automatique des langues est le processus par lequel la voix d'une personne est transformée en texte<sup>130</sup>, que ce soit au moyen de différentes approches incluant l'utilisation de réseaux de neurones artificiels<sup>131</sup>. Il s'agit d'une technique similaire, mais diamétralement opposée à celle de la synthèse du langage, le *text-to-speech*, qui cherche à synthétiser une voix humaine depuis un texte écrit. Dans le cas des assistants vocaux, ces deux éléments fonctionnent

---

*TechCrunch* (2018), en ligne : <<http://social.techcrunch.com/2018/02/07/nest-is-being-rolled-into-googles-hardware-team/>>.

<sup>129</sup> Le professeur Legg soutient que l'information a priori inaccessible aux justiciables pourrait éventuellement l'être en utilisant des mécanismes qui existent déjà en droit procédural et de la preuve. Écouter : E. VOWLES et J. STORY CARTER, préc., note 119.

<sup>130</sup> Le traitement automatique des langues est un champ d'études qui existe depuis le début des années cinquante et qui s'est développé concurremment aux recherches en linguistiques. Voir à ce sujet : M BATES, « Models of natural language understanding. », (1995) 92-22 *Proc Natl Acad Sci U S A* 9967, 9977.

<sup>131</sup> Le traitement automatique des langues peut aussi faire appel à des techniques n'étant pas en elle-même de l'intelligence artificielle, comme la classification au moyen d'arbre de décision ou encore la reconnaissance de certains termes en mémoire. Elle repose aussi essentiellement sur l'analyse sonore de l'information captée. Voir à ce sujet l'ouvrage : Alexander CLARK, Chris FOX et Shalom LAPPIN, *The Handbook of Computational Linguistics and Natural Language Processing*, Chichester, John Wiley & Sons, 2013.



souvent en simultané, les assistants vocaux devant écouter, mais tentant aussi de répondre à leur interlocuteur.

Pour fonctionner, la reconnaissance vocale doit écouter l'utilisateur et comparer les données recueillies avec le contenu de sa base de données, c'est-à-dire les échantillons de sons et de voix qu'a catégorisés et organisés le fournisseur du service, souvent en collectant l'information des utilisateurs eux-mêmes au fil du temps<sup>132</sup>. La reconnaissance vocale transforme alors — avec plus ou moins d'efficacité — la voix en texte.

Ce texte est par la suite utilisé par l'assistant vocal, soit pour effectuer une recherche ou pour déclencher d'autres mécanismes faisant eux aussi appel à des agents autonomes soutenus par des outils d'intelligence artificielle<sup>133</sup>. L'assistant vocal peut ainsi avoir recours à une base de connaissances pour répondre à une question précise, par exemple la température extérieure à un endroit donné, ou effectuer une recherche sur Internet, par le biais d'un navigateur Web. Les auteurs Kēpuska et Bohouta décrivent le fonctionnement général des assistants vocaux de la manière suivante :

« [T] here are many different architectures for dialog systems. Which sets of components are included in a dialog system, and how those components divide up responsibilities differs from system to system. A dialogue system has mainly seven components: Input Decoder, Natural Language Understanding, Dialogue Manager, Domain Specific Component, Response Generator, and Output Renderer. However, there are six main components in the general dialogue systems, which includes the Speech Recognition (ASR), the Spoken Language Understanding (SLU), Dialog Manager (DM), Natural Language Generation (NLG), Text to Speech Synthesis (TTS), and the knowledge base. »<sup>134</sup>

(Références omises)

---

<sup>132</sup> Dr Michael J. GARBADE, « A Simple Introduction to Natural Language Processing », *Medium* (15 octobre 2018), en ligne : <<https://becominghuman.ai/a-simple-introduction-to-natural-language-processing-ea66a1747b32>> ; Julia HIRSCHBERG et Christopher D. MANNING, « Advances in Natural Language Processing », (2015) 349-6245 *Science* 261 ; A. CLARK, C. FOX et S. LAPPIN, préc., note 131.

<sup>133</sup> Veton KĚPUSKA et Gamal BOHOUTA, *Next-generation of virtual personal assistants (Microsoft Cortana, Apple Siri, Amazon Alexa and Google Home)*, 2018 *IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC)*, Las Vegas, Institute of Electrical and Electronics Engineer, 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC), janvier 2018, p. 99-103, en ligne: <<https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8301638&tag=1>>.

<sup>134</sup> *Id.*, p. 100.

Les outils de traitement automatique des langues s'enrichissent au fur et à mesure de l'utilisation qu'on en fait. Dit autrement, plus un assistant vocal est utilisé – ou tout autre outil qui implique la reconnaissance vocale – plus cet outil vocal aura de la facilité à comprendre son utilisateur et à lui répondre. Il en est ainsi à cause de la nature des algorithmes soutenant ces outils, qui s'améliorent de manière autonome.

Sur le plan du droit de la preuve, le traitement automatique des langues pose plusieurs questions intéressantes. D'abord, il y a la collecte des données, laquelle est effectuée par les outils auprès des utilisateurs au moment de l'utilisation. Ces données peuvent prendre la forme d'extraits audios. Dans ces cas, ces extraits s'ajoutent au matériel à la disposition du juriste pour étayer sa preuve, tant que ces enregistrements soient accessibles a posteriori. En effet, les historiques d'utilisation de certains outils permettent d'avoir accès à ces traces, notamment les historiques des produits proposés par Google et Amazon.

Toutefois, un autre élément est disponible, dans la majorité des cas, soit l'historique de ce que l'assistant vocal a compris des commandes de son utilisateur. Ces commandes sont transformées, comme nous l'avons expliqué, en texte, par un algorithme d'intelligence artificielle. Elles constituent en quelque sorte une forme de transcription, de propos rapportés par une machine. Quiconque s'est déjà adressé à un agent autonome incluant une fonction de reconnaissance vocale sait que ces outils manquent encore de précision à l'heure actuelle et ne peuvent adéquatement comprendre leurs utilisateurs dans plusieurs contextes<sup>135</sup>. On peut donc ici sérieusement douter de l'authenticité de ce qui a été dit, de la véracité des propos tenus. Une situation qui pourra, selon notre analyse, influencer la recevabilité du genre de preuve dont nous discutons.

En somme, la reconnaissance de la voix humaine par une machine est un domaine en constante évolution et se révélant d'une très grande complexité. Si les résultats des outils de reconnaissance vocale peuvent être impressionnants, en l'absence d'enregistrement, la

---

<sup>135</sup> Les travaux du professeur Frederic Lederer montrent cependant que lorsque ce genre de système de reconnaissance vocale est adapté à un locuteur particulier, il peut être très précis. Dans ces recherches, le professeur Lederer a mené des expériences sur l'utilisation de la reconnaissance vocale pour remplacer le sténographe dans un cyber tribunal. Voir notamment : Fredric LEDERER, « The Road to the Virtual Courtroom? A Consideration of Today's and Tomorrow's High Technology Courtrooms », (1999) 50 *S.C. L. Rev.* 800; Miklós KENGYEL et Zoltán NEMESSÁNYI, *Electronic Technology and Civil Procedure. New Paths to Justice from Around the World*, New York, Springer, 2012.

transcription automatique faite par ces outils pourrait poser des problèmes de recevabilité, considérant la nature même de ces transcriptions, soit le fait qu'elles résultent essentiellement de comparaisons statistiques produites par un algorithme et de certains processus qui échappent à la connaissance de l'utilisateur et peuvent varier d'un fournisseur à l'autre ; Google et Apple n'utilisant pas les mêmes procédés pour comprendre et répondre aux questions de leurs utilisateurs.

Parallèlement et dans la même veine, les problématiques conceptuelles et techniques précédemment évoquées mises à part, il y a aussi le but inhérent des assistants vocaux — soit répondre à des commandes — qui les conditionnent à répondre à des questions lorsqu'elles sont formulées d'une certaine manière. Sans avoir connaissance de la manière dont ils sont configurés, il est difficile de comprendre les réponses qu'ils donnent à leurs utilisateurs.

### 1.1.5 Compréhension des questions et recherche d'information

L'intelligence artificielle ne se compare pas aisément à l'intelligence humaine, en ce sens où elle n'implique pas la conjonction de connaissances et de la compréhension<sup>136</sup>, mais plutôt l'habileté de mettre en relation de l'information de manière cohérente. L'habileté des assistants vocaux à répondre aux questions qui leur sont posées relève essentiellement de deux choses. D'abord, ils sont tributaires des avancées en analyse logique, un champ des mathématiques s'intéressant à la structure des phrases et des questions posées par l'utilisateur<sup>137</sup>.

---

<sup>136</sup>Il existe de nombreuses définitions de l'intelligence. L'approche cognitive en psychologie nous enseigne que l'intelligence humaine se déclinerait en trois volets, soit l'intelligence composite (traitement de l'information), l'intelligence appliquée (adaptation à des situations nouvelles) et l'intelligence contextuelle (adaptation à son environnement). Nous avons repris ici la définition du dictionnaire *Le Petit Robert*. Voir à ce sujet : Paul ROBERT, *Le Petit Robert*, Paris, Éditions Le Robert, 2015, v° « Intelligence » ; Carol TAVRIS et Carole WADE, *Introduction à la psychologie. Les grandes perspectives*, traduit par Alain GAGNON, Claude GOULET et Patrice WIEDMAN, Saint-Laurent, ERPI, 2007, p. 271 à 272 citant ; Robert J. STERNBERG, *The Triarchic Mind. A New Theory of Human Intelligence*, New York, Viking, 1988.

<sup>137</sup> Ulrich FURBACH, Ingo GLÖCKNER et Björn PELZER, « An Application of Automated Reasoning in Natural Language Question Answering », (2010) 23 *AI Commun.* 24 ; Bernard J. JANSEN et Soo Young RIEH, « The Seventeen Theoretical Constructs of Information Searching and Information Retrieval », (2010) 61-8 *J Am Soc Inf*

Ensuite, les assistants vocaux ne contiennent pas dans leur mémoire interne les réponses à l'ensemble des questionnements qui leur sont adressés, mais savent cependant comment accéder à l'information nécessaire pour formuler une réponse.

Les assistants vocaux, comme d'autres outils d'intelligence artificielle, ont accès à des bases de connaissances leur permettant de toucher à de l'information de nature factuelle. Une base de connaissances ou *knowledge base*, dans le contexte de l'intelligence artificielle, est une tierce source d'informations, elle-même une base de données, organisée de manière à permettre, entre autres, à des agents intelligents de la consulter<sup>138</sup>. La référence à de l'information externe, par exemple dans un cadre contractuel, n'est pas un phénomène nouveau ou propre à l'intelligence artificielle. Un contrat de financement, par exemple, pourrait faire référence au taux d'intérêt publié périodiquement par un quotidien en particulier, invitant les cocontractants à s'y référer pour calculer un montant à rembourser.

L'information fournie par les tiers est primordiale pour assurer le fonctionnement des assistants vocaux. Sans eux, les assistants vocaux ne pourraient pas répondre à des questions simples, du genre « quelle température fait-il à l'extérieur ? ». En effet, lorsqu'ainsi interrogés, les assistants vocaux, après avoir compris la question en effectuant un travail de reconnaissance vocale, interrogent des sources susceptibles de leur fournir une réponse.

Dans l'écosystème organisé et développé des assistants vocaux, les sources sont d'ores et déjà identifiées. En tout premier lieu, l'outil tente de se situer lui-même dans l'espace. Pour se faire, l'assistant vocal accède aux données du système de positionnement d'un téléphone cellulaire ou de la connexion Internet de l'appareil sur lequel il est installé. Ensuite, il se tourne vers des sources externes pour connaître la température à cet endroit précis. Ainsi, lorsque l'on demande à l'Assistant Google le temps qu'il fait, celui-ci consulte le site Web *The Weather Channel*,

---

*Sci Technol* 1517; L. HIRSCHMAN et R. GAIZAUSKAS, « Natural Language Question Answering. The View from Here », (2001) 7-4 *Nat. Lang. Eng.* 275.

<sup>138</sup>Parmi ces bases de connaissances, l'une des plus impressionnantes est sans doute Wikidata qui se trouve être une version de l'encyclopédie collaborative Wikipédia pouvant être utilisée par les outils d'intelligence artificielle. Les réponses fournies par les assistants vocaux provenant de Wikipédia passent essentiellement par Wikidata. Les bases de connaissances sont aussi la source d'information des « systèmes experts » qui ne sont pas forcément des agents intelligents. Voir à ce sujet : Denny VRANDEČIĆ et Markus KRÖTZSCH, « Wikidata. A Free Collaborative Knowledgebase », (2014) 57-10 *Commun. ACM* 78 ; OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE, *Grand dictionnaire terminologique*, Québec, Publications du Québec, 2017, v° « Système expert », en ligne : <[http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id\\_Fiche=8368220](http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=8368220)>.

tirant lui-même ses informations de plusieurs sources comme les relevés météorologiques des autorités aéroportuaires ou de différentes agences gouvernementales.

La qualité des réponses des assistants vocaux sera directement tributaire de la qualité de l'information fournie par ces bases de connaissances. Or, les liens juridiques entre les fournisseurs de services et les personnes ou entités qui rendent l'information disponible sont souvent inconnus du grand public.

L'exhaustivité ou encore à la validité de l'information contenue dans la réponse d'un assistant vocal à la requête d'un utilisateur n'est pas garantie dans ce contexte. Malgré tout, le fonctionnement de ces outils bénéficie de présomptions en vertu de la LCCJTI<sup>139</sup>, lesquelles ont suscité plusieurs discussions. L'exemple des réponses erronées fournies par un outil d'intelligence artificielle nous semble être l'illustration par excellence que la présomption créée à l'article 7 de la LCCJTI doit être interprétée limitativement.<sup>140</sup> Bien qu'il soit raisonnable de croire que les tiers mettent tout en œuvre pour proposer une information valide, il n'y a certes aucune garantie à cet effet. Dans le cas de Wikipédia, considérant la nature ouverte et collaborative de l'outil, il est n'est pas certain que l'information présentée soit exacte. Ce genre d'information dynamique présente sur le Web est susceptible d'être modifiée sur une base très fréquente et ne peut donc pas être tenue pour véridique dans un contexte judiciaire. Pour la même raison qu'une page Wikipédia est peu fiable<sup>141</sup>, les réponses données par un assistant vocal puisant ses informations à même ce genre de pages le sont tout autant. La réponse pourrait-elle être différente si en lieu et place de Wikipédia, l'intelligence artificielle avait interrogé une autre base de connaissances, fournie par exemple par un éditeur réputé dans le domaine de la santé ?

À notre sens, le contexte dans lequel évolue l'utilisateur est ici très important pour déterminer la réponse à ces questions. Dans le cas où l'utilisateur a toutes les raisons de croire la réponse, il ne semble pas être déraisonnable de s'en remettre à un tiers, surtout si l'information en

---

<sup>139</sup> *Loi concernant le cadre juridique des technologies de l'information*, préc., note 14, art. 7.

<sup>140</sup> Vincent GAUTRAIS et Patrick GINGRAS, « La preuve des documents technologiques », dans *Congrès annuel du Barreau*, coll. « Services de formation permanente du Barreau du Québec », Cowansville, Éditions Yvon Blais, 2012 aux pages 27 et suivantes.

<sup>141</sup> Lucy THOMSON, *Admissibility of Electronic Documentation as Evidence in U. S. Courts*, coll. « Human Rights Electronic Evidence Study », Chicago, nter for Research Libraries, 2011, p. 19, en ligne: <<https://www.crl.edu/sites/default/files/d6/attachments/pages/Thomson-E-evidence-report.pdf>>.

question est généralement connue. Parallèlement, il convient aussi de mettre en doute la diligence d'un utilisateur qui aurait questionné un assistant vocal pour obtenir une réponse à une question engageant de lourdes conséquences. Ainsi, il ne serait pas raisonnable pour un médecin de consulter Wikipédia en lieu et place d'une encyclopédie médicale reconnue avant une chirurgie afin de se remémorer l'emplacement de certains vaisseaux sanguins. Les questions d'ordre factuel dont la réponse peut influencer grandement le cours d'un processus décisionnel devraient-elles être posées à des outils d'intelligence artificielle dont les sources ne peuvent que difficilement être vérifiées par la suite étant donné la nature de leur fonctionnement ? Il s'agit là d'une interrogation qui dépasse le strict cadre des assistants vocaux et peut aisément se poser dans le cas des véhicules autonomes ou encore des outils d'aide à la décision dans les milieux judiciaires ou médicaux. Cela étant, nous n'aborderons pas davantage cet aspect.

Dans le contexte du droit de la preuve, l'aspect pertinent en lien avec les tierces sources d'information est de vérifier comment celles-ci entrent dans la chaîne de fonctionnement des assistants vocaux et influencent l'information transmise à l'utilisateur. Si la question peut avoir une grande importance, sur le plan du droit de la preuve, révélant par exemple l'intention de l'utilisateur au moment de l'interrogation, nous sommes d'avis que la réponse donnée peut aussi présenter un intérêt. Par contre, puisque la nature de la réponse reposant surtout sur le fonctionnement des algorithmes et l'information fournie par les tiers, il est difficile de comprendre la relation exacte qu'entretiennent ces éléments entre eux. Ces détails ne sont pas révélés à l'utilisateur<sup>142</sup>.

Notamment, il ne faut guère oublier que les bases de connaissances sont d'abord des bases de données accessibles via le Web. La raison pour laquelle ces bases de connaissances sont accessibles aux géants du Web et que leur contenu est rendu librement disponible aux utilisateurs des outils d'intelligence artificielle, découle de leur nature « ouverte ». Le qualificatif « ouvert » dans le cas présent signifie que l'objet peut être modifié par les utilisateurs

---

<sup>142</sup> Interrogé par l'équipe de l'émission radiophonique *The Law Report* au sujet des éventuels éléments de preuve que l'on pourrait dégager de l'utilisation d'objets issus de l'IoT, le professeur Michael Legg de l'Université de Nouvelle-Galles du Sud avançait qu'un justiciable pourrait tenter d'user des moyens procéduraux conventionnels pour obtenir de la part des manufacturiers l'information généralement inaccessible aux utilisateurs. Voir à ce sujet : E. VOWLES et J. STORY CARTER, préc., note 119.

qui le consultent<sup>143</sup> — à l'image de Wikipédia — ce qui le rend susceptible de contenir des données erronées, tel que nous l'avons précédemment évoqué. Le caractère ouvert fait aussi connaître à l'objet une évolution inorganique et artificielle de son contenu. Une telle perturbation peut potentiellement introduire des disparités dans la performance, dans le temps, des algorithmes sous-jacents aux assistants vocaux via la manipulation directe. Cette situation est différente de l'évolution organique de la base de données du fait de l'ajout des données collectées dans le cours de l'utilisation des programmes connectés. De fait, le caractère ouvert de certaines bases de connaissances peut être le point faible de celles-ci, expliquant leur vulnérabilité et le dysfonctionnement des outils d'intelligence artificielle.

En somme, pour répondre aux questions de ses utilisateurs, l'intelligence artificielle se réfère généralement, sur le plan factuel, à des bases de connaissances, soit des bases de données appartenant parfois à des tiers, lesquels fournissent ainsi de l'information dont la qualité peut varier. En passant par l'assistant vocal, la source de l'information fournie à l'utilisateur peut devenir difficile à vérifier. De ce fait, il est aisé de mettre en doute la véracité des réponses fournies à l'utilisateur et dont il pourrait nous rester des traces. Le contexte de l'utilisation spécifique devient alors très pertinent afin d'analyser si la réponse était raisonnable à l'égard de la question. Cependant, une variable reste inchangée : l'ensemble de ces opérations nécessite une connexion à l'Internet.

---

<sup>143</sup> L'idée même de la « source ouverte » est surtout mise de l'avant par le programmeur Richard Stallman ayant milité dès 1983 pour la promotion des logiciels au code source ouvert, c'est-à-dire pouvant être modifiée par tous. Il théorise son idée en publiant « The Open Source Definition » en 1997, une série de règles composant l'accise théorique de son mouvement. Elles sont dérivées des travaux de Bruce Perens. Voir entre autres : « The Open Source Definition », *Open Source Initiative* (2007), en ligne : <<https://opensource.org/osd>> ; Chris DiBONA, Sam OCKMAN et Mark STONE (dir.), *Open Sources. Voices from the Open Source Revolution*, 1<sup>re</sup> éd., Sebastopol, O'Reilly, 1999; Josh LERNER et Jean TIROLE, « Some Simple Economics of Open Source », (2002) 50-2 *J Ind Econ* 197-234.

## 1.1.6 L'Internet comme canal unique de communication

L'IoT dans lequel s'insèrent les assistants vocaux repose sur la prémisse d'un canal unique de transmission pour l'information, soit l'Internet. Sur le plan du droit de la preuve, cela présente des avantages et des inconvénients. En premier lieu, comme l'Internet est un univers absolument artificiel — contrairement au monde réel — il serait possible de prétendre que toutes les variables qui le gouvernent sont potentiellement identifiables, bien que l'étendue de cet univers artificiel soit aujourd'hui très vaste, ce qui nous pousse à nuancer la précédente affirmation. Malgré tout, il est donc raisonnable de croire que l'on pourrait en documenter tous les aspects globalement, en les exprimant à titre de tendances et de principes évolutifs. Si la surveillance du trafic Internet à grande échelle est techniquement possible<sup>144</sup>, sur le plan de la pratique, une telle ambition se révélerait matériellement impossible sans y engager des ressources considérables, tant l'Internet est immense, à l'heure actuelle, et est appelé à le devenir suivant une trajectoire exponentielle. Encore, il faut distinguer ici l'analyse du trafic Internet et l'analyse du contenu consulté par un utilisateur en particulier. Si le second révèle les agissements d'une personne sur la Toile, le premier illustre surtout des tendances au sein d'un groupe plus large. Au surplus, si on le conçoit comme un réseau — à l'image par exemple du réseau sanguin du corps humain, chaque élément qu'on y ajoute — lire ici chaque élément de l'IoT — en augmente la complexité et la « taille ». Cartographier l'ensemble de l'Internet devient donc de plus en plus difficile.

Les gardiens contrôlant l'accès à ce réseau pour le grand public — les fournisseurs d'accès Internet — sont ceux qui, en sachant où prêter attention, peuvent documenter avec le plus de précision l'utilisation faite par une personne de sa connexion à la Toile. C'est toutefois dans la

---

<sup>144</sup> Les programmes de surveillance américains PRISM et Xkeyscore de la NSA, révélés par le lanceur d'alerte Edward Snowden en 2013, laissent entendre que des agences gouvernementales pourraient avoir la capacité de surveiller l'ensemble du trafic sur Internet, mais ce genre de surveillance demeure hautement controversée et inaccessible au grand public et aux forces de l'ordre. Voir à ce sujet : Glenn GREENWALD, « Xkeyscore. Nsa Tool Collects 'Nearly Everything a User Does on the Internet' », *The Guardian*, sect. US News (31 juillet 2013), en ligne : <<https://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data>>; Glenn GREENWALD et Ewen MACASKILL, « NSA Prism Program Taps in to User Data of Apple, Google and Others », *The Guardian*, sect. US News (7 juin 2013), en ligne : <<https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data>>.



diversification de ces moyens de connexions — ainsi que dans l’augmentation du volume du trafic en général. — que repose l’inconvénient du canal de communication unique qu’est l’Internet.

L’inconvénient de voir l’ensemble de cette information passer par un seul endroit s’explique essentiellement par le fait que l’information qui y passe est maintenant de nature beaucoup plus variée qu’auparavant. L’information est le plus souvent cryptée, peut porter plusieurs chapeaux alors qu’elle provient toutefois de la même personne, et, surtout, le volume d’information est maintenant si grand qu’aucun filtrage exhaustif ne peut y être appliqué, ce qui pousse les acteurs de l’industrie à adopter des méthodes alternatives pour traiter l’information<sup>145</sup>, méthodes qui ne seront pas expliquées en détail ici, mais qui complexifient le travail du juriste en quête de preuve.

#### 1.1.6.1 Le rôle du fournisseur d’accès Internet

Les FAI sont un rouage important de l’Internet et, par extension, de l’intelligence artificielle. Les FAI assurent la liaison entre les fournisseurs de services — fabricants des outils d’intelligence artificielle ou simple distributeur — et les utilisateurs. Les FAI permettent la communication des données entre les appareils connectés et les serveurs des compagnies telles que Google, Amazon ou Apple, où se déploie l’ensemble des programmes d’ordinateur dont il est question ici<sup>146</sup>. Les algorithmes de traitement automatique des langues, les moteurs de recherches et les processus qui assurent la communication avec les autres éléments composant

---

<sup>145</sup> S.-Y. TSAI et S.-I. SOU, préc., note 30 ; J. GUBBIA, R. BUYTAB, M. PALANISWAMIA et S. MARUSICA, préc., note 117.

<sup>146</sup> La reconnaissance vocale, par exemple, est l’un de ces processus qui n’a pas lieu dans l’appareil de l’utilisateur, mais dans le nuage. Plusieurs applications au « cloud-based automatic speech recognition » ont d’ailleurs fait l’objet de recherches, notamment en matière de santé. Voir à ce sujet : Zdenek BUMBALEK, Jan ZELENKA et Lukas KENCL, *Cloud-Based Assistive Speech-Transcription Services*, Klaus MIESENBERGER, Arthur KARSHMER, Petr PENAZ et Wolfgang ZAGLER (dir.), *Computers Helping People with Special Needs*, coll. « Lecture Notes in Computer Science », Berlin, Springer, 2012, p. 113; Heidi CHRISTENSEN, Iñigo CASANUEVA, Stuart CUNNINGHAM, Phil GREEN et Thomas HAIN, *Homeservice. Voice-Enabled Assistive Technology in the Home Using Cloud-Based Automatic Speech Recognition*, 4th Workshop on Speech and Language Processing for Assistive Technologies, Grenoble, Association for Computational Linguistics, 4th Workshop on Speech and Language Processing for Assistive Technologies, 21 août 2013, p. 29-34, en ligne: <<https://www.aclweb.org/anthology/W13-3906.pdf>>; V. KĚPUSKA et G. BOHOUTA, préc., note 133.

l'IoT ne fonctionneraient pas sans une connexion à l'Internet. Les FAI voient donc tout. Ils sont les témoins passifs de l'ensemble des flux d'information entre les objets connectés et les fournisseurs de services et fabricants. L'information qu'ils conservent est précieuse, car rien ne leur échappe — en théorie.

D'abord, la quantité d'information fait en sorte que les FAI ne peuvent conserver l'historique d'utilisation de chaque utilisateur pour une période indéfinie. Déjà en 2011, dans un texte à l'attention des juristes américains au sujet des historiques d'utilisation d'une connexion Internet dans un contexte de droit pénal, on écrivait :

« Log records are usually maintained for a very limited period. Each provider or company determines how long to retain its records. In past cases, many providers have maintained log records for only a few days. Other providers may retain the records for a week or so. Some providers may not log all events. Because of the limited retention period for log records, it is useful to consider other places to find the same or similar data. »<sup>147</sup>

(Notre soulignement)

En plus de la quantité, il faut aussi prendre en considération le mode d'utilisation de ces outils. Le caractère portable et mobile des appareils technologiques d'aujourd'hui permet aux utilisateurs de se connecter à l'Internet à différents endroits. La journée typique d'un utilisateur nomade peut débuter à son domicile, où son ordinateur portable et son téléphone cellulaire seront alors connectés à son réseau sans fil personnel, puis sur la route, l'utilisateur pourrait s'arrêter dans un café et se connecter au réseau sans fil de celui-ci afin d'utiliser son ordinateur portable. Au fil de ses déplacements, l'utilisateur, sans le savoir, est constamment localisé par tous les réseaux sans fil publics. En effet, le téléphone mobile qu'il transporte avec lui identifie avec acharnement, mais avec discrétion tout réseau avec lequel il pourrait bénéficier d'une connexion, en prévision de l'éventualité selon laquelle l'utilisateur désirerait accéder au Web. Enfin, l'utilisateur pourrait se connecter sur son lieu de travail à un autre réseau. Cela fait

---

<sup>147</sup> Mark L KROTOSKI et Jason PASSWATERS, "Using Log Record Analysis to Show Internet and Computer Activity in Criminal Cases", (2011) 6–59 *United States Attorneys' Bulletin* 1, 5 à 6.

certainement trois FAI différents et potentiellement des dizaines d'autres rencontrés en chemin. Ce sont là autant d'acteurs à contacter pour reconstituer les activités d'une personne sur et via l'Internet.

Dans un contexte de droit de la preuve, il faut aussi discuter de la difficulté résultant de l'interprétation des données que l'on pourrait potentiellement obtenir d'un FAI. Celle-ci se présenterait dans un langage technique systématiquement dénué de contexte, exprimé en langage de programmation machine ou Web, mais constituerait sans doute la preuve la plus près d'être la plus probante. Elle permettrait vraisemblablement de lier un appareil particulier — poste d'ordinateur, appareil mobile ou enceinte connectée — à un comportement précis sur ou via le Web.

Un premier conflit se dessine ici entre la facilité d'accès à la preuve et sa valeur probante. L'information pourrait en effet s'avérer complexe à obtenir et relativement difficile à interpréter sans l'intervention d'un expert<sup>148</sup>. Nous discuterons davantage de ce conflit plus loin dans ce mémoire relativement alors que nous discuterons de l'admissibilité. Observons maintenant l'autre pendant de la preuve entre les mains du FAI, soit l'information qui se retrouve entre les mains des fabricants et fournisseurs de services.

#### **1.1.6.2 Le rôle des fabricants et fournisseurs de services**

L'information à propos des utilisateurs et de leur utilisation des assistants vocaux est vraisemblablement entre les mains d'au moins une autre catégorie d'acteurs dans ce contexte : leurs fabricants, soit ceux qui fournissent les services liés aux assistants vocaux. Dans le cas du marché nord-américain des assistants vocaux, nous pouvons en nommer au moins quatre, soit Amazon, Apple, Google et Microsoft. Ceux-ci conservent et organisent l'information qu'ils collectent dans d'immenses bases de données. Ces données servent principalement à améliorer leurs produits respectifs.

---

<sup>148</sup> *Id.*, 10 et suivantes.

Bien que la présente discussion pourrait porter avec grand intérêt sur différentes questions de droit, par ailleurs très pertinentes, touchant par exemple la propriété des données relatives à la personne<sup>149</sup>, la sécurité entourant leur conservation ou encore les tierces utilisations qui en sont faites par les fournisseurs — la création de profils d'utilisateurs très précis permettant la publicité ciblée<sup>150</sup>, au premier chef — nous ferons abstraction de ces questions d'une importance autrement capitale, préférant nous concentrer sur les problématiques liées au droit de la preuve.

Dans le contexte actuel, une fois l'information collectée par le fabricant et consignée par celui-ci dans de grands ensembles, celle-ci peut présenter un intérêt pour la personne désirant prouver un fait grâce à elle. Pour ce faire, un justiciable pourra tenter d'accéder à cette information, là où elle se trouve. Cependant, croire que les fabricants et fournisseurs de ces services ouvriront toutes grandes les portes de leurs installations pour permettre à quiconque le demande de venir chercher l'information dont il a besoin dans le cadre d'un litige ou d'une investigation relève de l'utopie. Dans les faits, bien que la situation ne se soit jamais présentée devant un tribunal canadien, une situation analogue s'est produite en 2015 dans l'État américain de l'Arkansas<sup>151</sup>, lorsqu'une enceinte connectée pouvait avoir enregistré les moments précédant et suivant le meurtre d'un homme.

Dans cette affaire relevant de la preuve pénale en droit américain, la multinationale Amazon a produit un mémoire étoffé<sup>152</sup> pour s'opposer à l'ordre de la cour de transmettre aux forces de l'ordre l'ensemble des données relatives à l'utilisateur en question.

Dans ce mémoire, Amazon soutenait que la saisie de ces données pourrait constituer une atteinte aux droits constitutionnellement garantis par le premier amendement de la Constitution américaine, soutenant que la liberté d'expression des utilisateurs serait brimée si l'on accordait

---

<sup>149</sup> P. TRUDEL, préc., note 102.

<sup>150</sup> Karim AMER et Jehane NOUJAIM, *The Great Hack*, Documentaire, Netflix, 24 juillet 2019, en ligne : <<https://www.netflix.com/ca/title/80117542>>.

<sup>151</sup> *State of Arkansas v. James A. Bates*, préc., note 121.

<sup>152</sup> AMAZON.COM, INC., *Memorandum of Law in Support of Amazon's Motion to Quash Search Warrant*, 2017, en ligne : <<https://regmedia.co.uk/2017/02/23/alexa.pdf>>.

aux autorités en l'espèce le droit d'accéder à l'information en question. Dans son mémoire, Amazon soutient à cet effet :

« Like cell phones, such modern 'smart' electronic devices contain a multitude of data that can 'reveal much more in combination than any isolated record,' allowing those with access to it to reconstruct '[t]he sum of an individual's private life'. The recordings stored by Amazon for a subscriber's Echo device will usually be both [...] the user's speech, in the form of a request for information from Alexa, and [...] a transcript or depiction of the Alexa Voice Service response conveying the information it determines would be most responsive to the user's query. Both types of information are protected speech under the First Amendment. »<sup>153</sup>

(Références omises)

Il faut savoir cependant que le motif principal avancé par Amazon pour s'opposer à l'ordre du tribunal de l'Arkansas n'a pas été analysé sur le fond, puisque l'individu en question a, par la suite, volontairement choisi de remettre les informations le concernant aux autorités. Il a ensuite été acquitté pour d'autres raisons. Cette occasion manquée de vérifier si la liberté d'expression protège les justiciables américains contre la saisie d'information partagée avec un assistant vocal est décevante.

Les arguments présentés dans le mémoire d'Amazon relevaient principalement du premier amendement américain, et non du quatrième amendement, qui protège pourtant les justiciables américains des saisies et perquisitions abusives. Or, la doctrine au sud de la frontière a d'ores et déjà avancé une réponse en l'espèce<sup>154</sup>. En effet, un citoyen américain disposant de protections constitutionnelles le protégeant contre certaines formes de fouilles et d'investigation à l'endroit d'informations très personnelles ou sensibles perdrait ces protections et garanties s'il révélait, de son propre chef, ces informations à des tiers, les rendant ainsi moins confidentielles qu'elles

---

<sup>153</sup> *Id.*, p. 9.

<sup>154</sup> Voir à ce sujet les articles suivants : Tara MELANCON, « Alexa, Pick an Amendment. A Comparison of First and First Amendment Protections of Echo Device Data », (2017) 45 *S.U. L. Rev.* 302; S. AITCHISON, préc., note 92.

l'étaient au départ. Dans le scénario qui nous concerne, Amazon est le tiers auquel l'utilisateur révèle ses informations confidentielles.

Si l'on suit cette logique, toute l'information communiquée avec un assistant vocal ne serait pas protégée par le quatrième amendement, puisque les fournisseurs sont des tiers et que le microphone placé dans le domicile de l'utilisateur y aurait été placé, selon toute vraisemblance, par l'utilisateur lui-même, et donc avec son consentement. Il va sans dire que c'est là une brèche considérable aux garanties constitutionnelles de nos voisins du Sud, dénoncée d'ailleurs par la doctrine de ce côté de la frontière<sup>155</sup>.

Ainsi, si obtenir l'information des fournisseurs de service peut s'avérer difficile<sup>156</sup>, il faudra vraisemblablement se contenter des historiques des applications elles-mêmes. Nous discuterons de ceux-ci plus loin dans le présent mémoire.

Pour conclure sommairement sur ce sujet, force est de constater que les fournisseurs du service collectent l'information et consignent forcément des traces de toutes les interactions des utilisateurs avec les assistants vocaux. Toutefois, cette information n'est peut-être pas conservée afin d'être ultérieurement utilisée en tant que preuve, mais plutôt afin de servir de matière première pour le raffinement des algorithmes d'intelligence artificielle. Ainsi, ce n'est pas parce que l'information existe qu'elle existe dans un état propice à faire de celle-ci un élément de preuve. En tentant de la rendre un tant soit peu digeste au système judiciaire, les possibilités de compromettre son intégrité existent et doivent être prises en considération lorsque l'on tentera de donner une valeur juridique à cette information. Cela est vrai en matière de preuve civile, mais davantage encore en matière de preuve pénale où des droits fondamentaux pourraient s'en retrouver compromis.

---

<sup>155</sup> T. MELANCON, préc., note 154.

<sup>156</sup> Difficile, sans forcément être impossible, comme l'expose le professeur Micheal Legg, avançant qu'il serait possible de recourir au droit procédural existant pour enjoindre les fabricants à rendre accessible les données en leur possession. Appliqué au contexte civil québécois, ce raisonnement signifie que l'article 251, al. 2 du *Code de procédure civile* serait le véhicule procédural approprié pour requérir d'un fabricant qu'il communique avec les parties l'information en sa possession. Ce raisonnement demeure à l'heure actuelle relativement spéculatif, en l'absence d'exemple jurisprudentiel. Voir à ce propos : E. VOWLES et J. STORY CARTER, préc., note 119 ; M. LEGG et C. GOULDING, préc., note 119 ; *Code de procédure civile*, préc., note 91, art. 251, al. 2.

## 1.2 Qualification juridique des assistants vocaux et des éléments de preuve découlant de leur utilisation

La définition juridique de l'assistant vocal nécessite une définition du concept d'agent autonome, soit des processus faisant appel à l'intelligence artificielle pour prendre des décisions essentiellement basées sur des inférences statistiques, sans l'intervention d'un tiers<sup>157</sup>. Dans le cas qui nous concerne, plusieurs agents autonomes sont impliqués, de manière générale : les agents conversationnels, et les processus qui effectuent la recherche d'information, le cas échéant. En fin de piste, les processus qui conditionnent les résultats de recherche supportent une part dominante des interactions avec les assistants vocaux, puisque ces interactions sont encore majoritairement des questions dont les réponses sont trouvées par l'assistant moyennant une recherche sur le Web.

