Université de Montréal

La protection des renseignements personnels dans l'exploitation des assistants vocaux

Par

Jad Rouhana

Faculté de Droit

Mémoire présenté en vue de l'obtention du grade de la maîtrise (LL.M.)

en Droit des technologies de l'information

Septembre 2020

Résumé

Les assistants vocaux ont mis au jour une nouvelle manière pour l'humain d'interagir avec les technologies en n'utilisant que la voix. Une technologie qui est également évolutive et interactive grâce à l'intelligence artificielle. Nous verrons que les caractéristiques techniques et logicielles les composant concourent à une collecte massive de renseignements personnels par les entreprises.

L'imprécision des politiques de confidentialité, l'absence d'information sur le mode de fonctionnement, l'imperfection du traitement automatique du langage naturel (ci-après le « TALN ») caractérisée par les faux positifs et les difficultés inhérentes à l'exercice par l'individu de certains de ses droits tendent à limiter l'effectivité des différentes lois existantes à l'assistant vocal. En outre, la possibilité pour plusieurs personnes d'interagir avec l'objet ainsi que son absence d'autonomie tendent à compliquer l'application des régimes de responsabilité civile, dont celui résultant du fait des biens.

Cette apparition récente de l'assistant vocal n'a pour l'heure pas permis au juge de se prononcer pour faire évoluer les jurisprudences relatives au droit à la vie privée, à la protection des renseignements personnels et à la responsabilité civile. Celles déjà existantes ne semblent plus être adaptées à ce contexte technologique autour de l'assistant vocal, et plus généralement autour de la voix. C'est ainsi que le test de *Oakes*, permettant de déterminer le caractère raisonnable d'une violation des droits et libertés énoncés dans la Charte canadienne, repris pour être appliqué à la LPRPDE, apparaît comme étant inadapté à ce nouveau contexte technologique. Enfin, le manque de pouvoirs conférés aux autorités compétentes représente un obstacle majeur dans le suivi de l'application des règles de droit.

Mots-clés : intelligence artificielle, renseignement personnel, responsabilité civile, vie privée, assistant vocal, algorithme, traitement automatique du langage naturel.

Abstract

Voice assistants bring a new way for humans to interact with technology by only using their voice. Scalable and interactive technology thanks to artificial intelligence. We will see that the technical and software characteristics of voice assistants contribute to a massive collection of personal information by companies.

The imprecision of confidentiality policies, the absence of information on the mode of operation, the imperfection of the Natural Language Processing characterized by false positives and the difficulties inherent in the exercise by individuals of some of their rights contribute to the mismatch between voice assistants and various existing laws. In addition, the possibility for people to interact with the object as well as its lack of autonomy tend to complicate the application of civil liability regimes, including that resulting from the act of thing.

This recent appearance of voice assistants has so far not giving judges the possibility to rule on the right to privacy, protection of personal information and civil liability. Current case law doesn't seem to be well adapted to the technological context around the voice assistant, and more generally the voice. The Oakes test, which was design to determining the reasonableness of a violation of the rights and freedoms set out in the Canadian Charter, appears to be unsuited to this new context. We will see that the lack of powers conferred on the competent authorities represents a major obstacle in monitoring the application of the rule of law.

Keywords : artificial intelligence, personal information, civil liability, privacy, voice assistant, algorithm, natural language processing.

Table des matières

Liste des annexes

Liste des extraits

Liste des figures

Liste des sigles et abréviations

AAPI	Association sur l'accès et la protection de l'information
ARP	Agent de renseignements personnels
Art.	Article
C.c.Q.	Code civil du Québec
CAI	Commission d'accès à l'information
CEPEJ	Commission européenne pour l'efficacité de la justice
CJUE	Cour de justice de l'Union européenne
CNIL	Commission nationale de l'informatique et des libertés
Cons. const.	Conseil constitutionnel
CPVP	Commissariat à la protection de la vie privée
CRIDS	Centre de recherche Information, Droit et Société
CSA	Conseil supérieur de l'audiovisuel
DARPA	Defense Advanced Research Projects Agency
DPO	Data protection officer
DUDH	Déclaration universelles des droits de l'Homme

HADOPI	Haute autorité pour la diffusion des œuvres et la protection des droits sur Internet
IdO	Internet des Objets
IEE	Institute of Electrical and Electronics Engineers
ISJLP	I/S: A Journal of Law and Policy for the Information Society
LCCJTI	Loi concernant le cadre juridique des technologies de l'information
LPRPSP	Loi sur la protection des renseignements personnels dans le secteur privé
LPRPDE	Loi sur la protection des renseignements personnels et les documents électroniques
Mass. MIT Press	Massachusetts Institute of Technology Press
Minn. L. Rev.	Minnesota Law Review
OCDE	Organisation de coopération et de développement économiques
OQLF	Office québécois de la langue française
RFID	Radio Frequency Identification
RGPD	Règlement général sur la protection des données

R. du B.	Revue du Barreau du Québec
R. du B. can.	Revue du Barreau du Canada
R.J.T.	Revue juridique Thémis
RJTUM	Revue juridique Thémis de l'Université de Montréal
TALN	Traitement automatique du langage naturel

“A child born today will grow up with no conception of privacy at all”

(Edward Snowden, Channel 4, Royaume-Uni, le 26 décembre 2013)

Remerciements

La rédaction de ce mémoire, dans le contexte de crise que nous traversons, n'a pu se faire sans le soutien indéfectible de certaines personnes que je tiens à remercier.