Considérant l'ensemble des éléments que nous avons abordés au cours des pages précédentes, nous sommes d'avis que l'assistant vocal, sur le plan juridique, doit être considéré comme un programme d'ordinateur. Cela étant dit, partant du point de vue que l'intelligence artificielle est une chose en elle-même, son caractère mathématique complexe rend difficile la preuve de l'authenticité de ses résultats. De fait, la preuve de son manque d'authenticité est tout aussi difficile à faire. C'est pour cette raison que l'on réfère d'ailleurs au fonctionnement de l'intelligence artificielle comme à une « boîte noire »<sup>158</sup>, dont certains intrants et extrants sont connus, mais dont les processus internes nous échappent. Le concept de la boîte noire est cependant très récemment remis en cause, et ce, par de nouveaux développements technologiques permettant à certains outils d'intelligence artificielle de rendre compte de leur cheminement<sup>159</sup>. Ces techniques ne sont toutefois pas propices à toutes les applications de

---

<sup>157</sup> *Agent autonome*, préc., note 63.

<sup>158</sup> Andrea ROTH, "Machine Testimony", (2017) 126-7 *Yale L.J.* 1972.

<sup>159</sup> Voir notamment les avancées relatives aux explications multimodales et aux développements vers un « explainable AI » qui trouvent cependant à l'heure actuelle surtout application dans le traitement des images. Voir à ce sujet, entre autres : Dong Huk PARK, Lisa Anne HENDRICKS, Zeynep AKATA, Anna ROHRBACH, Bernt SCHIELE, Trevor DARRELL et Marcus ROHRBACH, « Multimodal Explanations. Justifying Decisions and Pointing to the Evidence », *ArXiv* 2018.arXiv:1802.08129, en ligne : <<http://arxiv.org/abs/1802.08129>> ; Wojciech SAMEK, Thomas WIEGAND et Klaus-Robert MÜLLER, « Explainable Artificial Intelligence. Understanding, Visualizing and

l'intelligence artificielle et requerront certaines adaptations avant de pouvoir expliquer en détail le parcours ayant permis à un assistant vocal d'arriver à une réponse particulière.

À la lumière du caractère illusoire revêtant toute tentative d'extirper des algorithmes supportant les assistants vocaux actuels une quelconque preuve contextualisée, intelligible pour le profane et circonscrite à l'intérêt essentiel du juriste, nous sommes d'avis qu'il est impératif de plutôt considérer le potentiel probant des produits intermédiaires et fonctionnalités accessoires de ces systèmes. Parmi ces produits et fonctionnalités, on retrouve des enregistrements audios, des relevés de positionnement géolocalisé et des historiques d'utilisation et de navigation Web. Nous traiterons donc plus loin de l'utilité de ceux-ci à titre de preuve matérielle.

### **1.2.1 L'information en contexte : questions et réponses**

L'information transmise par l'utilisateur à un assistant vocal est sans doute la partie la plus importante dans l'analyse des traces laissées par son utilisation. L'information transmise par l'utilisateur porte en elle-même un certain sens pouvant mener à des conclusions. Toutefois, le traitement appliqué par l'intelligence artificielle à cette information est aussi pertinent. Il permet à l'intelligence artificielle de produire des réponses à l'utilisateur. Ces réponses fournies sont aussi, selon nous, d'une pertinence certaine dans la compréhension d'un contexte particulier. Retrouver l'information transmise par l'utilisateur est le défi auquel vaudra se livrer le praticien qui souhaitera déposer en preuve les interactions avec un assistant vocal. L'autre pendant — les réponses — pourrait potentiellement l'aider.

Dans le cadre d'un dialogue asymétrique dont il ne nous est présenté que les réponses à des questions dont nous ignorons la teneur, il serait possible en présence d'un être humain de faire certaines inférences, mais il ne s'agirait là que de spéculations dont nous ne pourrions tirer des conclusions qu'en ayant la capacité de les rattacher à d'autres éléments contextuels. En présence

---

Interpreting Deep Learning Models”, *ArXiv* 2017.arXiv:1708.08296, en ligne : <<http://arxiv.org/abs/1708.08296>>; Derek DORAN, Sarah SCHULZ et Tarek R. BESOLD, « What Does Explainable AI Really Mean? A New Conceptualization of Perspectives », *ArXiv* 2017.arXiv:1710.00794, en ligne : <<http://arxiv.org/abs/1710.00794>>.



d'un algorithme, pour comprendre le fonctionnement et les réponses, il faut comprendre l'algorithme lui-même, c'est-à-dire le protocole mathématique complexe mettant en relation les données. Cela pose les problèmes dont nous avons précédemment discuté.

Premièrement, les algorithmes sont protégés par certains mécanismes du droit de la propriété intellectuelle, comme nous en avons discuté précédemment. Y accéder pour analyser les processus ayant mené à une réponse précise est donc difficilement envisageable. Encore, ils sont en constant développement et peuvent ne plus correspondre à ce qu'ils étaient au moment où une question leur a été posée. En second lieu, les bases de données qui ont participé à générer la réponse sont elles aussi des objets de propriété intellectuelle dont l'accès peut être restreint, et le contenu connaît une constante évolution.

Les réponses d'un assistant vocal à un utilisateur ne présentent donc que peu d'intérêt si elles ne sont pas accompagnées des questions que cet utilisateur aura posées à l'assistant vocal. Seules, les réponses sont susceptibles d'être influencées par plusieurs éléments et, de ce fait, aucun exercice de raisonnement logique ne pourrait permettre d'en déduire une proposition certaine dont la signification pourrait nous éclairer.

Ainsi, ce n'est qu'en conjonction avec d'autres éléments qu'une réponse donnée par un assistant vocal pourrait prendre un sens susceptible de permettre d'en dégager une conclusion logique.

### **1.2.2 Sous quelle forme la preuve se présente-t-elle ?**

Nos interactions avec les composantes de l'IoT, dont les assistants vocaux, prennent plusieurs formes. Leur intervention peut être déclenchée par d'autres processus, comme un thermostat connecté ou un hygromètre, lesquels pourraient commander à une prise de courant connectée d'allumer un ventilateur ou un climatiseur pour refroidir une pièce. Encore, la localisation de notre téléphone peut engendrer la réaction de certains appareils connectés, comme des ampoules qui pourraient s'allumer alors que l'on arrive à notre domicile. Toutefois, dans le cas des assistants vocaux, c'est avant tout les opérations que l'on dicte directement à

l'assistant vocal et qui sont traitées par les algorithmes de traitement automatique des langues qui sont en cause.

Sur le plan probatoire, l'ensemble de ces « événements technologiques » a pour dénominateur commun le fait qu'ils se produisent via une connexion Internet. C'est donc dire que tous ces processus laissent forcément des traces, lorsqu'ils se déclenchent, puisque l'Internet n'est pas autre chose qu'un assemblage d'ordinateurs et de relais. Les différentes formes que peuvent prendre les preuves de nos interactions avec les assistants vocaux sont au nombre d'au moins deux.

D'abord, il y a les historiques d'utilisation des applications elles-mêmes, s'ils existent. Ensuite, il y a les données qui sont collectées par les fournisseurs d'accès au réseau, les fabricants et les autres fournisseurs de services. Ceux-ci sont témoins de plusieurs processus auxquels l'utilisateur n'a pas directement accès, comprenant entre autres les données de géolocalisation et d'horodatage.

### **1.2.2.1 Les historiques issus des applications elles-mêmes**

Lorsque l'on utilise les services d'assistants vocaux, comme l'assistant Google, Alexa d'Amazon ou encore Siri d'Apple, il est possible d'avoir accès, au sein même des fonctionnalités de ces applications, à un historique recensant certaines de nos interactions avec celles-ci. Cet accès est toutefois relativement inégal d'un fournisseur à l'autre et aussi en fonction de l'interface utilisée pour récupérer l'information.

Par exemple, pour l'assistant vocal Apple, Siri, il n'est pas possible d'accéder directement à un historique de nos interactions avec l'assistant. À tout le moins, il est possible de consulter nos plus récentes requêtes. En ce qui concerne Alexa d'Amazon et l'Assistant de Google, ces deux derniers outils permettent à leurs utilisateurs d'avoir accès à l'ensemble de leurs requêtes antérieures en consultant les sites Web respectifs de ces fabricants au moyen d'un navigateur Web.

L'utilisateur pourrait alors effectuer des captures d'écran, une pratique qu'a reconnue la jurisprudence québécoise<sup>160</sup>, ou encore enregistrer la page Web en tant que telle sur son ordinateur, et ce, sous différents formats en fonction de son navigateur Internet. Le format HTML, avec l'option « page complète », permet une relecture subséquente de la page, dans l'exact état où elle était au moment de sa sauvegarde<sup>161</sup>. Il existe aussi la possibilité de sauvegarder un fichier MHTML, développé spécifiquement pour restituer un fichier HTML<sup>162</sup>, mais cette fonctionnalité n'est maintenant disponible que sur les navigateurs Microsoft Edge et Internet Explorer, ayant été retirée de Google Chrome en 2019<sup>163</sup>. Les fichiers ainsi créés seront l'une des composantes du support — nous reviendrons sur ce sujet. Ce support portera de l'information, laquelle se présentera sous différentes formes en fonction des produits utilisés.

Les utilisateurs d'Alexa, par exemple, peuvent ainsi mettre la main sur le texte généré par l'assistant vocal, c'est-à-dire l'interprétation de leur voix par l'algorithme de l'outil de reconnaissance vocal, la réponse donnée par Alexa, un enregistrement de leur propre voix ainsi que l'heure à laquelle la requête a eu lieu (Figures 1 et 2).

---

<sup>160</sup>La jurisprudence québécoise jusqu'ici n'a rejeté les captures d'écran que lorsque des doutes ont été soulevés relativement à leur intégrité et la possibilité qu'un montage de celles-ci puisse être réalisé. Voir à ce sujet : *B.C. c. Loto-Québec*, 2011 QCCA 133 ; *Droit de la famille — 161206*, 2016 QCCS 2378.

<sup>161</sup> Voir à ce sujet la page d'aide du navigateur Google Chrome : GOOGLE, « Read Pages Later and Offline », *Google Chrome Help* (2019), en ligne : <<https://support.google.com/chrome/answer/7343019?co=GENIE.Platform%3DDesktop&hl=en&oco=0>> Voir aussi, relativement à l'archivage de pages et sites web : ; William JONES, Harry BRUCE et Susan DUMAIS, *Keeping Found Things Found on the Web, Proceedings of the Tenth International Conference on Information and Knowledge Management*, coll. « CIKM '01 », New York, ACM, 2001, p. 119; Jinfang NIU, « An Overview of Web Archiving », (2012) 18-4 *D-Lib Magazine*, en ligne : <[https://scholarcommons.usf.edu/si\\_facpub/308](https://scholarcommons.usf.edu/si_facpub/308)> ; Peter LYMAN, « Archiving the World Wide Web », dans NATIONAL DIGITAL INFORMATION INFRASTRUCTURE AND PRESERVATION PROGRAM (U.S.) (dir.), *Building a National Strategy for Digital Preservation: Issues in Digital Media Archiving*, coll. « National Digital Information Infrastructure and Preservation Program (U.S.) », Washington, D.C, Council on Library and Information Resources and Library of Congress, 2002, en ligne : <<https://pdfs.semanticscholar.org/2323/b3921357b203e80e031d79990383a0b0b39b.pdf#page=42>>.

<sup>162</sup> Lire à ce sujet le blogue personnel du professeur retraité Jacob Palme où il retrace les étapes ayant mené au développement du protocole ouvert MHTML : Jacob PALME, « MHTML - Sending HTML in E-mail » (11 juin 2005), en ligne : <<https://people.dsv.su.se/~jpalme/ietf/mhtml.html>>.

<sup>163</sup> Le retrait de cette fonctionnalité n'a pas été expliqué par Google. Lire à ce sujet : VENKAT, « Google removes 'Save Page as MHTML' flag from Chrome Canary », *Techdows* (4 juin 2019), en ligne : <<https://techdows.com/2019/06/google-removes-save-page-as-mhtml-flag-from-chrome.html>>.

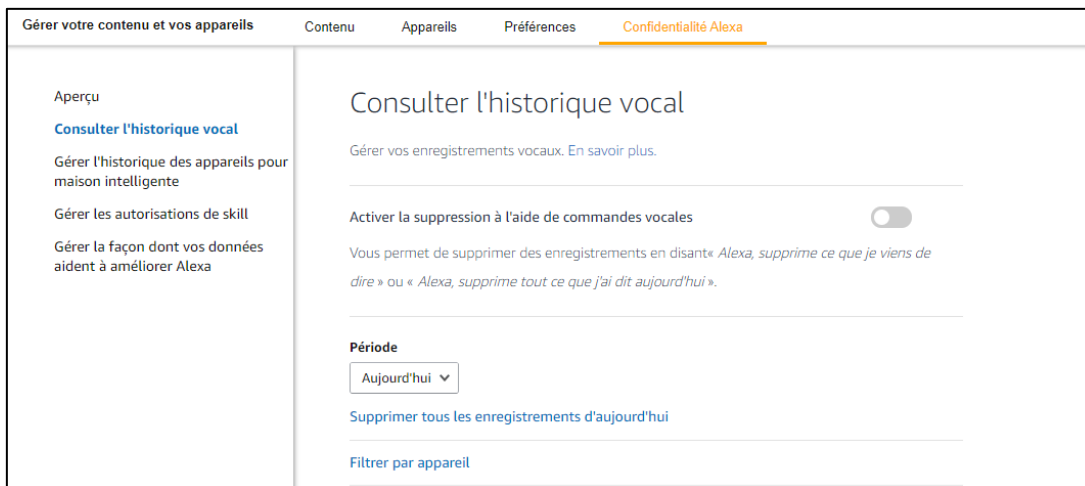


Figure 1. Interface d'accueil de l'historique de l'assistant vocal Alexa d'Amazon

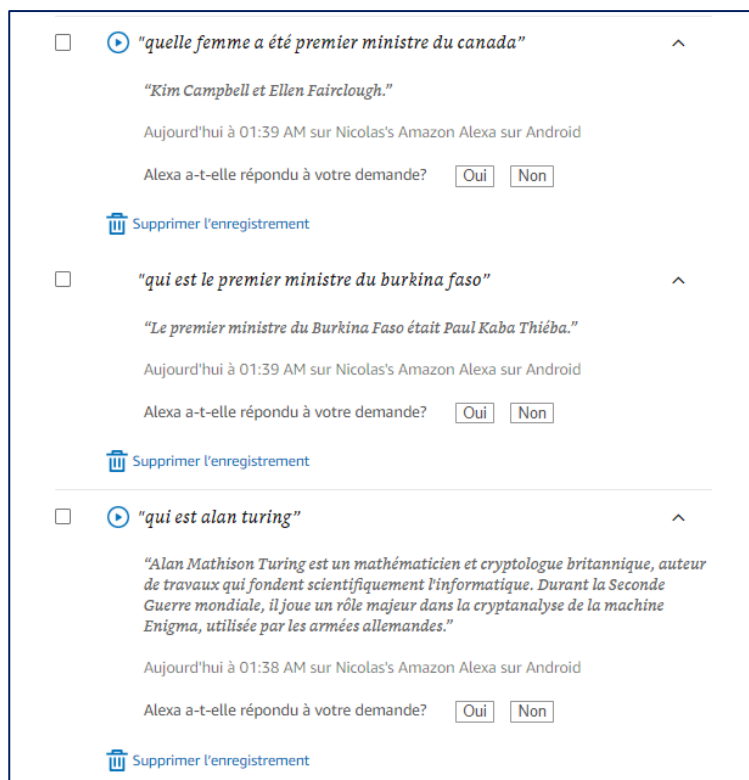


Figure 2. Entrées dans l'historique d'utilisation de l'assistant vocal Alexa d'Amazon

Dans le cas de Google, l'utilisateur peut aussi accéder à des données de géolocalisation, en plus des enregistrements de sa voix, de la réponse donnée par l'outil et de l'interprétation faite par

celui-ci de sa requête (Figure 3 à 5.). L'outil permet même de télécharger en fichier MP3 les enregistrements sonores ayant servi à la reconnaissance vocale<sup>164</sup>, ce que ne permet pas l'historique d'utilisation d'Alexa.

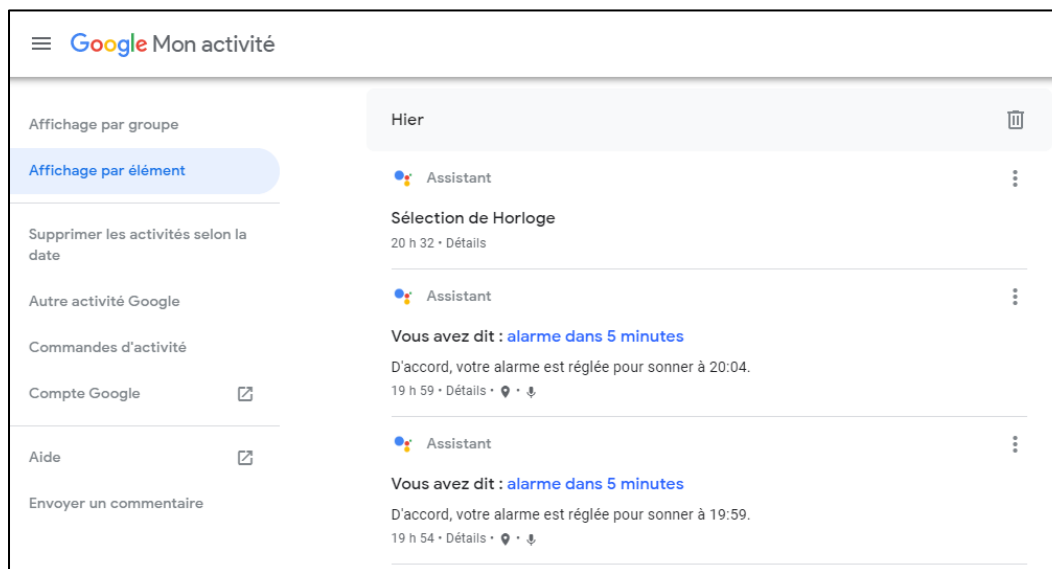


Figure 3. Accueil de l'historique d'utilisation de l'Assistant Google.

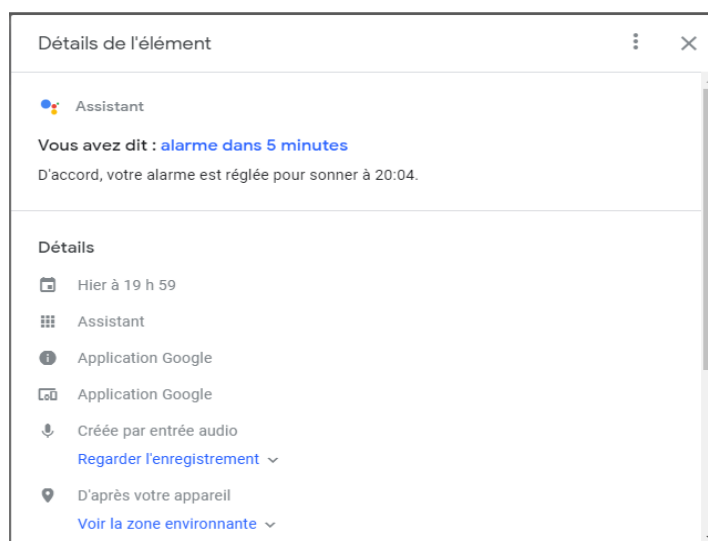


Figure 4. Détails d'un élément dans l'historique d'utilisation de l'Assistant Google

<sup>164</sup> GOOGLE, « Gérer l'historique Google des activités vocales et audio », *Google Assistant Help* (2019), en ligne : <<https://support.google.com/websearch/answer/6030020?hl=en>>.

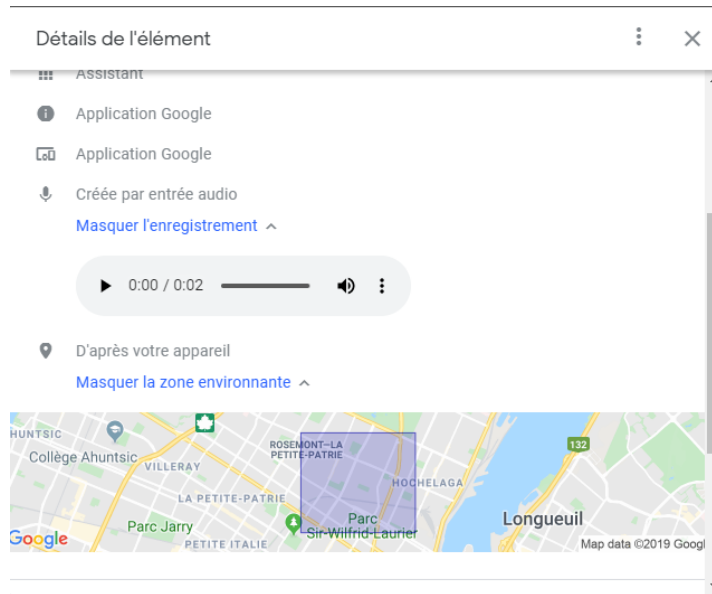


Figure 5. Détails d'un élément dans l'historique d'utilisation de l'Assistant Google

Les historiques d'utilisation des outils Google Assistant et Alexa permettent, à l'image des historiques de navigation classiques de supprimer soit l'ensemble ou une partie des entrées dans l'historique. Google, pour sa part, explique que la suppression de l'information par l'utilisateur n'entraîne pas forcément sa destruction immédiate sur les serveurs de Google, certaines informations pouvant être conservées tant et aussi longtemps que le compte demeure actif<sup>165</sup>, et donc demeurer potentiellement disponibles.

Dans son état original, l'utilisateur consulte ces historiques de la même manière qu'il consulte une page Web, c'est-à-dire au moyen d'un navigateur Internet et d'une connexion réseau. La nature de ce document mérite cependant que l'on s'y attarde quelque peu. En effet, ces historiques d'utilisation permettent la consultation d'extraits sonores et d'autres données, eux-mêmes des éléments relativement autonomes, mais intimement liés à l'historique lui-même.

---

<sup>165</sup> Entre autres, Google explique que « [m]ême lorsque l'activité est supprimée, certaines données relatives à votre utilisation des services Google peuvent être conservées pendant toute la durée de vie de votre compte Google. Par exemple, lorsque vous supprimez une recherche dans "Mon activité", votre compte enregistre le fait que vous avez effectué une recherche, mais pas son contenu. » Voir à ce sujet : GOOGLE, « Supprimer vos activités », *Google Assistant Help* (2019), en ligne : <<https://support.google.com/websearch/answer/465?hl=fr>>.

Au moment de circonscrire le document en question, doit-on considérer l'ensemble de l'historique d'utilisation? Bien que potentiellement immense, un historique d'utilisation est structuré de manière logique et porteur d'informations. En ce sens, il correspond aux critères<sup>166</sup> de la LCCJTI pour la définition du concept de « document ».

Toutefois, certains outils, en l'occurrence l'Assistant Google, permettent d'isoler des éléments particuliers, soit les données d'horodatage, de géolocalisation et l'enregistrement sonore se rapportant à une requête particulière. Dans ce cas, nous sommes d'avis qu'il y a lieu de considérer, ces historiques d'utilisation comme des banques de données, puisqu'ils correspondent à la définition de l'article 3 (2) de la LCCJTI :

« Pour l'application de la présente loi, est assimilée au document toute banque de données dont les éléments structurants permettent la création de documents par la délimitation et la structuration de l'information qui y est inscrite. »<sup>167</sup>

(Notre soulignement)

En vertu de l'article 3 (2) de la LCCJTI, la banque de données est « assimilée » à un document lorsque ces caractéristiques permettent de créer des documents en interrogeant cette banque de données. Si l'on devait considérer chaque entrée dans l'historique comme un document particulier — susceptible d'être analysé indépendamment — la nécessaire preuve de l'intégrité et l'analyse relative à la force probante prendraient une tout autre allure que si l'on devait considérer l'historique d'utilisation comme un tout, facilement modifiable par l'utilisateur.

Dans ce cas de figure, si l'entrée était l'objet sur lequel situer le point focal de l'analyse, le juriste bénéficierait de plusieurs présomptions, dans le contexte québécois. Il ne serait pas nécessaire de faire la preuve du bon fonctionnement de l'environnement technologique dans lequel évolue l'information, soit la plateforme sur laquelle l'information aura pu être récupérée ou encore la page Web au travers de laquelle l'utilisateur aura pu y accéder et, en bout de piste,

---

<sup>166</sup> *Loi concernant le cadre juridique des technologies de l'information*, préc., note 14, art. 3, al. 1.

<sup>167</sup> *Id.*, art. 3, al. 2.

le fichier de sauvegarde ou la capture d'écran qui aura été créé. Nul besoin, non plus, de faire la preuve du bon fonctionnement de l'enceinte connectée. Enfin, une lecture de l'article 7 de la LCCJTI pourrait mener à croire que la présomption créée par celui-ci ferait en sorte que la preuve du bon fonctionnement des algorithmes de traitement automatique des langues ne serait pas nécessaire :

« 7. Il n'y a pas lieu de prouver que le support du document ou que les procédés, systèmes ou technologies utilisés pour communiquer au moyen d'un document permettent d'assurer son intégrité, à moins que celui qui conteste l'admission du document n'établisse, par prépondérance de preuve, qu'il y a eu atteinte à l'intégrité du document. »<sup>168</sup>

(Notre soulignement)

Or, les mots de l'article 7 LCCJTI sont « communiquer au moyen d'un document » et cet article se concentre essentiellement sur le support, c'est-à-dire le canevas portant un contenu informationnel. Une autre lecture de la situation pourrait donc s'appliquer à la partie de l'assistant vocal qui transmet le message à l'utilisateur — la communication — alors que l'on pourrait légitimement croire que la présomption de l'article 7 LCCJTI ne s'applique pas au processus ayant mené à la formulation de la réponse. Il est difficile cependant d'isoler chacun de ces processus, puisqu'ils se présentent à l'utilisateur comme un tout, l'assistant vocal. C'est donc dire que si l'on considère l'algorithme comme étant partie intégrante de l'environnement technologique, il n'a pas lieu d'en prouver le fonctionnement correct. Or, si l'on considère qu'il y a une décision, un choix qui est fait par l'algorithme, il pourrait ne pas tirer profit de la présomption de l'article 7 LCCJTI et de fait être considéré comme n'importe quelle autre machine, dont le fonctionnement peut être mis en doute.

Ici, la confusion entre le produit de l'intelligence artificielle et la matière première que celle-ci utilise suscite une certaine confusion. Ajoutons, pour finir que le juriste souhaitant apporter en preuve une entrée particulière dans un historique de navigation devra malgré tout faire la preuve de l'authenticité de l'information en présence — laquelle doit être distinguée de l'intégrité du

---

<sup>168</sup> *Id.*, art. 7.



support, comme nous le rappellent Gautrais<sup>169</sup> et la Cour d'appel<sup>170</sup>, et ce, malgré un mésentendu jurisprudentiel<sup>171</sup> et doctrinal<sup>172</sup> de plus d'une décennie. Le professeur Gautrais explique :

« L'article 7 de la [LCCJTI] [...] est l'un de ceux qui posent le plus de difficultés interprétatives. En effet, il est possible de déceler deux manières de le considérer : l'une prétend qu'une présomption d'intégrité du document en découle et l'autre croit qu'elle ne s'applique pas au document à proprement parler, mais au support et à l'environnement technologique dans lequel le document est géré. »<sup>173</sup>

(Références omises)

Ainsi, même si la preuve du fonctionnement d'un navigateur Web utilisé pour consulter un historique d'utilisation n'est pas forcément nécessaire, encore faut-il convaincre la Cour de l'authenticité de l'information que l'on tentera de mettre en preuve. Ainsi, il faudra appuyer le fait que la géolocalisation d'une personne ou encore un enregistrement de ses paroles concerne bien cette personne et que celle-ci avait l'appareil en sa possession au moment de la création de l'entrée dans l'historique d'utilisation.

Prouver l'intégrité de l'information ne semble toutefois pas toujours si facile à faire. Par exemple, si le document généré par l'utilisation d'un assistant vocal se présente sous une forme

---

<sup>169</sup> V. GAUTRAIS, préc., note 12.

<sup>170</sup> *Benisty c. Kloda*, préc., note 15.

<sup>171</sup> Gautrais, dans ses commentaires sur la LCCJTI, dresse une liste des décisions et des auteurs défendant la position contraire à la sienne dans le cadre de son analyse du concept d'intégrité. Voir ici ainsi qu'à la note suivante : *Montréal (Ville de) c. Bolduc*, 2009 QCCM 185 ; *Id.* ; *Stefanovic c. ING Assurances inc.*, 2007 QCCQ 10363 ; *Vandal c. Salvas*, [2005] 587 RL (C.Q.) ; *Citadelle, Cie d'assurance générale c. Montréal (Ville)*, [2005] CanLII 24709 (CSQ) ; *Enercon Canada inc. c. Commission de la construction du Québec*, 2015 QCCRT 0394 ; *Compagnie des chemins de fer nationaux du Canada c. Compagnie d'arrimage de Québec ltée*, [2010] QCCQ 942.

<sup>172</sup> Christopher RICHTER et Pierre-Alexandre VIAU, « Les règles de preuve s'appliquant à la documentation électronique et aux technologies de l'information », dans *Congrès annuel du Barreau du Québec*, Montréal, Barreau du Québec, 2007, p. 43-70 ; Léo DUCHARME, *Précis de la preuve*, 6<sup>e</sup> éd., coll. « Bleue », Série Précis, Montréal, Wilson & Lafleur, 2005 ; Michel GAGNÉ, « La preuve dans un contexte électronique », dans *Service de la formation permanente du Barreau du Québec*, 160, coll. « Développements récents en droit de l'Internet », Cowansville, Éditions Yvon Blais, 2001, p. 55-105 ; Claude FABIEN, « La preuve par document technologique », (2004) 38 *R.J.T.* 553 ; Donald BÉCHARD, *Manuel de l'objection*, 3<sup>e</sup> éd., coll. « La référence », Cowansville, Éditions Yvon Blais, 2009, en ligne : <<https://www.lareference.editionsyvonblais.com/maf/app/authentication/signon?sp=montreal-13>> ; Marie-Ève BÉLANGER, « Documents technologiques, copies et documents résultants d'un transfert », dans *Fascicule 5, JurisClasseur Québec — Preuve et prescription*, Montréal, LexisNexis Canada, 2010.

<sup>173</sup> Vincent GAUTRAIS, « Intégrité », *LCCJTI.ca* (2017), en ligne : <<https://www.lccjti.ca/definitions/integrite/>>.

moins élaborée que le produit mis en marché par Google, à l'image de l'historique proposé par Amazon, il pourrait s'agir d'un document et non d'une banque de données. Le cas d'Amazon est cependant particulier, puisque l'outil dispose de certaines fonctions de recherche permettant de délimiter l'information, militant en faveur de sa qualification en tant que base de données. En cas contraire, prouver l'intégrité d'un historique conçu comme un tout, par exemple une liste, serait moins simple puisque ceux-ci sont relativement faciles à modifier par l'utilisateur.

Les outils dont nous discutons en l'espèce sont conçus pour permettre à l'utilisateur de détruire toutes les traces de son utilisation ou, encore, de faire un nettoyage très spécifique, n'effaçant que certaines parties disgracieuses de ses allées et venues sur le Web, complexifiant la qualification qu'aura à faire le juriste au temps de choisir les éléments qu'il voudra mettre en preuve.

### **1.2.2.2 Les autres sources d'information**

Les traces de nos interactions avec les assistants vocaux pourraient aussi se trouver ailleurs que dans les historiques des assistants eux-mêmes. Les assistants vocaux étant, par nature, des interfaces conçus pour naviguer sur l'Internet, leur utilisation laisse d'autres traces, notamment auprès des FAI. Nous avons discuté du rôle des FAI précédemment. Observons maintenant ce que l'on pourrait obtenir d'eux et d'autres acteurs de l'IoT.

Lorsqu'ils savent où prêter l'oreille, les FAI peuvent permettre d'atteindre un degré de certitude assez élevé relativement à la navigation d'un utilisateur particulier, sous réserve cependant d'analyser le trafic Internet de cet utilisateur particulier de manière intentionnelle. S'il sait où regarder, le FAI peut techniquement tout voir. C'est donc dire que — dans le cas de la navigation Internet conventionnelle — une personne qui visite une page Web proposant du contenu illégal — de la pornographie juvénile par exemple — pourrait difficilement contester la preuve électronique montée contre elle si les forces de l'ordre peuvent montrer — au moyen des données fournies par un FAI — que l'adresse IP de l'appareil de cette personne a accédé au serveur — représenté par une autre adresse IP — où cette information illicite se trouvait être hébergée. C'est d'ailleurs de cette manière que la preuve pénale à l'endroit des cyberpédophiles

s'est généralement construite. Les forces de l'ordre ayant des soupçons relativement à un individu peuvent généralement obtenir un mandat permettant de requérir d'un FAI que celui-ci remette aux policiers les preuves qu'une personne a consulté des sites Web où se trouve hébergé du matériel illégal<sup>174</sup>.

La question de la preuve de la navigation Internet, dans le cas des interactions avec les assistants vocaux, pourrait être d'un autre ordre. La nature du trafic lié à l'intelligence artificielle n'est généralement pas similaire à la nature du trafic conventionnel.

Dans certains cas, elle pourrait toutefois s'y apparenter. Ainsi, lorsqu'un utilisateur utilise sa voix pour effectuer une recherche qu'il aurait autrement effectuée dans un moteur de recherche — par exemple, rechercher la capitale d'un pays — la situation s'apparente à une utilisation conventionnelle de l'Internet. Dans d'autres cas, par contre, s'il s'agit de commandes destinées à déclencher des actions au moyen d'un objet connecté, par exemple demander à son téléphone de faire jouer de la musique ou d'allumer une lumière, et l'information recueillie par le FAI n'est pas de la même nature. L'information ne pourrait que difficilement être utilisée comme preuve autonome, mais pourrait appuyer une preuve existante. Si l'on reprend notre exemple, les traces en possession d'un FAI, laissées par l'utilisation d'un assistant vocal pour allumer ou éteindre une lumière, seraient selon nous surtout utiles pour corroborer l'historique d'utilisation de cet assistant vocal. Ainsi, l'information fournie par un FAI pourrait servir de preuve extrinsèque visant à prouver, par exemple, l'authenticité de l'information contenue dans l'historique d'utilisation.

---

<sup>174</sup> *R. c. Spencer*, 2014 CSC 43 (Décision relative à la légalité de l'utilisation de l'adresse IP et la nécessité pour les forces de l'ordre d'obtenir un mandat de perquisition); *R. c. Millette*, 2015 QCCQ 16688 (L'adresse IP est utilisée pour révéler l'identité de l'expéditeur de courriel de menace et d'intimidation); *R. c. Girard Lévesque*, 2015 QCCQ 4509 (Le juge discute longuement de l'utilisation de l'adresse IP comme un moyen efficace de relier un utilisateur à un compte de messagerie précis.); *R. c. Faivre*, 2018 QCCQ 7467 (Un informateur de police met au jour les tactiques très élaborées d'un présumé pédophile afin de camoufler son identité sur le Web en masquant son adresse IP); *Directeur des poursuites criminelles et pénales c. Deramchi*, 2018 QCCQ 7424 (L'adresse IP est utilisée pour relier l'accusé à des cybercrimes sexuels commis à l'endroit de personnes mineures); *R. c. L.M.*, [2005] CanLII 24988 (C.Q.) (Affaire datant de 2005 où le juge entend le témoignage d'un policier expliquant le fonctionnement de l'adresse IP, sa signification et la force probante qu'elle devrait avoir dans le but de relier un appareil à une utilisation particulière sur le Web); Voir aussi, pour d'autres techniques d'enquête *R. c. Mills*, 2019 CSC 22 (Utilisation d'un logiciel de capture d'écran et comparaison avec des fragments de messages retrouvés sur l'ordinateur de l'accusé); *R. v. Levigne*, 2010 CSC 25 (Utilisation d'un logiciel de capture d'écran pour enregistrer des séances de clavardage).

Lorsque l'utilisation de l'assistant vocal a pour but d'effectuer une recherche sur le Web, les traces de cette navigation — la consultation de la page Web — seront pertinentes et feront preuve en elles-mêmes.

Dans un scénario comme dans l'autre, la preuve obtenue des FAI pourrait prendre la forme de relevés d'analyse ou encore de témoignages de techniciens expliquant à la Cour le processus ayant mené à la collecte des données. Il serait possible de comparer les informations fournies par le FAI avec l'historique d'un assistant vocal. Du même souffle, une personne pourrait aussi contester l'intégrité d'un historique d'utilisation en confrontant celui-ci aux données générales issues du FAI, lesquelles ne peuvent être contrôlées par un utilisateur. L'analyse de cette preuve se fera sans doute grâce à un expert, il n'est pas certain qu'elle soit accessible à tous les justiciables, puisque les témoins experts ne sont que rarement gratuits. De fait, il se peut qu'elle se révèle disproportionnée dans certains cas. Nous aborderons ce sujet ultérieurement alors que nous discuterons de la recevabilité.

Sur un autre plan, en ce qui concerne l'information collectée par les autres acteurs de l'IoT, celle-ci peut prendre plusieurs formes. Le fabricant de produits connectés chinois Merross, lequel propose entre autres des ampoules, des commutateurs et des interrupteurs que l'utilisateur peut contrôler au moyen de différentes applications, dont l'Assistant Google et Alexa mentionne dans sa politique de confidentialité que l'entreprise recueille certaines informations :

« Whenever you interact with our Services [...] we may automatically collect and store information on our servers, logs and databases from your browser, application, services or device(s). In particular, our Services are designed to allow you to connect various physical devices [...] to the Services. While connected to the Services, these devices automatically report information to our servers (including information that you may have provided when setting up or configuring that device), which may include Personal Information. Such as device name, device location, model number, firmware version, hardware version, activation time, online time, app open frequency, crash logs, settings parameters.

Other information collected automatically through the foregoing means may include your IP address, MAC address, location details, 'cookie' information, device type, unique device identifiers, advertising identifiers, mobile device, operating system, the type of browser, demographic information, application and/or device(s) you're using to access our Services, click-through paths, the identity of the page or feature you are requesting or

interacting with, time on page, and other indicators of how you are interacting with the Services. »<sup>175</sup>

(Notre soulignement)

Pour ainsi dire, l'ensemble des interactions d'un utilisateur qui implique un produit Meross qu'elles aient été réalisées au moyen d'un assistant vocal ou directement au moyen de l'application du fabricant sont enregistrées par le fabricant. On peut donc conclure que l'information, si elle est détruite au sein de l'historique d'utilisation de l'assistant vocal, pourrait parallèlement se retrouver entre les mains d'un tiers, fabricant d'un autre élément de l'écosystème de l'IoT, mais qu'elle se présentera alors sous une forme moins conviviale nécessitant peut-être l'intervention d'un expert, avec toutes les conséquences que cela peut avoir.

### 1.2.3 La nature des moyens de preuve en présence

Avant de poursuivre l'analyse des éléments qu'il est possible d'extraire afin de prouver un fait pertinent dans un cas particulier, il convient de s'intéresser aux différentes qualifications possibles pour ces éléments.

Au regard du droit québécois, il y a longtemps eu une certaine confusion au niveau des documents technologiques et, auparavant, des enregistrements sonores ou vidéos. La jurisprudence et la doctrine québécoise, avant et depuis l'introduction de l'élément matériel de preuve dans le *Code civil du Québec* en 1991<sup>176</sup>, ont eu tendance à traiter les enregistrements

---

<sup>175</sup> CHENGDU MERROSS TECHNOLOGY CO., LTD., « Privacy Policy », *Meross.com* (2017), en ligne : <<https://us-iot.meross.com/public/smart/policy.html>>.

<sup>176</sup> *Code civil du Québec*, préc., note 90.

audios comme des éléments matériels<sup>177</sup>, desquels les juges avaient la tâche de tirer leurs propres conclusions. Cette tendance s'est aussi manifestée avec l'avènement de l'ère informatique.

Cependant, la qualification juridique des éléments de preuve technologiques, en fonction du droit québécois, se heurte aux technologies qui évoluent rapidement et crée une confusion dans les genres, non seulement parce que les technologies changent, mais aussi parce que les comportements des utilisateurs changent tout autant.

Dans le traité sur la preuve de Phipson, illustrant l'état du droit de la preuve au Royaume-Uni, les auteurs indiquent que la preuve technologique doit être abordée par deux angles distincts, en fonction des circonstances menant à sa création. Si la preuve est essentiellement générée par l'action d'une machine — par exemple, un capteur enregistre la température ambiante à heure fixe et enregistre cette information dans un fichier — il s'agit de preuve réelle — « real evidence ». Alors, le cadre juridique pertinent à la preuve matérielle s'y applique.

Dans le cas où l'information est fournie à la machine par un être humain — par exemple un employé saisi des données dans un tableur — il s'agit d'une forme de déclaration extrajudiciaire qui constitue, dans ces circonstances, du ouï-dire. Cette dernière preuve peut malgré tout demeurer admissible, en vertu d'une exception au ouï-dire<sup>178</sup>.

On peut avancer que les éléments de preuve tirés des assistants vocaux pourraient à la fois se composer de déclarations extrajudiciaires et de preuves réelles. En effet, il y a à la fois de l'information qui est transmise au système par l'utilisateur et de l'information que le système collecte automatiquement à l'occasion de son utilisation. Cette avenue de qualification, sans être la mieux adaptée selon nous, permet à tout le moins d'assimiler l'élément de preuve à un cadre existant.

---

<sup>177</sup> *Youroukova c. Dellorefice*, 2013 QCCQ 11055 (l'enregistrement audio sur une bande magnétique est forcément un élément matériel de preuve) ; *Métallurgistes unis d'Amérique, section locale 7785 et Caradon Indalex (division de Caradon ltée)*, [2000] CanLII 46584 (QC SAT) ; Jean-Claude ROYER, *La preuve civile*, Cowansville, Éditions Yvon Blais, 1987, par. 887 et 906 ; Henri KÉLADA, *Notion et technique de la preuve civile*, Montréal, Wilson Lafleur, 1986, p. 365, 368 à 369 ; *Erez Sewing Machine Co. Ltd c. Vêtement Super Vogue Inc.*, [1980] C.P. 157.

<sup>178</sup> Hodge M. MALEK, *Phipson on Evidence*, coll. « The Common law Library », Londres, Sweet & Maxwell, 2013, par. 28-28.

Dans le contexte américain, le droit se développant grâce à des lois particulières et à la common law, on constate qu’au regard des règles fédérales<sup>179</sup> de la preuve et de la procédure civile, l’information recueillie par les assistants vocaux est considérée comme étant de l’information sauvegardée sur un support électronique, ou « electronically stored information », pouvant être demandée à la partie adverse dans le processus de « discovery », c’est-à-dire lors de la communication de la preuve. Ce vocable a été introduit dans le droit de la preuve fédéral américain en 2006 par un amendement au *Federal Rules of Civil Procedures*<sup>180</sup>, lequel a modifié la Rule 34 pour y inclure les ESI :

« Rule 34. Producing Documents, Electronically Stored Information, and Tangible Things, or Entering onto Land, for Inspection and Other Purposes

(a) A party may serve on any other party a request within the scope of Rule 26(b):

(1) to produce and permit the requesting party or its representative to inspect, copy, test, or sample the following items in the responding party’s possession, custody, or control:

(A) any designated documents or electronically stored information—including writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations—stored in any medium from which information can be obtained either directly or, if necessary, after translation by the responding party into a reasonably usable form. »<sup>181</sup>

(Notre soulignement)

Cette règle, reprenant des catégories existantes, précisée et créée par d’autres textes législatifs, brosse cependant un portrait exhaustif des différents moyens de preuve en droit fédéral américain en matière civile. Parmi ceux-ci, les plus intéressants pour le présent exercice sont sans doute les « sound recordings » ainsi que des « other data or data compilations » qui pourraient selon nous, inclure de l’information comme les données de géolocalisation ainsi que

---

<sup>179</sup> Il faut aussi prendre en considération que la plupart des États américains disposent de règles de procédures civiles et de preuve. Bien que celles-ci peuvent apporter un éclairage pertinent en l’espèce, nous nous pencherons exclusivement ici sur les textes fédéraux afin de simplifier l’exercice de comparaison.

<sup>180</sup> *Federal Rules of Civil Procedures*, Rule 34.

<sup>181</sup> “Rule 34. Producing Documents, Electronically Stored Information, and Tangible Things, or Entering onto Land, for Inspection and Other Purposes”, *LII/Legal Information Institute*, p. 34, en ligne: <[https://www.law.cornell.edu/rules/frcp/rule\\_34](https://www.law.cornell.edu/rules/frcp/rule_34)>.

l'ensemble des sous-produits vraisemblablement pertinents générés par l'utilisation des assistants vocaux.

En droit européen continental, la preuve technologique est aussi admise, et ce, depuis près de deux décennies. En 1999, une directive européenne enjoignait les états membres à intégrer dans leurs droits de la preuve des dispositions relatives aux écrits technologiques et aux signatures électroniques<sup>182</sup>. Dans le contexte français, ce changement a eu lieu en mars 2000 par le biais de la *Loi n° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique*<sup>183</sup>. Bien que des réflexions<sup>184</sup> aient lieu en France relativement aux critères d'admissibilité d'éléments de preuve technologique, le fonctionnement inquisitoire du système juridique français laisse beaucoup de marge de manœuvre aux magistrats dans l'appréciation de la preuve matérielle visant à prouver des faits en litige dont les moyens de preuve ne sont pas autrement prévus par les textes de loi. Ainsi, on a vu des magistrats français accepter en preuve des messages texte<sup>185</sup>, voir même récemment des données de géolocalisation issues de la plateforme Instagram dans le cadre du litige successoral opposant différents héritiers de Jean-Philippe Smet, mieux connu sous le nom de Johnny Hallyday<sup>186</sup>. Dans aucun de ces contextes, les magistrats français n'ont-ils semblé ressentir la nécessité de discuter la force probante ou encore la nature des éléments de preuve en question.

Depuis le début de 2019 cependant, des lignes directrices du Conseil de l'Europe existent pour guider les législateurs européens dans la mise en place d'un cadre juridique pour les technologies

---

<sup>182</sup> CE, *Directive 1999/93/CE du Parlement européen et du Conseil, du 13 décembre 1999, sur un cadre communautaire pour les signatures électroniques*, JO, L 13/12 Voir aussi : ; CE, *Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur*, JO, L 178/1.

<sup>183</sup> *Loi n° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique*.

<sup>184</sup> Marylou GARCIAS et Max CHOUZIER, « La preuve informatique. Quelles nouveautés techniques pour quelles évolutions juridiques ? », *LexBase Hebdo* 2012.280, en ligne : <[http://www.adij.fr/wp-content/uploads/2012/01/CompteRendu\\_PpreuveInformatique.pdf](http://www.adij.fr/wp-content/uploads/2012/01/CompteRendu_PpreuveInformatique.pdf)>.

<sup>185</sup> *Cour de cassation, civile, Chambre sociale, 23 mai 2007, 06-43.209, Publié au bulletin*, [2007] Publié au bulletin (Cour de cassation) (messages textes dits « SMS » sont admissibles en preuve, car l'expéditeur sait qu'ils seront enregistrés par le destinataire) ; *Cour de Cassation, Chambre civile 2, du 7 octobre 2004, 03-12.653, Publié au bulletin*, (les enregistrements téléphoniques à l'insu de l'un des deux interlocuteurs sont irrecevables, car déloyaux).

<sup>186</sup> *Tribunal de grande instance de Nanterre*, [2019] RG 18/01502.



de l'information en matière civile et administrative<sup>187</sup>. Ces lignes directrices résultent d'un travail du Comité européen de coopération juridique et d'un rapport sur les pratiques relatives à la preuve technologique en Europe, dont nous discuterons davantage dans la seconde partie de ce mémoire. Citons seulement pour l'instant la définition de la « preuve technologique » proposée par le Conseil de l'Europe :

« On entend par “preuve électronique” toute preuve qui découle de données contenues ou produites par un dispositif dont le fonctionnement dépend d'un logiciel ou de données stockées ou transmises sur un système ou un réseau informatique. »<sup>188</sup>

(Notre soulignement)

Parallèlement, lors d'une récente conférence à Kobe au Japon, le professeur Sugiyama, agissant à titre de rapporteur général, faisait état d'une enquête menée auprès de répondants de différents pays au sujet de la preuve technologique, lesquels avaient préparé une série de rapports nationaux<sup>189</sup>. Cette enquête révèle que sur le plan de la qualification, les juridictions ne disposant pas de règles de recevabilité strictes n'avaient pas procédé à une définition de la preuve technologique, alors que celles où la recevabilité est encadrée s'étaient engagées dans un tel processus<sup>190</sup>.

Il ressort de l'analyse de Sugiyama que les juridictions, dont le Québec, où la recevabilité de la preuve est encadrée, distinguent généralement deux types de preuve, soit « oral evidence » et « real evidence »<sup>191</sup>, dont nous avons discuté brièvement ci-haut. Sugiyama avance que la preuve technologique est, de manière générale, considérée comme de la « real evidence », c'est-à-dire

---

<sup>187</sup> CONSEIL DE L'EUROPE, *Lignes directrices du Comité des Ministres du Conseil de l'Europe sur les preuves électroniques dans les procédures civiles et administratives*, (2019) CM (2018) 169-add1final, en ligne : <[https://search.coe.int/cm/Pages/result\\_details.aspx?ObjectId=0900001680902dc9](https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=0900001680902dc9)>.

<sup>188</sup> *Id.*

<sup>189</sup> Etsuko SUGIYAMA, *General Report on Current Situations and Problems Regarding New Types of Evidences, Challenges for Civil Justice As We Move Beyond Globalization and Technical Change*, Kobe, XVI World Congress on Procedural Law, 5 novembre 2019, p. 484.

<sup>190</sup> *Id.*, p. 504.

<sup>191</sup> *Id.*, p. 504 et suivantes.

de la preuve sujette à une forme de « judicial inspection »<sup>192</sup>. L'élément matériel de preuve québécois entre sans conteste dans cette catégorie générale. Cependant, l'approche développée par le professeur Vincent Gautrais et mise de l'avant par la Cour d'appel du Québec<sup>193</sup> pourrait apporter un éclairage différent sur le plan de la qualification des éléments de preuve dans un contexte technologique. Nous en discuterons dans la prochaine sous-section.

Considérant l'intérêt de ces questionnements, observons maintenant l'approche québécoise, qui s'oriente vers la fonction des éléments de preuve documentaire. Nous avons fait le choix d'aborder l'approche fonctionnelle de manière critique, considérant que celle-ci est relativement récente. Afin d'aborder les assistants vocaux, il nous a semblé plus efficace d'identifier les raisons pour lesquelles les catégories d'éléments de preuve existantes en droit civil québécois peuvent être inadéquates pour assurer la qualification des preuves issues des assistants vocaux.

### 1.2.3.1 Une critique de l'approche fonctionnelle

Le retour à la raison d'être des règles existantes est le fondement de la démarche du professeur Vincent Gautrais. Nous appliquerons ici la logique de son approche aux éléments de preuve que l'on pourra dégager de l'utilisation des assistants vocaux. En droit québécois, l'élément matériel de preuve, catégorie à laquelle on rattache le plus souvent les données issues de l'utilisation des assistants vocaux, n'est peut-être pas suffisante comme catégorie pour permettre un encadrement adéquat de ces nouveaux éléments émergeant de notre utilisation de ces technologies. À ce titre, l'approche fonctionnelle prônée par Gautrais et une certaine doctrine<sup>194</sup>, laquelle est soutenue par un courant jurisprudentiel jeune, mais établi<sup>195</sup>, se veut peut-être une réponse qui nous permettrait de trouver un sens à la présente situation.

---

<sup>192</sup> *Id.*, p. 511.

<sup>193</sup> *Benisty c. Kloda*, préc., note 15.

<sup>194</sup> V. GAUTRAIS, préc., note 12 Voir aussi : Catherine PICHÉ, *La preuve civile*, 5<sup>e</sup> éd., Montréal, Éditions Yvon Blais, 2016.

<sup>195</sup> *Benisty c. Kloda*, préc., note 15 Voir aussi, citant cette décision dans le contexte de la preuve technologique : *Autorité des marchés financiers c. Baazov*, 2018 QCCS 3422 ; *Giannini c. De Montigny*, 2018 QCCQ 6414 ; *Lauzon c. Noel*, 2018 QCCS 3903 ; *Drouin (Succession de Côté-Drouin) c. Pepin*, 2019 QCCS 848 ; *Holland c. St-*

Cependant, l'approche fonctionnelle peut être critiquée. Elle adapte des catégories existantes afin d'y assimiler des réalités nouvelles. Une autre approche consisterait peut-être à se questionner sur la nécessité d'élaborer de nouvelles catégories, sans hésiter à remettre en question celles qui existent déjà. Cette posture consiste à retourner à l'origine des raisonnements juridiques pour trouver les fondements qui les supportent — ce que propose aussi, d'ailleurs, l'approche fonctionnelle. De plus, l'approche fonctionnelle pourrait éventuellement créer, selon nous, une certaine confusion, car elle propose de distinguer la signification que pouvaient auparavant avoir certains concepts en leur attribuant une nouvelle signification. Il serait toutefois juste de soutenir que l'évolution de la signification d'un terme juridique dans le temps n'est pas un phénomène nouveau et que l'étude, en contexte, de la doctrine et de la jurisprudence permet d'éviter cette confusion<sup>196</sup>. Or, contrairement aux autres concepts juridiques dont le sens a évolué dans le temps, l'approche fonctionnelle pourrait engendrer des changements relativement rapides ne permettant pas aux années de faire évoluer les significations actuelles.

Au détour, l'approche fonctionnelle semble aussi consacrer, en droit québécois, trois principales catégories d'éléments de preuve, fermant la porte à l'élaboration d'une autre classification. Les nouvelles catégories pourraient cependant apporter des clarifications importantes et permettre de mieux distinguer différents moyens de preuve, à l'aune d'une évolution technologique incessante. L'approche fonctionnelle a cet avantage de permettre aux juristes de faire évoluer le droit, sans en changer la lettre. Au Québec, cette approche aurait pour effet de faire tendre le droit civil vers une rédaction davantage neutre sur le plan technologique, proche de l'énoncé général capable de durer dans le temps. Le pragmatisme commande peut-être cependant de faire des lois pour l'air du temps, moins sensibles à l'interprétation judiciaire.

Comment toutefois y parvenir sans créer des catégories si spécifiques qu'elles courent le risque de s'avérer rapidement obsolètes, face à l'avancée technologique rapide que nous connaissons ? Cette question renvoie à la comparaison mainte fois faite entre les systèmes juridiques de

---

*Eustache Mitsubishi*, 2019 QCCQ 4035; *Papp c. Alexeev*, 2019 QCCQ 4809 ; *M.F. c. Gravel*, 2019 QCCS 2521 ; *Fraternité des policiers et policières de Sherbrooke c. Sherbrooke (Ville)*, [2019] CanLII 82465 (QCTAT).

<sup>196</sup> On peut ici penser à l'évolution du concept de « personne raisonnable », lequel a déjà été assimilé au « bon père de famille ». Voir au sujet de la normativité des concepts juridiques : Mistral Goudreau, « Légiférer par généralités ou en termes précis ? Quelle question ! », *Institut canadien d'administration de la justice* 2019, en ligne : <<https://edoctrine.caij.qc.ca/ciaj-icaj/blogue/i962b7226-cb0f-46c7-9394-f474708f3e33/>>.

tradition civiliste et ceux de tradition de common law. Dans ces deux traditions, lesquelles cohabitent d'une unique manière dans le système judiciaire québécois, les juges ont un rôle identique et des approches de plus en plus semblables. Ces approches convergent en effet sous l'influence du bijuridisme canadien, du droit transnational en général, mais aussi de la nature du système judiciaire québécois qui est accusatoire et contradictoire.

Les catégories du droit de la preuve québécois, énoncées au *Code civil du Québec*, à savoir l'écrit, le témoignage, l'élément matériel, l'aveu et la présomption<sup>197</sup> sont remaniées par l'approche fonctionnelle qui ne considère que les trois premières comme des moyens de preuve « documentaire » — l'écrit, le témoignage et l'élément matériel. Le professeur Gautrais avance essentiellement que l'aveu est un témoignage particulier et que la présomption, bien qu'étant un procédé de preuve, n'est pas un procédé de preuve « documentaire » se révélant être essentiellement une application de la logique<sup>198</sup>.

Malgré les critiques que l'on puisse adresser à l'approche fonctionnelle, nous partirons ici de la prémisse qu'il n'est pas nécessaire d'élaborer de nouvelles catégories et observerons celles qui pourraient se révéler adéquates pour les assistants vocaux afin d'analyser celles qui existent déjà. Cependant, il n'est pas dit qu'une réflexion plus approfondie sur la possibilité d'élaborer de nouvelles catégories soit inutile, bien au contraire.

### **1.2.3.2 L'approche fonctionnelle appliquée aux éléments de preuve issus de l'utilisation des assistants vocaux**

L'approche fonctionnelle propose de se pencher sur ce que l'élément de preuve cherche à accomplir, soit sa fonction. Le professeur Gautrais avance qu'un élément de preuve relatant des faits à venir est un écrit, alors que celui qui relate des faits passés est un témoignage. L'élément de preuve qui rendrait compte d'un moment particulier — un arrêt sur image en quelque sorte

---

<sup>197</sup> *Code civil du Québec*, préc., note 90, art. 2811.

<sup>198</sup> V. GAUTRAIS, préc., note 12, par. 339.

— serait un élément matériel de preuve. Cette classification temporelle concorde avec les définitions doctrinales classiques de l'écrit et du témoignage, lesquels se veulent respectivement des preuves préconstituées<sup>199</sup> et des preuves à l'égard de faits passés dont une personne a eu personnellement connaissance. Arrivant aussi à ce constat, la Cour d'appel a appliqué ce raisonnement dans l'affaire *Benisty c. Kloda* où il était essentiellement question d'enregistrements sonores :

« [57] Si le contenu de l'enregistrement est la déclaration d'une personne sur des faits passés dont elle a eu personnellement connaissance, il s'agit d'un témoignage (2843 C.c.Q.).

[58] Pour que cette déclaration extrajudiciaire soit admise en preuve, elle doit d'abord répondre aux règles prévues par les articles 2869 à 2874 C.c.Q. compte tenu des dispositions de l'article 2874 C.c.Q., son authenticité doit aussi être démontrée. Sauf exception, cet enregistrement valant témoignage ne peut pas non plus servir à prouver un acte juridique ou un écrit (2860 à 2862 C.c.Q.) ni contredire un acte juridique constaté par écrit (2863 C.c.Q.).

[59] Si le contenu de l'enregistrement permet plutôt au tribunal de constater un fait documenté par une personne à un moment précis, il s'agit d'un élément matériel de preuve (2854 C.c.Q.). Ainsi, lorsque l'enregistrement capte un fait contemporain ou sur le vif, s'il s'agira d'un élément matériel.

[60] À titre d'exemple, lorsqu'une personne est enregistrée à son insu durant une conversation téléphonique ou un entretien, on considérera qu'il s'agit d'un élément matériel de preuve, alors qu'une personne qui s'enregistre elle-même et dicte un récit tend plutôt à établir un témoignage.

[61] Il ne faut pas perdre de vue qu'en vertu des règles relatives à la présentation d'un élément matériel de preuve, tout comme le témoignage enregistré (article 2874 C.c.Q.), l'enregistrement doit faire l'objet d'une preuve distincte de son authenticité (article 2855 C.c.Q.). »<sup>200</sup>

(Références omises ; notre soulignement)

---

<sup>199</sup>Une idée que l'on retrouve déjà chez l'auteur Louis Josserand : « [L'écrit] est la preuve par excellence, notamment à raison de son caractère préconstitué ; elle est instaurée à l'avance, avant qu'il soit question de la mettre à profit et non pour les besoins de la cause », cité par : Paul FORIERS, « Introduction au droit de la preuve », dans *La Preuve en droit. Études*, coll. « Travaux du Centre national de recherches de logique », Bruxelles, Bruylant, 1981 à la page 18.

<sup>200</sup> *Benisty c. Kloda*, préc., note 15, par. 56 à 61.

Dans cette vision des choses, il n'y a pas de considération particulière pour la nature tangible des objets mis en preuve. Ils doivent répondre aux impératifs du droit de la preuve présents au *Code civil du Québec*<sup>201</sup> et dans les autres lois particulières<sup>202</sup>. Dans le cas des assistants vocaux, ces éléments de preuve prendraient forcément une forme technologique<sup>203</sup>. De fait, ils devraient répondre aux conditions de recevabilité prévues à la LCCJTI.

Technologiques ou non, en fonction de l'approche du professeur Gautrais, les éléments de preuves documentaires entrent dans les trois catégories que sont le témoignage, l'écrit et l'élément matériel. Cela étant dit, toutes ne sont pas les plus appropriées, et ce, considérant la nature de l'utilisation qui est faite des assistants vocaux, bien que l'on puisse concevoir que toutes les catégories pourraient être représentées.

En premier lieu, la catégorie des écrits s'applique relativement mal aux traces des interactions entre les utilisateurs et leurs assistants vocaux. L'écrit, en droit français, se compose d'une suite de mots. Le droit québécois ne fait pas de telle distinction. Comme le souligne Gautrais<sup>204</sup>, l'écrit n'a pas de définition stricte. Les auteurs le décrivent comme une preuve préconstituée<sup>205</sup> ou encore comme un document constatant certains faits<sup>206</sup>. Gautrais rappelle aussi que ce n'est pas forcément parce que quelque chose est écrit, c'est-à-dire représenté par une écriture, qu'il s'agit forcément d'un écrit au sens du moyen de preuve<sup>207</sup>. La catégorie de l'écrit s'intéresse, du point de vue de l'approche fonctionnelle, aux fonctions de l'instrument que les cocontractants préparent en prévision de faits juridiques futurs ou encore à la fonction probatoire que certains

---

<sup>201</sup> *Code civil du Québec*, préc., note 90.

<sup>202</sup> *Loi concernant le cadre juridique des technologies de l'information*, préc., note 14 ; *Loi sur la preuve au Canada*, préc., note 18.

<sup>203</sup> La qualification de document « technologique » en droit québécois a suscité un débat dans la doctrine, lequel a fait l'objet d'une analyse par la Cour d'appel dans la récente affaire *Benisty*. Au sortir de cette analyse, la Cour se range derrière les arguments de Gautrais et Gingras ainsi que ceux de Fabien dans son appréciation du terme « technologique », lequel doit avoir une portée large. Voir à ce sujet : *Benisty c. Kloda*, préc., note 15, par. 64 et suivants ; C. FABIEN, préc., note 172 ; V. GAUTRAIS et P. GINGRAS, préc., note 140.

<sup>204</sup> V. GAUTRAIS, préc., note 12.

<sup>205</sup> C. PICHÉ, préc., note 194, par. 251 ; L. DUCHARME, préc., note 172, par. 153, 154 ainsi que 342 (écrits sous seing privé).

<sup>206</sup> C. PICHÉ, préc., note 194, par. 252 et 253 ; L. DUCHARME, préc., note 172, par. 158 (actes authentiques).

<sup>207</sup> V. GAUTRAIS, préc., note 12, par. 496 et suivants.

documents sont destinés à avoir au moment de leur confection. L'écrit est avant toute chose une preuve préconstituée laquelle, pour son auteur, sert une fonction protectrice.

La définition de l'écrit peut aussi prendre la forme d'un document pouvant être consulté ultérieurement à sa confection, pour servir de référence. Cette dernière caractéristique issue des travaux de la CNUDCI est toutefois contestée<sup>208</sup> puisque trop générale. Cette critique nous semble par ailleurs des plus légitimes dans un contexte technologique en vertu duquel presque l'ensemble de ce qui est produit par ou au moyen d'un ordinateur est susceptible d'être conservé pour une consultation ultérieure.

L'approche fonctionnelle proposée par le professeur Gautrais pourrait permettre de qualifier un enregistrement sonore en tant qu'écrit. Avant les récents développements doctrinaux et jurisprudentiels, un enregistrement sonore aurait sans doute été systématiquement qualifié d'élément matériel de preuve<sup>209</sup>, tant qu'il ne recèle pas un témoignage, un aveu ou une déclaration extrajudiciaire<sup>210</sup>. Toutefois, cela ne signifie pas pour autant que l'ensemble des enregistrements sonores sont des écrits ou des témoignages, loin de là. L'exercice de réflexion devient alors nécessaire. Une grande partie de la jurisprudence antérieure devra donc sans doute être nuancée, remise en contexte, afin de prendre en considération l'évolution de la relation des utilisateurs avec les technologies.

Pour l'ensemble de ces raisons, bien que plusieurs éléments écrits soient susceptibles d'exister en lien avec l'utilisation des assistants vocaux, l'écrit ne nous semble pas être la catégorie appropriée pour qualifier ce qui est le plus susceptible de ressortir de ces interactions, puisque ces outils ne seront vraisemblablement pas utilisés pour créer des contrats entre les individus, sauf dans l'optique des commandes réalisées pour effectuer des achats avec la voix, au moyen d'applications de commerce en ligne comme la plateforme Amazon<sup>211</sup>.

Ainsi, au moment de leur création, les enregistrements audios créés par Alexa ou l'Assistant Google, tout comme les historiques d'utilisation qui en permettent la consultation, ne servent

---

<sup>208</sup> *Id.*, n° 351.

<sup>209</sup> Voir, notamment : H. KÉLADA, préc., note 177 ; J.-C. ROYER, préc., note 177.

<sup>210</sup> C. PICHÉ, préc., note 194, par. 828 ; Voir aussi : *R. c. M. G.*, 2015 QCCQ 4864.

<sup>211</sup> Nombreux diront qu'Alexa, l'assistant virtuel d'Amazon, n'est pas au premier chef un assistant virtuel autant qu'une manière de rendre encore plus accessible la plateforme Amazon à ces utilisateurs.

pas de visées probatoires futures pour l'utilisateur, mais sont plutôt, pour celui-ci, une trace de son utilisation, certes pour une consultation ultérieure, mais pas forcément à dessein de servir éventuellement à titre de preuve. Ces historiques, rendus disponibles pour les utilisateurs via leur compte ou différentes plateformes en fonction des produits, se veulent aussi une manière pour ces entreprises de montrer patte blanche relativement à l'information qu'elles collectent sur ces utilisateurs, au-delà des définitions strictes des conditions d'utilisation liées à leurs produits.

Ouvrons toutefois ici une parenthèse. Dans l'optique où un litige se déclarerait entre un fournisseur de services — par exemple Amazon — et un utilisateur, les conversations et autres données enregistrées par Amazon et en sa possession avantageraient démesurément la compagnie au détriment de l'utilisateur. Avec cet enregistrement, Amazon peut donc, pour sa part, avoir des visées probatoires futures. Ce genre de situation n'est aucunement prise en compte par le droit de la consommation. Pourtant, le rapport asymétrique que nous venons de décrire pose de sérieuses questions d'équité en l'espèce.

Encore est-il pertinent de mentionner que l'assistant vocal Alexa renferme peut-être des fonctions rapprochant les documents qu'il produit d'un écrit, puisque ceux-ci pourraient être appelés à documenter une transaction de vente. Cependant, la conclusion du contrat, réalisé au moyen de la voix, dépendra de la manière dont l'utilisateur aura préalablement paramétré<sup>212</sup> son assistant vocal, puisque, pour éviter de commettre des erreurs, Amazon offre la possibilité à ses clients d'utiliser un code vocal à quatre chiffres afin d'augmenter le niveau de sécurité lié aux transactions vocales. Les utilisateurs peuvent aussi confirmer les commandes passées au moyen d'Alexa via un appareil mobile et disposent d'un certain temps pour les modifier ou les annuler sans frais, comme les autres commandes passées sur le site transactionnel.

Une commande ainsi confirmée au moyen d'un code vocal ou d'un appareil mobile ne serait véritablement conclue qu'au moment de sa confirmation – et le contrat la représentant le serait tout autant. L'utilisateur peut toutefois désactiver cette fonction protectrice. Sa désactivation rend possible la formation de contrat au moyen de sa seule voix. Ces transactions, ne l'oublions

---

<sup>212</sup> AMAZON.COM, INC., "Aide. Gérer les paramètres d'achats vocaux», *Amazon.com* (2019), en ligne : <<https://www.amazon.ca/-/fr/gp/help/customer/display.html?nodeId=201952610>>.



pas, demeurent assujetties au cadre général de l'utilisation d'Amazon et d'Alexa, permettant d'assouplir les formalités au moment d'acheter quoi que ce soit<sup>213</sup>.

Cette forme de commerce en ligne, où la navigation est dématérialisée, pose des questions intéressantes en matière de preuve. La commande passée au moyen de la voix présente-t-elle un quelconque intérêt ou d'autres écrits, comme la facture envoyée par courriel au client à la suite de la vente, devraient-ils prendre une place plus importante dans notre analyse ? Les factures, par exemple, suivent un formalisme certain, contrairement à l'enregistrement de la voix de l'utilisateur qui pourrait être comparé à une caméra de surveillance située au-dessus de la caisse enregistreuse d'un magasin de détail.

Aussi, pendant cette réflexion sur la qualification du moyen de preuve, il faut aussi prendre en considération que l'assistant vocal, tel qu'il en a été question précédemment dans ce mémoire, parvient à déceler la signification de ce que lui dit son interlocuteur au moyen d'algorithmes d'intelligence artificielle qui lui permettent concurremment de répondre. L'interprétation que fait l'intelligence artificielle de la voix d'une personne est tributaire de l'état de sa base de données et de son entraînement à un moment précis dans le temps. La réponse que l'assistant vocal donne est, quant à elle, le plus souvent fonction des bases de connaissances que l'assistant aura consultées à un moment précis pour satisfaire la commande de l'utilisateur.

Ce constat technique révèle donc une difficulté : même si les traces documentaires des interactions entre un utilisateur et son assistant vocal pourraient constituer une certaine preuve d'un accord de volonté entre un marchand et un utilisateur, il est difficile d'imaginer que l'interprétation faite par l'assistant vocal ainsi que sa réponse puissent être autre chose que des éléments matériels de preuve, dans le cadre de l'approche fonctionnelle. En effet, ces éléments sont le reflet de l'état précis d'un algorithme et d'une base de connaissances à un moment donné. L'information fournie au système déclenche, certes, la réponse, mais cette réponse ne saurait être une preuve préconstituée, car il est impossible pour l'utilisateur de savoir présomptivement et avec certitude ce que l'algorithme comprendra de sa commande vocale. Ainsi, la nature de l'information enregistrée par les assistants vocaux et la nature du traitement qu'ils appliquent à

---

<sup>213</sup> Par exemple, les produits commandés vocalement au moyen d'Alexa sont sélectionnés dans un bassin de produits vedettes (bénéficiant du programme « Amazon Prime ») et ayant été achetés aux préalables par le consommateur.

celle-ci font en sorte que les éléments de preuve qui en découlent sont forcément des éléments matériels de preuve.

Malgré cette constatation, la question du témoignage présente aussi un intérêt certain. On peut se demander si, dans certains contextes, les interactions que l'on pourrait avoir avec un assistant vocal pourraient être des déclarations extrajudiciaires ou des aveux. Le professeur Gautrais, au moment de discuter de l'approche fonctionnelle, a sciemment mis de côté l'aveu, qualifiant ce moyen de preuve de témoignage particulier<sup>214</sup>. Cette position est cohérente avec l'approche qu'il met de l'avant dans son ouvrage sur la preuve technologique et l'idée que l'aveu est une forme de témoignage très différente du témoignage en général.

En effet, l'aveu est défini comme la « reconnaissance d'un fait de nature à produire des conséquences juridiques contre son auteur »<sup>215</sup>, sur ce plan il se distingue du témoignage<sup>216</sup>. Parallèlement, le témoignage, pour sa part, peut se définir comme étant une déclaration à propos d'un fait antérieur dont le témoin a eu personnellement connaissance<sup>217</sup>. La connaissance personnelle prohibe donc le témoignage d'un tiers à qui on aurait relaté certaines informations. Le oui-dire est ainsi prohibé, de manière générale, en droit québécois<sup>218</sup> – une prohibition que l'on retrouve tout autant d'autres systèmes juridiques, tant du côté américain<sup>219</sup> qu'européen<sup>220</sup>.

L'approche du professeur Gautrais propose que le témoignage soit un moyen de preuve portant sur des faits situés dans le passé, par rapport à la déclaration le composant. Ce constat, dans le contexte des assistants vocaux, nous pousse à croire que les traces de l'utilisation de ceux-ci ne s'imaginent que difficilement en tant que témoignages.

---

<sup>214</sup> V. GAUTRAIS, préc., note 12, par. 339.

<sup>215</sup> *Code civil du Québec*, préc., note 90, art. 2850.

<sup>216</sup> *Id.* ; C. PICHÉ, préc., note 194, par. 1043 ; Voir aussi : L. DUCHARME, préc., note 172, par. 643 (définition de l'aveu).

<sup>217</sup> *Code civil du Québec*, préc., note 90, art. 2843 ; C. PICHÉ, préc., note 194, par. 514 ; Voir aussi : L. DUCHARME, préc., note 172, par. 523 et 524 (définition du témoignage).

<sup>218</sup> C. PICHÉ, préc., note 194, par. 736 à 739 ; *Code civil du Québec*, préc., note 90, art. 2843 (définition du témoignage) ainsi que 2860 (meilleure preuve) ; L. DUCHARME, préc., note 172, par. 1255, 1266 ainsi que 1269 et suivants (preuves écrites) ; Voir aussi, dans un contexte canadien : David M PACIOCCO et Lee STUESSER, *The Law of Evidence*, 7<sup>e</sup> éd., coll. « Essentials of Canadian Law », Toronto, Irwin Law Inc, 2015, p. 113.

<sup>219</sup> Voir notamment la Rule 802 prohibant le oui-dire (*hearsay*) dans : *Federal Rules of Evidence*, préc., note 20, art. 802.

<sup>220</sup> *Code de procédure civile*, art. 199.

Dans le même esprit, la prohibition du oui-dire, découlant de certaines garanties procédurales historiques, jette généralement une certaine ombre sur les enregistrements audiovisuels, puisque ceux-ci ne permettent pas à la partie adverse de contre-interroger un témoin. Or, dans le cas des informations recueillies par un assistant vocal, la catégorie de l'aveu pourrait être d'un grand intérêt. Les informations recueillies par un assistant vocal le sont souvent dans un contexte domestique et privé, où le justiciable est susceptible de dire la vérité. De ce fait, nous soumettons donc l'hypothèse que l'aveu pourrait représenter une avenue de qualification intéressante pour les traces des interactions entre l'utilisateur et son assistant vocal. Cependant, ici s'arrête l'optimisme, car il nous semble possible, mais peu probable que ces traces répondent aux exigences entourant l'aveu extrajudiciaire<sup>221</sup>.