Je remercie en premier lieu mes parents qui, malgré la distance, ont toujours su trouver les mots pour me motiver et à ne pas abandonner alors même qu'ils ont dû subir mes crises après mes journées de travail dans un service essentiel.

Je remercie également ma famille au Québec qui a été d'une aide précieuse de mon arrivé dans la province jusqu'aujourd'hui.

Enfin, je remercie très chaleureusement le professeur Vermeys qui a accepté d'encadrer mon travail de recherche. Sa disponibilité et ses conseils prodigués lors de la rédaction ont grandement contribuer à façonner ce travail de recherche.

Introduction

La constante évolution des technologies change pour le meilleur ou pour le pire notre quotidien. L'arrivée des téléphones nous a permis d'effacer la distance, du moins virtuellement, pouvant nous séparer d'une personne. L'introduction de logiciels les rendant plus intelligents, en offrant la possibilité aux utilisateurs d'avoir un véritable ordinateur de poche, a conduit à diversifier leurs usages. Les fabricants ont toujours su faire preuve d'ingéniosité pour attirer les individus vers une utilisation de plus en plus importante de ces appareils en mettant en avant leur capacité d'évolution (par le biais de mises à jour, applications nouvelles etc.). L'assistant vocal n'est qu'un exemple à la fois de cet exploit technologique mais également de l'impact sociojuridique qu'il entraîne. Un exemple qui sera toutefois l'objet principal de notre mémoire. Avant de pouvoir étudier les relations juridiques entre l'assistant vocal et le cadre juridique actuel en matière de vie privée, de protection des renseignements personnels et de responsabilité civile, intéressons-nous tout d'abord à son identification sémantique.

Le grand public a eu accès à l'assistant vocal en 2011 avec l'iPhone 4S[1]. Au regard de l'engouement suscité chez les individus, d'autres entreprises ont décidé de se lancer dans la commercialisation d'objets accompagnés d'un assistant vocal, dont les enceintes connectées[2]. La présence aussi importante de l'assistant vocal a induit une certaine banalisation de son appellation pour évoquer en grande partie ces enceintes connectées. Celles-ci ont pour fonction principale l'exécution de diverses tâches à la demande de l'utilisateur. Cependant, le terme même de « assistant vocal » renvoie en réalité à une forme de logiciel intégrée dans certains objets connectés et terminaux mobiles. Un téléphone intelligent aura par exemple un assistant vocal intégré offrant à son propriétaire la possibilité de réaliser certaines actions. Pour être en phase avec la réalité, sans pour autant concourir à cette banalisation, et à moins d'une précision contraire, nous parlerons tout au long de ce mémoire de l'assistant vocal en tant qu'enceinte connectée. Le recours à une telle

[1] FONTAINE, P., et LEPESQUEUR, B., « Découvrez l'iPhone 4S et son étonnant assistant vocal Siri », 01net.com, 12 décembre 2011, en ligne : < https://www.01net.com/actualites/decouvrez-l-and-039-iphone-4s-et-son-etonnant-assistant-vocal-siri-video-543854.html >.

[2] PESTANES, P. et GAUTIER, B., « Essor des assistants vocaux : Nouveau gadget pour votre salon ou fenêtre d'opportunité pour rebattre les cartes de l'économie du web ? », wavestone.com, 2017, en ligne : <https://www.wavestone.com/app/uploads/2017/09/Assistants-vocaux-04.pdf >, p.3.

notion pour qualifier l'enceinte connectée nous paraît comme étant la plus adéquate étant donné sa fonction primaire mais également en phase avec les questions concernant le droit à la vie privée et la protection des renseignements personnels.

Selon le dictionnaire Larousse, le verbe « assister » se définit comme étant le fait de « [s]econder, aider quelqu'un dans son activité »[3]. Dans le domaine de l'informatique, la définition est quasiment la même en ce qu'elle concerne davantage l'aide d'un logiciel dans l'exécution de certaines opérations à la demande de l'homme[4]. Pour certains, le rôle joué par l'assistant vocal le définirait comme un véritable majordome numérique[5].

L'assistant vocal, du fait de son arrivée récente a donné un souffle nouveau au secteur de l'Internet des Objets (ci-après « IdO »). Jusqu'en 2011, l'IdO s'articulait autour des objets du quotidien connectés à Internet par le biais d'une puce RFID[6]. L'assistant vocal est donc venu bouleverser cette tendance, notamment en intégrant une prouesse technologique que représente le traitement automatique du langage naturel (ci-après « TALN »)[7] associée aux nouvelles techniques de transmission des données à distance, particulièrement en délocalisant virtuellement leur stockage.