En effet, l'aveu extrajudiciaire pourrait se composer des enregistrements des paroles d'un utilisateur ayant l'intention de déclencher une certaine commande au moyen de son assistant vocal. Dans ce cas, l'aveu serait consigné dans une forme de document<sup>222</sup>, un enregistrement sonore, et pourrait produire des effets contre son auteur. Or, il faudrait que cet aveu soit univoque, en ce sens où sa clarté ne laisse pas de doute relativement à l'intention de l'utilisateur déclarant<sup>223</sup>. L'aveu est généralement indivisible, en ce sens où celui qui désire l'utiliser en tant que preuve ne peut pas retrancher d'une telle déclaration certaines parties qui ne lui conviennent pas. Dans le cas des assistants vocaux, la qualification d'aveu se bute à une autre problématique : on pourrait aisément soutenir que l'assistant vocal n'a pas enregistré l'ensemble d'une déclaration, ou encore que ce qu'il a enregistré ne peut être mis en contexte. Cela pose des questions sérieuses quant à la recevabilité et la force probante de l'aveu. Ces réserves nous poussent à croire que l'aveu n'est peut-être pas la catégorie qu'il convient d'utiliser pour qualifier les traces laissées par l'utilisation des assistants vocaux.

Dans la même veine, nous sommes d'avis qu'une commande involontaire ne pourrait être qualifiée d'aveu, car l'intention de déclarer quelque chose serait manquante. Une telle

---

<sup>221</sup> Cela nous semble peu probable, car les interactions avec les assistants vocaux sont par nature courtes. Or, l'aveu n'a pas à être explicite, il peut aussi être implicite. Voir à ce sujet : C. PICHÉ, préc., note 194, par. 1045 et 1056 ; *Code civil du Québec*, préc., note 90, art. 2851.

<sup>222</sup> C. PICHÉ, préc., note 194, par. 1054 ; Voir aussi : L. DUCHARME, préc., note 172, par. 672 à 675 (forme de l'aveu).

<sup>223</sup> C. PICHÉ, préc., note 194, par. 1055 ; L. DUCHARME, préc., note 172, par. 669 et 670.

commande involontaire serait alors un élément matériel de preuve. Dans un contexte similaire, l'aveu pourrait avoir été capté par un assistant vocal activé pour une raison complètement indépendante. Ainsi, une conversation pourrait avoir été enregistrée par un assistant vocal à la suite d'une commande sans aucun lien avec cette conversation, par exemple allumer une lumière. Dans ce cas, un aveu pourrait être enregistré par un assistant vocal, en bruit de fond.

Enfin, pour être qualifiée d'aveu — malgré toutes les réserves que nous venons d'évoquer — une déclaration enregistrée par un assistant vocal devra produire des effets contre son auteur et non pas lui être favorable. Dans ce dernier cas, l'auteur pourra selon nous tenter d'utiliser cet enregistrement en proposant la qualification d'élément matériel.

On peut conclure, à la lumière des réflexions que nous venons de tenir, qu'en fonction des catégories analysées par le professeur Gautrais dans sa théorisation de l'approche fonctionnelle, les éléments de preuves recueillis de l'utilisation des assistants vocaux ne correspondent pas nettement aux catégories de preuve classiques. Nous avançons, dans la même veine que le professeur Gautrais, que ces éléments de preuve devraient être analysés suivant certains facteurs. D'abord, leur fonction initiale devrait prendre une grande place dans l'analyse. Les éléments avaient-ils une fonction probative future ou visaient-ils uniquement à faire fonctionner un algorithme ? Ensuite, la temporalité de la preuve pourrait s'avérer un facteur important. Les propos enregistrés se réfèrent-ils au passé, au futur ou au présent ? Encore, l'étendue de l'information enregistrée sera selon nous déterminante. Est-ce que l'assistant vocal n'a capté que quelques bribes de conversation ou a-t-il enregistré un extrait complet ou même un échange verbal complexe entre plusieurs personnes ? Enfin, l'utilité de cette preuve pour le justiciable nous semble un point à considérer pour les fins de qualification. Souhaite-t-on utiliser un tel élément pour faire une preuve directe que certains propos ont été tenus, ou est-ce pour illustrer certaines circonstances dans un contexte plus large ?

S'il ressort, certes que les catégories de l'écrit et de la déclaration extrajudiciaire ne pourraient que difficilement s'appliquer, nous avons pu constater que l'aveu — autrement exclu par Gautrais de son analyse — pourrait être une avenue possible de qualification. La déclaration enregistrée par un assistant vocal pourrait faire ressortir une volonté manifeste, mais peut-être pas suffisante pour correspondre aux conditions d'admissibilité de l'aveu. Devant l'impossibilité de satisfaire ces conditions, le juriste pourrait avoir à changer son fusil d'épaule

et opter pour une autre voie de qualification, comme la déclaration extrajudiciaire autrement admissible selon certaines exceptions, pour servir de preuve de son contenu.

Force est de constater toutefois que la majorité des éléments que l'on pourrait titrer des assistants vocaux seraient sans doute considérés comme des instantanés, représentant une situation factuelle précisément située dans le temps et, dès lors, des éléments matériels de preuve dont l'authenticité doit être prouvée par tout moyen afin d'assurer leur recevabilité et dont la détermination de la force probante incombe au tribunal, deux sujets dont nous allons discuter à la prochaine section.

## 2. Recevabilité et force probante

La recevabilité de la preuve technologique, à l'image de sa qualification, a fait l'objet de quelques textes législatifs et paralégislatifs tant au Canada qu'ailleurs<sup>224</sup>. On pense à certaines lois<sup>225</sup>, normes<sup>226</sup> ou standards<sup>227</sup> qui guident — souvent de manière très générale — parties et magistrats dans l'administration de ce type de preuve, le plus souvent avec des références technologiques dépassées ou trahissant l'âge du texte<sup>228</sup>. Dans le cas précis du Québec, la

---

<sup>224</sup> Consulter à ce sujet l'étude comparative de Mason et Rasmussen préparée à la demande du Conseil de l'Europe où ceux-ci effectuent un recensement complet des cadres juridiques applicables à la qualification et la recevabilité de la preuve technologique au sein des États membres : Stephen MASON et Uwe RASMUSSEN, *L'utilisation des preuves électroniques dans les procédures civiles et administratives et son impact sur les règles et modes de preuve. Étude comparative et analyse*, CDCJ (2015) 14, Strasbourg, Comité européen de coopération juridique du Conseil de l'Europe, 2016, en ligne : <<https://rm.coe.int/16807007ca>>.

<sup>225</sup> *Loi concernant le cadre juridique des technologies de l'information*, préc., note 14.

<sup>226</sup> SECRÉTARIAT DU CONSEIL DU TRÉSOR DU CANADA, *Norme pour les systèmes de gestion électronique des documents et des dossiers (SGEDD)*, 26 mai 2010, en ligne : <<https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=18910>> ; OFFICE DES NORMES GÉNÉRALES DU CANADA, *Enregistrements électroniques utilisés à titre de preuves documentaires*, CAN/CGSB-72.34-2017, en ligne : <[http://publications.gc.ca/collections/collection\\_2018/ongc-cgsb/P29-072-034-1-2017-fra.pdf](http://publications.gc.ca/collections/collection_2018/ongc-cgsb/P29-072-034-1-2017-fra.pdf)>.

<sup>227</sup> On pense par exemple aux standards techniques dans le domaine de la sécurité de l'information de la famille ISO 27000 dont le professeur Gautrais fait l'analyse dans son ouvrage. Voir : V. GAUTRAIS, préc., note 12, par. 221 et suivants.

<sup>228</sup> Un exemple intéressant est celui de la « sortie imprimée » qui dans la *Loi sur la preuve* permet de satisfaire la règle de la meilleure preuve. Cet article, édicté en l'an 2000, ne nous semble plus en phase avec les différentes réalités technologiques depuis son entrée en vigueur. Voir : *Loi sur la preuve au Canada*, préc., note 18, art. 31,2, al. 2.

recevabilité, comme nous le montrerons, repose essentiellement sur certaines étapes préliminaires de vérification de l'intégrité, lesquelles s'ajoutent au cadre général du droit de la preuve.

Néanmoins, la nature technologique de certains éléments de preuve suscite des réflexions sur les aspects procéduraux liés à l'administration de ce genre de preuves et sur la possibilité et, en certains cas, sur la pertinence de les mettre à l'épreuve. Croire que toutes les preuves technologiques sont parfaites sur les plans de l'authenticité et de la force probante, et ce parce qu'elles ont pris naissance au sein d'un système informatique, relève d'une logique défailante. L'exercice cherchant à dégager la signification des éléments de preuve technologique ne doit pas être escamoté, celui cherchant à montrer que ces éléments sont ce qu'ils prétendent non plus.

D'un autre côté, confronter chaque élément de preuve aux potentiels défauts de sa nature ferait peser sur les épaules des justiciables et de l'appareil judiciaire un fardeau énorme, lequel réduirait l'accès à la justice. Concurrément, faire preuve d'un relativisme aveuglant ne permettrait d'arriver à aucune conclusion et paralyserait tout travail judiciaire.

C'est pour pallier ces effets potentiellement pervers que plusieurs législateurs, dont le législateur québécois, ont mis en place des présomptions facilitant l'administration de la preuve technologique. Sur le plan de la force probante cependant, le juge conserve une marge de manœuvre considérable.

Ainsi, les éventuelles traces de l'utilisation des assistants vocaux que nous avons identifiées dans la première partie de ce mémoire feront maintenant l'objet d'une analyse de leur recevabilité, des exceptions à celle-ci et, pour conclure, de leur force probante. Pour accomplir cet exercice, nous adopterons le même style comparatif que précédemment afin de tenter de dégager le parcours procédural efficace pour ces traces documentaires et évaluer en toute connaissance de cause ce qu'elles signifient.

## 2.1 Conditions de recevabilité

La qualification d'un objet présenté au tribunal, en droit, peut sembler n'être qu'une considération de moindre importance, la jurisprudence ayant déjà laissé sous-entendre que les débats sur la nature des éléments de preuves pouvaient se révéler d'un caractère doctrinal et éloigné de la pratique et des réalités juridiques en cause. La Cour d'appel du Québec mentionnait en 2018 :

« [La] qualification me semble toutefois plus théorique que pratique. En effet, tel que je l'expliquerai plus loin, je dois reconnaître qu'une partie qui souhaite présenter un document technologique à titre d'élément matériel ou de témoignage ne sera pas dispensée de faire la preuve de son authenticité. »<sup>229</sup>

C'est le plus souvent au profit de l'analyse de la force probante que l'on tend à délaissier la discussion relativement à la qualification et la catégorisation des éléments de preuve. On préfère couper court à la recherche du mot juste pour dire *de quoi il s'agit*, cherchant plutôt *les effets* de la chose en question. Cependant, considérant la nature nouvelle des objets qui nous intéressent en l'espèce, la réponse à cette question nous semblait pertinente, puisque la question *de quoi s'agit-il ?* est bien souvent la prémisse aux questions *comment en faire la preuve ?* Et, corollairement, *que cette preuve signifie-t-elle ?* deux questionnements que nous analyserons ici dans une discussion qui s'articulera autour d'un retour sur l'importance du support technologique, de la pertinence, de l'intégrité, l'authenticité et de l'intelligibilité de l'information.

---

<sup>229</sup> *Benisty c. Kloda*, préc., note 15, par. 84.

## 2.1.1 Circonscrire l'information et son support

Avant de nous attarder aux différentes conditions de recevabilité des éléments de preuve technologique, nous croyons pertinent de discuter davantage de la distinction entre le support et l'information composant un document. Il s'agit d'une distinction qui prend beaucoup d'importance en l'espèce. En droit québécois, le concept de « document » est au centre du concept de preuve technologique. Il s'agit de l'unité de base, de l'objet de droit qu'il convient d'analyser en considérant les règles du droit de la preuve. Or, la seule définition de ce concept pose ses propres défis, le terme « document » n'étant pas à priori issu du vocabulaire juridique, mais trouvant plutôt origine en bibliothéconomie.

Sur le plan strict, il s'agit de la conjonction d'une information et d'un support<sup>230</sup>. L'information se décline en une infinité de possibilités. Les supports aussi peuvent être nombreux. Dans un contexte classique, antérieur à la révolution technologique, une feuille de papier portant des inscriptions manuscrites constituait un document. Une photographie entre aussi dans cette définition qui est par nature plus large que les qualificatifs propres aux moyens de preuve présents dans notre corpus juridique. Toutefois, le contexte technologique des vingt dernières années opère un bouleversement créant une confusion des genres.

Le concept de « document » semble intuitivement être associé à l'écrit, un moyen de preuve. Cette confusion repose essentiellement sur la rapide évolution technologique et l'idée reçue que le « document » et la feuille de papier sont intrinsèquement liés. Le papier a historiquement servi de support aux documents depuis le onzième siècle en Europe<sup>231</sup>. Cela permet de comprendre pourquoi document et papier ont parfois été considérés synonymes. Nous savons aujourd'hui que tel n'est pas le cas.

---

<sup>230</sup> « Un document est constitué d'information portée par un support. », *Loi concernant le cadre juridique des technologies de l'information*, préc., note 14, art. 3.

<sup>231</sup> La première mention du papier, sous une forme primitive, dans le contexte européen a lieu en Espagne vers l'an 1000. On peut toutefois faire remonter son origine en Asie ainsi qu'en Afrique. Voir à ce sujet : Thomas COLLINGS et Derek MILNER, "A New Chronology of Papermaking Technology", (1990) 14-1 *Journal of the Institute of Paper Conservation* 58.



Dans le cas des assistants vocaux, l'information se présentera sous la forme de pages Web, d'enregistrements sonores, de code machine, ou encore de documents générés par une fonctionnalité de l'assistant en vue de leur consultation par l'utilisateur, à l'instar de l'historique des commandes vocales. Dans tous ces cas, les supports sont dits « technologiques » au sens du droit québécois<sup>232</sup>. Bien que la doctrine québécoise présente le support technologique de manière large, elle l'associe toutefois à un élément physique<sup>233</sup>, sur lequel se trouve l'information. Selon nous, elle escamote de ce fait une réalité nouvelle propre à l'infonuagique, technologie faisant appel à des périphériques informatiques distants de l'utilisateur. Ainsi, bien que l'information de l'utilisateur soit forcément sauvegardée sur un support physique quelque part, il y a peu de chance que ce support soit identifiable pour l'utilisateur, qui n'a pas accès aux serveurs des grandes entreprises qui proposent ce genre de services. Encore, l'information pourrait être fragmentée et disséminée sur différents serveurs<sup>234</sup>.

Toutefois, puisque l'historique d'utilisation, le document que nous avons identifié dans la première partie de ce mémoire, se manifeste sous la forme d'une page Web<sup>235</sup>, il est pertinent de rappeler que cette page se matérialise dans l'ordinateur d'un utilisateur au moyen d'un navigateur Web. Les fichiers composant la page se téléchargent et forment un tout grâce à un logiciel, le navigateur Web. Nous avons discuté du fait qu'il est possible de télécharger un fichier d'archivage permettant de restituer une page Web dans l'état où elle se trouvait au moment de sa consultation. En soi, ce fichier d'archivage est le document technologique que l'on tentera vraisemblablement d'utiliser en preuve.

---

<sup>232</sup> *Loi concernant le cadre juridique des technologies de l'information*, préc., note 14, art. 1 al. 1 par. 2.

<sup>233</sup> Par exemple, le disque dur, la carte mémoire, la clef USB. Voir notamment : M. PHILLIPS, préc., note 13, par. 31 à 33 ; V. GAUTRAIS, préc., note 12, p. 186 à 188.

<sup>234</sup> Mehdi BAHRAMI et Mukesh SINGHAL, « The Role of Cloud Computing Architecture in Big Data », dans Witold PEDRYCZ et Shyi-Ming CHEN (dir.), *Information Granularity, Big Data, and Computational Intelligence*, coll. « Studies in Big Data », Cham, Springer, 2015, p. 275 aux pages 291 et suivantes (relativement aux enjeux entourant le « Cloud computing »), en ligne : <[https://doi.org/10.1007/978-3-319-08254-7\\_13](https://doi.org/10.1007/978-3-319-08254-7_13)> ; Yashpalsinh JADEJA et Kirit MODI, *Cloud Computing. Concepts, Architecture and Challenges, 2012 International Conference on Computing, Electronics and Electrical Technologies (ICCEET)*, 2012 International Conference on Computing, Electronics and Electrical Technologies (ICCEET), 2012, p. 877, p. 878, en ligne : <<https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6203873>>.

<sup>235</sup> Du moins pour les produits mis en marché par Google et Amazon.

Or, la doctrine nous enseigne que trois éléments en l'espèce sont indissociables, soit le support, l'information et le format de l'information<sup>236</sup>. Dans le contexte de l'infonuagique et des opérations se déroulant sur l'Internet, le support est en quelque sorte technologique par défaut. Il est porteur d'une information, par exemple les données liées à l'utilisation d'un assistant vocal, lesquelles se présentent sous un format particulier, c'est-à-dire dans un fichier faisant appel à une technologie particulière. C'est ce double emploi du vocable « technologie » qui fera dire à Gautrais que ce terme s'applique à la fois au support qui doit être « technologique » ainsi qu'à « la technologie » portée par le support. Sans ce deuxième sens, on pourrait aisément utiliser un crayon-feutre pour écrire un contrat sur un disque dur, créant techniquement un « document technologique » et pervertissant le sens de la LCCJTI.

Ce double sens du terme « technologique » nous pousse donc, dans le contexte des assistants vocaux, à considérer à la fois l'environnement technologique dans lequel l'ensemble de ces opérations ont lieu, d'une part et les traces qui en résultent ; d'autre part. Les événements et les faits pertinents se déroulent dans l'environnement technologique, alors que l'élément de preuve est le document présentant les traces de ces événements.

---

<sup>236</sup>Voir notamment Senécal : « Sous l'effet des technologies de l'information, “la notion de support se complexifie et devient ambiguë. Est-ce le fichier, l'outil matériel qui l'héberge ou encore la surface de l'écran sur lequel il s'affiche” ? Il en est de même pour la notion d'inscription. Le document devient programme informatique (programme = logiciel + données), où le logiciel structure le contenu. L'équation finale devient ainsi “document numérique = structure + données”. En d'autres mots, “[u]n document numérique est un ensemble de données organisées selon une structure stable associée à des règles de mise en forme permettant une lisibilité partagée entre concepteurs et ses lecteurs” » dans François SENÉCAL, *L'écrit électronique*, Mémoire de maîtrise, Montréal, Faculté des études supérieures, Université de Montréal, 2010, en ligne : <<https://papyrus.bib.umontreal.ca/xmlui/handle/1866/3471>>.

## 2.1.2 La pertinence de la preuve technologique

La relation entre l'évènement technologique — le fait — et la trace de celui-ci, dans un contexte de preuve, est la première porte d'entrée pour une analyse de la pertinence<sup>237</sup> d'une telle preuve technologique. À l'instar de tout élément de preuve, la preuve technologique doit répondre aux impératifs généraux gouvernant la recevabilité, y compris la pertinence.

La pertinence de la preuve est un critère de recevabilité dans l'ensemble des juridictions dont nous avons précédemment observé les cadres juridiques. Toutefois, quelques distinctions doivent être faites. En droit québécois, la preuve doit avoir un lien de connexité avec un fait en litige<sup>238</sup>, c'est-à-dire une question posée au tribunal. Ce lien peut s'avérer ténu, mais doit malgré tout exister. Cette position québécoise résulte de l'influence du droit anglo-saxon<sup>239</sup> et s'oppose à la tradition française où la preuve est plus libérale, le juge disposant d'une plus grande latitude pour l'admettre ou la rejeter<sup>240</sup>.

En contraste, le droit américain a une définition précise de la pertinence — « relevance » — laquelle se trouve au sein des *Federal Rules of Evidence* :

« 401. Evidence is relevant if:

(a) it has any tendency to make a fact more or less probable than it would be without the evidence; and

(b) the fact is of consequence in determining the action.

[...]

---

<sup>237</sup> *Code civil du Québec*, préc., note 90, art. 2857.

<sup>238</sup> Claude MARSEILLE, *La règle de la pertinence en droit de la preuve civile québécois*, coll. « Points de droit », Cowansville, Éditions Yvon Blais, 2004, par. 13 ; *Fuoco c. Société générale de financement du Québec*, 2006 QCCA 1491, par. 6 à 8 ; *Bolduc c. Arthur*, [1996] J.E. 96-1569 (C.S.) ; Dans le contexte des technologies de l'information, voir notamment : *Laushway v. Messervey*, 2014 NSCA 77, par. 86.

<sup>239</sup> C. MARSEILLE, préc., note 238, par. 9.

<sup>240</sup> C. PICHÉ, préc., note 194, par. 220 ; Voir, relativement au droit « à la preuve » : Gaëtan KLEIN, « Le droit à la preuve. Une étude comparée de la procédure civile allemande et française », *Les blogs pédagogiques de l'Université Paris Nanterre* (6 février 2009), en ligne : <<https://blogs.parisnanterre.fr/content/le-droit-%C3%A0-la-preuve-une-%C3%A9tude-compar%C3%A9e-de-la-proc%C3%A9dure-civile-allemande-et-fran%C3%A7aise-par-ga>>.

403. The court may exclude relevant evidence if its probative value is substantially outweighed by a danger of one or more of the following: unfair prejudice, confusing the issues, misleading the jury, undue delay, wasting time, or needlessly presenting cumulative evidence. »<sup>241</sup>

(Notre soulignement)

On remarque que la force probante s'invite ici dans l'analyse de la pertinence. Ces deux concepts, bien que distincts, sont analysés conjointement. Ainsi, un élément de preuve pourrait être pertinent, mais sera malgré tout irrecevable si sa force probante est si faible que sa présence ou son absence n'influencerait pas la décision du tribunal. Alors que la pertinence de la preuve technologique est une question de connexité avec les faits en litige, la force probante est pour sa part une question de preuve, notamment la preuve de l'authenticité et, dans le cas des documents technologiques, de l'intégrité<sup>242</sup>.

### 2.1.3 Authenticité et intégrité

Afin d'être recevable et d'avoir une certaine force probante, un élément de preuve doit avoir un caractère authentique. Dans certains cas, l'authenticité fait l'objet d'une présomption. C'est le cas par exemple de l'acte authentique<sup>243</sup> dont l'authenticité est présumée puisque sa confection est encadrée strictement sur le plan formel. Or, dans le cas de l'élément matériel de preuve du *Code civil du Québec*, par exemple, une preuve distincte de l'authenticité doit être réalisée<sup>244</sup> puisque ce genre d'élément de preuve n'est soumis à aucun réel formalisme. L'authenticité comporte deux composantes distinctes, soit l'intégrité et l'identité<sup>245</sup>. Faire la

---

<sup>241</sup> *Federal Rules of Evidence*, préc., note 20, art. 401 et 403.

<sup>242</sup> Voir notamment L. DUCHARME, préc., note 172, par. 502 et suivant ; C. PICHÉ, préc., note 194, par. 488 et 490.

<sup>243</sup> *Code civil du Québec*, préc., note 90, art. 2813.

<sup>244</sup> *Id.*, art. 2855.

<sup>245</sup> L. DUCHARME, préc., note 172, par. 477.

preuve de l'authenticité d'un document consiste donc à prouver à la fois qui en est l'auteur et l'intégrité de son contenu, c'est-à-dire de l'information qu'il contient.

L'intégrité est l'une des conditions importantes que pose le droit québécois pour l'utilisation d'un document technologique en preuve. L'intégrité peut se définir comme la nature d'une chose qui n'a pas été altérée et à laquelle rien ne manque. Le *Code civil du Québec* reprend d'ailleurs ces éléments :

« 2839. L'intégrité d'un document est assurée, lorsqu'il est possible de vérifier que l'information n'en est pas altérée et qu'elle est maintenue dans son intégralité, et que le support qui porte cette information lui procure la stabilité et la pérennité voulue.

Lorsque le support ou la technologie utilisée ne permet ni d'affirmer ni de dénier que l'intégrité du document est assurée, celui-ci peut, selon les circonstances, être reçu à titre de témoignage ou d'élément matériel de preuve et servir de commencement de preuve.

2840. Il n'y a pas lieu de prouver que le support du document ou que les procédés, systèmes ou technologies utilisés pour communiquer au moyen d'un document permettent d'assurer son intégrité, à moins que celui qui conteste l'admissibilité du document n'établisse, par prépondérance de preuve, qu'il y a eu atteinte à l'intégrité du document. »<sup>246</sup>

(Notre soulignement)

La lecture des articles 2839 et 2840 du *Code civil du Québec* peut malheureusement engendrer une confusion relativement à l'intégrité. Gautrais nous rappelle qu'il faut distinguer deux choses à la lecture du C.c.Q. et de la LCCJTI, soit l'intégrité de l'information et l'intégrité de son support. L'intégrité de l'information doit être prouvée, au même titre que l'identité de l'auteur du document que l'on tentera de produire en preuve, et cela, dans le contexte de la preuve de l'authenticité. Toutefois, et c'est ici que la confusion prend naissance, le support de l'information — en l'occurrence technologique — doit aussi être intègre. Or, puisqu'il serait complexe et redondant d'en faire la preuve, l'intégrité du support est présumée. Pour reprendre l'exemple évoqué par le professeur Gautrais dans son commentaire sur l'article 7 de la LCCJTI,

---

<sup>246</sup> *Code civil du Québec*, préc., note 90, art. 2839 ; *Id.*, art. 2840.

l'idée sous-jacente à la présomption d'intégrité du support se veut une manière de faciliter la recevabilité des preuves technologiques en « [calquant] quelque peu la situation qui s'applique au papier »<sup>247</sup> pour lequel la question de l'intégrité va généralement de soi.

### 2.1.3.1 Différentes approches relatives à l'intégrité

Le législateur québécois n'est pas le seul à inclure une telle présomption relativement à l'environnement technologique sous-jacent au document technologique. Une enquête du Comité européen de coopération juridique du Conseil de l'Europe révélait en 2016 que plusieurs juridictions européennes avaient mis en place des dispositions similaires. Par exemple, la neuvième question de l'enquête se lisait comme suit :

« Existe-t-il dans votre juridiction une présomption en vertu de laquelle les preuves électroniques sont considérées comme “fiables”, “recevables”, “précises”, “convenablement définies ou calibrées” ou “fonctionnant convenablement” ? »<sup>248</sup>

Une question à laquelle plusieurs réponses furent produites par les ministères de la Justice des États membres du Conseil de l'Europe. Les auteurs, dans leur rapport, résument ainsi les réponses des États :

« Il existe une présomption de ce type en Angleterre & au Pays-de-Galles, introduite par la Commission des Lois, qui est critiquée. La présomption que toute preuve est présumée fiable s'applique en Estonie, étant entendu cependant que si la partie adverse conteste la preuve, cette dernière doit alors être authentifiée. En Hongrie, la situation dépend des méthodes utilisées pour la signature du document. Il n'y a pas de certitude en ce qui concerne la situation au Monténégro. En Roumanie, l'article 265 (a) du Nouveau Code de procédure civile dispose que “l'entrée de données à partir d'un instrument légal sur un ordinateur est présumée donner des garanties suffisamment pertinentes de sa fiabilité si cette entrée est réalisée de manière systématisée et sans ruptures et lorsque les données

---

<sup>247</sup> Vincent GAUTRAIS, « Article 7 », *LCCJTI.ca* (29 janvier 2017), en ligne : <<https://www.lccjti.ca/articles/article-7/>>.

<sup>248</sup> S. MASON et U. RASMUSSEN, préc., note 224, par. 53.

informatisées sont protégées contre toutes altérations et contrefaçons de sorte que l'intégrité du document est totalement assurée". En Fédération de Russie, il y a une présomption lorsque les données électroniques sont obtenues de la manière prévue par la loi. En Espagne, une présomption s'appliquera, si les données sous forme numérique sont "signées" par une signature électronique avancée. »<sup>249</sup>

(Références omises)

Le caractère intègre et la fiabilité ne sont pas directement des synonymes, mais on remarque que les réponses des États membres tendent à montrer que certains ont opté pour une présomption de fonctionnement convenable des environnements technologiques, alors que d'autres n'ont pas modifié leur droit de la preuve à cet effet. La dixième question de cette enquête portait sur la procédure applicable afin de soumettre une preuve technologique :

« Si une partie souhaite soumettre des éléments de preuve électronique dans les procédures civiles ou administratives, est-il nécessaire de recourir à une procédure spécifique, tel que requis par la loi ou autres textes réglementaires ? »<sup>250</sup>

Les réponses des États ont permis aux auteurs d'arriver à la conclusion qu'il n'y a pas au sein des membres du Conseil de l'Europe « d'obligation légale d'obtenir de la preuve électronique selon une procédure spécifique »<sup>251</sup>. Plus loin dans leur analyse, les auteurs discutent de la question numéro dix de leur enquête, soulignant que :

« Les réponses indiquent qu'aucun État membre n'a prévu de disposition légale visant à ce que la preuve électronique soit obtenue selon une procédure spécifique, même si des règles de procédure civile pourraient trouver à s'appliquer pour ce qui concerne l'obtention et l'admission des preuves. [...] De manière générale, la réponse a été qu'un tribunal évaluerait la preuve qui lui est présentée dans le cours normal des procédures judiciaires, en tenant compte de l'intégralité des preuves techniques à sa disposition. Dans

---

<sup>249</sup> *Id.*, par. 54.

<sup>250</sup> *Id.*, par. 56.

<sup>251</sup> *Id.*, par. 57.

certaines juridictions, le juge décidera quel élément de preuve est accepté et quel élément de preuve il fera tester pour ce qui est de l'authenticité. »<sup>252</sup>

(Notre soulignement)

Ce qui se dégage de l'enquête du Comité européen de coopération juridique est le fait qu'en 2016, il n'existait pas de cadre unique en Europe ni au sein du Conseil de l'Europe ni au sein de l'Union européenne relativement à la preuve technologique. Des questions relatives à la recevabilité et à la procédure applicable étaient tranchées en fonction du droit particulier de chaque État, certains ayant développé un cadre plus étoffé que d'autres. En 2019, le Comité des ministres du Conseil de l'Europe sur la recommandation du Comité européen de coopération juridique a adopté des lignes directrices sur les preuves électroniques dans les procédures civiles et administratives. Ces lignes directrices définissent plusieurs concepts clés et proposent certains principes afin de guider les États membres, notamment celui voulant que :

« Les preuves électroniques devraient être appréciées de la même manière que les autres types de preuves, en particulier pour ce qui est de leur recevabilité, leur authenticité, leur exactitude et leur intégrité. »<sup>253</sup>

(Notre soulignement)

Sans toutefois contenir de dispositions explicites relativement à la marche à suivre en présence de preuve technologique, les lignes directrices du Conseil de l'Europe enjoignent les États à ne pas traiter différemment la preuve issue de l'environnement des technologies de l'information, renforçant la volonté de neutralité technologique déjà exprimée par d'autres instruments européens<sup>254</sup>.

---

<sup>252</sup> *Id.*, par. 89.

<sup>253</sup> *Lignes directrices du Comité des Ministres du Conseil de l'Europe sur les preuves électroniques dans les procédures civiles et administratives*, préc., note 187.

<sup>254</sup> *Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur*,



Dans leur rapport de 2016, Mason et Rasmussen font état d'une initiative de l'Union européenne se déroulant en parallèle de leur enquête<sup>255</sup>, le projet EVIDENCE : *European Informatics Data Exchange Framework for Courts and Evidence*, lequel avait entre autres pour objectif, dans une optique de droit pénal, de recenser les connaissances en matière de preuve technologique, de déterminer des normes relativement à l'intégrité de la preuve technologique et à la chaîne de possession des éléments de preuve, et de jeter les bases d'un système de partage et de coopération entre les États membres de l'UE en matière de preuve technologique<sup>256</sup>. Le projet s'est étalé de 2014 à 2016 et a donné lieu à des conclusions, lesquelles n'ont toutefois pas permis la mise en place d'un cadre législatif pour l'instant. L'une des conclusions du projet avance ::

« a) There is no comprehensive EU legal framework regarding electronic evidence. There are only a number of EU instruments which may be directly or indirectly relevant to the collection, preservation, use and exchange of electronic evidence. Most of them have been implemented in the European Member States but often in a very different manner according to the single legal systems and traditions. The increasing use of digital technologies in individuals' daily activities, including criminal ones and their cross-border nature have posed new challenges to the European and national legal systems, especially as far as the collection, preservation and exchange of evidence is concerned. Laws and practices of the different Member States treat differently electronic evidence, contributing to create a situation of legal and practical uncertainty.

b) Although some regulations exist, clarity on the collection, preservation and exchange of electronic evidence relevant in criminal investigations is missing. Differences through European Member States may be in some cases significant, especially as far as the admissibility of electronic evidence is concerned. These differences (due to the traditional competence attributed to MS in criminal matters but also to the distinctive constitutional traditions) are not necessarily a weakness in the European legal framework. However, a clear and more harmonized framework is desirable in order to facilitate efficient cooperation in criminal matters.

[...]

e) Although the specific knowledge and expertise of the main actors involved in the handling of e-evidence seems to increase and best practices are gradually developing,

---

préc., note 182 ; *Directive 1999/93/CE du Parlement européen et du Conseil, du 13 décembre 1999, sur un cadre communautaire pour les signatures électroniques*, préc., note 182.

<sup>255</sup> S. MASON et U. RASMUSSEN, préc., note 224, par. 16.

<sup>256</sup> « Concept and objectives | Evidence », *Evidence—evidenceproject.eu*, en ligne : <<http://www.evidenceproject.eu/about-evidence/concept-and-objectives.html>>.

there is a lack of specific standards on the procedures and modalities to follow in the phase of gathering, preserving and especially exchanging electronic evidence. »<sup>257</sup>

(Références omises ; notre soulignement)

S'il existe différents cadres juridiques en Europe relativement à l'admissibilité de la preuve technologique, il est pertinent de se tourner, afin d'effectuer une comparaison pertinente, vers le cadre juridique américain en la matière afin de vérifier l'approche de cet État fédéral relativement à cette question.

Le droit américain de la preuve technologique est morcelé, chacun des États de l'union ayant légiféré en la matière. Par souci d'économie, nous nous pencherons ici sur les règles fédérales, les *Federal rules of Evidence*<sup>258</sup>, précisément sur les dispositions concernant les données stockées sur des supports électroniques — *Electronically stored information* — dont nous avons discuté précédemment dans notre exercice de qualification de la preuve potentiellement issue de l'utilisation des assistants vocaux.

Les règles fédérales américaines de la preuve civile exigent que l'authenticité des éléments de preuve technologiques soit prouvée par une preuve extrinsèque. Cette preuve extrinsèque peut prendre la forme d'un témoignage<sup>259</sup>, d'éléments circonstanciels<sup>260</sup> ou encore de constatations faites par la Cour<sup>261</sup>. Or, de récentes modifications aux textes de loi créent une certaine forme de présomption relativement aux éléments de preuve qui apportent eux-mêmes la preuve de leur authenticité — « Evidence That Is Self-Authenticating »<sup>262</sup>.

Les récents ajouts relatifs à la preuve supportant sa propre authenticité n'ont pas encore fait l'objet de décisions jurisprudentielles substantielles permettant, au sud de la frontière, d'évaluer la portée exacte. Toutefois, le juge Paul Grimm notait dans un article en 2018 que, bien

---

<sup>257</sup> *Final Report EVIDENCE (European Informatics Data Exchange Framework for Courts and Evidence)*, European Commission, 2016, en ligne : <<https://cordis.europa.eu/project/rcn/185514/reporting/fr>>.

<sup>258</sup> *Federal Rules of Evidence*, préc., note 20.

<sup>259</sup> Daniel CAPRA, "Authenticating Digital Evidence", (2017) 69 *Baylor L. Rev.* 1, 12.

<sup>260</sup> *Id.*, 15.

<sup>261</sup> *Id.*, 14.

<sup>262</sup> Le premier alinéa de la règle 902 se lit d'ailleurs : « The following items of evidence are self-authenticating; they require no extrinsic evidence of authenticity in order to be admitted ». Voir : *Federal Rules of Evidence*, préc., note 20, art. 902.

qu'elles faciliteraient forcément l'utilisation en preuve de certains éléments de preuve technologiques, notamment ceux mentionnés aux règles numéro 902 (13) et 902 (14) soit « [a] record generated by an electronic process or system that produces an accurate result, as shown by a certification of a qualified person » ainsi que les « [d] ata copied from an electronic device, storage medium, or file, if authenticated by a process of digital identification, as shown by a certification of a qualified person », la certification par une personne qualifiée pouvait — au final — ramener les parties au même endroit qu'elles l'étaient avant l'apparition de ces règles, le juge étant chargé de déterminer qui est une personne qualifiée et ce qu'est un processus de certification<sup>263</sup>. Encore, Grimm soulève une problématique constitutionnelle à propos des procédés de « certification ». Ceux-ci ne peuvent souvent pas être contestés. En droit américain cela pourrait être contraire aux garanties liées à la « confrontation clause », soit la possibilité de contester une preuve testimoniale<sup>264</sup> en questionnant l'auteur de celle-ci.

Dans le cas qui nous intéresse, l'authenticité de l'information contenue dans un document retraçant l'utilisation d'un assistant vocal nous semble être un élément dont la preuve est plus simple à effectuer en Amérique du Nord qu'en Europe où les cadres juridiques varient encore, malgré la claire volonté de l'Union européenne de mettre en place des règles communes. Tant aux États-Unis qu'au Québec<sup>265</sup>, les cadres juridiques offrent certaines présomptions simples relativement à l'intégrité et à la fiabilité — soit l'élément le plus difficile à établir, dans le cas de preuves faisant appel à l'intelligence artificielle — sans toutefois accorder à ces éléments des privilèges les rendant incontestables.

---

<sup>263</sup> Paul GRIMM, « New Evidence Rules and Artificial Intelligence », (2018) 45-1 *Litigation Journal*, en ligne : <[https://www.americanbar.org/groups/litigation/publications/litigation\\_journal/2018-19/fall/new-evidence-rules-and-artificial-intelligence/](https://www.americanbar.org/groups/litigation/publications/litigation_journal/2018-19/fall/new-evidence-rules-and-artificial-intelligence/)>.

<sup>264</sup> Dans ce contexte, surtout pénal, Grimm cite en exemple l'affaire *Melendez-Diaz* où la certification relativement à une autre règle de preuve que celle en lien avec les preuves technologiques a malgré tout été approuvée par la Cour suprême des États-Unis. Voir à ce sujet : *Id.* ; *Melendez-Diaz v. Massachusetts*, [2009] U.S. (U.S. Supreme Court) (Certiorari to the Appeals Court of Massachusetts).

<sup>265</sup> Les lois à l'égard de la preuve technologique au Canada, dans les autres provinces que le Québec, disposent aussi pour la plupart de loi particulière dont la plupart ont été inspirées des travaux de la Conférence pour l'harmonisation des lois au Canada. Voir à ce sujet : David OUTERBRIDGE et Ezra SILLER, « The Admissibility of Electronic Evidence », (2006) *The Advocate's Journal* (Osgoode Professional Development), 31, en ligne : [http://advocast.ca/assets/pdf/electronic2015/11%20The%20Admissibility%20of%20Electronic%20Evidence%20Outerbridge\\_Siller.pdf](http://advocast.ca/assets/pdf/electronic2015/11%20The%20Admissibility%20of%20Electronic%20Evidence%20Outerbridge_Siller.pdf) ; UNIFORM LAW CONFERENCE OF CANADA, « Uniform Electronic Evidence Act (1998) », *Uniform Law Conference of Canada* (1999), en ligne : <<https://www.ulcc.ca/en/older-uniform-acts/electronic-evidence/1924-electronic-evidence-act>>.

Dans l'ensemble des cadres juridiques sur lesquels nous nous sommes penchés, la preuve extrinsèque de l'authenticité et de l'intégrité du « contenu », c'est-à-dire de l'information véhiculée par les éléments de preuve technologique, est nécessaire ou, à tout le moins, utile pour établir ou soutenir davantage la recevabilité de ce genre d'éléments de preuve. Cette preuve parallèle apporte davantage d'information au décideur et, dans l'optique de la recherche de la vérité, elle est importante, surtout si l'élément en question n'est pas une preuve préconstituée, comme l'écrit, mais est une preuve documentaire illustrant un évènement — un élément matériel, en droit québécois. Dans son ouvrage, le professeur Gautrais utilise le vocable « documentation » pour décrire cette « preuve à propos de la preuve », un concept qu'il tire de la LCCJTI qui à son article dix-sept portant sur le transfert discute de certaines caractéristiques de la documentation.

### 2.1.3.2 La documentation, une preuve à propos de la preuve

La tâche de présenter un élément issu de l'utilisation d'assistants vocaux en preuve, sur le plan strictement pratique, demandera au juriste d'extraire de l'information d'une plateforme Web afin de l'apporter devant le tribunal. Dans le contexte québécois, la loi fait la distinction entre le support et l'information dans la description d'un document. Il y existe également certaines présomptions<sup>266</sup>, mais faire passer l'information d'un support à un autre est qualifié de « transfert ». C'est dans ce contexte que la LCCJTI aborde la « documentation » :

« La documentation comporte au moins la mention du format d'origine du document dont l'information fait l'objet du transfert, du procédé de transfert utilisé ainsi que des garanties qu'il est censé offrir, selon les indications fournies avec le produit, quant à la préservation de l'intégrité, tant du document devant être transféré, s'il n'est pas détruit, que du document résultant du transfert.

---

<sup>266</sup> Outre les présomptions du *Code civil du Québec*, la LCCJTI crée une présomption à l'endroit des copies effectuées par une entreprise ou l'État. Voir à cet effet : *Code civil du Québec*, préc., note 90 ; *Loi concernant le cadre juridique des technologies de l'information*, préc., note 14, art. 15.

La documentation, y compris celle relative à tout transfert antérieur, est conservée durant tout le cycle de vie du document résultant du transfert. La documentation peut être jointe, directement ou par référence, soit au document résultant du transfert, soit à ses éléments structurants ou à son support. »<sup>267</sup>

(Notre soulignement)

L'article 17 de la LCCJTI traite du transfert, soit le fait de prendre l'information sur un support particulier, par exemple une page Web, et de la transférer sur un support « faisant appel à une technologie différente »<sup>268</sup>, par exemple une feuille de papier au moyen de l'impression. La distinction entre la copie et le transfert est expliquée par le professeur Gautrais dans sa loi commentée disponible en ligne :

« Le transfert est le processus par lequel les données du document source se verront déplacées, sans que leur contenu ne soit modifié, sur un support faisant appel à une technologie différente. Contrairement à la copie, le transfert peut impliquer une modification de la forme, soit la manière dont sont agencées les informations. Le document résultant du transfert pourra légalement tenir lieu du document source, qui pourra être détruit, si le transfert est documenté. »<sup>269</sup>

(Notre soulignement)

Aux yeux du professeur Gautrais donc, le transfert peut avoir lieu au sein même d'un environnement technologique, par exemple lorsqu'un document change de format, passant d'un fichier propriétaire à un autre — l'exemple classique étant le fichier MS Word transformé en fichier PDF. La position voulant que le changement de format soit un transfert est cependant contredite par une doctrine antérieure<sup>270</sup>.

---

<sup>267</sup> *Loi concernant le cadre juridique des technologies de l'information*, préc., note 14, art. 17, al. 2 et 3.

<sup>268</sup> *Id.*, art. 17, al. 1.

<sup>269</sup> Vincent GAUTRAIS, « Quelle est la différence entre une copie et un transfert ? », *LCCJTI.ca* (3 mai 2012), en ligne : <<https://www.lccjti.ca/faq/quelle-est-la-difference-entre-une-copie-et-un-transfert/>>.

<sup>270</sup> M. PHILLIPS, préc., note 13, par. 214.

Dans le cas qui nous intéresse, la création de fichiers de sauvegarde d'une page Web en fonction de leur nature pourrait être un transfert — dans les cas les plus élaborés où toutes les informations de la page Web sont formatées afin de pouvoir être restituées ultérieurement — ou encore des copies — dans le cas où seul le format est le même, par exemple HTML. Encore, la réalisation d'une capture d'écran est indubitablement un transfert; la nature du nouveau document créé étant différente de la nature de la page Web.

Tant dans les cas de transfert que de copie, la documentation assure à la fois la recevabilité et la valeur juridique du nouveau document créé. Dans le cas du document né du transfert, la documentation est une condition de forme et de fond<sup>271</sup>. En présence d'une copie, le régime est moins strict, mais « le procédé employé [pour réaliser la copie] doit présenter des garanties suffisamment sérieuses pour établir le fait qu'elle comporte la même information que le document source »<sup>272</sup>.

C'est en considérant cette similarité que le professeur Gautrais entrevoit la documentation dans un contexte plus large que celui du transfert, la définissant comme une « procédure qui explicite comment un document est géré »<sup>273</sup>, supportant ainsi l'idée que la documentation est une bonne pratique à adopter afin d'assurer une meilleure recevabilité et une meilleure appréciation de la force probante de l'élément de preuve par le juge, le cas échéant.

Tel qu'il le souligne d'ailleurs, la documentation est similaire à la preuve distincte qui doit être faite de l'authenticité de l'enregistrement sonore ou encore de l'élément matériel de preuve, des conditions prévues au *Code civil du Québec* et connues des praticiens, et ce, depuis près d'une décennie avant l'arrivée de la LCCJTI. Le professeur Gautrais souligne de plus que la documentation peut aussi être partie intégrante au document, en la forme des métadonnées, soit des « données à propos des données »<sup>274</sup>. Les métadonnées présentent un intérêt certain pour documenter le cycle de vie et la gestion d'un document et sont souvent créées automatiquement, ce qui ne les rend pas tributaires du respect d'un protocole par un être humain. Cependant, dans

---

<sup>271</sup> *Loi concernant le cadre juridique des technologies de l'information*, préc., note 14, art. 17.

<sup>272</sup> *Id.*, art. 15.

<sup>273</sup> V. GAUTRAIS, préc., note 12, par. 208 et 209.

<sup>274</sup> *Id.*, par. 201 à 203. Un concept qui nous évoque un certain rapprochement avec les éléments de preuve qui apportent eux-mêmes la preuve de leur authenticité, les « Evidence That [are] Self-Authenticating » décrit ci-avant dans le contexte américain.

le cas qui nous concerne, peu de métadonnées touchant les actions mêmes de l'assistant vocal semblent accessibles aux utilisateurs, les processus les générant ne se déroulant pas dans leurs appareils, mais entre les mains des fabricants. En revanche, les métadonnées peuvent être une avenue de documentation efficace pour les documents tirés des historiques d'utilisation, comme le fichier d'archivage ou la capture d'écran.

Au surplus, comme la majorité des documents que l'on pourra tirer de l'utilisation des assistants vocaux seront des éléments matériels de preuve, l'exercice de description des circonstances entourant leur création et la preuve de leur authenticité représente déjà une partie appréciable de l'effort à faire pour documenter leur transfert ou leur copie, le cas échéant.

### **2.1.3.3 L'authenticité des éléments matériels de preuve dans le contexte des assistants vocaux**

L'élément matériel de preuve mérite une analyse particulière en l'espèce, considérant que la plupart des traces de l'utilisation d'un assistant vocal seraient vraisemblablement des éléments matériels. Ce moyen de preuve nécessite une preuve indépendante — *distincte* — de son authenticité, laquelle exigence est prévue au *Code civil du Québec*<sup>275</sup>. Cette preuve distincte pourrait prendre plusieurs formes en présence des traces de l'utilisation d'un assistant vocal.

En premier lieu, nous sommes d'avis qu'il faudra que le justiciable fasse la preuve que les données enregistrées par l'assistant vocal, à savoir des données de géolocalisation ainsi que des enregistrements sonores, proviennent bien de la personne qu'il soutient. En ce sens, il pourra faire témoigner ou produire une déclaration sous serment du propriétaire d'un téléphone cellulaire ou d'une enceinte connectée afin de soutenir que l'objet lui appartient bel et bien et qu'il était en sa possession au moment où les données ont été enregistrées.

Parallèlement, pour les enregistrements sonores, il faudra se référer aux critères jurisprudentiels afin de permettre l'authentification de ces éléments de preuve. Le degré de certitude requis est

---

<sup>275</sup> *Code civil du Québec*, préc., note 90, art. 2855.

relativement élevé, tel qu'en font foi les motifs du juge Gendreau dans l'affaire *Cadieux c. Service de gaz naturel Laval inc.* :

« Aussi, la production d'un enregistrement mécanique impose à celui qui la recherche la preuve, d'abord, de l'identité des locuteurs, ensuite que le document est parfaitement authentique, intégral, inaltéré et fiable et enfin que les propos sont suffisamment audibles et intelligibles. Les conséquences d'une erreur dans l'appréciation du document subséquemment admis en preuve sont si importantes que le juge doit être "entièrement convaincu" [...] Cette conviction n'est certes pas régie par la règle du droit criminel ; mais le juge devra ici exercer sa discrétion avec une grande rigueur. »<sup>276</sup>

(Notre soulignement)

Les critères jurisprudentiels posés par *Cadieux* pourraient s'avérer difficiles à rencontrer dans le cas d'enregistrements réalisés par les assistants vocaux, puisque ces enregistrements sonores sont par nature relativement courts et que leur qualité peut laisser à désirer. De ce fait, il pourrait s'avérer difficile de conclure avec certitude qu'une personne en particulier donne une commande à un assistant vocal. Le caractère audible, pour sa part, sera forcément rencontré puisque sans lui l'outil n'aurait vraisemblablement pas détecté la commande de l'utilisateur.

Dans un second temps, tant pour l'enregistrement sonore que pour toutes autres données collectées par l'assistant vocal ou transmises par lui, le caractère « inaltéré et fiable », bref l'intégrité de l'information contenue, renvoie essentiellement à la démonstration de la gestion saine du document, donc à la possibilité de documenter le ou les transferts ayant permis de présenter une telle preuve à la Cour.

Dans un même spectre d'idées, les données générées par l'assistant vocal — les « réponses aux questions » — au moyen des données qui lui sont transmises ne sauraient selon nous faire l'objet d'une preuve de leur authenticité. On pourra tout au plus montrer qu'elles n'ont pas été altérées depuis leur isolation par le justiciable et qu'elles sont issues du système auquel l'utilisateur a transmis ses données. Dans ce cas, faire la preuve que l'ensemble de l'information — tant celle

---

<sup>276</sup> *Cadieux c. Service de gaz naturel Laval inc.*, [1991] RJQ 2490 (C.A.).



fournie à l'assistant vocal que celle générée par lui — provient du bon compte d'utilisateur et est associé à la bonne personne sera, selon nous, la manière la plus efficace de procéder.

Un dernier angle mort demeure toutefois, relativement aux enceintes connectées. Celles-ci, contrairement aux téléphones mobiles, sont davantage susceptibles d'être utilisées par plus d'une personne. En effet, tant les produits proposés par Google<sup>277</sup> qu'Amazon<sup>278</sup> permettent d'enregistrer jusqu'à deux modèles vocaux et peuvent aussi être utilisés, avec cependant moins de fonctionnalités, par toute personne y ayant accès. Différentes personnes d'une même famille peuvent donc utiliser ces produits s'ils sont, par exemple, placés dans une salle commune accessible par tous, comme la cuisine ou le salon.

L'identification vocale est aussi une technologie faisant appel à la reconnaissance vocale et à l'intelligence artificielle. Il est difficile de connaître exactement les rouages précis du fonctionnement de ces outils, mais rappelons seulement qu'en 2019, la compagnie Google a retiré l'option permettant de déverrouiller un appareil mobile au moyen du modèle vocal Voice Match, jugeant les performances de son outil insatisfaisantes et de ce fait, non sécuritaires<sup>279</sup>. Les performances de l'identification vocale d'Amazon sont aussi remises en doute, mais cette fois par plusieurs événements ayant fait les manchettes. L'Amazon Echo aurait en effet été utilisé avec succès par des enfants<sup>280</sup> et des animaux<sup>281</sup> pour commander des produits en ligne.

Dans ces cas de figure, comme il n'est pas possible d'exclure qu'un tiers ait pu utiliser l'appareil sur lequel une commande aurait été passée à un assistant vocal, la preuve extrinsèque peut jouer un rôle important relativement à l'identification de qui a passé une commande, permettant de déterminer qui pouvait avoir accès à l'appareil. Le fait qu'il soit impossible d'entendre un extrait sonore de la commande, qui a effectivement été passée, pose aussi un problème dans certains

---

<sup>277</sup> GOOGLE, « Set up Multiple Users for Your Speaker or Smart Display », *Google Assistant Help* (2019), en ligne : <<https://support.google.com/assistant/answer/9071681?hl=en-GB>>.

<sup>278</sup> AMAZON.COM, INC., « Help. Using Household Profiles on Alexa Devices », *Amazon.com* (2019), en ligne : <<https://www.amazon.com/gp/help/customer/display.html?nodeId=201628040>>.

<sup>279</sup> Abner LI, « Google begins replacing full 'Voice Match' phone unlock », *9to5Google* (1<sup>er</sup> mars 2019), en ligne : <<https://9to5google.com/2019/02/28/google-replacing-voice-match-unlock/>>.

<sup>280</sup> Andrew LIPTAK, « Amazon's Alexa started ordering people dollhouses after hearing its name on TV », *The Verge* (7 janvier 2017), en ligne : <<https://www.theverge.com/2017/1/7/14200210/amazon-alexa-tech-news-anchor-order-dollhouse>>.

<sup>281</sup> Sarah BERGER, « This naughty parrot was caught ordering items off Amazon's Alexa—here's how much he spent », *CNBC* (21 décembre 2018), en ligne : <<https://www.cnbc.com/2018/12/21/african-grey-parrot-rocco-was-caught-ordering-items-off-amazons-alexa.html>>.

cas. D'ailleurs, l'assistant vocal Siri, développé par Apple, ne permet pas de consulter un tel historique.

#### 2.1.4 La proportionnalité

La proportionnalité est l'un des principes généraux du droit québécois, et ce, même avant la récente réforme du droit procédural opérée en 2016. Il est désormais codifié à l'article dix-huit du nouveau *Code de procédure civile* :

« 18. Les parties à une instance doivent respecter le principe de proportionnalité et s'assurer que leurs démarches, les actes de procédure, y compris le choix de contester oralement ou par écrit, et les moyens de preuve choisis sont, eu égard aux coûts et au temps exigé, proportionnés à la nature et à la complexité de l'affaire et à la finalité de la demande.

Les juges doivent faire de même dans la gestion de chacune des instances qui leur sont confiées, et ce, quelle que soit l'étape à laquelle ils interviennent. Les mesures et les actes qu'ils ordonnent ou autorisent doivent l'être dans le respect de ce principe, tout en tenant compte de la bonne administration de la justice. »<sup>282</sup>

Ce principe est aussi connu en Europe<sup>283</sup> et aux États-Unis, quoique dans une moindre mesure<sup>284</sup>.

Dans le contexte québécois, on peut résumer le concept de proportionnalité comme suit : :

« [La] proportionnalité juridique vise à effectuer un double contrôle sur l'instance. D'abord, un contrôle de pertinence, de justification : le moyen employé "doit permettre effectivement d'atteindre le but poursuivi" par le recours. C'est ainsi que les justiciables

---

<sup>282</sup> *Code de procédure civile*, préc., note 91, art. 18.

<sup>283</sup> Notamment au Royaume-Uni où l'on a codifié ce principe à la suite du rapport Woolfe. Voir à ce sujet l'article de Yves-Marie Morissette, juge à la Cour d'appel du Québec : Yves-Marie MORISSETTE, « Gestion d'instance, proportionnalité et preuve civile. État provisoire des questions », (2009) 50-2 *C. de D.* 381.

<sup>284</sup> Prévu à la règle 26 des *Federal Rules of Civil Procedures* depuis 1983, il est toutefois appliqué de manière inégale et couvre surtout le processus de « discovery ». Voir : Philip J. FAVRO et Derek P. PULLAN, « New Utah Rule 26. A Blueprint for Proportionality Under the Federal Rules of Civil Procedures », (2012) 2012 *Mich. St. L. Rev.* 933-979, 939 et suivantes; *Federal Rules of Civil Procedures*, préc., note 180, art. 26.

pourront, par exemple, se voir refuser le droit de se faire entendre quant à une procédure que le tribunal juge a priori vouée à l'échec. Ensuite, "un contrôle d'incidence ou de conséquences", de sorte que le moyen n'a pas de conséquences excessives sur les droits ou intérêts de la partie poursuivie. »<sup>285</sup>

(Références omises)

La proportionnalité s'évalue au cas par cas. Si l'on peut croire avec raison que les technologies de l'information permettent généralement d'atteindre un meilleur équilibre sur le plan de l'équité du procès favorisant l'accès à la justice et l'accès à l'information juridique, en matière de preuve technologique, les technologies peuvent produire l'effet contraire.

Un exemple en matière de preuve technologique, l'affaire *Laushway*, permet de mettre en contexte ce principe. La proportionnalité occupe une place importante dans l'analyse du juge dans cette affaire datant de 2014<sup>286</sup>. Dans ce cas, la Cour d'appel de Nouvelle-Écosse s'est penchée sur les règles de common law gouvernant l'admissibilité en preuve des métadonnées contenues dans l'ordinateur d'un travailleur. Ce travailleur prétendait que depuis un accident, source du litige en question, il n'était plus à même de travailler autant qu'auparavant. Eu égard à la proportionnalité de la demande de production des métadonnées, le juge propose de répondre à la question suivante :

« Will the anticipated time and expense required to discover the sought-after information be reasonable having regard to the importance of the sought-after information to the issues in dispute? »<sup>287</sup>

Dans ce cas précis, le magistrat arrive à la conclusion que l'effort est nécessaire, considérant la question en litige et le fait qu'il n'y a pas de mesures alternatives aussi probantes. Ainsi, même si elle est plus complexe, la preuve demeure proportionnelle aux yeux du juge. Or, nous avons

---

<sup>285</sup> Catherine PICHÉ, « La proportionnalité procédurale. Une perspective comparative », (2009) 40 *R.D.U.S.* 552, 556 à 557.

<sup>286</sup> *Laushway v. Messervey*, préc., note 238.

<sup>287</sup> *Id.*, par. 86.

vu jusqu'ici que la preuve technologique impliquant l'intelligence artificielle peut présenter un degré de complexité très élevé.

Les exemples les plus récents en jurisprudence<sup>288</sup> nous enseignent que l'information issue des assistants vocaux prendra vraisemblablement la forme d'enregistrements sonores. Cependant, il est possible que les données issues des assistants vocaux et des objets interagissant avec eux se présentent sous de multiples formes. Il se pourrait alors que ces éléments soient moins compréhensibles que des enregistrements sonores, ces derniers étant des objets auxquels les tribunaux ont déjà été confrontés dans le passé. Devant ces informations d'un genre nouveau, il est possible que plaideurs et magistrats soient perplexes, confrontés par le rapide avancement technologique.

En réponse à cette complexité, on pourrait soutenir l'argument qu'une preuve alternative existe. Une personne pourrait, par exemple, témoigner du fait qu'elle a visité un magasin en particulier un jour donné. Cependant, ce témoignage serait-il aussi probant que la balise de positionnement de son téléphone mobile qui pourrait, si correctement consultée, apporter au tribunal l'éclairage précis de coordonnées géographiques et d'un horodatage mécanique ? L'histoire de l'inclusion de l'élément matériel de preuve dans le droit québécois illustre justement que cette preuve « objective » et détachée de la subjectivité du témoignage est l'une des raisons pour lesquelles on a milité en faveur de l'inclusion de cette catégorie dans le droit de la preuve<sup>289</sup>.

Ainsi, certaines questions se posent. Est-ce que la complexité est susceptible d'être évaluée en fonction du profil et des capacités respectives des parties ? Le cas échéant, le tribunal pourrait-il, par exemple, refuser à une multinationale ou à la Couronne de présenter une expertise, parce qu'il serait disproportionné d'obliger un individu privé à recourir à la contre-expertise pour éviter le déséquilibre ?

---

<sup>288</sup> *State of Arkansas v. James A. Bates*, préc., note 121; *Commonwealth v. Denison*, 2015 Mass. Super. Ct.

<sup>289</sup> Pierre PATENAUDE, « Science et techniques en preuve. Nécessaire réforme du droit civil, indispensable adaptation du système et des acteurs », dans *Développements récents en droit civil*, 32, coll. « Service de la formation permanente », Barreau du Québec, Cowansville, Éditions Yvon Blais, 1993 à la page 79 cité par : V. GAUTRAIS, préc., note 12, n° 557.

D’abord, rappelons que la relation entre la preuve et les questions litigieuses doit servir de base pour répondre à la question de la proportionnalité<sup>290</sup>. Dans le cadre d’une affaire où la question en litige est essentiellement technologique, le rejet d’un élément de preuve pourrait compromettre l’issue du litige. Qu’en serait-il toutefois si l’élément de preuve était rattaché à une affaire où la question en litige n’est pas fondamentalement technologique ?

Avec la très grande pénétration des technologies de l’information dans le quotidien des individus, il y a fort à parier que les éléments de preuve technologiques prendront de plus en plus d’importance dans la vie des justiciables. L’idée que cette preuve pourrait être écartée si sa complexité semble déraisonnable, au regard de la question en litige, des droits ou des sommes monétaires en jeu nous semble aller à l’encontre d’un autre principe de droit important : la recherche de la vérité. Cependant. Il est difficile d’affirmer avec certitude qu’une preuve complexe, ou encore l’expertise s’y rattachant, ne seraient pas rejetées sous prétexte que son admission nuirait à l’équité du procès. Une critique que l’on pourrait adresser à la proportionnalité, dans ce cas, serait qu’elle corresponde en un sens à la « jurisprudence du moindre excès », ou du moindre effort, où la décision est écartée, la réflexion semblant trop lourde. L’auteur Guillemain l’expose dans un article où il avance :

« Le juge peut ainsi mettre en perspective des intérêts en conflit afin de déterminer celui qui, dans une situation donnée et conformément au bon sens, doit avoir la priorité sur l’autre. De fait, il peut “réaliser, au grand jour, le vieux rêve d’équité qui, jusqu’alors, n’avait pu survivre que dans la clandestinité d’un droit dur et formel en se dissimulant sous les oripeaux trop ajustés du syllogisme judiciaire” »<sup>291</sup>

(Références omises)

---

<sup>290</sup> *Laushway v. Messervey*, préc., note 238 ; Patricia MITCHELL et Jennifer TAYLOR, « Case Commentary on *Laushway v. Messervey*, 2014 NSCA 7. Old Evidence Law Dogs, New Technology Tricks », (2015) 12 *Digital Evidence & Elec. Signature L. Rev.* 13.

<sup>291</sup> Antoine GUILMAIN, « Sur les traces du principe de proportionnalité. Une esquisse généalogique », (2015) 61-1 *R. D. McGill* 87, 129.

Cette approche de la proportionnalité entre en conflit de manière assez singulière avec l'idée d'une preuve complexe, mais probante ; difficile d'accès, mais nécessaire. Une preuve à l'image de celle que peut représenter la preuve par expert.

Ainsi, dans un second temps, dans l'éventualité où un justiciable souhaiterait soulever une problématique relevant de données techniques complexes, il devrait malgré tout en faire la preuve. Il y a fort à parier que peu d'avocats comprennent effectivement l'activité technique supportant un programme d'ordinateur ou une page Web. De fait, tels qu'ils le font lorsqu'ils ne peuvent éclairer eux-mêmes la Cour, les plaideurs se retourneront vers un expert. À l'instar des autres domaines techniques, l'expert deviendra dans le cas de l'intelligence artificielle la source d'un savoir particulier. Le rôle de l'expert consiste à éclairer la Cour, tel qu'en fait foi le nouvel article 22 du *Code de procédure civile* :

« 22. L'expert dont les services ont été retenus par l'une des parties ou qui leur est commun ou qui est commis par le tribunal a pour mission, qu'il agisse dans une affaire contentieuse ou non contentieuse, d'éclairer le tribunal dans sa prise de décision. Cette mission prime les intérêts des parties.

L'expert doit accomplir sa mission avec objectivité, impartialité et rigueur. »<sup>292</sup>

(Notre soulignement)

La mission lumineuse de l'expert est longuement expliquée par la doctrine es professeurs Piché et Ducharme<sup>293</sup>. L'expertise étant un témoignage particulier, elle se fonde sur les compétences de l'expert, lequel est appelé à aider le tribunal à prendre sa décision, au-delà des volontés des parties en présence. Lorsque l'expertise rencontre la proportionnalité, il en ressort que l'expertise doit avoir, pour être admissible, deux caractéristiques, soient l'utilité et, surtout, la nécessité.

Dans le cas de l'intelligence artificielle en général, et des assistants vocaux en particulier, l'expertise pourrait s'avérer utile et nécessaire afin de prouver le mauvais fonctionnement d'un

---

<sup>292</sup> *Code de procédure civile*, préc., note 91, art. 22.

<sup>293</sup> C. PICHÉ, préc., note 194, par. 529 et suivants ; Voir aussi : L. DUCHARME, préc., note 172, par. 526.

algorithme ou une autre problématique technique. Dans d'autres circonstances, par exemple pour expliquer le fonctionnement général d'un assistant vocal, l'expertise pourrait être utile, mais ne serait pas forcément nécessaire. Dans un article publié en 2013 à ce sujet, l'auteur Paciocco tentait de dresser un portrait des aspects du droit de la preuve qui seront le plus affectés par les nouvelles technologies. Celui-ci soutenait que l'expertise en matière technologique pouvait être abordée de deux angles distincts. À ces yeux, plusieurs considérations pratiques doivent guider les juges dans l'appréciation de la nécessité de celle-ci. Il avance :

« [It] is helpful to recognize that technological information comes in different forms. It includes not only the 'technical forensic evidence' and 'computer by-product evidence' I have described. There is also what I call 'mundane technology evidence.' 'Mundane technologies' are the day-to-day uses to which information technology is put. It includes the use of social media such as Facebook and Twitter; the operation of search engines to retrieve data; the operation of computers, tablets, and smart phones; and the use of digitized technology to take and edit photographs, digitized movies, and audio-recorded information, including computer stored 911 calls. These are things that require special training to use or understand, yet they are not the stuff of expert evidence. No Mohan vetting is required before testimony about their use or operation is offered. For example, no expertise is required to explain Facebook to a judge, including how it works or how access is granted, or how messages are posted, sent, or received. Any witness who uses Facebook can offer this information. Similarly, iPhone users can explain what 'apps' are and what use they make of them, without furnishing expert evidence. Ultimately courts requiring help in understanding 'mundane technologies' can rely on ordinary members of the public to describe those uses that ordinary members of the public make of the technology in question. It is only when subjects move into the more rarified and technical questions, such as what time and date stamps attached to messages signify, that ordinary witnesses are not apt to have the expertise to assist. »<sup>294</sup>

(Références omises)

Dans cet extrait, Paciocco pose une distinction intéressante. Il mentionne que certains aspects des technologies de l'information doivent faire l'objet de preuves expertes, alors que d'autres ne doivent pas être amenés devant la Cour par un expert, au risque de faire perdre du temps

---

<sup>294</sup> David M. PACIOCCO, « Proof and progress. Coping with the law of evidence in a technological age », (2013) 11-2 *Can. J.L. & Tech.*, 186, en ligne : <<https://ojs.library.dal.ca/CJLT/article/view/6001>>.

précieux au tribunal. En d'autres mots, l'utilisation de l'expertise pour des concepts relevant de la technologie « banale » va à l'encontre du principe de proportionnalité et la preuve technologique ne devrait pas être abordée de manière différente que la preuve analogique, selon cet auteur. Ainsi, tant pour les messages Facebook que pour le fonctionnement des assistants vocaux, il faudra essentiellement distinguer les fonctionnalités et le fonctionnement de ces processus. Si les fonctionnalités d'un assistant vocal ne sauraient faire l'objet d'une expertise pour être expliquées au tribunal, la Cour devrait certainement entendre un expert pour se faire expliquer le fonctionnement de l'intelligence artificielle — et surtout son dysfonctionnement.

De fait, la proportionnalité peut s'avérer une question importante relativement à la recevabilité et l'administration de la preuve issue des assistants vocaux à notre avis. Dans la mesure où l'on tentera de contredire les assistants vocaux sur la base du fait qu'ils n'ont pas fonctionné correctement ou encore que leur fonctionnement particulier résulte d'un biais, la présence d'experts coûteux pourrait devenir nécessaire. À ce sujet, nous avançons l'hypothèse que le degré de complexité de cette preuve technologique appelle peut-être une redéfinition du rôle de notre système judiciaire dans la recherche des faits. Nous sommes essentiellement d'avis que cette entreprise de recherche de la vérité doit reposer, à l'image d'autres juridictions comme la France, sur les nouveaux pouvoirs du juge québécois de requérir une expertise commune, et ce, même d'office. Si la proportionnalité n'est pas en tant que telle une cause d'irrecevabilité, certaines sont autrement prévues par le droit québécois. C'est de ce dont il sera question dans la prochaine sous-section.



## 2.2 Exceptions à la recevabilité

Sous réserve d'être autrement recevables en fonction de leur nature de document technologique, en droit québécois, les éléments de preuve issus de nos relations avec les assistants vocaux doivent aussi, comme tous éléments de preuve, être admissibles en vertu des conditions de recevabilité générales prévues au *Code civil du Québec*.

À ce chapitre, nous sommes d'avis qu'une discussion relative aux autres possibilités pouvant mener au rejet d'une telle preuve est nécessaire, considérant qu'il s'agit ici d'éléments de preuve d'une nature nouvelle devant s'intégrer au cadre législatif en place.

Nous nous pencherons donc sur deux exceptions classiques à la recevabilité des éléments de preuves composées des traces de nos interactions avec les assistants vocaux, soit les potentielles atteintes aux droits fondamentaux que pourraient susciter la réception en preuve de tels éléments et dans quelles mesures cela pourrait déconsidérer l'administration de la justice et, dans un second temps, nous nous pencherons sur les relations entre ces éléments de preuve et les règles relatives au secret professionnel, notamment le privilège qui existe entre l'avocat et son client.

### 2.2.1 Atteinte aux droits fondamentaux

Au Québec, un élément de preuve portant atteinte aux droits fondamentaux doit être rejeté d'office par le tribunal, dans la mesure où cet élément de preuve « déconsidère l'administration de la justice », et ce, en vertu de l'article 2858 du *Code civil du Québec* :

« 2858. Le tribunal doit, même d'office, rejeter tout élément de preuve obtenu dans des conditions qui portent atteinte aux droits et libertés fondamentaux et dont l'utilisation est susceptible de déconsidérer l'administration de la justice.

Il n'est pas tenu compte de ce dernier critère lorsqu'il s'agit d'une violation du droit au respect du secret professionnel. »<sup>295</sup>

(Notre soulignement)

Dans le contexte américain, la règle 403 des *Federal Rules of Evidence*<sup>296</sup> permet d'exclure un élément de preuve s'il est « inéquitablement préjudiciable »<sup>297</sup>. Le « unfair prejudice » est difficile à définir et a une portée très large. Victor Gold mettait de l'avant que cette notion ne renvoie pas à un sujet en particulier, mais davantage à une erreur d'argumentation :

« Evidence presents the danger of unfair prejudice when it threatens the fundamental goals of the Federal Rules and Rule 403: accuracy and fairness. [...]. The results of logic [...] can be no more accurate or fair than are the premises from which the logician proceeds. Evidence is not necessarily unfairly prejudicial because of the methodology it induces the decision maker to employ. [...] Under such an approach, the goals of Rule 403 suggest that evidence is unfairly prejudicial to the extent it has a tendency to cause the trier of fact to commit inferential error. »<sup>298</sup>

Donc, dans une certaine mesure, le préjudice inéquitable permet une certaine protection des droits fondamentaux, ouvrant la porte à l'exclusion de certains éléments de preuve en matière civile. Cependant, force est de constater que les droits constitutionnels et fondamentaux des justiciables américains ne sont pas aussi protégés en matière civile qu'en matière pénale où plusieurs protections constitutionnelles sont en place<sup>299</sup>.

Dans le contexte européen, la protection des droits fondamentaux se fraye un chemin de multiples manières jusque dans l'enceinte du domaine de la preuve. Ainsi, en droit français, le rôle du juge est particulièrement important dans la mise en équilibre de la recherche de la vérité

---

<sup>295</sup> *Code civil du Québec*, préc., note 90, art. 2858.

<sup>296</sup> *Federal Rules of Evidence*, préc., note 20, art. 403.

<sup>297</sup> Traduction libre depuis « unfair prejudice ».

<sup>298</sup> Victor J. GOLD, «Federal Rule of Evidence 403. Observations on the Nature of Unfairly Prejudicial Evidence », (1983) 58-3 *Wash. L. Rev.* 497.

<sup>299</sup>Notamment, des protections à l'encontre de l'admissibilité de la preuve obtenue illégalement ou encore de la preuve obtenue en violation du droit au silence. « Exclusionary Rule », *LII/Legal Information Institute*, en ligne : <[https://www.law.cornell.edu/wex/exclusionary\\_rule](https://www.law.cornell.edu/wex/exclusionary_rule)>.

et la protection des droits des justiciables, tel que l'expliquait la Cour de cassation dans un rapport sur l'administration de la preuve en 2012 :

« Le juge dans sa mission d'administration des preuves doit contribuer à la manifestation de la vérité en assurant le respect des droits et libertés des justiciables. Il doit, à cette fin, conduire un travail délicat de conciliation ne sacrifiant ni l'exigence de liberté ni les droits substantiels des justiciables et des tiers au litige. Le contrôle du juge porte en la matière sur deux points. Certains éléments de preuve doivent, en raison de leur nature, faire l'objet d'une protection particulière. La réalisation de la justice n'impose pas au justiciable de procéder à toutes les révélations. Le contrôle du juge porte également sur la manière d'obtenir des preuves. Il s'attache à cet égard à vérifier que, pour faire apparaître la vérité, les procédés employés ont été respectueux des droits des justiciables. »<sup>300</sup>

Ce bref survol des cadres juridiques que nous avons mis en parallèle tout au long de ce mémoire doit s'accompagner d'un constat. Les assistants vocaux sont susceptibles de produire un certain nombre d'éléments de preuve où plusieurs droits fondamentaux pourraient être compromis. Nous n'avons qu'à penser ici à la vie privée, reconnue comme un droit fondamental<sup>301</sup>. Ainsi, on peut imaginer que le fait d'installer une enceinte connectée équipée d'un assistant vocal diminue de manière substantielle le degré de vie privée auquel on peut légitimement s'attendre dans sa demeure. Si l'utilisateur d'une enceinte connectée ne donnait pas son consentement, on ne pourrait penser à une mesure qui contreviendrait davantage au caractère inviolable de la demeure, protégé par la *Charte des droits et libertés de la personne*<sup>302</sup>, que l'écoute en continu opérée par cet objet.

---

<sup>300</sup> Jean-François CESARO (dir.), « Études. La preuve », dans *Rapport annuel 2012. La preuve dans la jurisprudence de la Cour de cassation*, Paris, Direction de l'information légale et administrative, 2013, en ligne : <[https://www.courdecassation.fr/2012admissibilite\\_modes\\_26241.html](https://www.courdecassation.fr/2012admissibilite_modes_26241.html)>.

<sup>301</sup> Dans un contexte québécois, « [l]e droit à la vie privée est un droit évolutif qui s'est toujours inscrit dans le milieu culturel où il est mis en application. Perçu à l'origine dans notre société comme une composante du droit de propriété, il s'est transformé pour s'attacher à la personne et au monde informationnel qui la suit. La mise en œuvre de ce droit protéiforme soulève de multiples questions. Pensons simplement à la façon dont il faut en assurer l'application lorsqu'il est confronté à d'autres valeurs que l'on juge tout aussi fondamentales : la liberté d'expression, l'audience publique, le droit au silence, etc. De plus, le concept de droit à la vie privée n'obéit pas à une définition précise. », dans : Jean-Pierre VILLAGGI, « Le droit à la vie privée. Un droit en mutation », dans *Mes amis facebook, moi et mon emploi. L'arbitrage de grief à l'ère des réseaux sociaux*, Montréal, Wilson & Lafleur, 2012, en ligne : <<https://edocrone.caij.qc.ca/wilson-et-lafleur-livres/85/1515756382>>.