Cette avancée majeure dans l'interaction homme-machine mérite que l'on accorde un court développement sur les différentes étapes de son évolution qui nous apparaissent comme étant les plus importantes, tant par leur apport, que par l'époque à laquelle elles ont été créées. Le lecteur trouvera une annexe 1 de ce mémoire une chronologie plus complète de cette évolution.

---

[3]LAROUSSE, « Définitions : assister », larousse.fr, en ligne : <https://www.larousse.fr/dictionnaires/francais/assister/5852?q=assister#5829 >.

[4] OFFICE QUEBECOIS DE LA LANGUE FRANCAISE, « Grand dictionnaire terminologique : assistant », domaine informatique, gdt.oqlf.gouv.qc.ca, 2007, en ligne : < http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=26538413 >.

[5] VERSET, J-C., « Les enceintes intelligentes seront-elles nos futurs majordomes numériques ? », rtbf.be, 26 juillet 2018, en ligne : < https://www.rtbf.be/info/medias/detail_les-enceintes-intelligentes-seront-elles-nos-futurs-majordomes-numeriques?id=9981502 >.

[6] Cette définition a été rapportée pour la premier fois par Kevin ASHTON pour désigner les IdO, GEOFFRAY, « [Infographie] Histoire de l'Internet des objets au fil du temps », meilleure-innovation.com, 11 août 2014, en ligne : < https://www.meilleure-innovation.com/infographie-internet-objets/ >.

[7] Nous invitons le lecteur à consulter les figures 5 et 6 en pages 62 et 64 portant sur les différentes briques technologiques composant le TALN et le schéma illustrant le fonctionnement d'une commande vocale. Aussi, nous souhaitons apporter une précision afin d'éviter toute confusion dans la lecture de la figure 5, la brique Natural Language Processing (ci-après « NLP ») n'est autre que la traduction anglaise du TALN.

La première machine à avoir été dotée du TALN est la machine Audrey de Bell Laboratories en 1952. Elle était alors capable de reconnaître seulement les nombres[8]. Par la suite, la Shoebox d'IBM, (sa ressemblance avec une boîte à chaussure lui a valu ce nom) est apparue dans les années 60 et a constitué une avancée majeure à son époque. Elle a été considérée comme « a forerunner of today's voice recognition systems »[9]. La Shoebox était capable de reconnaître jusqu'à 16 mots, les chiffres de 0 à 9 et réaliser un calcul pouvant inclure le signe négatif[10]. À l'issue de cette découverte, d'autres technologies intégrant le TALN ont vu le jour. C'est ainsi qu'en 1972 l'université Carnegie Mellon en Pennsylvanie, avec l'appui de la DARPA[11], parvient à mettre au point un logiciel, Harpy, pouvant reconnaître près d'un millier de mots[12].

La généralisation du TALN à travers les objets et appareils connectés ne surviendra que très récemment. Deux évènements y ont concouru. Le premier étant celui de la machine Watson d'IBM. La renommée de ce robot découle de sa participation au jeu télévisé *Jeopardy!* face à deux champions. Sa participation et sa victoire ont permis de montrer au grand public la capacité de la machine dotée de l'intelligence artificielle à adopter un raisonnement quasi-similaire à celui d'un humain avant de fournir la réponse appropriée. Comme signe de nécessité de perfection du TALN, Watson a dû au préalable de sa participation au jeu bénéficier de l'apprentissage supervisé pour utiliser sa base de données afin d'être en mesure de participer au jeu. À la différence des participants qui recevait la question à l'oral, Watson la recevait à l'écrit et : « [w]hen a question is put to Watson, more than 100 algorithms analyze the question in different ways, and find many different plausible answers–all at the same time. »[13] (notre soulignement). Une fois la réponse la

[8] PINOLA, M., « Speech Recognition Through the Decades: How we Ended Up With Siri », pcworld.com, 2 November 2011, en ligne : <https://www.pcworld.com/article/243060/speech_recognition_through_the_decades_how_we_ended_up_with_siri.html >.
[9] IBM, « Shoebox », archives, ibm.com, en ligne : <https://www.ibm.com/ibm/history/exhibits/specialprod1/specialprod1_7.html >.
[10] Ibid.
[11] Agence rattachée au département de la défense des États-Unis et chargée de développer des projets à des fins militaires, DEFENSE ADVANCED RESEARCH PROJECTS AGENCY, « about DARPA », darpa.mil, : <https://www.darpa.mil/about-us/about-darpa >.
[12] PINOLA, M., « Speech Recognition Through the Decades: How we Ended Up With Siri », pcworld.com, 2 November 2011, en ligne : <https://www.pcworld.com/article/243060/speech_recognition_through_the_decades_how_we_ended_up_with_siri.html >.
[13] Ibid.

plus appropriée choisie, le robot Watson la transmettait par le biais de sa voix de synthèse[14]. Cependant, bien que son usage ne soit pas accessible au public, son apparition a permis de montrer l'utilité des progrès réalisés dans les domaines du TALN, en mettant en avant une de ses parties celle de la voix de synthèse, et de l'intelligence artificielle. Deux éléments qui se retrouvent au sein de l'assistant vocal.