<sup>302</sup> *Charte des droits et libertés de la personne*, RLRQ, c. C -12, ci-après la « Charte québécoise ».

Les éléments de preuves recueillis par les assistants vocaux et les autres éléments de l'IoT étant potentiellement attentatoires à la vie privée des justiciables faut-il pour autant les rejeter d'office, dans un contexte québécois ? La doctrine a déjà répondu à cette question dans un contexte non technologique. En effet, la professeure Piché nous rappelle que l'approche du tribunal dans le cadre d'une instance civile n'est pas gouvernée par les mêmes contraintes que dans le cadre d'une instance pénale<sup>303</sup>. Dans un contexte de droit pénal, l'atteinte aux droits fondamentaux doit être traitée avec une beaucoup plus grande prudence, considérant l'atteinte potentielle aux droits fondamentaux en jeu. Relativement à l'instance civile, l'auteure mentionne :

« En droit civil, une partie peut être contrainte à témoigner contre elle-même, à remettre des documents à son adversaire et parfois à se soumettre à un examen physique ou mental ou encore psychosocial. [...] Aussi, la découverte et même la création d'une preuve en obtenant d'une partie, en violation d'un droit fondamental n'ont pas les mêmes conséquences sur l'équité du procès dans les affaires civiles que dans les matières pénales. »<sup>304</sup>

(Références omises)

Dans ce contexte, la technologie complexifie grandement les choses, notamment quand vient le temps de collecter des éléments de preuve de manière sélective. Si les téléphones et les ordinateurs posent problème relativement à la quantité d'information qu'ils contiennent, il faut comprendre que les assistants vocaux et les autres éléments de l'IoT nous épient en permanence. On peut poser l'hypothèse qu'ils contiennent ou permettent l'accès à davantage d'informations biographiques pouvant devenir dommageables pour l'individu que tous autres appareils. À ce sujet, dans le contexte américain, Corrales et *al.* abordent la saisie d'un téléphone intelligent et mettent l'accent sur les conséquences d'une telle saisie :

« [I] f a smart phone is seized, the situation changes significantly. The device typically contains personal data reflecting vast parts of the professional and/or private life of its

---

<sup>303</sup> C. PICHÉ, préc., note 194, par. 1170 Voir aussi ; L. DUCHARME, préc., note 172, par. 804 à 808 et 811 à 814.

<sup>304</sup> C. PICHÉ, préc., note 194, par. 1164 à la page 951.

user. Hence, the fundamental rights impacted are not only property rights, but also those related to privacy/data protection and, additionally, potentially the privacy of telecommunications (depending on the case and the legal system). LEAs accessing such device gain control of data vaults that reveal various details on the user and various third parties in very high granularity. Most of the information available would likely not be case-relevant at all, so that further analysis would be needed to identify the relevant pieces of information. Finally, unless the data was mirrored in the Cloud or any type of online service, the loss of the device would mean, for the user, not only the loss of a multi-purpose device, but also the loss of that data (potentially triggering severe consequences, if e.g., the address book had not been backed-up).

This example may underpin the crucial difference of investigative measures in a physical and in a digital environment. Where the impact on fundamental rights (massively) increases when applying measures in the digital world, the safeguards have to rise equally. As a consequence, the existing legal framework needs constant revision. »<sup>305</sup>

(Références omises)

Les balises — « safeguards » — auxquelles font référence les auteurs dans l'extrait précité peuvent faire écho au cadre juridique québécois. Dans le *Code civil du Québec*, il est question d'un test cumulatif d'atteinte et de déconsidération d'administration de la justice. Les droits fondamentaux protégés par l'article 2858 C.c.Q. dont nous avons brièvement discuté correspondent essentiellement, dans le contexte québécois, aux droits garantis par la *Charte québécoise* et ceux garantis par la *Charte canadienne*<sup>306</sup>, dans la mesure où ils sont concernés par l'instance civile, puisque la procédure civile permet plusieurs écarts. Sur le plan pratique, dans un contexte technologique, l'article 2858 C.c.Q. doit être analysé en deux temps, comme l'explique l'auteur Gingras :

« Le premier critère de l'article 2858 C.c.Q. traite du mode d'obtention de la preuve technologique. Afin d'y satisfaire, elle doit avoir été obtenue de façon illicite, c'est-à-dire

---

<sup>305</sup> Marcelo CORRALES, Mark FENWICK et Nikolaus FORGÓ, *New Technology, Big Data and the Law*, coll. « Perspectives in Law, Business and Innovation », Singapour, Springer, 2017, p. 254, en ligne: <<http://dx.doi.org/10.1007/978-981-10-5038-1>>.

<sup>306</sup> *Charte canadienne des droits et libertés*, Partie I de la Loi constitutionnelle de 1982, c. 11 (R-U), la « Charte canadienne »

de façon à porter atteinte aux droits et libertés fondamentaux de la personne à l'encontre de laquelle la preuve sera utilisée, et ce, par la personne qui souhaite l'admettre en preuve.

[...]

Le second critère de l'article 2858 C.c.Q. concerne l'effet de l'admissibilité de la preuve. En d'autres mots, est-ce que le fait d'admettre cette preuve au procès déconsidérerait l'administration de la justice dans l'esprit d'une personne raisonnable, objective et bien informée. »<sup>307</sup>

(Références omises ; notre soulignement)

Contrairement à l'instance pénale où le droit au silence est généralement consacré, il est possible de contraindre une personne à témoigner, et ce, contre elle-même, dans le cadre d'une instance civile au Québec. Il serait donc possible de contraindre une personne à remettre les données témoignant de son utilisation des outils d'intelligence artificielle, comme les assistants vocaux — si cela est autrement pertinent. Cependant, subtiliser de l'information de son compte en violant sa vie privée ou en commettant un acte illicite serait susceptible de mener à l'exclusion de la preuve ainsi obtenue<sup>308</sup>.

Parallèlement, l'information issue de l'utilisation des assistants vocaux risque de révéler, comme nous l'avons évoqué, bien davantage que ce que la partie adverse cherchera à prouver. Dès lors, est-ce que requérir de la partie adverse qu'elle apporte devant le tribunal le contenu des historiques d'utilisation des assistants vocaux qu'elle utilise, comme Google Assistant ou Alexa, ne porterait pas trop atteinte à la vie privée de cette partie ? Dans la mesure où la portée de l'analyse de ces outils peut s'étendre à toutes les sphères de la vie de leurs utilisateurs, répertoriant leurs achats dans différents commerces, leur position géographique en tout lieu, des extraits de leur voix, leurs goûts musicaux et — peut-être le plus délicat — toutes les recherches effectuées avec la voix qui n'ont pas été supprimées par l'utilisateur, la question se pose.

---

<sup>307</sup> Patrick GINGRAS, « Quand la preuve technologique est susceptible de déconsidérer l'administration de la justice », dans Patrick GINGRAS et Nicolas VERMEYS, *Technologies de l'information — En bref*, n° 4, Cowansville, Éditions Yvon Blais, 2013, en ligne : <<https://www.lccjti.ca/files/sites/105/2013/05/bulletinPGingras.pdf>>.

<sup>308</sup> *Id.*

La question est bien évidemment tout autre si une personne décide de déposer en preuve les données issues de sa propre utilisation des assistants vocaux. Une personne qui voudrait, par exemple, prouver qu'elle était à un endroit précis à un moment donné pourrait déposer en preuve une commande passée à son assistant vocal qui, non seulement l'aura géolocalisée, mais permettra de constater qu'il s'agit bien d'elle, dans le cas où l'assistant vocal aura conservé un extrait audio de cette commande.

Dans le premier cas, si l'information est obtenue par un tiers au moyen d'un subterfuge ou encore par un moyen illégal ou frauduleux, elle ne saurait généralement être recevable. Par exemple, une personne qui utiliserait le mot de passe de son époux pour se connecter à son compte Google et en extraire l'ensemble de ses données d'utilisation de l'Assistant Google, y compris des données de géolocalisation et ses recherches Web en désirant utiliser ces informations dans le cadre d'un divorce ne saurait pouvoir le faire, tant l'atteinte à la vie privée de l'autre époux serait importante. Du même souffle, un tribunal qui recevrait en preuve de l'information ainsi obtenue enverrait le signal qu'il cautionne ce genre de méthode déloyale.

Dans le second cas, celui où une personne dépose en preuve ses propres données, l'objection ne peut être soulevée d'office par le tribunal<sup>309</sup> puisque la preuve n'aurait vraisemblablement pas été « obtenue » en portant atteinte aux droits et libertés du justiciable. Dans la même veine, si les informations ainsi révélées étaient protégées par le secret professionnel, le justiciable pourrait toujours y renoncer et légitimement<sup>310</sup> étaler sa vie privée devant le tribunal, sous réserve de pertinence.

---

<sup>309</sup> *Code civil du Québec*, préc., note 90, art. 2858.

<sup>310</sup> *Charte des droits et libertés de la personne*, préc., note 302, art. 9.

## 2.2.2 Le secret professionnel

Le secret professionnel gouverne les relations entre les individus et de nombreux acteurs de la société<sup>311</sup>. L'exemple le plus évocateur de ce genre de relation est celui entre l'avocat et son client. On pourrait aussi citer en exemple la relation entre le médecin et son patient ou encore la relation entre le psychologue et son client. En droit québécois, le secret professionnel est garanti par la *Charte québécoise* :

« 9. Chacun a droit au respect du secret professionnel.

Toute personne tenue par la loi au secret professionnel et tout prêtre ou autre ministre du culte ne peuvent, même en justice, divulguer les renseignements confidentiels qui leur ont été révélés en raison de leur état ou profession, à moins qu'ils n'y soient autorisés par celui qui leur a fait ces confidences ou par une disposition expresse de la loi.

Le tribunal doit, d'office, assurer le respect du secret professionnel. »<sup>312</sup>

Il va sans dire que l'introduction en preuve d'éléments violant le secret professionnel ne se fait pas sans heurts. Au Québec, le tribunal est tenu de rejeter d'office ces éléments de preuve, et ce, même s'ils n'ont pas été obtenus par un moyen illicite ou attentatoire aux droits fondamentaux du justiciable. En effet, on présume que leur utilisation en preuve déconsidère forcément l'administration de la justice et qu'à ce titre ils doivent être inadmissibles<sup>313</sup>.

Dans le contexte américain, le privilège avocat client en contexte civil n'est pas gouverné par les *Federal Rules of Evidences*, mais plutôt par la législation étatique<sup>314</sup>. Cependant, une fois le privilège identifié, le juge est tenu de le considérer<sup>315</sup>. Sur le plan européen, le secret

---

<sup>311</sup> *Id.*

<sup>312</sup> *Id.*

<sup>313</sup> L. DUCHARME, préc., note 172, par. 872.

<sup>314</sup> *Federal Rules of Evidence*, préc., note 20, art. 502.

<sup>315</sup> *Id.*, art. 104.



professionnel est un motif implicite d'irrecevabilité de la preuve<sup>316</sup>. Au surplus, rompre le secret professionnel est une infraction pénale en France passible, pour l'avocat, d'amendes et de peines de prison<sup>317</sup>. Encore, le *Code de déontologie des avocats européens* pose le secret professionnel comme principe, soutenant que « [s]ans certitude de confidentialité, la confiance ne peut exister »<sup>318</sup>.

Les assistants vocaux pourraient poser de sérieuses problématiques de confidentialité s'ils étaient utilisés dans le contexte de communications privilégiées. En effet, plusieurs professionnels, dont les avocats, pourraient être tentés par les promesses faites par les fabricants de ces produits, intéressés par les gains en efficacité que pourraient leur procurer ces outils. Cependant, l'utilisation d'assistants vocaux pourrait aller à l'encontre des obligations déontologiques de certains professionnels. À cet effet, les auteurs Nelson et Simek<sup>319</sup> expliquent que l'utilisation d'assistants vocaux pourrait contrevenir aux obligations de confidentialité de l'avocat parce que ces outils peuvent provoquer des fuites d'information de manières inattendues<sup>320</sup>.

On imagine généralement le cas d'un accès non autorisé au compte auquel l'assistant vocal est relié comme la faille de sécurité principale. Cependant, les auteurs soulèvent que le secret professionnel pourrait être compromis par des utilisateurs à même un bureau d'avocat, entre autres. Illustrant cette possibilité, une personne pourrait demander à l'assistant vocal de relever ses courriels, exposant ainsi à toutes les personnes pouvant l'entendre, le contenu d'une communication potentiellement protégée par le secret professionnel, surtout considérant que les

---

<sup>316</sup> « Le secret professionnel, dont la violation est pénalement sanctionnée par les articles 226-13 et 226-14 du Code pénal, constitue, en principe, un empêchement légitime faisant obstacle à la mesure d'instruction ou à une demande de communication de pièces. » J.-F. CESARO (dir.), préc., note 300 à la page 269.

<sup>317</sup> *Code pénal*, art. 226-13.

<sup>318</sup> CONSEIL DES BARREAUX EUROPÉENS, *Charte des principes essentiels de l'avocat européen et Code de déontologie des avocats européens*, 2018, p. 8, en ligne : <[https://www.ccbe.eu/fileadmin/speciality\\_distribution/public/documents/DEONTOLOGY/DEON\\_CoC/FR\\_DEON\\_CoC.pdf](https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/DEONTOLOGY/DEON_CoC/FR_DEON_CoC.pdf)>.

<sup>319</sup> Sharon NELSON et John SIMEK, "Are Alexa and Her Friends Safe for Office Use?", (2017) 43-5 *ABA's Law Practice* 26.

<sup>320</sup> Voir aussi : Christine Chambers GOODMAN, "AI/Esq. Impacts of Artificial Intelligence in Lawyer-Client Relationships", (2019) 72-1 *Oklahoma Law Review* 149.

outils de reconnaissance vocale des assistants vocaux peinent encore, à l'heure actuelle, à distinguer la voix d'un utilisateur particulier.

Enfin, le fait que les assistants vocaux fonctionnent généralement dans le nuage, en ce sens où l'information est traitée par des processus se déroulant sur les serveurs des fabricants, place sans doute certains professionnels dans une position délicate relativement à leurs obligations envers leurs clients. Les avocats québécois, par exemple, pourraient en utilisant des assistants vocaux comme Alexa ou l'Assistant Google, contrevenir au *Règlement sur la comptabilité et les normes d'exercice professionnel des avocats*<sup>321</sup>, principalement à son article dix-sept qui prévoit que les dossiers de l'avocat doivent demeurer confidentiels. C'est sur la base de ce règlement et du *Code de déontologie des avocats*<sup>322</sup> que l'utilisation de services de courriels gratuits est strictement déconseillée par le Barreau du Montréal :

« Les services de courriels gratuits (ex. Hotmail, Gmail ou Yahoo Mail) ne conviennent pas à la pratique du droit et mènent presque inévitablement à la violation d'obligations déontologiques de l'avocat. Comme le démontrent les conditions d'usage (terms and conditions) de ces services, leur prix est en fait le secret professionnel de vos clients et votre vie privée.

De plus, la majorité de ces services sont offerts par des entreprises étrangères qui conservent vos données sur des serveurs hébergés dans d'autres juridictions, les soumettant ainsi aux lois de ces pays (ex. le Patriot Act). Les avocats devraient s'assurer de conserver leurs données et celles de leurs clients au Québec. Bon nombre de fournisseurs d'accès Internet québécois offrent d'ailleurs de tels services. »<sup>323</sup>

Si l'accent est mis sur la protection des données récoltées par les fournisseurs de services de messagerie gratuits et sur la réticence que devraient avoir les avocats à utiliser ce genre de services, la même attention devrait être portée aux assistants vocaux. Ceux-ci ne devraient pas être utilisés par un avocat. Concomitamment, dans la mesure où un justiciable les utilise pour communiquer avec son avocat, la recevabilité des historiques d'utilisation des outils tels qu'Alexa et l'Assistant Google devra faire l'objet d'une analyse précise et, en fonction de la

---

<sup>321</sup> *Règlement sur la comptabilité et les normes d'exercice professionnel des avocats*, RLRQ, c. B -1, r. 5, art. 17.

<sup>322</sup> *Code de déontologie des avocats*, RLRQ, c. B -1, r. 3,1.

<sup>323</sup> BARREAU DE MONTRÉAL, *Guide des technologies de l'information. Les courriels*, 2017, en ligne : <[https://www.barreaudemontreal.qc.ca/sites/default/files/guideti\\_courriels\\_fev2017.pdf](https://www.barreaudemontreal.qc.ca/sites/default/files/guideti_courriels_fev2017.pdf)>.

détermination faite par le tribunal, ceux-ci devront être rejetés si l'on doit considérer l'historique comme un tout, ou si l'on permet de s'attarder à chaque entrée de manière particulière.

## 2.3 La force probante

La force probante est un concept qui a essentiellement été analysé à l'aune d'une catégorie de preuve particulière par la doctrine. Le professeur Gautrais, au sujet de la force probante d'un document technologique, avançait que celle-ci « varie en fonction de la qualification à titre de moyen de preuve qui lui est donné et selon que son intégrité est assurée ou non. »<sup>324</sup> Cette définition renvoie essentiellement la force probante à un autre facteur, l'intégrité et sur cette base elle prête flanc à la critique. Or, d'autres facteurs ont été identifiés dans la doctrine pour évaluer la force probante, dans un contexte général.

Paciocco dans son ouvrage sur le droit de la preuve discute du « poids » de la preuve et propose en substance que le « poids » influence le caractère persuasif — « believability » — d'un élément de preuve. Ce caractère persuasif serait lui-même fonction de la fiabilité ou de la crédibilité de la preuve. L'aspect persuasif, une fois mis en relation avec le caractère informatif — « informativeness » — de l'élément de preuve permettrait de faire émerger la valeur probante — « probative value » de cet élément<sup>325</sup>.

Parallèlement, dans le même esprit, les auteurs Sopinka, Lederman et Bryant proposent de définir la valeur probante comme étant le caractère d'un élément de preuve à rendre plus ou moins probable un fait en litige<sup>326</sup>. Ces auteurs semblent aussi partager l'idée que la force probante est intimement liée au contexte de la preuve et qu'elle ne peut pas être analysée dans l'abstrait<sup>327</sup>.

---

<sup>324</sup> Vincent GAUTRAIS, « Document technologique », *LCCJTI.ca* (26 janvier 2017), en ligne : <<https://www.lccjti.ca/definitions/document-technologique/#ancre33>>.

<sup>325</sup> D. M. PACIOCCO et L. STUOSSER, préc., note 218, p. 36.

<sup>326</sup> Sidney N. LEDERMAN, Alan W. BRYANT, Michelle FUERST et John SOPINKA, *The Law of Evidence in Canada*, 5<sup>e</sup> éd., Toronto, LexisNexis, 2018, par. 11.47.

<sup>327</sup> *Id.*, par. 11.48.

En droit québécois, l'auteur Hubert Reid définit la force probante comme la « valeur et [l'] efficacité d'un moyen de preuve comme élément de conviction »<sup>328</sup>, une définition qui ressemble essentiellement à celle proposée par l'ouvrage de Gérard Cornu, lequel met aussi l'accent sur le concept de conviction<sup>329</sup>. La professeure Piché dans son ouvrage sur la preuve civile discute de la force probante des documents technologiques en soutenant essentiellement que celle-ci doit être la même que celle des documents analogiques<sup>330</sup>. De fait donc, la force probante d'un contrat écrit sur le papier devrait être la même qu'un contrat électronique ; un dessin à la main devrait avoir la même force probante qu'un dessin réalisé à l'aide d'un logiciel — le cas échéant<sup>331</sup>. Il faut donc observer la force probante inhérente à chaque catégorie d'élément de preuve en droit québécois pour arriver à une définition de la force probante. Au sujet de la force probante de la preuve matérielle, la professeure Piché cite les propos du ministre de la Justice du Québec :

« [L'article 2856 C.c.Q.] découle de la nature même du moyen de preuve prévu à la présente section. S'agissant d'une perception directe du juge, donc subjective, il n'est pas possible d'établir en principe une force probante objective et totale, comme dans le cas d'un acte authentique, d'un acte signé par les parties ou d'un aveu judiciaire. Cependant, il peut arriver, dans certains cas, qu'une telle preuve entraîne la conviction totale du juge et dispose de tout le litige ; aussi établit-on que le juge peut en tirer toute conclusion qu'il estime raisonnable. »<sup>332</sup>

(Notre soulignement)

Il ressort essentiellement des propos du ministre que les éléments constituant la force probante, du moins en ce qui a trait aux preuves matérielles sont la perception du juge et la conviction

---

<sup>328</sup> Hubert REID, *Dictionnaire de droit québécois et canadien*, v° « Force probante », Montréal, Wilson & Lafleur, 2015.

<sup>329</sup> Voir entre autres la distinction faite par le tribunal entre la force probante et la pertinence, citant Cornu : *Atlas Copco Canada inc. c. Commission d'appel en matière de lésions professionnelles*, [1995] CALP 909 (C.S.).

<sup>330</sup> C. PICHÉ, préc., note 194, par. 488.

<sup>331</sup> Il s'agit ici essentiellement du concept d'équivalence fonctionnelle pour lequel la professeure Piché nous renvoie aux articles 1, 2, 5 et 9 de la LCCJTI. Voir : *Loi concernant le cadre juridique des technologies de l'information*, préc., note 14, art. 1, 2, 5 et 9.

<sup>332</sup> MINISTÈRE DE LA JUSTICE DU QUÉBEC, *Commentaire du ministre de la Justice*, n° 2, Québec, Publications du Québec, 1993, p. 1778, art. 2856, en ligne : <<https://elois.caij.qc.ca/CCQ-1991/article2856>>.

découlant de cette perception. Malgré le fait que le ministre de la Justice se garde d'établir des principes, la professeure Piché avance toutefois que les preuves matérielles ne sont pas toutes égales entre elles, soutenant :

« Les différentes preuves matérielles n'ont pas toutes la même valeur probante. Les conclusions tirées d'empreintes digitales ou d'un test d'ADN sont plus difficiles à réfuter. Par ailleurs, les résultats d'un test polygraphique ont peu ou pas de valeur probante [...] Certains enregistrements sonores ont peu ou pas de valeur probante, tandis que des enregistrements vidéo ont la force probante requise. »<sup>333</sup>

(Références omises)

On doit donc déduire que certains facteurs doivent éventuellement influencer un tel ordonnancement, tel que le rapporte la professeure Piché dans son étude de la jurisprudence québécoise pertinente.

Des éléments de réponse se trouvent peut-être dans l'ouvrage de Phipson sur le droit de la preuve au Royaume-Uni. Dans cet ouvrage, les auteurs actuels discutent du fait que l'évaluation du poids de la preuve est une question qui ne peut faire l'objet de règles strictes. Bien que les principes dont ils discutent relèvent aussi de la preuve pénale, ces principes peuvent nous éclairer dans notre démarche exploratoire. Les auteurs soutiennent :

« Questions of admissibility of evidence belong, as we have seen to the judge; those of its weight, credibility and sufficiency to the jury (or if there is no jury, to the judge). Unlike admissibility, the weight of evidence cannot be determined by fixed rules, since it depends mainly on common sense, logic and experience. »<sup>334</sup>

(Références omises ; notre soulignement)

---

<sup>333</sup> C. PICHÉ, préc., note 194, par. 1141 à la page 923.

<sup>334</sup> H. M. MALEK, préc., note 178, par. 7-17.

L'ouvrage de Phipson cite par la suite deux décisions jurisprudentielles pour appuyer son propos :

« For weighing evidence and drawing inferences from it, there can be no canon. Each case presents its own peculiarities and in each common sense and shrewdness must be brought to bow upon the facts elicited »<sup>335</sup>

« The weight of evidence depends on rules of common sense »<sup>336</sup>

Pour leur part, certains juristes américains ont tenté de mathématiser le concept de force probante — ou « probative value », littéralement *valeur* probante — en le décrivant comme une expression mathématique. Richard Friedman, dans un article de 1986<sup>337</sup>, enseigne que la valeur probante est intimement liée à la pertinence, au regard des *Federal Rules of Evidences*<sup>338</sup>, principalement les règles 401 et 403 dont nous avons précédemment discuté dans ce mémoire<sup>339</sup>.

Friedman explique, avant de tenter réduire la force probante à une expression mathématique, que la celle-ci est le caractère d'un élément de preuve qui rend davantage probable ou moins probable un fait en litige. La force probante serait ce caractère et sa quantification permettrait d'évaluer, au-delà de l'atteinte par l'une des parties du seuil de son fardeau de preuve, le concept de pertinence en droit américain. On remarque donc aisément, tant en droit canadien<sup>340</sup> qu'américain<sup>341</sup> que le concept est relativement semblable. Il se distingue peut-être dans l'esprit, en ce sens où les juristes américains semblent résolus à le mathématiser.

Enfin, s'éloignant des contextes américain et québécois, la force probante est, dans la sphère civiliste continentale, évaluée par le juge sur la base de l'intime conviction, laquelle est

---

<sup>335</sup> *R c. Madhub Chunder*, [1874] 21 WRCr 13.

<sup>336</sup> *Lord Advocate c. Lord Blantyre*, [1879] 4 App Cas 770.

<sup>337</sup> Richard D. FRIEDMAN, « A Close Look at Probative Value », (1986) 66-4 *B.U. L. Rev.* 733.

<sup>338</sup> *Federal Rules of Evidence*, préc., note 20, art. 401 et 403, Voir aussi ; H. M. MALEK, préc., note 178, par. 7-06 à 7-09 (comparaison des méthodes d'évaluation de la pertinence en droit d'origine anglo-saxonne).

<sup>339</sup> Voir la section 2.1.2, « La pertinence de la preuve technologique », ci-haut.

<sup>340</sup> *Force probante*, préc., note 328.

<sup>341</sup> Voir entre autres, en réponse à l'article de Friedman : D. H. KAYE, « Quantifying Probative Value Symposium. Comment », (1986) 66-4 *B.U. L. Rev.* 761. Voir aussi, dans un contexte anglo-saxon ; « The elements of probative value are cogency, strenght of inference, and nature and degree of relevance » dans : H. M. MALEK, préc., note 178, par. 19-48.

cependant encadrée, en France, dans un contexte civil, par les modes de preuve prévus, par exemple, au Code civil, lesquels emportent une certaine forme de conviction. Toutefois, comme nous le rappelle Dominique Inchauspé, l'intime conviction est profondément ancrée dans le système judiciaire français :

« Tant au regard de l'évolution historique que de la pratique contemporaine et au regard du simple bon sens, l'intime conviction se révèle être le véritable mécanisme par lequel un ou plusieurs juges prennent leur décision. Il s'agit du processus usuel par lequel n'importe quelle personne arrête son sentiment sur un sujet quelconque. L'esprit fait masse des informations multiples qu'il reçoit ; il les synthétise de manière plus inconsciente que consciente ; et, bien souvent, l'inconscient s'impose à la réflexion raisonnée. En tout cas, il la précède et la pousse en avant ; il est la matière quand la seconde n'est que son moule. Les juges ne se départiront jamais de ce propre de l'homme. »<sup>342</sup>

(Notre soulignement)

Cependant, dans l'ensemble des pistes de définitions soulevées cependant, la force probante ne semble jamais s'appuyer sur un critère objectif. Elle demeure, même lorsqu'elle est encadrée<sup>343</sup> par les codes de lois et les précédents jurisprudentiels, une question pour le juge reposant sur son bon sens et son appréciation subjective d'une certaine réalité, surtout en présence de preuves matérielles. Malgré cela, on peut constater que certaines tendances se dessinent. Même en l'absence de principes stricts, une hiérarchie de la force probante des preuves matérielles peut s'opérer. Nous nous pencherons maintenant sur un facteur qui, nous le croyons, a un impact significatif sur la détermination de la force probante de la preuve technologique : la compréhension de la technologie.

---

<sup>342</sup> Dominique INCHAUSPÉ, « Chapitre 6. Intime conviction », dans *L'innocence judiciaire*, coll. « Questions judiciaires », Paris, Presses Universitaires de France, 2012, p.155-178 à la page 47, en ligne : <<https://www.cairn.info/l-innocence-judiciaire--9782130606994-p-155.htm>> ; Voir aussi à ce sujet la discussion de Bidaud-Garon relativement à la force probante en France, dans le contexte de l'appréciation d'acte d'état civil étrangers : Christine BIDAUD-GARON, « La force probante des actes de l'état civil étrangers après la loi du 26 novembre 2003 », (2006) 1-49 *Revue Critique de Droit International Privé*, en ligne : <<https://halshs.archives-ouvertes.fr/halshs-02238258>>.

<sup>343</sup> Voir notamment les exemples de différences dans la procédure et l'approche judiciaire sous les différents régimes de preuve dans : C. PICHE, préc., note 194, par. 11 à 15.

### 2.3.1 La compréhension de la technologie

Nous posons ici l'hypothèse que l'analyse de la force probante d'un élément de preuve technologique repose sur la compréhension de la technologie qui le véhicule. En effet, si l'on accepte la proposition voulant que la force probante corresponde au caractère persuasif d'un élément de preuve, comme nous venons de l'aborder, la compréhension du contexte technologique nous semble être un prérequis à toute forme de conviction. Comprendre permet ainsi d'apprécier les autres critères que l'on connaît déjà : l'authenticité et l'intégrité, mis en relation avec le contexte particulier de chaque cas d'espèce. Or, là est l'écueil, la technologie évolue rapidement et un fossé générationnel semble se creuser, avec des effets négatifs pour l'ensemble des acteurs :

« [I]mproving the knowledge and skills of judges and lawyers is crucial. On this point, we should also care about a generation gap with new technology; the younger generations tend to overly rely on the technology and pay little attention to risk. On the contrary, senior generations are not familiar with new technology and too cautious with risk. Therefore, they need to improve their knowledge and consciousness depending on their situations as well as seek the assistance of experts. »<sup>344</sup>

(Notre soulignement)

Cette situation nous renvoie à celle que nous avons abordée précédemment alors que nous discutons de l'authenticité<sup>345</sup>. Comme dans ce cas, l'écueil potentiel le plus dommageable réside sans doute à l'enseigne de l'illusion de compréhension. Dans ce cas de figure, puisque l'évaluation de l'élément de preuve est biaisée, la réponse à une question de droit s'en trouve influencée. La conjoncture technologique à laquelle les juristes et les systèmes judiciaires sont confrontés depuis une quinzaine d'années est singulière, mais il ne s'agit pas du premier

---

<sup>344</sup> E. SUGIYAMA, préc., note 189, p. 539.

<sup>345</sup> D. M. PACIOCCO, préc., note 294.



bouleversement technologique auquel le droit a dû faire face. En 2007, le professeur Gregory Mandel<sup>346</sup> faisait une comparaison entre différents bouleversements technologiques et les réponses du système judiciaire américain à ces situations. Il mettait alors en parallèle les changements liés aux technologies de l'information avec les révolutions qu'ont pu représenter à une certaine époque l'apparition des empreintes digitales comme moyen de preuve, la télégraphie ainsi que la preuve par ADN.

Mandel expose les difficultés rencontrées par le système au fil du temps. À ces yeux, la compréhension de la technologie joue un rôle important dans le développement d'un nouveau cadre juridique adapté aux nouvelles technologies. Il identifie un phénomène temporaire qui se manifeste selon lui lors des périodes de transition suivant l'apparition de nouvelles technologies :

« It is inevitable that legal disputes concerning the new technology will be handled under the preexisting legal scheme in early stages of technological development. At this stage, there often will not be enough information and knowledge about nascent technologies to develop or modify appropriate legal rules, or there may not have been enough time to establish new statutes, regulations, or common law for managing the technology. »<sup>347</sup>

(Notre soulignement)

Dans cette phase de transition, caractérisée par un manque de données factuelles ou une inaction législative, la manière la plus appropriée de traiter les questions relatives à l'appréciation de la force probante, selon l'auteur, repose dans une attitude de réflexion sur le sens de la preuve et sur ses fondements. Mandel identifie un piège important en citant les faits d'une affaire prenant place cinq ans avant la publication de son article :

« In 2002, a district court judge held that evidence of identity based on fingerprints was inadmissible because it was unreliable. This holding led to somewhat of an uproar and the

---

<sup>346</sup> Gregory MANDEL, « History Lessons for a General Theory of Law and Technology », (2007) 8-2 *Minn JL Sci & Tech* 551.

<sup>347</sup> *Id.*, 563.

United States filed a motion to reconsider. The court held a hearing on the accuracy of fingerprint identification, at which two FBI agents testified. The court reversed its earlier decision and admitted the fingerprint testimony. The lesson learned from these cases for law and technology is relatively straightforward: decision-makers must not get blinded by the wonder or promise of new technology when judging the new legal issues created by impressive technological advance. It is a lesson that is easy to state, but clearly more difficult to apply in practice, particularly when a decision maker is confronted with the new technology for the first time and a cadre of experts testifies to its spectacular abilities. »<sup>348</sup>

(Notre soulignement)

Dans le cas des assistants vocaux, la nature complexe de l'intelligence artificielle, illustrée notamment par l'interdépendance de très nombreuses variables impliquées dans son fonctionnement et la présence de différents acteurs, peut susciter suffisamment de confusion pour aveugler un juriste profane. On peut aussi se demander qui serait le mieux placé pour éclairer la Cour au sujet de ces nouvelles technologies<sup>349</sup>. De plus, considérant le dynamisme et la complexité de l'intelligence artificielle, on peut se demander ce qu'un expert apporterait au tribunal. Si l'on conçoit l'intelligence artificielle comme étant la résultante de calculs mathématiques à la fois nombreux et complexes, aujourd'hui rendus possibles grâce au développement des ordinateurs, il serait peu probable qu'un être humain puisse réaliser, aussi rapidement que l'ordinateur, l'ensemble de ces calculs afin de les vérifier ou faire la démonstration qu'ils sont corrects. Cela rend donc l'expertise dans ce domaine peu pertinente pour répondre à des questions précises, en dehors de l'aspect méthodologique de l'intelligence artificielle.

Une expertise relative au fonctionnement adéquat d'un système à un moment précis n'est peut-être pas humainement possible. Cependant, les récents développements de l'« explainable AI » pourraient apporter la réponse dont ont besoin les juristes pour juger de l'intelligence artificielle. L'*explainable AI* — que l'on pourrait traduire librement par « l'IA compréhensible » — est un

---

<sup>348</sup> *Id.*

<sup>349</sup> Le *Code de procédure civile* québécois prévoit expressément que la mission de l'expert est d'éclairer le tribunal, et non de défendre la position de l'une ou l'autre des parties au litige. Voir : *Code de procédure civile*, préc., note 91, art. 22 et 231.

champ de recherche récent. Il consiste, au moment de la conception de nouveaux outils d'intelligence artificielle, à y intégrer une forme d'analyse introspective automatisée permettant à l'outil de produire, en plus de sa réponse, un compte-rendu de sa démarche pour l'utilisateur humain<sup>350</sup>. Le caractère « explicable » — *Explainability* — de l'intelligence artificielle peut se définir ainsi :

« [The] explainability of an AI model's prediction is the extent of transferable qualitative understanding of the relationship between model input and prediction (i.e., selective/suitable causes of the event) in a recipient friendly manner. »<sup>351</sup>

(Notre soulignement)

Cette avenue est particulièrement intéressante pour comprendre le fonctionnement de l'intelligence artificielle en action. Elle permet de déterminer pourquoi un outil d'intelligence artificielle arrive à un résultat particulier<sup>352</sup> et pourrait, au final, être la meilleure manière d'évaluer la force probante des éléments de preuve issus des assistants vocaux et de l'intelligence artificielle en général. Toutefois, l'idée de la machine qui analyse la machine pose une certaine problématique conceptuelle. Comment savoir si l'outil d'analyse introspectif est lui-même défaillant<sup>353</sup>? Si ces questionnements sont intéressants pour la science, le droit pourrait à notre avis se satisfaire de réponses intermédiaires, prenant soin de les mettre en perspective.

---

<sup>350</sup> Ehud REITER, *Natural Language Generation Challenges for Explainable AI*, Tokyo, International Conference on Natural Language Generation, 1st Workshop on Interactive Natural Language Technology for Explainable Artificial Intelligence, 2019, p. 2, en ligne : <<http://arxiv.org/abs/1911.08794>>.

<sup>351</sup> Sheikh Rabiul ISLAM, William EBERLE et Sheikh K. GHAFOR, « Towards Quantification of Explainability in Explainable Artificial Intelligence Methods », *ArXiv* 2019.arXiv:1911.10104, 2, en ligne : <<http://arxiv.org/abs/1911.10104>>.

<sup>352</sup> Thai LE, Suhang WANG et Dongwon LEE, « Why X rather than Y? Explaining Neural Model' Predictions by Generating Intervention Counterfactual Samples », *ArXiv* 2019.arXiv:1911.02042, 2, en ligne : <<http://arxiv.org/abs/1911.02042>>.

<sup>353</sup> Il existe à l'heure actuelle, en effet plusieurs approches pour développer une intelligence artificielle compréhensible et, des doutes subsistent. Voir : Oana-Maria CAMBURU, Eleonora GIUNCHIGLIA, Jakob FOERSTER, Thomas LUKASIEWICZ et Phil BLUNSOM, « Can I Trust the Explainer? Verifying Post-hoc Explanatory Methods », *ArXiv* 2019.arXiv:1910.02065, en ligne : <<http://arxiv.org/abs/1910.02065>>.

En effet, l'*explainable AI*, s'il devait se généraliser, donnerait suffisamment d'information pour permettre au juriste de comprendre ce qui s'est passé au sein de l'intelligence artificielle et de constater lui-même quelle force probante doit avoir la preuve issue de celle-ci<sup>354</sup>. De tels développements scientifiques pourraient permettre de venir à bout des critiques relatives à l'opacité de l'intelligence artificielle que l'on qualifie souvent de boîte noire. L'*Explainable AI* pourrait aussi servir de base pour une réflexion sur les enjeux éthiques engendrés par cette opacité, surtout lorsque les outils d'intelligence artificielle sont utilisés pour prendre des décisions. Or, à l'heure actuelle, une telle technologie n'est pas implantée dans aucun des assistants vocaux sur le marché et n'est pas encore une avenue permettant de comprendre leur fonctionnement.