C'est lors de l'introduction au grand public de l'iPhone 4S[15] d'Apple que l'assistant vocal se démocratise véritablement. En effet, alors qu'il a été proposé comme application indépendante sur la plateforme App Store[16], Siri est devenu à compter de cette nouvelle gamme de téléphone intelligent l'assistant vocal d'office[17] dans tous les produits de la marque à la pomme. Cette technologie sera par la suite reprise par d'autres constructeurs.

À l'origine de Siri nous retrouvons la DARPA appuyée par le centre de recherche Stanford Research Institute[18], qui travaillait sur un programme dont l'objectif était de mettre en place un assistant virtuel afin d'aider les officiers de l'armée américaine dans leur prise de décision[19]. Si Apple a réussi à imposer l'assistant vocal dans ses téléphones, c'est grâce aux évolutions technologiques et aux mises à jour. Au fil du temps, Siri est passé d'un simple moteur de recherche à un « moteur actif » capable d'exécuter certaines tâches comme éteindre ou allumer la lumière dans le cadre de l'écosystème d'Apple, HomeKit[20]. À cet effet, Apple promeut ce kit en évoquant le contrôle de l'utilisateur sur Siri par sa voix comme étant « l'interrupteur »[21].

Aussi, la personnification de l'assistant vocal en lui attribuant un nom et sa simplicité dans son utilisation dans un cadre privé, généralement le domicile, ont concouru à le rendre davantage

[14]IBM, « A computer called Watson », ibm.com, en ligne : <https://www.ibm.com/ibm/history/ibm100/us/en/icons/watson/ >.
[15] APPLE, « Apple Launches iPhone 4S, iOS 5 & iCloud », apple.com, Apple Newsroom, 4 October 2011, en ligne : <https://www.apple.com/newsroom/2011/10/04Apple-Launches-iPhone-4S-iOS-5-iCloud/ >.
[16] KUMPARAK, G., « The original Siri app gets pulled from the App store, servers to be killed », techcrunch.com, 4 October 2011, en ligne : < https://techcrunch.com/2011/10/04/the-original-siri-app-gets-pulled-from-the-app-store-servers-killed/ >.
[17] SANT SANTOLARIA, N., *« Dis Siri » Enquête sur le génie à l'intérieur du smartphone,* Anamosa, 2016, p.49.
[18] Devenu par la suite SRI Ventures avant d'être rachetée par Apple en 2010, ibid, p.39.
[19] Ibid, pp.31-32.
[20] Ibid, pp.64-65.
[21] APPLE, « Contrôler votre domicile avec Siri », support.apple.com, en ligne : < https://support.apple.com/fr-ca/HT208280 >.

attrayant car ne nécessitant aucune compétence technique de la part de son utilisateur, si ce n'est que de parler.

Pour que l'assistant vocal puisse répondre à la requête introduite par l'utilisateur et interagir avec lui, il doit également être en mesure de comprendre ce qu'il lui est dit avant de fournir un résultat pertinent. Pour y parvenir, l'assistant vocal a recours à l'intelligence artificielle lui offrant cette capacité de compréhension et dans le même temps la capacité d'évoluer en apprenant de ses interactions avec l'utilisateur tout en restant sous la supervision de son entraîneur.

La longue attente pour obtenir l'intégration du TALN dans les objets connectés s'explique par l'association entre son fonctionnement et les récents développements en intelligence artificielle, rendant ainsi sa maîtrise plus complexe. Cette intégration mérite d'être étudiée afin de mieux saisir le fonctionnement plus général de l'assistant vocal que peu de personnes connaissent.

Si effectivement il a le mérite de porter assistance à l'utilisateur dans des tâches assez simples en l'affranchissant de toute action physique, nous verrons que son utilisation au quotidien n'est pas sans conséquence sur le respect de la vie privée et de la protection des renseignements personnels de l'habitant[22]. L'assistant vocal collecte des données en masse, dont certaines ne font pas l'objet d'un chiffrement[23], sur les habitudes des personnes se trouvant à l'intérieur tout en alimentant la base de données de son fabricant.

Cependant, la commercialisation de l'assistant vocal, son intégration dans tous les objets possibles voire de son interconnexion avec eux sont de nature à remettre en cause la notion de vie privée. Cette notion est très ancienne et remonterait jusqu'à Aristote distinguant alors la sphère publique englobant l'activité politique et la cité, de la sphère privée concernant l'activité domestique et la vie familiale[24].

---

[22] Nous aborderons plus en détails dans la partie II les conséquences de l'utilisation de l'assistant vocal sur les dispositions encadrant la protection des renseignements personnels et le droit à la vie privée.

[23] CHATELLIER, R., « L'espion qui me logeait : assistants vocaux et objets connectés dans la maison », linc.cnil.fr, 10 avril 2018, en ligne : < https://linc.cnil.fr/fr/lespion-qui-me-logeait-assistants-vocaux-et-objets-connectes-dans-la-maison >.

[24] ROCHELANDET, F., « I. Définition : vie privée et données personnelles », dans *Économie des données personnelles et de la vie privée,* cairn.info, 2010, en ligne : < https://www.cairn.info/Economie-des-donnees-personnelles-et-de-la-vie-pri--9782707157652-page-6.htm >, p.6.

La vie privée prendrait réellement naissance dans les sociétés modernes avec l'article *The Right to privacy* de Warren et Brandeis[25]. Nous verrons ultérieurement que ce droit à la vie privée ne bénéficie à ce jour d'aucune définition universellement acceptée. À cet effet, Warren et Brandeis ont affirmé que :

> « That the individual shall have full protection in person and in property is a principal as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection. Political, social and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meets the demands of society »[26] (notre soulignement).

Aujourd'hui la vie privée est évoquée à divers niveaux dans la hiérarchie des normes étatiques. Celle-ci est tout d'abord énoncée dans la Constitution d'un État, implicitement ou non. C'est ainsi qu'en France, le Conseil constitutionnel a été amené à consacrer le droit à la vie privée[27] comme étant prévu implicitement au sein de l'article 2 de la Déclaration des Droits de l'Homme et du Citoyen de 1789 énonçant la liberté personnelle[28] car la Constitution ne prévoyant pas en elle-même un tel droit[29]. Au Canada, ce droit est également implicitement prévu par la Charte *canadienne des droits et libertés* sous les articles 7 et 8[30] alors qu'il apparaît explicitement au sein

[25] WARREN, S., D., et BRANDEIS, L., D., *The right to privacy,* 15 December 1890, Havard Law Review, Vol. 4, No. 5, pp 193-220, en ligne : < https://www.jstor.org/stable/1321160?seq=1#metadata_info_tab_contents > ; ROCHELANDET, F., « I. Définition : vie privée et données personnelles », dans *Économie des données personnelles et de la vie privée,* cairn.info, 2010, en ligne : < https://www.cairn.info/Economie-des-donnees-personnelles-et-de-la-vie-pri--9782707157652-page-6.htm >, p.7.

[26] WARREN, S., D., et BRANDEIS, L., D., *The right to privacy,* 15 December 1890, Havard Law Review, Vol. 4, No. 5, pp 193-220, en ligne : < https://www.jstor.org/stable/1321160?seq=1#metadata_info_tab_contents >, p.193.

[27] Cons. const. n°99-416 DC du 23 juillet 1999, *Loi portant création d'une couverture maladie universelle*.

[28] Ce texte, bien qu'il ne constitue pas la Constitution française, fait partie du bloc de constitutionnalité en vertu de la décision du Conseil constitutionnel : Cons. const. n° 71-44 DC du 16 juillet 1971, *Liberté d'association.*

[29] MAZEAUD, V., « La constitutionnalisation du droit au respect de la vie privée », dans *Nouveaux cahiers du Conseil constitutionnel n°48 (dossier : Vie privée)*, juin 2015, pp.7 à 20.

[30] *Charte canadienne des droits et libertés,* Annexe B de la loi de 1982 sur le Canada (R-U), 1982, c 11 ; PELLETIER, B., « Droit constitutionnel : la protection de la vie privée au Canada », revue juridique Thémis, 2001 35 R.J.T., pp. 485-522 ; THIBEAULT, A., *La surveillance électronique et métadonnées. Vers une nouvelle conception constitutionnelle du droit à la vie privée au Canada ?,* Mémoire de maîtrise, Université de Montréal, Mars 2015, en ligne : <https://papyrus.bib.umontreal.ca/xmlui/bitstream/handle/1866/12496/Thibeault_Alexandre_2015_memoire.pdf?sequence=2&isAllowed=y >.

de la *Charte des droits et libertés de la personne*[31]. Nous reviendrons plus en détail sur cette notion et son évolution au regard des technologies.