---

<sup>354</sup> Arrieta et al. expliquent notamment pourquoi l'*explainable AI* représente un champ de recherche nécessaire : « As black-box Machine Learning models are increasingly being employed to make important predictions in critical contexts, the demand for transparency is increasing from the various stakeholders in AI. The danger is on creating and using decisions that are not justifiable, legitimate, or that simply do not allow obtaining detailed explanations of their behaviour. Explanations supporting the output of a model are crucial, e.g., in precision medicine, where experts require far more information from the model than a simple binary prediction for supporting their diagnosis. Other examples include autonomous vehicles in transportation, security, and finance, among others. In general, humans are reticent to adopt techniques that are not directly interpretable, tractable and trustworthy, given the increasing demand for ethical AI » Voir : Alejandro Barredo ARRIETA, Natalia DÍAZ-RODRÍGUEZ, Javier DEL SER, Adrien BENNETOT, Siham TABIK, Alberto BARBADO, Salvador GARCÍA, Sergio GIL-LÓPEZ, Daniel MOLINA, Richard BENJAMINS, Raja CHATILA et Francisco HERRERA, « Explainable Artificial Intelligence (XAI). Concepts, Taxonomies, Opportunities and Challenges toward Responsible AI », *ArXiv* 2019.arXiv:1910.10045, 2, en ligne : <<http://arxiv.org/abs/1910.10045>>.

## Conclusions

Pour conclure ce mémoire, il convient de faire un bref retour sur les différentes étapes de notre démarche. Nous avons d'abord tenté de définir les assistants vocaux, tant de manière technique que de manière juridique. À cet effet, nous avons principalement observé les cadres juridiques québécois, canadien, américain et européen en quête de pistes de réponse. Puis, nous avons entrepris de vérifier dans quelles mesures des éléments de preuves issus des assistants vocaux pourraient être recevables et, le cas échéant, comment analyser leur force probante. L'objectif était de déterminer la nature de ces éléments de preuve potentiels et, de manière plus large, de déterminer la nature des éléments de preuve issus de l'intelligence artificielle, évoluant dans l'univers de l'Internet des objets.

Au terme de cette démarche exploratoire non exhaustive, l'évaluation de la force probante nous a confrontés à une question à laquelle des juristes avant nous ont aussi été appelés à répondre : doit-on approcher les aspects juridiques des technologies de l'information au moyen d'un nouveau cadre normatif, ou peut-on emprunter le chemin connu pour répondre à de nouvelles questions ? On peut préciser cette question, dans le contexte du droit de la preuve : faut-il traiter la preuve technologique différemment de la preuve analogique ?

Nous sommes d'avis qu'il faut répondre affirmativement à cette question. Toutefois, traiter la preuve technologique différemment de la preuve analogique n'implique pas forcément, selon nous, de renoncer à l'ensemble des mécanismes et catégories existants du droit de la preuve civile. Nous croyons que cela signifie trois choses. D'abord, cela signifie qu'il faut être conscient des différences au niveau de la nature des moyens de preuve. Ensuite, cela implique de comprendre adéquatement les technologies sous-jacentes à ces moyens de preuve. Enfin, nous sommes d'avis que pour traiter différemment la preuve technologique, il faut faire preuve, en tant que juriste, d'ouverture d'esprit et de doute relativement à la possibilité de devoir changer notre droit pour assurer son efficacité et l'atteinte de ses objectifs fondamentaux.

Notre droit de la preuve, et par extension notre droit, reposent sur la prémisse qu'il existe une vérité et que celle-ci est accessible au travers d'une méthode qui nous mène à elle. Plusieurs philosophes remettent en question cette prémisse voulant qu'il existe quelque chose comme

« l'absence de doute » ou encore une idée de la « certitude »<sup>355</sup>. Sans nous élever au niveau de ces débats philosophiques, nous sommes d'avis que ceux-ci doivent nous éclairer et nous pousser à remettre en perspective notre approche à l'endroit de la preuve technologique. Elle sera toujours, à l'image de la perception de la vérité, une question relative ; relative à l'époque, aux mœurs, à l'état de la science et de la technologie. En bref, la vérité est fonction de la société dans laquelle elle s'incarne ; les réponses aux questions relatives à la preuve le sont donc tout autant.

Les biais inhérents aux technologies doivent aussi être pris en compte au moment d'évaluer un élément de preuve technologique. L'intelligence artificielle est le résultat de la conjonction de multiples éléments, dont certains sont eux-mêmes porteurs de biais subjectifs reflétant le contexte social et historique dans lesquels ils ont été développés. Ainsi, les algorithmes sont programmés par des informaticiens, eux-mêmes des êtres humains porteurs de biais. Les bases de données sont en majorité constituées et organisées par ces mêmes informaticiens. Ils ont aussi un rôle à jouer dans l'entraînement des algorithmes et dans l'architecture des réseaux. Encore, le langage même peut avoir un impact important sur les résultats de ces outils, et ce, sans que cela ne puisse apparaître au premier regard. En bref, il faut être conscient du caractère artificiel de l'univers technologique et du fait qu'il est à l'image de ceux qui l'ont construit. Être attentif à ces facteurs nous semble devenir de plus en plus important dans l'interprétation de la preuve technologique.

En 1996, dans l'affaire *R. c. Nikolovski*, l'honorable juge Cory de la Cour suprême du Canada, discutait des objectifs du droit de la preuve dans un contexte de droit pénal. Dans cette décision, le juge Cory soutenait que l'objectif du procès est de découvrir la vérité. En seulement deux paragraphes, il effectuait un survol presque complet du droit de la preuve et de ces objectifs, produisant ainsi un rappel simple, mais efficace de la majorité des points abordés dans ce mémoire. Bien que nous soyons d'avis que la vérité est un concept plus diffus que celui dépeint

---

<sup>355</sup>On peut citer en exemple la philosophie post-moderne et sa critique des Lumières. À ce sujet, les travaux du philosophe américain Richard Rorty permettent une bonne compréhension de ce mouvement de pensée : Richard RORTY, *Essays on Heidegger and Others*, Cambridge, Cambridge University Press, 1991, en ligne : <<https://doi.org/10.1017/CBO9780511609039>> ; Richard RORTY, *Objectivity, Relativism, and Truth*, Cambridge, Cambridge University Press, 1991, en ligne : <<https://doi.org/10.1017/CBO9781139173643>>.

par le magistrat ici, ses propos au sujet de l'évolution des moyens de preuve devraient, selon nous, continuer d'éclairer les juristes, même dans le contexte du droit civil :

« 13. L'objectif ultime d'un procès, criminel ou civil, doit être la recherche et la découverte de la vérité. Dans un procès criminel, on recherche la vérité afin de déterminer si l'accusé devant le tribunal est, hors de tout doute raisonnable, coupable du crime dont il est inculpé. La preuve produite doit être pertinente et admissible. C'est-à-dire qu'elle doit être probante sur le plan de la logique et recevable sur le plan juridique. La preuve peut émaner de témoins oculaires ou être circonstanciels, on peut également produire des éléments de preuve tangible, souvent appelés "preuve matérielle". Dans toute affaire criminelle, pour qu'il y ait déclaration de culpabilité, la preuve doit être suffisamment concluante pour que le juge des faits soit convaincu hors de tout doute raisonnable de la culpabilité de l'accusé.

14. Avec les progrès réalisés dans les domaines scientifiques et technologiques, la preuve présentée aux tribunaux, particulièrement en matière d'identification, a changé au fil des ans. Même si, au départ, il y a souvent une résistance à l'admission de nouvelles sortes de preuve, ces nouvelles preuves finissent par être acceptées et deviennent par la suite répandues et essentielles à la découverte de la vérité. La preuve par empreintes digitales est peut-être le premier exemple de preuve scientifique contribuant à l'identification. De même, le typage sanguin, avec ses raffinements incessants, peut être extrêmement utile en matière d'identification. Le test d'empreintes génétiques en est un autre exemple. Il ne faut jamais oublier que ce genre de preuve peut servir à établir l'innocence d'une personne tout aussi sûrement et efficacement que sa culpabilité. »<sup>356</sup>

(Notre soulignement)

Malgré l'ensemble des zones d'ombre dans l'appréciation de la preuve issue des outils d'intelligence artificielle, rejeter ce genre d'éléments de preuve — y compris la preuve témoignant de l'utilisation des assistants vocaux — serait se priver de pistes potentielles pour arriver à une vérité. Bien que les enjeux ne soient pas aussi importants que l'innocence ou la culpabilité dans un contexte civil, ils peuvent être importants dans certaines circonstances. On peut penser, par exemple, à la protection de l'intérêt supérieur de l'enfant en matière familiale.

---

<sup>356</sup> R. c. *Nikolovski*, [1996] 3 RCS 1197.

L'appréciation de cette preuve nouvelle demande cependant d'en comprendre les limites. Ces limites sont importantes et, dans la conjoncture technologique actuelle, l'adoption massive des technologies par les consommateurs n'est pas parallèlement suivie d'une compréhension généralisée de leur fonctionnement. Ainsi, une part de mystère relativement au fonctionnement de l'intelligence artificielle demeure toujours, puisque beaucoup de variables demeureront inconnues ou changeantes. De ce fait, cela nous permet d'identifier une autre limite majeure : une forme d'asymétrie entre la position du justiciable désirant utiliser un élément de preuve technologique et soutenant qu'il est probant et authentique, d'une part ; et la position du justiciable souhaitant contredire la force probante et l'authenticité d'un tel élément d'autre part. Dans ce scénario, l'un aura beaucoup plus de facilité à présenter sa preuve, alors que l'autre devra déployer des efforts importants qu'il ne pourrait peut-être pas forcément se permettre, faute de moyens, et ce, du fait de la nature éminemment complexe des éléments de preuve en question.

À propos de ces problématiques, nous avons présenté certaines solutions potentielles. L'une d'entre elles, dont nous avons longuement discuté, propose de se questionner sur la fonction des moyens de preuve documentaire. L'approche fonctionnelle proposée par le professeur Gautrais repose essentiellement sur un référent temporel et se veut une manière de permettre d'utiliser les véhicules existants pour de nouveaux passagers — les éléments de preuve technologiques. L'approche fonctionnelle peut être critiquée. Nous avons soulevé le fait qu'elle s'attardait essentiellement à adapter les catégories existantes du droit de la preuve québécois aux réalités des nouvelles technologies, alors que l'élaboration de nouvelles catégories pourrait peut-être s'avérer une meilleure solution.

Malgré nos critiques, nous avons adopté cette approche pour observer comment il serait possible de qualifier les éléments de preuve issus de l'utilisation d'assistants vocaux. En droit québécois, sans grande surprise, nous sommes arrivés à la conclusion que les traces de l'utilisation des assistants vocaux devraient être qualifiées d'éléments matériels de preuve et qu'elles seraient dès lors soumises au régime approprié du *Code civil du Québec*. Cette conclusion relève en un sens d'une certaine tautologie que nous avons nous-mêmes dénoncée à certains égards. Néanmoins, elle permet à notre cadre juridique de conserver une certaine cohérence s'inscrivant dans la continuité.



Or, il serait peut-être pertinent de considérer d'autres approches. C'est pour cette raison que nous sommes d'avis que la preuve technologique subit actuellement une certaine mutation et qu'une autre catégorie de preuve technologique se dessine à l'horizon. Ce que des chercheurs coréens désignent comme des « quasi-documents »<sup>357</sup>, c'est-à-dire un regroupement d'information ne contenant aucune « idée humaine », mais seulement des données mises en forme par des processus purement technologiques, porte à réflexion. L'une des conclusions que nous tirons de cet exercice comparatif est que le droit de la preuve ne pourra pas se permettre d'évoluer en vase clos s'il veut relever le défi des technologies de l'information. L'interdisciplinarité et le droit comparé ne seront plus seulement intéressants pour aborder de nouvelles perspectives, ils seront nécessaires. L'apport d'autres disciplines que le droit fut essentiel à l'analyse que nous avons réalisée dans le cadre de notre recherche pour comprendre et vulgariser l'intelligence artificielle. Dans un univers globalisé, pour s'inspirer des meilleures pratiques et s'assurer de pouvoir travailler de concert avec d'autres juridictions, nous sommes d'avis que les juristes ne pourront pas se limiter à la recherche du droit au Québec et, dans une certaine mesure, à la recherche du droit uniquement.

Sur un autre plan, nous avons discuté du facteur qui influence selon nous la force probante des éléments de preuve technologiques, soit la compréhension de la technologie sous-jacente à la preuve présentée. À l'heure actuelle, la preuve dite technologique désigne des procédés de preuves qui trouvent écho dans le monde prétechnologique. Le courriel était une lettre, l'enregistrement vidéo était un témoignage et ainsi de suite. Or, il pourrait éventuellement apparaître des éléments de preuve technologiques inédits, sans commune mesure avec l'ère analogique. Ces éléments de preuve nouveaux nécessiteraient alors le développement de nouveaux référents permettant leur analyse. Nous sommes d'avis que la preuve issue de l'intelligence artificielle fait partie de cette catégorie nouvelle.

Cette conclusion nous pousse à croire que cette nouvelle forme d'élément de preuve technologique est pour l'instant à sa face même moins probante que toute autre preuve, et ce, parce qu'elle est au premier regard incompréhensible ou du moins impossible à questionner et mettre en doute. Cette proposition est contre-intuitive, mais nous sommes d'avis que telle doit

---

<sup>357</sup> E. SUGIYAMA, préc., note 189, p. 511.

être la posture du juriste devant une preuve inédite ou radicalement différente de tout ce à qui il ou elle aurait pu être préalablement confronté, c'est-à-dire le doute. Cette situation ne saurait toutefois perdurer puisque l'on travaille déjà à créer des intelligences artificielles pouvant rendre compte de leur démarche. L'équilibre pourrait éventuellement être rétabli et le concept de « boîte noire » définitivement abandonné pour désigner le fonctionnement de l'intelligence artificielle. Cependant, les récentes percées de l'*explainable AI* sont encore embryonnaires et soulèvent, à leur tour, de nouvelles questions relativement à la fiabilité de ces procédés et le sentiment de sécurité qu'ils apportent. De plus, encore faudra-t-il que cette technologie fasse son chemin jusqu'au consommateur, celle-ci n'étant pour l'instant destinée qu'à des applications spécialisées de l'intelligence artificielle.

D'ici là, cependant, nous identifions des failles empêchant les juristes et les juges de pleinement comprendre les éléments de preuve qui leur sont soumis. L'une de ces failles est la conséquence du principe accusatoire et contradictoire sur lequel reposent plusieurs des systèmes judiciaires que nous avons abordés. Les parties étant maîtres de la preuve, elles pourraient ne pas parvenir à l'expliquer correctement, et de fait, voir celle-ci mise de côté par le juge, celui-ci ne disposant pas d'assez d'information pour en évaluer la teneur.

Pire encore, un juge pourrait voir en un élément technologique quelque chose qui ne s'y trouve pas et prendre une décision valide en droit, mais erronée sur la base des faits. De là, nous avançons l'hypothèse que la complexification de la preuve technologique présentée appelle peut-être une redéfinition du rôle de notre système judiciaire dans la recherche des faits et de la connaissance permettant d'évaluer les preuves technologiques d'un genre nouveau. Nous avons brièvement évoqué que la solution à pareille situation résidait peut-être dans le recours à l'expertise unique, afin d'éviter une escalade des coûts pour les parties. Or, les questions relatives aux coûts de la preuve par expert n'étaient pas le sujet exact de ce mémoire et ne sont d'ailleurs pas des enjeux propres à la preuve technologique. Ainsi, limitons-nous à souligner que le coût de l'expertise en matière technologique risque le plus souvent d'être une entrave à l'accès à la justice, ce qu'elle est malheureusement dans plusieurs domaines.

Quoi qu'il en soit, tant les assistants vocaux que l'intelligence artificielle et l'Internet des objets laissent place à d'autres débats juridiques des plus pertinents allant bien au-delà des questions de droit de la preuve en touchant des aspects fondamentaux de notre société démocratique

comme la protection de la vie privée et des libertés fondamentales. La prolifération de l'Internet des objets — dont font partie les assistants vocaux — laisse entrevoir un avenir où l'utilisateur sera constamment épié, et ce, dans des proportions jusqu'ici inégalées. Cette nouvelle réalité signifie peut-être un changement de paradigme qui forcera les juristes à revoir leur conception de la vie privée. Peut-être devrions-nous en revoir la définition, à l'aune des nouveaux comportements dominants dans notre société. Ne devient-il pas difficile de prétendre que la demeure est le refuge inviolable du citoyen lorsque celui-ci l'expose allègrement sur les médias sociaux et le place sous écoute de son propre gré ? Cette question est pour un autre temps. Paradoxalement, ces outils qui pourraient s'avérer attentatoire à la vie privée présente au moins l'intérêt de multiplier les sources d'information disponibles pour faire la preuve de certains faits, autrefois impossibles à prouver avec autant de précision et de détails. Un gain pour la preuve, peut-être, mais à quel prix pour la vie privée ?

Enfin, et ce seront ici nos derniers mots sur le sujet, nos principales conclusions sont au nombre de deux. Premièrement, il faut mettre en doute le fonctionnement de ces nouveaux outils et refuser de les accepter tout bonnement sans se questionner. Deuxièmement, il faut réfléchir aux fondements juridiques sur lesquels reposent nos cadres normatifs. Il s'agit là, selon nous, de l'unique manière d'assurer la sauvegarde des droits des utilisateurs des nouvelles technologies. Il faut retourner aux sources du droit, plus que jamais, pour comprendre les phénomènes qui ont fait évoluer le droit et prévenir de potentielles mutations néfastes.

La posture appropriée est celle du doute ; le doute envers la science et le doute envers le droit. Au moment présent, même si les assistants vocaux sont utilisés par un grand nombre de personnes, ils le sont malheureusement, comme bien d'autres technologies modernes, de manière aveugle et dans l'ignorance de leur réelle nature. On les adopte trop souvent sans égard aux dangers éventuels et sans précautions. Une telle ignorance pourrait, subtilement, mais sûrement, modifier notre relation avec certains principes fondamentaux du droit et amener des changements normatifs à notre insu et peut-être même fragiliser certains de nos droits les plus précieux. Là est l'écueil.

# Table de la législation

## *Législation québécoise*

*Charte des droits et libertés de la personne*, RLRQ, c. C-12.

*Code civil du Québec*, L.Q. 1991, c. C-64.

*Code de procédure civile*, RLRQ, c. C-25.01.

*Loi concernant le cadre juridique des technologies de l'information*, RLRQ, c. C-1.1.

*Loi sur le Barreau*, RLRQ, c. B-1.

*Code de déontologie des avocats*, RLRQ, c. B-1, r. 3.1.

*Règlement sur la comptabilité et les normes d'exercice professionnel des avocats*, RLRQ, c. B-1, r. 5.

*Loi sur la protection des renseignements personnels dans le secteur privé*, RLRQ, c. P-39.1.

## *Législation canadienne*

*Charte canadienne des droits et libertés*, Partie I de la *Loi constitutionnelle de 1982*, c. 11 (R-U).

*Code criminel*, L.R.C. (1985), c. C-46.

*Loi sur la preuve au Canada*, L.R.C. (1985), c. C-5.

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

*Loi sur le droit d'auteur*, L.R.C. (1985), c. C-42.

*Loi sur les brevets*, L.R.C. (1985), c. P-4.

## *Législation américaine*

*Federal Rules of Civil Procedures*

*Federal Rules of Evidence*

## *Législation française*

*Code pénal*

*Code de procédure civile*

*Loi n° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique*

## *Instruments législatifs et réglementaires européens*

*CE, Directive 1996/9/CE du Parlement européen, du 11 mars 1996 concernant la protection juridique des bases de données, JO, L 77/20.*

*———, Directive 1999/93/CE du Parlement européen et du Conseil, du 13 décembre 1999, sur un cadre communautaire pour les signatures électroniques, JO, L 13/12.*

*———, Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur, JO, L 178/1.*

*CONSEIL DE L'EUROPE, Lignes directrices du Comité des Ministres du Conseil de l'Europe sur les preuves électroniques dans les procédures civiles et administratives, (2019).*

# Table de la jurisprudence

## *Jurisprudence québécoise*

- Atlas Copco Canada inc. c. Commission d'appel en matière de lésions professionnelles*, [1995] CALP 909 (C.S.).
- Autorité des marchés financiers c. Baazov*, 2018 QCCS 3422.
- B.C. c. Loto-Québec*, 2011 QCCAI 133.
- Benisty c. Kloda*, 2018 QCCA 608.
- Bolduc c. Arthur*, [1996] J.E. 96-1569 (C.S.).
- Cadieux c. Service de gaz naturel Laval inc.*, [1991] RJQ 2490 (C.A.).
- Citadelle, Cie d'assurance générale c. Montréal (Ville)*, [2005] CanLII 24709 (CSQ).
- Compagnie des chemins de fer nationaux du Canada c. Compagnie d'arrimage de Québec ltée*, [2010] QCCQ 942.
- Directeur des poursuites criminelles et pénales c. Deramchi*, 2018 QCCQ 7424.
- Droit de la famille — 161206*, 2016 QCCS 2378.
- Drouin (Succession de Côté-Drouin) c. Pepin*, 2019 QCCS 848.
- Enercon Canada inc. c. Commission de la construction du Québec*, 2015 QCCRT 0394.
- Erez Sewing Machine Co. Ltd c. Vêtement Super Vogue Inc.*, [1980] C.P. 157.
- Fraternité des policiers et policières de Sherbrooke c. Sherbrooke (Ville de)*, [2019] CanLII 82465 (QCTAT).
- Fuoco c. Société générale de financement du Québec*, 2006 QCCA 1491.
- Giannini c. De Montigny*, 2018 QCCQ 6414.
- Holland c. St-Eustache Mitsubishi*, 2019 QCCQ 4035.
- Lauzon c. Noel*, 2018 QCCS 3903.
- Métallurgistes unis d'Amérique, section locale 7785 et Caradon Indalex (division de Caradon ltée)*, [2000] CanLII 46584 (QC SAT).
- M.F. c. Gravel*, 2019 QCCS 2521
- Montréal (Ville de) c. Bolduc*, 2009 QCCM 185.
- Papp c. Alexeev*, 2019 QCCQ 4809.
- R. c. Faivre*, 2018 QCCQ 7467.
- R. c. Girard Lévesque*, 2015 QCCQ 4509.
- R. c. L.M.*, [2005] CanLII 24988 (C.Q.)
- R. c. M.G.*, 2015 QCCQ 4864.
- R. c. Milette*, 2015 QCCQ 16688.
- Stefanovic c. ING Assurances inc.*, 2007 QCCQ 10363.
- Vandal c. Salvas*, [2005] 587 RL (C.Q.).
- Youroukova c. Dellorefice*, 2013 QCCQ 11055.

*Jurisprudence canadienne – fédérale*

*Apple Computer, Inc. c. Mackintosh Computers Ltd.; Apple Computer, Inc. c. 115778 Canada Inc.*, [1990] 2 RCS 209.  
*CCH Canadienne Ltée c. Barreau du Haut-Canada*, 2004 CSC 13.  
*Canada (Procureur général) c. Amazon.com*, 2 RCF 459 (CAF).  
*Dell Computer Corp. c. Union des consommateurs*, 2007 CSC 34.  
*R. c. Levigne*, 2010 CSC 25.  
*R. c. Mills*, 2019 CSC 22.  
*R. c. Nikolovski*, [1996] 3 RCS 1197.  
*R. c. Spencer*, 2014 CSC 43.  
*Tele-Direct (Publications) Inc. c. American Business Information*, [1998] 134 FTR 80 (CAF).

*Jurisprudence canadienne – provinciale*

*A1702178 (Re)*, CanLII 95902 (BC WCAT).  
*Ainger v. Posendorf*, ONSC 2220.  
*Laushway v. Messervey*, 2014 NSCA 7.

*Jurisprudence américaine*

*Alice Corp. v. CLS Bank Int'l*, [2014] 573 U.S. 208.  
*Commonwealth v. Denison*, [2015] Mass. Super. Ct.  
*Feist Publications, Inc. v. Rural Telephone Service Co.* [1991] 499 U.S. 340.  
*Melendez-Diaz v. Massachusetts*, [2009] U.S. (U.S. Supreme Court) (Certiorari to the Appeals Court of Massachusetts).  
*State of Arkansas v. James A. Bates*, [2016] Ark. Cir.

*Jurisprudence française*

*Cour de Cassation, Chambre civile 2, du 7 octobre 2004*, 03-12.653, Publié au bulletin, [2004].  
*Cour de cassation, Chambre sociale, 23 mai 2007*, 06-43.209, Publié au bulletin, [2007].  
*Tribunal de grande instance de Nanterre*, [2019] RG 18/01502.

*Jurisprudence du Royaume-Uni*

*R. v. Madhub Chunder*, [1874] 21 WRCr 13.

*Lord Advocate v. Lord Blantyre*, [1879] 4 App Cas 770.



# Bibliographie

## *Monographies et ouvrages collectifs*

- ALPAYDIN, E., *Introduction to Machine Learning*, Cambridge, MIT Press, 2009.
- BÉCHARD, D., *Manuel de l'objection*, 3<sup>e</sup> éd., coll. « La référence », Cowansville, Éditions Yvon Blais, 2009
- BOSTROM, N., *Superintelligence. Paths, Dangers, Strategies*, Oxford, Oxford University Press, 2014.
- CLARK, A., C. FOX et S. LAPPIN, *The Handbook of Computational Linguistics and Natural Language Processing*, Chichester, John Wiley & Sons, 2013.
- CORRALES, M., M. FENWICK et N. FORGÓ, *New Technology, Big Data and the Law*, coll. « Perspectives in Law, Business and Innovation », Singapour, Springer, 2017, en ligne : <<http://dx.doi.org/10.1007/978-981-10-5038-1>>.
- DAVISON, M. J., W. R. CORNISH, F. DESSEMONTET, P. GOLDSTEIN et R. JACOB, *The Legal Protection of Databases*, Cambridge, Cambridge University Press, 2003.
- DESCARTES, R., *Discours de la méthode*, Trois-Rivières, Les Échos du Maquis, 2011, en ligne : <<https://philosophie.cegeptr.qc.ca/wp-content/documents/Discours-de-la-m%C3%A9thode.pdf>>.
- DIBONA, C., S. OCKMAN et M. STONE (dir.), *Open Sources. Voices from the Open Source Revolution*, 1<sup>re</sup> éd., Sebastopol, O'Reilly, 1999.
- DUCHARME, L., *Précis de la preuve*, 6<sup>e</sup> éd., coll. « Bleue », Série « Précis », Montréal, Wilson & Lafleur, 2005.
- ENSMENGER, N., *The Computer Boys Take Over. Computers, Programmers, and the Politics of Technical Expertise*, coll. « History of Computing », Cambridge, MIT Press, 2010.
- GAUTRAIS, V., *Neutralité technologique. Rédaction et interprétation des lois face aux changements technologiques*, Montréal, Éditions Thémis, 2012.
- , *La preuve technologique*, 2<sup>e</sup> éd., Montréal, LexisNexis, 2018.
- GOURMONT, R. de, *Promenades philosophiques*, 10<sup>e</sup> éd., Paris, Mercure de France, 1925.
- HASSAN, Q. F., *Internet of Things A to Z. Technologies and Applications*, Hoboken, John Wiley & Sons, 2018, en ligne : <<https://onlinelibrary.wiley.com/doi/book/10.1002>>.
- KÉLADA, H., *Notions et techniques de la preuve civile*, Montréal, Wilson Lafleur, 1986.
- KENGYEL, M. et Z. NEMESSÁNYI, *Electronic Technology and Civil Procedure. New Paths to Justice from Around the World*, New York, Springer, 2012.
- LA METTRIE, J. O. de, *L'homme machine*, Leyde, Elie Luzac fils, 1748, en ligne : <[https://fr.wikisource.org/wiki/L%E2%80%99Homme\\_Machine](https://fr.wikisource.org/wiki/L%E2%80%99Homme_Machine)>.

- LEDERMAN, S. N., A. W. BRYANT, M. FUERST et J. SOPINKA, *The Law of Evidence in Canada*, 5<sup>e</sup> éd., Toronto, LexisNexis, 2018.
- MAGLOGIANNIS, I. G., *Emerging Artificial Intelligence Applications in Computer Engineering. Real World AI Systems with Applications in EHealth, HCI, Information Retrieval and Pervasive Technologies*, Amsterdam, IOS Press, 2007.
- MALEK, H. M., *Phipson on Evidence*, coll. « The Common law library », Londres, Sweet & Maxwell, 2013.
- MARSEILLE, C., *La règle de la pertinence en droit de la preuve civile québécois*, coll. « Points de droit », Cowansville, Éditions Yvon Blais, 2004.
- MAYER-SCHÖNBERGER, V. et K. CUKIER, *Big Data. A Revolution that Will Transform How We Live, Work, and Think*, New York, Houghton Mifflin Harcourt, 2013.
- MINISTÈRE DE LA JUSTICE DU QUÉBEC, *Commentaire du ministre de la Justice*, n°2, Québec, Publications du Québec, 1993, en ligne : <<https://elois.caij.qc.ca/CCQ-1991/article2856>>.
- NILSSON, N. J., *The Quest for Artificial Intelligence. A History of Ideas and Achievements*, Cambridge, Cambridge University Press, 2010.
- O'HARE, G. M. P. et N. R. JENNINGS, *Foundations of Distributed Artificial Intelligence*, John Wiley & Sons, 1996.
- ORWELL, G., *1984*, traduit par Amélie AUDIBERTI, Paris, Gallimard, 1993.
- PACIOCCO, D. M. et L. STUESSER, *The Law of Evidence*, 7<sup>e</sup> éd., coll. « Essentials of Canadian Law », Toronto, Irwin Law Inc, 2015.
- PANDOLFINI, B., *Kasparov and Deep Blue. The Historic Chess Match Between Man and Machine*, New York, Simon and Schuster, 1997.
- PHILLIPS, M., *La preuve électronique au Québec*, Montréal, LexisNexis, 2010.
- PICHÉ, C., *La preuve civile*, 5<sup>e</sup> éd., Montréal, Éditions Yvon Blais, 2016.
- RORTY, R., *Essays on Heidegger and Others*, Cambridge, Cambridge University Press, 1991, en ligne : <<https://doi.org/10.1017/CBO9780511609039>>.
- , *Objectivity, Relativism, and Truth*, Cambridge, Cambridge University Press, 1991, en ligne : <<https://doi.org/10.1017/CBO9781139173643>>.
- ROYER, J.-C., *La preuve civile*, Cowansville, Éditions Yvon Blais, 1987.
- RUSSELL, S. J. et P. NORVIG, *Intelligence artificielle*, 3<sup>e</sup> éd., Paris, Pearson Éducation, 2010.
- SCHWAB, K., *The Fourth Industrial Revolution*, 1<sup>re</sup> éd., New York, Crown Business, 2016.
- SILVA, I. N. DA, D. H. SPATTI, R. A. FLAUZINO, L. H. BARTOCCI LIBONI et S. F. DOS REIS ALVES, *Artificial Neural Networks*, New York, Springer, 2016, en ligne : <<https://link.springer.com/content/pdf/10.1007/978-3-319-43162-8.pdf>>.
- SPRINGER, P. J., *Military Robots and Drones. A Reference Handbook*, Santa Barbara, ABC-CLIO, 2013.
- STERNBERG, R. J., *The Triarchic Mind. A New Theory of Human Intelligence*, New York, Viking, 1988.
- TAMARO, N., *Loi sur le droit d'auteur, texte annoté*, 10<sup>e</sup> éd., Toronto, Carswell, 2015.

- TANAKA, K., *An Introduction to Fuzzy Logic for Practical Applications*, New York, Springer, 1997.
- TAVRIS, C. et C. WADE, *Introduction à la psychologie. Les grandes perspectives*, traduit par Alain GAGNON, Claude GOULET et Patrice WIEDMAN, Saint-Laurent, ERPI, 2007.
- THEOLEYRE, F. et A.-C. PANG, *Internet of Things and M2M Communications*, Algade, River Publishers, 2013.
- WARWICK, K., *Artificial Intelligence. The Basics*, Londres, Routledge, 2013, en ligne : <<https://www.taylorfrancis.com/books/9780203802878>>.

*Articles de revues, études d'ouvrages collectifs et billets de blogues scientifiques*

- AITCHISON, S., « Privacy in the Cloud. The Fourth Amendment Fog », (2018) 93 *Wash. L. Rev.* 1019.
- ALLEN, S., « Privacy in the Twenty-First Century Smart Home », (2018) 19 *JHTL* 162.
- ALOM, Z., T. M. TAHA, C. YAKOPCIC, S. WESTBERG, P. SIDIKE, S. NASRIN, B. C. VAN ESESN, A. A. S. AWWAL et V. K. ASARI, « The History Began from AlexNet. A Comprehensive Survey on Deep Learning Approaches », *ArXiv* 2018.arXiv:1803.01164, en ligne : <<http://arxiv.org/abs/1803.01164>>.
- ALTMAN, N. S., « An Introduction to Kernel and Nearest Neighbor Nonparametric Regression », (1992) 46-3 *Am. Stat.* 175.
- ARRIETA, A. B., N. DÍAZ-RODRÍGUEZ, J. DEL SER, A. BENNETOT, S. TABIK, A. BARBADO, S. GARCÍA, S. GIL-LÓPEZ, D. MOLINA, R. BENJAMINS, R. CHATILA et F. HERRERA, « Explainable Artificial Intelligence (XAI). Concepts, Taxonomies, Opportunities and Challenges toward Responsible AI », *ArXiv* 2019.arXiv:1910.10045, en ligne : <<http://arxiv.org/abs/1910.10045>>.
- BAHRAMI, M. et M. SINGHAL, « The Role of Cloud Computing Architecture in Big Data », dans Witold PEDRYCZ et Shyi-Ming CHEN (dir.), *Information Granularity, Big Data, and Computational Intelligence*, coll. « Studies in Big Data, Cham », Springer, 2015, p. 275, en ligne : <[https://doi.org/10.1007/978-3-319-08254-7\\_13](https://doi.org/10.1007/978-3-319-08254-7_13)>.
- BARR, J. et L. F. CABRERA, « AI Gets a Brain », (2006) 4-4 *Queue* 24.
- BARREAU DE MONTRÉAL. *Guide des technologies de l'information. Les courriels* (2017), en ligne : <[https://www.barreaudemontreal.qc.ca/sites/default/files/guideti\\_courriels\\_fev](https://www.barreaudemontreal.qc.ca/sites/default/files/guideti_courriels_fev)>
- BATES, M., « Models of natural language understanding. », (1995) 92-22 *Proc Natl Acad Sci U S A* 9967.
- BAYERN, S., « Are Autonomous Entities Possible? », (2019) 114-23 *Northwestern University Law Review Online*, en ligne : <<https://papers.ssrn.com/abstract=3410395>>.

- BÉLANGER, M.-È., « Documents technologiques, copies et documents résultants d'un transfert », dans *Fascicule 5, JurisClasseur Québec – Preuve et prescription*, Montréal, LexisNexis Canada, 2010.
- BENCH-CAPON, T., M. ARASZKIEWICZ, K. ASHLEY, K. ATKINSON, F. BEX, *et al.*, « A History of Ai and Law in 50 Papers. 25 Years of the International Conference on Ai and Law », (2012) 20-3 *Artif Intell Law* 215.
- BENGIO, Y., « Learning Deep Architectures for AI », (2009) 2-1 *Foundations and Trends in Machine Learning* 1.
- BENGIO, Y. et A. COURVILLE, « Neural Network Architectures », dans Monica BIANCHINI et Marco MAGGINI, *Handbook on Neural Information Processing*, 1<sup>re</sup> éd., coll. « Intelligent Systems Reference Library », n°49, New York, Springer, 2013, en ligne : <<https://link.springer.com/content/pdf/10.1007/978-3-642-36657-4.pdf>>.
- BIDAUD-GARON, C., « La force probante des actes de l'état civil étrangers après la loi du 26 novembre 2003 », (2006) 1-49 *Revue Critique de Droit International Privé*, en ligne : <<https://halshs.archives-ouvertes.fr/halshs-02238258>>.
- BOHM, A. S., E. J. GEORGE, B. CYPHERS et S. LU, « Privacy and Liberty in an Always-on, Always-Listening World », (2017) 19-1 *Colum. Sci. & Tech. L. Rev.* 1.
- BUCHANAN, B. G., « A (Very) Brief History of Artificial Intelligence », (2005) 26-4 *AI Magazine* 53.
- BUMBALEK, Z., J. ZELENKA et L. KENCL, « Cloud-Based Assistive Speech-Transcription Services », dans Klaus MIESENBERGER, Arthur KARSHMER, Petr PENAZ et Wolfgang ZAGLER (dir.), *Computers Helping People with Special Needs*, coll. « Lecture Notes in Computer Science », Berlin, Springer, 2012, p. 113.
- BURKETT, C., « "I Call Alexa to the Stand". The Privacy Implications of Anthropomorphizing Virtual Assistants Accompanying Smart-Home Technology », (2018) 20 *Vand. J. Ent. & Tech. L.* 1181.
- CABITZA, F., D. CIUCCI et R. RASOINI, « A Giant with Feet of Clay. On the Validity of the Data That Feed Machine Learning in Medicine », dans *Organizing for the Digital World*, New York, Springer, 2018, p. 121-136, en ligne : <[https://link.springer.com/content/pdf/10.1007%2F978-3-319-90503-7\\_10.pdf](https://link.springer.com/content/pdf/10.1007%2F978-3-319-90503-7_10.pdf)>.
- CAMBURU, O.-M., E. GIUNCHIGLIA, J. FOERSTER, T. LUKASIEWICZ et P. BLUNSOM, « Can I Trust the Explainer? Verifying Post-hoc Explanatory Methods », *ArXiv* 2019.arXiv:1910.02065, en ligne : <<http://arxiv.org/abs/1910.02065>>.
- CAPRA, D., « Authenticating Digital Evidence », (2017) 69 *Baylor L. Rev.* 1.
- CARON, S., « Une introduction aux arbres de décision », *Stéphane Caron* (31 août 2011), en ligne : <<https://scaron.info/doc/intro-arbres-decision/intro.pdf>>.
- CASSENS WEISS, D., « Data on Man's Pacemaker Led to His Arrest on Arson Charges », *ABA Journal* (2017), en ligne : <[http://www.abajournal.com/data\\_on\\_mans\\_pacemaker\\_led\\_to\\_his\\_arrest\\_on\\_arson\\_charges/](http://www.abajournal.com/data_on_mans_pacemaker_led_to_his_arrest_on_arson_charges/)>.