D'ailleurs s'agissant des lois en matière de protection des renseignements personnels, nous estimons qu'il soit nécessaire dès notre introduction d'opérer une distinction entre les secteurs privés et publics pour éviter toute confusion du lecteur tout au long de ce mémoire. Les lois du secteur public, tant au fédéral, qu'au provincial ne trouvent application qu'aux institutions fédérales et provinciales. C'est le cas de la *Loi sur la protection des renseignements personnels*[32] applicable au fédéral et conférant certains droits aux individus à l'égard de celles-ci[33]. Cette loi a son penchant au Québec avec la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*[34] (ci-après la « Loi sur l'accès »). S'agissant du secteur privé, il se trouve être régi au niveau fédéral par la *Loi sur la protection des renseignements personnels et les documents électroniques*[35] (ci-après la « LPRPDE ») et au Québec par la *Loi sur la protection des renseignements personnels dans le secteur privé*[36](ci-après la « LPRPSP »). En raison de l'apport de la loi québécoise pour le secteur privé, dont le contenu est équivalent à la loi fédérale, cette dernière se trouve être écartée pour toutes les activités se déroulant au Québec[37].

Au-delà même de la vie privée et de la protection des renseignements personnels, l'utilisation quotidienne de l'assistant vocal soulève l'épineuse question de la responsabilité civile prévue par les différentes dispositions du Code civil du Québec. En effet, la reconnaissance de la responsabilité d'une personne pour le fait qu'elle a commis ou par un bien qu'elle en avait la garde se trouve être inadapté à cette nouvelle situation. L'accessibilité d'un tel objet par plusieurs personnes, même par des enfants en bas âge[38], associée à l'absence de sécurité robuste, principalement dû au fait de son

---

[31] Art. 5 de la *Charte des droits et libertés de la personne,* RLRQ c C-12.
[32] *Loi sur la protection des renseignements personnels*, L.R.C. (1985), ch. P-21.
[33] Art. 2 et articles 12 et s., *Loi sur la protection des renseignements personnels*.
[34] *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, RLRQ c A-2.1.
[35] *Loi sur la protection des renseignements personnels et les documents électroniques*, LC 2000, c 5.
[36] *Loi sur la protection des renseignements personnels dans le secteur privé,* RLRQ c P-39.1.
[37] COMMISSARIAT A LA PROTECTION DE LA VIE PRIVEE, *Lois provinciales qui peuvent s'appliquer au lieu de la LPRPDE,* priv.gc.ca, mai 2020, en ligne : < https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/lois-sur-la-protection-des-renseignements-personnels-au-canada/la-loi-sur-la-protection-des-renseignements-personnels-et-les-documents-electroniques-lprpde/r_o_p/prov-lprpde/ >.
[38] Voir LACHANCE, F., *« O.K. Google, assiste-moi » Les parcours des utilisateurs et des familles qui domestiquent le Google Home,* papyrus.bib.umontreal.ca, Mémoire de maîtrise, Avril 2019, en ligne :

utilisation strictement privée, font obstacle à l'application des différents régimes de responsabilité. L'obstacle résidant essentiellement dans la complexité, voire l'impossibilité, à identifier le gardien au moment de l'utilisation et l'absence de toute autonomie de la part de l'assistant vocal primordial pour tenter de se prévaloir d'un régime de responsabilité. D'un point de vue de la sécurité de l'information, l'assistant vocal ne comporte pas de mesures de sécurité efficace. Sa récente émergence n'a pour l'heure pas permis de dégager des procédés solides pour garantir une sécurité optimale. Une situation qui place l'assistant vocal dans une position de grande vulnérabilité d'autant plus que sa connexion à un réseau domiciliaire privé ne lui offre pas toute la sécurité nécessaire. Pour pousser les entreprises à employer des moyens appropriés, le législateur fédéral a opéré une modification de la *Loi sur la protection des renseignements personnels et les documents électroniques* afin d'instaurer une obligation de notification des incidents de sécurité. Nous verrons qu'une telle obligation comporte un effet préventif sur la notification en contraignant les entreprises à adopter les mesures de sécurité nécessaires sous peine de devoir s'engager dans une procédure d'enquête plus ou moins contraignante selon les législations.

Au travers de ce mémoire nous étudions les rapports entre l'assistant vocal et le cadre juridique canadien et québécois de la protection des renseignements personnels, allant des lois sectorielles au Code civil du Québec en passant par les dispositions constitutionnelles. Nous verrons qu'en raison de l'évolution fulgurante de l'assistant vocal, les lois en matière de protection de renseignements personnels se retrouvent être dépassées. Pour comprendre un tel phénomène, nous présenterons en première partie l'aspect technique de l'assistant vocal, notamment au regard de ses caractéristiques tant matériels (microphones, haut-parleurs etc.) que logiciels (algorithme et TALN). Nous aborderons par la suite les différentes notions clés régissant le droit à la vie privée et la protection des renseignements personnels tant au niveau constitutionnel que législatif. Ces éléments rattachés à l'utilisation de la voix ne sont pas sans conséquences pour l'utilisateur et ses renseignements personnels.

Les conséquences juridiques découlant des limites techniques du TALN sur la protection légale et constitutionnelle de la vie privée et des renseignements personnels seront donc traitées dans la

<https://papyrus.bib.umontreal.ca/xmlui/bitstream/handle/1866/22464/Lachance_Francois_2019_memoire.pdf?sequence=2&isAllowed=y >

seconde partie. Dans la première sous-partie nous mettrons en lumière l'inadéquation entre les dispositions constitutionnelles du droit à la vie privée, les principes fondamentaux de la protection des renseignements personnels et l'utilisation de l'assistant vocal. Nous terminerons cette seconde partie par évoquer les différents régimes de responsabilité civile consacrés par le Code civil du Québec, qui ne semblent plus être aussi effectifs que l'on ne pense. Nous les évoquerons dans le cadre de la seconde sous-partie avec l'obligation de notification des incidents de sécurité et ses effets préventifs.

Nous portons d'ores et déjà à la connaissance du lecteur que le manque de précision des lois canadiennes et québécoises eu égard à leur adoption dans un contexte dans lequel l'assistant vocal n'existait, ou n'était pas encore commercialisable, et l'absence de jurisprudences disponibles sur ce sujet, nous obligent à nous référer à des textes juridiques plus récents comme le *Règlement général sur la protection des données* de l'Union européenne[39] (ci-après « RGPD »). Nous précisons également qu'au cours de la rédaction de ce mémoire, le projet de loi n°64 portant *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*[40] a été présenté le 12 juin 2020 à l'Assemblée nationale du Québec, n'ayant pas reçu la sanction royale, nous nous appuierons sur la loi toujours en vigueur dans le secteur privé. Enfin, nous informons le lecteur que la Commission européenne a annoncé le 17 juillet avoir lancé une enquête sectorielle sur les fabricants d'assistants vocaux et leur pratique anticoncurrentielles, particulièrement dans la collecte et l'utilisation des renseignements personnels[41] dont le présent mémoire en souligne l'inadaptation.

---

[39] *Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE*, 27 avril 2016, Journal Officiel n° L 119/1 du 4 mai 2016.

[40] ASSEMBLEE NATIONALE DU QUEBEC, *Projet de loi n°64 : Loi modernisant des dispositions législatives en matière de protection des renseignements personnels,* présenté par Mme Sonia LeBel, Ministre responsable des Institutions démocratiques, de la Réforme électorale et de l'Accès à l'information, première session, 42e législature, 2020. Ce projet de loi vise à modifier la LPRPSP et la loi sur l'accès pour ce qui est du secteur public.

[41] COMMISSION EUROPEENNE, *Pratique anticoncurrentielle : La Commission ouvre une enquête sectorielle sur l'internet des objets pour les consommateurs,* communiqué de presse, 16 juillet 2020, Bruxelles, en ligne : <https://ec.europa.eu/commission/presscorner/detail/fr/ip_20_1326 >.

I. Le fonctionnement de l'assistant vocal et l'identification des principes clés de la protection des renseignements personnels

Petit gadget pour certains[42], véritable assistant pour d'autres, les fabricants d'assistants vocaux ont su profiter de l'essor technologique et des progrès réalisés dans le domaine de la reconnaissance vocale pour les intégrer dans différents objets technologiques. Ses caractéristiques techniques favorisent à la fois son intégration dans un environnement plus connecté et sa faculté d'apprentissage par le biais de l'intelligence artificielle le rendant plus attractif et utile à l'utilisateur (A). Son interaction vocale avec l'utilisateur renforce davantage son intérêt, notamment lorsqu'il s'agit d'entamer une recherche ou de commander une action. Pour tenter de prévenir toute dérive dans l'utilisation de l'assistant vocal, un cadre juridique propre à la protection des renseignements personnels a été bâti (B).

A. Le mode de fonctionnement de l'assistant vocal

La recherche par le biais de l'assistant vocal s'apparente à l'utilisation d'un moteur de recherche classique. La principale différence réside dans l'introduction de la requête. Celle-ci ne se fait plus à la frappe du clavier mais exclusivement à l'oral. Pour être en mesure de recevoir et analyser la requête, l'assistant vocal est équipé d'un certain nombre de capteurs, principalement des microphones, qui bien que problématique sur la question de la vie privée, sont essentiels à son fonctionnement (1). De plus, le recours à l'intelligence artificielle liée à l'apprentissage supervisé rend l'assistant vocal évolutif et plus interactif avec l'utilisateur (2). Une interaction dépendant en grande partie du traitement automatique du langage naturel offrant la capacité à l'assistant vocal

[42] HADOPI et CSA, *Assistants vocaux et enceintes connectées : l'impact de la voix sur l'offre et les usages culturels et médias*, Rapport, mai 2019 ; LACHANCE, F., *« O.K. Google, assiste-moi » Les parcours des utilisateurs et des familles qui domestiquent le Google Home,* papyrus.bib.umontreal.ca, Mémoire de maîtrise, Avril 2019, en ligne : <https://papyrus.bib.umontreal.ca/xmlui/bitstream/handle/1866/22464/Lachance_Francois_2019_memoire.pdf?sequence=2&isAllowed=y >.

non seulement de comprendre la parole humaine mais également de répondre par le biais d'une voie de synthèse (3).