- CHEN, J. et P. BURGESS, « The Boundaries of Legal Personhood. How Spontaneous Intelligence Can Problematiser Differences Between Humans, Artificial Intelligence, Companies and Animals », (2019) 27-1 *AI & L* 73-92.
- COLLINGS, T. et D. MILNER, « A New Chronology of Papermaking Technology », (1990) 14-1 *Journal of the Institute of Paper Conservation* 58.
- DORAN, D., S. SCHULZ et T. R. BESOLD, « What Does Explainable AI Really Mean? A New Conceptualization of Perspectives », *ArXiv* 2017.arXiv:1710.00794, en ligne : <<http://arxiv.org/abs/1710.00794>>.
- DUFFY, B. R., « Anthropomorphism and the Social Robot », (2003) 42-3 *Robotics and Autonomous Systems* 177.
- EASTERBROOK, F. H., « Cyberspace and the Law of the Horse », (1996) 166-1 *U. Chi. Legal F.* 207.
- FABIEN, C., « La preuve par document technologique », (2004) 38 *R.J.T.* 553.
- FAVRO, P. J. et D. P. PULLAN, « New Utah Rule 26. A Blueprint for Proportionality Under the Federal Rules of Civil Procedures », (2012) 2012 *Mich. St. L. Rev.* 933.
- FENG-HSIUNG HSU, « IBM's Deep Blue Chess grandmaster chips », (1999) 19-2 *IEEE Micro* 70.
- FERRUCCI, D., E. BROWN, J. CHU-CARROLL, J. FAN, D. GONDEK, A. A. KALYANPUR, *et al.*, « Building Watson. An Overview of the DeepQA Project », (2010) 31-3 *AI Magazine* 59.
- FORIERS, P., « Introduction au droit de la preuve », dans *La Preuve en droit. Études*, coll. « Travaux du Centre national de recherches de logique », Bruxelles, Bruylant, 1981.
- FRIEDMAN, R. D., « A Close Look at Probative Value », (1986) 66-4 *B.U. L. Rev.* 733.
- FURBACH, U., I. GLÖCKNER et B. PELZER, « An Application of Automated Reasoning in Natural Language Question Answering », (2010) 23 *AI Commun.* 24.
- GAGNÉ, M., « La preuve dans un contexte électronique », dans *Service de la formation permanente du Barreau du Québec*, 160, coll. « Développements récents en droit de l'Internet », Cowansville, Éditions Yvon Blais, 2001, p. 55-105.
- GAON, A. et I. STEDMAN, « A Call to Action. Moving Forward with the Governance of Artificial Intelligence in Canada », (2019) 56-4 *Alta. L. Rev.* 1137.
- GARCIAS, M. et M. CHOUZIER, « La preuve informatique. Quelles nouveautés techniques pour quelles évolutions juridiques ? », (2012) *LexBase Hebdo* 280, en ligne : <[http://www.adij.fr/wpcontent/uploads/2012/01/CompteRendu\\_PreuveInformatique](http://www.adij.fr/wpcontent/uploads/2012/01/CompteRendu_PreuveInformatique)>.
- GAUTRAIS, V., « Quelle est la différence entre une copie et un transfert? », LCCJTI.ca (3 mai 2012), en ligne : <<https://www.lccjti.ca/faq/quelle-est-la-difference-entre-une-copie-et-un-transfert/>>.
- , « Intégrité », LCCJTI.ca (2017), en ligne : <<https://www.lccjti.ca/definitions/integrite/>>.
- , « Document technologique », LCCJTI.ca (26 janvier 2017), en ligne : <<https://www.lccjti.ca/definitions/document-technologique/#ancre33>>.

- , « Article 7 », LCCJTI.ca (29 janvier 2017), en ligne : <<https://www.lccjti.ca/articles/article-7/>>.
- GINGRAS, P., « Quand la preuve technologique est susceptible de déconsidérer l'administration de la justice », dans Patrick GINGRAS et Nicolas VERMEYS, *Technologies de l'information - En bref, n°4*, Cowansville, Éditions Yvon Blais, 2013, en ligne : <<https://www.lccjti.ca/files/sites/105/2013/05/bulletinPGingras.pdf>>.
- GIUFFRIDA, I., « Liability Risk for Artificial Intelligence Predictive Decision-Making », (2019) 88 (Soumis pour publication) *Fordham L. Rev.*
- GOLD, V. J., « Federal Rule of Evidence 403. Observations on the Nature of Unfairly Prejudicial Evidence », (1983) 58-3 *Wash. L. Rev.* 497.
- GOODMAN, C. C., « AI/Esq. Impacts of Artificial Intelligence in Lawyer-Client Relationships », (2019) 72-1 *Oklahoma Law Review* 149.
- GOUDREAU, M., « Légiférer par généralités ou en termes précis ? Quelle question ! », Institut canadien d'administration de la justice 2019, en ligne : <<https://edoctrine.caij.qc.ca/ciaj-icaj/blogue/i962b7226-cb0f-46c7-9394-f474708f3e33/>>.
- GREGORY, J., « Devices Gone Wild », (2018) *Slaw Canada's Online Legal Magazine*, en ligne : <<http://www.slaw.ca/2018/05/03/devices-gone-wild/>>.
- GRIMM, P., « New Evidence Rules and Artificial Intelligence », (2018) 45-1 *Litigation Journal*, en ligne : <<https://www.americanbar.org/groups/litigation/publications/litigation>>.
- GUBBIA, J., R. BUYTAB, M. PALANISWAMIA et S. MARUSICA, « Internet of Things (iot). A Vision, Architectural Elements, and Future Directions », (2013) 29-7 *Future Generation Computer Systems* 1645.
- GUILMAIN, A., « Sur les traces du principe de proportionnalité. Une esquisse généalogique », (2015) 61-1 *R.D. McGill* 87.
- HIRSCHBERG, J. et C. D. MANNING, « Advances in Natural Language Processing », (2015) 349-6245 *Science* 261.
- HIRSCHMAN, L. et R. GAIZAUSKAS, « Natural Language Question Answering. The View from Here », (2001) 7-4 *Nat. Lang. Eng.* 275.
- INCHAUSPÉ, D., « Chapitre 6. Intime conviction », dans *L'innocence judiciaire*, coll. « Questions judiciaires », Paris, Presses Universitaires de France, 2012, p. 155-178, en ligne : <<https://www.cairn.info/l-innocence-judiciaire--9782130606994-p-155.htm>>.
- ISLAM, S. R., W. EBERLE et S. K. GHAFOR, « Towards Quantification of Explainability in Explainable Artificial Intelligence Methods », *ArXiv* 2019.arXiv:1911.10104, en ligne : <<http://arxiv.org/abs/1911.10104>>.
- JACOBOWITZ, J. L. et J. ORTIZ, « Happy Birthday Siri! Dialing in Legal Ethics for Artificial Intelligence, Smartphones, and Real Time Lawyers », (2018) 4-5 *Texas A&M Journal of Property Law* 408.
- JANSEN, B. J. et S. Y. RIEH, « The Seventeen Theoretical Constructs of Information Searching and Information Retrieval », (2010) 61-8 *J Am Soc Inf Sci Technol* 1517.

- JIANG, F., Y. JIANG et H. ZHI, « Artificial Intelligence in Healthcare. Past, Present and Future », (2017) 2-4 *Stroke Vasc Neurol* 230.
- KASHYAP, V., J. RUCHTI, L. KOT, E. TURETSKY, R. SWORDS, S. A. PAN, J. HENRY, D. MELSKI et E. SCHULTE, « Automated Customized Bug-Benchmark Generation », *ArXiv* 2019.arXiv:1901.02819, en ligne : <<http://arxiv.org/abs/1901.02819>>.
- KAYE, D. H., « Quantifying Probative Value Symposium. Comment », (1986) 66-4 *B.U. L. Rev.* 761.
- KLEIN, G., « Le droit à la preuve. Une étude comparée de la procédure civile allemande et française », (2009) *Les blogs pédagogiques de l'Université Paris Nanterre*, en ligne : <<https://blogs.parisnanterre.fr/content/le-droit-%C3%A0-la-preuve-une-%C3%A9tude-compar%C3%A9e-de-la-proc%C3%A9dure-civile-allemande-et-fran%C3%A7aise-par-ga>>.
- KLEINDIENST, M. R., « On Naming Things », dans Erella HOVERS et Steven L. KUHN (dir.), *Transitions Before the Transition. Evolution and Stability in the Middle Paleolithic and Middle Stone Age*, coll. Interdisciplinary Contributions To Archaeology, Boston, Springer, 2006, p. 13.
- KOTSIANTIS, S., « Supervised Machine Learning. A Review of Classification Techniques », dans I. MAGLOGIANNIS, *Emerging Artificial Intelligence Applications in Computer Engineering*, Amsterdam, IOS Press, 2007.
- KROTOSKI, M. L. et J. PASSWATERS, « Using Log Record Analysis to Show Internet and Computer Activity in Criminal Cases », (2011) 6-59 *United States Attorneys' Bulletin* 1.
- LANG, R. et L. BENESSERE, « Alexa, Siri, Bixby, Google's Assistant, and Cortana Testifying in Court », (2018) 74-1 *Journal of the Missouri Bar* 20.
- LAVALLÉE, É., « La propriété intellectuelle de l'intelligence artificielle », *Lavery* (5 octobre 2017), en ligne : <<https://www.lavery.ca/fr/publications/nos-publications/3037-la-propriete-intellectuelle-de-lintelligence-artificielle.html>>.
- LE, T., S. WANG et D. LEE, « Why X rather than Y? Explaining Neural Model' Predictions by Generating Intervention Counterfactual Samples », *ArXiv* 2019.arXiv:1911.02042, en ligne : <<http://arxiv.org/abs/1911.02042>>.
- LEDERER, F., « The Road to the Virtual Courtroom? A Consideration of Today's and Tomorrow's High Technology Courtrooms », (1999) 50 *S.C. L. Rev.* 800.
- LEGG, M. et C. GOULDING, « Technology. How the Internet of Things Will Affect the Future of Litigation », (2016) 28 *Univ. of NSWLJ*, 88.
- LERNER, J. et J. TIROLE, « Some Simple Economics of Open Source », (2002) 50-2 *J Ind Econ* 197
- LESSIG, L., « The Law of the Horse. What Cyberlaw Might Teach », (1999) 113-2 *Harv. L. Rev.* 501.

- LOGSDON SMITH, A., « Alexa, Who Owns My Pillow Talk? Contracting, Collateralizing, and Monetizing Consumer Privacy Through Voice-Captured Personal Data », (2018) 27-1 *Cath. U. J. L. & Tech* 187.
- LYMAN, P., « Archiving the World Wide Web », dans NATIONAL DIGITAL INFORMATION INFRASTRUCTURE AND PRESERVATION PROGRAM (U.S.) (dir.), *Building a National Strategy for Digital Preservation. Issues in Digital Media Archiving*, coll. « National Digital Information Infrastructure and Preservation Program (U.S.) », Washington, D.C, Council on Library and Information Resources and Library of Congress, 2002, en ligne : <<https://pdfs.semanticscholar.org/2323/b3921357b203e80e031d79990383a0b0b39b.pdf#page=42>>.
- MANDEL, G., « History Lessons for a General Theory of Law and Technology », (2007) 8-2 *Minn JL Sci & Tech* 551.
- MELANCON, T., « Alexa, Pick an Amendment. A Comparison of First and First Amendment Protections of Echo Device Data », (2017) 45 *S.U. L. Rev.* 302.
- MINHAS, F., A. ASIF et A. BEN-HUR, « Ten Ways to Fool the Masses with Machine Learning », *ArXiv* 2019.arXiv:1901.01686, en ligne : <<http://arxiv.org/abs/1901.01686>>.
- MITCHELL, P. et J. TAYLOR, « Case Commentary on *Laushway v. Messervey*, 2014 NSCA 7. Old Evidence Law Dogs, New Technology Tricks », (2015) 12 *Digital Evidence & Elec. Signature L. Rev.* 13.
- MOINI, C., « Protecting Privacy in the Era of Smart Toys. Does Hello Barbie Have a Duty to Report », (2017) 25-2 *Cath. U. J. L. & Tech* 281.
- MORISSETTE, Y.-M., « Gestion d'instance, proportionnalité et preuve civile. État provisoire des questions », (2009) 50-2 *C. de D.* 381.
- MUZYKA, K., « The Outline of Personhood Law Regarding Artificial Intelligences and Emulated Human Entities », (2013) 4-3 *Journal of Artificial General Intelligence* 164.
- NELSON, S. et J. SIMEK, « Are Alexa and Her Friends Safe for Office Use? », (2017) 43-5 *ABA's Law Practice* 26.
- NIU, J., « An Overview of Web Archiving », (2012) 18-4 *D-Lib Magazine*, en ligne : <[https://scholarcommons.usf.edu/si\\_facpub/308](https://scholarcommons.usf.edu/si_facpub/308)>.
- ORLHAC, T. « La brevetabilité des logiciels », (1995) *Robic, agents de brevets et de marques de commerce*, en ligne : < <https://www.robic.ca/wp-content/uploads/2017/05/166-TOR.pdf> >
- OUTERBRIDGE, D. et E. SILLER, « The Admissibility of Electronic Evidence », (2006) *The Advocates' Journal* (Osgoode Professional Development), 31, en ligne : < [http://advocast.ca/assets/pdf/electronic2015/11%20The%20Admissibility%20of%20Electronic%20Evidence%20Outerbridge\\_Siller.pdf](http://advocast.ca/assets/pdf/electronic2015/11%20The%20Admissibility%20of%20Electronic%20Evidence%20Outerbridge_Siller.pdf) >
- PACIOCCO, D. M., « Proof and progress. Coping with the law of evidence in a technological age », (2013) 11-2 *Can. J.L. & Tech.*, en ligne : <<https://ojs.library.dal.ca/CJLT/article/view/6001>>.



- PAGALLO, U., « Vital, Sophia, and Co. The Quest for the Legal Personhood of Robots », (2018) 9-9 *Information* 230.
- PALME, J., « MHTML - Sending HTML in E-mail » (2005) *Jacob Palme*, en ligne : <<https://people.dsv.su.se/~jpalme/ietf/mhtml.html>>.
- PARK, D. H., L. A. HENDRICKS, Z. AKATA, A. ROHRBACH, B. SCHIELE, T. DARRELL et M. ROHRBACH, « Multimodal Explanations. Justifying Decisions and Pointing to the Evidence », *ArXiv* 2018.arXiv:1802.08129, en ligne : <<http://arxiv.org/abs/1802.08129>>.
- PATENAUDE, P., « Science et techniques en preuve. Nécessaire réforme du droit civil, indispensable adaptation du système et des acteurs », dans *Développements récents en droit civil*, 32, coll. « Service de la formation permanente », Barreau du Québec, Cowansville, Éditions Yvon Blais, 1993.
- PICHÉ, C., « La proportionnalité procédurale. Une perspective comparative », (2009) 40 *R.D.U.S.* 552.
- POLLMAN, E., « Reconceiving Corporate Personhood », (2011) 4 *Utah L. Rev.* 1629.
- QUINLAN, J. R., « Induction of Decision Trees », (1986) 1-1 *Mach. Learn* 81.
- RAMBAUD, T., « Introduction générale », dans *Introduction au droit comparé. Les grandes traditions juridiques dans le monde*, coll. « Quadrige », Paris, Presses Universitaires de France, 2014, p. 1, en ligne : <<https://www.cairn.info/introduction-au-droit-compare--9782130624554-p-1.htm>>.
- ROTH, A., « Machine Testimony », (2017) 126-7 *Yale L.J.* 1972.
- SAFAVIAN, S. R. et D. LANDGREBE, « A Survey of Decision Tree Classifier Methodology », (1991) 21-3 *IEEE Transactions on Systems, Man, and Cybernetics* 660.
- SAMEK, W., T. WIEGAND et K.-R. MÜLLER, « Explainable Artificial Intelligence. Understanding, Visualizing and Interpreting Deep Learning Models », *ArXiv* 2017.arXiv:1708.08296, en ligne : <<http://arxiv.org/abs/1708.08296>>.
- SCHERER, M., « Is AI personhood already possible under U.S. LLC laws? », *Law and AI* (14 mai 2017), en ligne : <<http://www.lawandai.com/2017/05/14/is-ai-personhood-already-possible-under-current-u-s-laws-dont-count-on-it-part-one/>>.
- SEBASTIANI, F., « Machine Learning in Automated Text Categorization », (2002) 34-1 *ACM Comput. Surv.* 1.
- SICARI, S., A. RIZZARDI, L. A. GRIECO et A. COEN-PORISINI, « Security, Privacy and Trust in Internet of Things. The Road Ahead », (2015) 76 *Comput. Netw.* 146.
- SURDEN, H. et M.-A. WILLIAMS, « Technological Opacity, Predictability, and Self-Driving Cars », 38 *Cardozo L. Rev.* 62.
- SUSSMAN, M., « Performing the Intelligent Machine. Deception and Enchantment in the Life of the Automaton Chess Player », (1999) 43-3 *The Drama Review* 80.
- THOMSON, L., *Admissibility of Electronic Documentation as Evidence in U. S. Courts*, coll. « Human Rights Electronic Evidence Study », Chicago, Center for Research Libraries,

- 2011, en ligne : <<https://www.crl.edu/sites/files/d6/attachments/pages/Thomson-E-evidence-report.pdf>>.
- TSAI, S.-Y. et S.-I. SOU, « Effects of Data Aggregation in M2M Networks », dans *Internet of Things and M2M Communications*, Algade, River Publishers, 2013, p. 3.
- VAN GERVEN, M. et S. BOHTE, « Artificial Neural Networks as Models of Neural Information Processing », (2017) 11 *Front. Comput. Neurosci.* 114.
- VILLAGGI, J.-P., « Le droit à la vie privée. Un droit en mutation », dans *Mes amis facebook, moi et mon emploi. L'arbitrage de grief à l'ère des réseaux sociaux*, Montréal, Wilson & Lafleur, 2012, en ligne : <<https://edoctrine.caij.qc.ca/wilson-et-lafleur-livres/85/1515756382>>.
- VHRANDEČIĆ, D. et M. KRÖTZSCH, « Wikidata. A Free Collaborative Knowledgebase », (2014) 57-10 *Commun. ACM* 78.
- WU, N. et E. A. SILVA, « Artificial Intelligence Solutions for Urban Land Dynamics. A Review », (2010) 24-3 *J. Plan. Lit* 246.
- XIA, F., L. T. YANG, L. WANG et A. VINEL, « Internet of Things », (2012) 25 *Int. J. Commun. Syst.* 1101.
- XIN YAO, « Evolving Artificial Neural Networks », (1999) 87-9 *Proceedings of the IEEE* 1423.
- ZATZ, C. J., J. MEADOWS, P. MATHIS et L. ARADI, « Recent IoT Device Cases », (2017) *Data Law Insights*, en ligne : <<https://www.crowelldatalaw.com/2017/07/recent-iot-device-cases/>>.

#### *Actes de conférences*

- CHRISTENSEN, H., IÑIGO CASANUEVA, S. CUNNINGHAM, P. GREEN et T. HAIN, « Homeservice. Voice-Enabled Assistive Technology in the Home Using Cloud-Based Automatic Speech Recognition », dans 4Th Workshop on Speech and Language Processing for Assistive Technologies, Grenoble, Association for Computational Linguistics, 2013, p. 29-34, en ligne : <<https://www.aclweb.org/anthology/W13-3906.pdf>>.
- GAUTRAIS, V. et P. GINGRAS, « La preuve des documents technologiques », dans *Congrès annuel du Barreau*, coll. « Services de formation permanente du Barreau du Québec », Cowansville, Éditions Yvon Blais, 2012.
- JADEJA, Y. et K. MODI, « Cloud Computing. Concepts, Architecture and Challenges », dans *2012 International Conference on Computing, Electronics and Electrical Technologies (ICCEET)*, 2012, p. 877, en ligne : <<https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6203873>>.
- JONES, W., H. BRUCE et S. DUMAIS, « Keeping Found Things Found on the Web », dans *Proceedings of the Tenth International Conference on Information and Knowledge Management*, coll. « CIKM '01 », New York, ACM, 2001, p. 119.

- KĚPUSKA, V. et G. BOHOUTA, « Next-generation of virtual personal assistants (Microsoft Cortana, Apple Siri, Amazon Alexa and Google Home) », dans *2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC)*, Las Vegas, Institute of Electrical and Electronics Engineer, 2018, p. 99, en ligne : <<https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8301638&tag=1>>.
- REITER, E., « Natural Language Generation Challenges for Explainable AI », *First Workshop on Interactive Natural Language Technology for Explainable Artificial Intelligence*, International Conference on Natural Language Generation, Tokyo 2019, en ligne : <<http://arxiv.org/abs/1911.08794>>.
- RICHTER, C. et P.-A. VIAU, « Les règles de preuve s'appliquant à la documentation électronique et aux technologies de l'information », dans *Congrès annuel du Barreau du Québec*, Montréal, Barreau du Québec, 2007, p. 43-70.
- SUGIYAMA, E., « General Report on Current Situations and Problems Regarding New Types of Evidences », dans *Challenges for Civil Justice As We Move Beyond Globalization and Technical Change*, Kobe, 2019, p. 484.
- TAN, L. et N. WANG, « Future internet. The Internet of Things », dans *2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE)*, 5, 2010, p. V5-376.

#### *Mémoires et thèses universitaires*

- SAINT-EXUPÉRY, G. DE, *Le document technologique original dans le droit de la preuve au Québec*, coll. « Thèses et mémoires électroniques de l'Université de Montréal », Mémoire de maîtrise, Montréal, Faculté des études supérieures, Université de Montréal, 2012, en ligne : <<https://papyrus.bib.umontreal.ca/xmlui/handle/1866/9043>>.
- SENÉCAL, F., *L'écrit électronique*, coll. « Thèses et mémoires électroniques de l'Université de Montréal », Mémoire de maîtrise, Montréal, Faculté des études supérieures, Montréal, Université de Montréal, 2010, en ligne : <<https://papyrus.bib.umontreal.ca/xmlui/handle/1866/3471>>.

#### *Documents gouvernementaux, normes et rapports institutionnels*

- CESARO, J.-F. (dir.), « Études. La preuve », dans *Rapport annuel 2012. La preuve dans la jurisprudence de la Cour de cassation*, Paris, Direction de l'information légale et administrative, 2013, en ligne : <[https://www.courdecassation.fr/2012admissibilite\\_modes\\_26241.html](https://www.courdecassation.fr/2012admissibilite_modes_26241.html)>.

- CONSEIL DES BARREAUX EUROPÉENS. *Charte des principes essentiels de l'avocat européen et Code de déontologie des avocats européens*, 2018.
- CRTC, *Communications Monitoring Report 2018*, Ottawa, Conseil de la radiodiffusion et des télécommunications canadiennes, 2018, en ligne : <<https://crtc.gc.ca/eng/publications/reports/policymonitoring/2018/cmrl.htm>>.
- EUROPEAN COMMISSION, « Final Report », *EVIDENCE* (European Informatics Data Exchange Framework for Courts and Evidence), European Commission, 2016, en ligne : <<https://cordis.europa.eu/project/rcn/185514/reporting/fr>>.
- MASON, S. et U. RASMUSSEN, *L'utilisation des preuves électroniques dans les procédures civiles et administratives et son impact sur les règles et modes de preuve. Étude comparative et analyse*, CDCJ (2015) 14, Strasbourg, Comité européen de coopération juridique du Conseil de l'Europe, 2016, en ligne : <<https://rm.coe.int/16807007ca>>.
- OFFICE DES NORMES GÉNÉRALES DU CANADA, *Enregistrements électroniques utilisés à titre de preuves documentaires*, CAN/CGSB-72.34-2017, en ligne : <[http://publications.gc.ca/collections/collection\\_2018/ongc-cgsb/P29-072-034-1-2017-fra.pdf](http://publications.gc.ca/collections/collection_2018/ongc-cgsb/P29-072-034-1-2017-fra.pdf)>.
- SECRETARIAT DU CONSEIL DU TRÉSOR DU CANADA, *Norme pour les systèmes de gestion électronique des documents et des dossiers (SGEDD)*, 26 mai 2010, en ligne : <<https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=18910>>.
- TRUDEL, P., D. POULIN et F. ARBAN, *La loi en ligne. La Loi concernant le cadre juridique des technologies de l'information*, Québec, Secrétariat du Conseil du trésor du Québec, 2001, en ligne : <<https://www.tresor.gouv.qc.ca/ressources-informationnelles/cadre-normatif-de-gestion-des-ressources-informationnelles/loi-concernant-le-cadre-juridique-des-technologies-de-linformation/>>.
- UNIFORM LAW CONFERENCE OF CANADA, « Uniform Electronic Evidence Act (1998) », *Uniform Law Conference of Canada* (1999), en ligne : <<https://www.ulcc.ca/en/older-uniform-acts/electronic-evidence/1924-electronic-evidence-act>>.

#### *Articles de journaux et autres billets de blogues*

- BERGER, S., « This naughty parrot was caught ordering items off Amazon's Alexa — here's how much he spent », *CNBC* (21 décembre 2018), en ligne : <<https://www.cnbc.com/2018/12/21/african-grey-parrot-rocco-was-caught-ordering-items-off-amazons-alexa.html>>.
- BOSKER, B., « Siri Rising. The Inside Story of Siri's Origins And Why She Could Overshadow the iPhone », *The Huffington Post* (22 janvier 2013), en ligne : <[https://www.huffingtonpost.com/2013/01/22/siri-do-engine-apple-iphone\\_n\\_2499165.html](https://www.huffingtonpost.com/2013/01/22/siri-do-engine-apple-iphone_n_2499165.html)>.

- BRAGA, M., « What Will the Year Hold for Alexa, Google, Siri and the Smart Speaker Vying for Space in Your Home? », *CBC News* (2019), en ligne : <<https://www.cbc.ca/news/technology/smart-speakers-voice-assistants-2019-google-amazon-apple-1.4966992>>.
- BURT, A., « Leave A.I. Alone », *The New York Times*, sect. Opinion (4 janvier 2018), en ligne : <<https://www.nytimes.com/2018/01/04/opinion/leave-artificial-intelligence.html>>.
- CHUNG, J. et C. MCNAIR, « Global Smart Speaker Users 2019 », *eMarketer* (2019), en ligne : <<https://www.emarketer.com/content/global-smart-speaker-users-2019>>.
- GARBADE, D. M. J., « A Simple Introduction to Natural Language Processing », *Medium* (15 octobre 2018), en ligne : <<https://becominghuman.ai/a-simple-introduction-to-natural-language-processing-ea66a1747b32>>.
- GARTENBERG, C., « Apple Announces Homepod Speaker to Take on Sonos », *The Verge* (5 juin 2017), en ligne : <<https://www.theverge.com/2017/6/5/15732144/apple-homepod-speaker-announced-siri-price-release-date-wwdc-2017>>.
- GREEN, P., « Alexa, Where Have You Been All My Life? », *The New York Times*, sect. Style (20 janvier 2018), en ligne : <<https://www.nytimes.com/2017/07/11/style/alexamazon-echo.html>>.
- GREENWALD, G., « Xkeyscore. NSA Tool Collects “Nearly Everything a User Does on the Internet” », *The Guardian*, sect. US News (31 juillet 2013), en ligne : <<https://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data>>.
- GREENWALD, G. et E. MACASKILL, « NSA Prism Program Ttaps in to User Data of Apple, Google and Others », *The Guardian*, sect. US News (7 juin 2013), en ligne : <<https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data>>.
- HAUSER, C., « In Connecticut Murder Case, a Fitbit Is a Silent Witness », *The New York Times*, sect. New York (22 décembre 2017), en ligne : <<https://www.nytimes.com/2017/04/27/nyregion/in-connecticut-murder-case-a-fitbit-is-a-silent-witness.html>>.
- KUMPARAK, G., « Nest Is Being Rolled into Google’s Hardware Team », *TechCrunch* (2018), en ligne : <<http://social.techcrunch.com/2018/02/07/nest-is-being-rolled-into-googles-hardware-team/>>.
- LI, A., « Google begins replacing full “Voice Match” phone unlock », *9to5Google* (1<sup>er</sup> mars 2019), en ligne : <<https://9to5google.com/2019/02/28/google-replacing-voice-match-unlock/>>.
- LIN, L., « Chinese smart speaker apps saw 822% hike in installations last year », *KrASIA* (6 mai 2019), en ligne : <<https://kr-asia.com/chinese-smart-speaker-apps-saw-822-hike-in-installations-last-year>>.
- LIPTAK, A., « Amazon’s Alexa started ordering people dollhouses after hearing its name on TV », *The Verge* (7 janvier 2017), en ligne :

- <<https://www.theverge.com/2017/1/7/14200210/amazon-alexa-tech-news-anchor-order-dollhouse>>.
- LOHR, S., « Big Data's Impact in the World », *The New York Times*, sect. Opinion (11 février 2012), en ligne : <<https://www.nytimes.com/2012/02/12/sunday-review/big-datas-impact-in-the-world.html>>.
- MCAFEE, A. et E. BRYNJOLFSSON, « Big Data. The Management Revolution », *Harvard Business Review* (1<sup>er</sup> octobre 2012), en ligne : <<https://hbr.org/2012/10/big-data-the-management-revolution>>.
- MUTCHLER, A., « A Timeline of Voice Assistant and Smart Speaker Technology. From 1961 to Today », *Voicebot* (28 mars 2018), en ligne : <<https://voicebot.ai/2018/03/28/timeline-voice-assistant-smart-speaker-technology-1961-today/>>.
- NEWNHAM, D., « The Story Behind Siri », *The Startup* (1<sup>er</sup> novembre 2015), en ligne : <<https://medium.com/swlh/the-story-behind-siri-fbeb109938b0>>.
- PANZARINO, M., « Google Is Buying Connected Device Company Nest For \$3.2B In Cash », *TechCrunch* (13 janvier 2014), en ligne : <<http://social.techcrunch.com/2014/01/13/google-just-bought-connected-device-company-nest-for-3-2b-in-cash/>>.
- RADIO-CANADA, « Apple sort son enceinte HomePod avec un mois de retard », *Radio-Canada.ca* (24 janvier 2018), en ligne : <<https://ici.radio-canada.ca/nouvelle/1079995/apple-homepod-enceinte-haut-parleur-connecte-commande-vocale-lancement-prevente>>.
- RAULINE, N. et S. GODELUCK, « Google fait son nid dans la maison intelligente », *Les Echos* (13 janvier 2014), en ligne : <<https://www.lesechos.fr/2014/01/google-fait-son-nid-dans-la-maison-intelligente-287819>>.
- RBC CAPITAL MARKETS et M. HARRIS, « Imagine 2025 - Themes, Opportunities & “The Law of Accelerating Returns” », *Banque Royale du Canada*, 2018, en ligne : <<https://www.rbccm.com/imagine2025/ai-race.html>>.
- ROUSE, M., « What is Machine-to-Machine (M2M)? », *IoT Agenda* (août 2019), en ligne : <<https://internetofthingsagenda.techtarget.com/definition/machine-to-machine-M2M>>.
- STACKHOUSE, J., « Hey Alexa, What's Next for Voice Tech? Five Insights into a Voice-First World », *RBC Capital Markets* (2019), en ligne : <<https://bit.ly/2QuH1gP>>.
- STANTON, B., « Smart Speaker Market Booms in 2018, Driven by Google, Alibaba and Xiaomi », *Canalys Newsroom*, en ligne : <<https://www.canalys.com/newsroom/smart-speaker-market-booms-in-2018-driven-by-google-alibaba-and-xiaomi>>.
- TURNER, K., « Meet ‘ross,’ the Newly Hired Legal Robot », *The Washington Post*, sect. Innovations (16 mai 2016), en ligne : <[https://www.washingtonpost.com/news/innovations/wp/2016/05/16/meet-ross-the-newly-hired-legal-robot/?noredirect=on&utm\\_term=.dd58a8d9fbf5](https://www.washingtonpost.com/news/innovations/wp/2016/05/16/meet-ross-the-newly-hired-legal-robot/?noredirect=on&utm_term=.dd58a8d9fbf5)>.

VENKAT, « Google removes “Save Page as MHTML” flag from Chrome Canary », *Techdows* (4 juin 2019), en ligne : <<https://techdows.com/2019/06/google-removes-save-page-as-mhtml-flag-from-chrome.html>>.

### *Pages de site Web*

« The Open Source Definition », *Open Source Initiative* (2007), en ligne : <<https://opensource.org/osd>>.

AMAZON.COM, INC., « Privacy Notice », *Amazon.com* (29 août 2017), en ligne : <[https://www.amazon.com/gp/help/customer/display.html?nodeId=468496#GUID-1B2BDAD4-7ACF-4D7A-8608-CBA6EA897FD3\\_SECTION\\_277A1D99140544EE9259ACA749AE3C3D](https://www.amazon.com/gp/help/customer/display.html?nodeId=468496#GUID-1B2BDAD4-7ACF-4D7A-8608-CBA6EA897FD3_SECTION_277A1D99140544EE9259ACA749AE3C3D)>.

———, « Conditions of Use », *Amazon.com* (21 mai 2018), en ligne : <<https://www.amazon.com/gp/help/customer/display.html/?nodeId=508088>>.

———, « Aide. Gérer les paramètres d’achats vocaux », *Amazon.com* (2019), en ligne : <<https://www.amazon.ca/-/fr/gp/help/customer/display.html?nodeId=201952610>>.

———, « Alexa Terms of Use », *Amazon.com* (0614 2019), en ligne : <<https://www.amazon.com/gp/help/customer/display.html?nodeId=201809740>>.

———, « Help. Using Household Profiles on Alexa Devices », *Amazon.com* (2019), en ligne : <<https://www.amazon.com/gp/help/customer/display.html?nodeId=201628040>>.

APPLE, « Présentation de la sécurité iCloud », *Apple Support* (3 juillet 2019), en ligne : <<https://support.apple.com/fr-ca/HT202303>>.

CHENGDU MEROSS TECHNOLOGY CO., LTD., « Privacy Policy », *Meross.com* (2017), en ligne : <<https://us-iot.meross.com/public/smart/policy.html>>.

DATAFLAIR, « Python Modules vs Packages. Differences Between Python Modules and Packages », *DataFlair* (27 février 2018), en ligne : <<https://data-flair.training/blogs/python-modules-vs-packages/>>.

———, « Python Libraries. Python Standard Library & List of Important Libraries », *DataFlair* (28 février 2018), en ligne : <<https://data-flair.training/blogs/python-libraries/>>.

GOOGLE, « Google Terms of Service », *Google Privacy & Terms* (25 octobre 2017), en ligne : <<https://policies.google.com/terms?hl=en-US>>.

———, « Gérer l’historique google des activités vocales et audio », *Google Assistant Help* (2019), en ligne : <<https://support.google.com/websearch/answer/6030020?hl=en>>.

———, « Read Pages Later and Offline », *Google Chrome Help* (2019), en ligne : <<https://support.google.com/chrome/answer/7343019?co=GENIE.Platform%3DDesktop&hl=en&oco=0>>.

———, « Set up Multiple Users for Your Speaker or Smart Display », *Google Assistant Help* (2019), en ligne : <<https://support.google.com/assistant/answer/9071681?hl=en-GB>>.

———, « Supprimer vos activités », *Google Assistant Help* (2019), en ligne : <<https://support.google.com/websearch/answer/465?hl=fr>>.  
SIGNIFY HOLDING, « Configuration de Hue à Google », *Philips Hue* (2018), en ligne : <<https://www2.meethue.com/fr-ca/friends-of-hue/google-home-products>>.

#### *Documents audiovisuels*

AMER, K. et J. NOUJAIM. *The Great Hack*, Documentaire, Netflix, 24 juillet 2019.  
TRUDEL, P., *Propriété ou liberté, La nécessité de faire revivre un débat initié il y a 30 ans*, Montréal, Centre de recherche en droit public, 2018, en ligne : <<https://www.youtube.com/watch?v=l70rPHvWdMo>>.  
VOWLES, E. et J. STORY CARTER. *Your Smart Device Could Be Used Against You in Court*, The Law Report, *ABC News*, émission diffusée le 9 mars 2018, en ligne : <<https://www.abc.net.au/news/2018-03-09/your-google-home-or-fit-bit-could-be-used-against-you-in-court/9510368>>

#### *Dictionnaires, ouvrages de référence et autres documents*

AMAZON.COM, INC., *Memorandum of Law in Support of Amazon's Motion to Quash Search Warrant*, 2017.  
*Le petit Larousse illustré*, en ligne : <<https://www.larousse.fr>>.  
OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE, *Grand dictionnaire terminologique*, Québec, Publications du Québec, en ligne : <<http://www.granddictionnaire.com/>>  
REID, H., *Dictionnaire de droit québécois et canadien*, Montréal, Wilson & Lafleur, 2015.  
ROBERT, P., *Le Petit Robert*, Paris, Éditions Le Robert, 2015.