1. Les caractéristiques techniques de l'assistant vocal

L'assistant vocal est composé de caractéristiques techniques sommes toutes simples. Le recueil de la requête va se faire par le microphone permettant sa transmission de l'utilisateur à la machine (a) avant de pouvoir transmettre le résultat à l'oral à l'utilisateur par le biais des haut-parleurs (b). Sa connectivité, que ce soit au réseau Internet du domicile ou aux objets connectés à proximité, contribue à la mise en place de la domotique (c)

a) La présence d'un microphone captant la parole de l'utilisateur … et de son environnement

La présence des microphones se justifie par le recours à la voix pour faire fonctionner l'assistant vocal. Selon les modèles, il se peut que plusieurs microphones soient installés. C'est par exemple le cas de l'enceinte connectée Google Home dotée de deux microphones alors que le modèle Max, du même constructeur, en comporte six[43]. Cette multitude de microphones permet selon les fabricants d'obtenir une meilleure écoute de la requête introduite par l'utilisateur quel que soit l'endroit où il se trouve et de pallier l'une des limites de l'utilisation de la parole que représente la variabilité de l'environnement acoustique[44]. Les microphones vont capter en même temps que la requête, des bruits ou des échanges qui risquent de perturber son enregistrement.

Cependant, ces nombreux capteurs interpellent. En effet, si l'on peut comprendre la raison de leur présence, leur nombre ainsi que l'utilisation de l'assistant, principalement dans un environnement

[43]GOOGLE, *Google home max : caractéristiques techniques,* store.google.com, en ligne : <https://store.google.com/ca/product/google_home_max_specs?hl=fr-CA >.
[44] MINKER, W., et NEEL, F., « Développement des technologies vocales », dans *Le travail humain*, vol. 65, 2002/3, en ligne : < https://www.cairn.info/revue-le-travail-humain-2002-3-page-261.htm#pa23 >, p.268.

fermé[45], soulèvent néanmoins quelques questions relevant du respect de la vie privée et de la protection des renseignements personnels des utilisateurs[46]. Au-delà du simple utilisateur souhaitant interagir avec l'assistant, son environnement est lui aussi mis sous écoute. Les exemples ne manquent pas pour illustrer l'atteinte à la vie privée par les assistants vocaux. Ainsi, aux États-Unis, un couple a été écouté à son insu par son assistant vocal[47]. En discutant, le couple aurait prononcé un mot phonétiquement proche du mot d'activation de leur assistant Alexa d'Amazon. Celui-ci a par la suite interprété certains termes de la conversation comme une demande d'action et a envoyé ladite conversation à un des contacts du couple, dont le nom a également été prononcé lors de leur conversation.

À travers cet exemple, nous constatons que l'intégration des microphones, bien qu'il existe une fonction permettant de les désactiver, peut porter préjudice à la vie privée de l'individu. En conversant à proximité de l'assistant vocal, le couple découvre que celui-ci était susceptible de servir de véritable magnétophone sans pour autant en être informé. Un tel cas démontre que des enregistrements sonores ont bel et bien lieu même si les fabricants tendent à affirmer que l'utilisateur garde toujours la maîtrise de ses échanges avec l'assistant vocal.

En ce qui concerne la collecte des renseignements personnels, nous nous contenterons pour l'instant d'évoquer l'existence de dispositions législatives tendant à interdire la collecte à l'insu de la personne[48].

L'expérience orale se caractérise également par la faculté de l'utilisateur à entendre l'assistant vocal répondre à sa demande. Cette réponse est rendue possible par des haut-parleurs.

---

[45] Quel que soit le type de technologie intégrant l'assistant vocal, dont nous les avons évoqué en introduction, celui-ci est généralement utilisé en milieu clos même si dans certains cas, comme pour le téléphone intelligent, l'utilisation en plein air est possible.

[46] Nous invitons le lecteur à se référer à la partie II.A. notamment en ce qui concerne l'atteinte à la protection des renseignements personnels et à la vie privée.

[47] RTBF, « Alexa, l'assistant vocal d'Amazon, envoie par erreur la conversation privée d'un couple à un collègue du mari », rtbf.be, 25 mai 2018, en ligne : < https://www.rtbf.be/info/insolites/detail_une-conversation-privee-envoyee-par-erreur-par-l-enceinte-connectee-d-amazon?id=9927755 >.

[48] Nous aborderons plus en détail au sein de la seconde sous-partie les principes fondamentaux en matière de protection des renseignements personnels, dont la collecte et le consentement.

b) Les haut-parleurs

Il s'agit d'une composante en complément du microphone visant à enrichir l'expérience vocale de l'utilisateur. La fonction des haut-parleurs consiste en la transmission orale du résultat de la requête au demandeur. La voix de l'assistant vocal est produite à l'aide de la synthèse de la parole, dont les haut-parleurs se chargent de la relayer vers le monde réel.

Les haut-parleurs ne portent pas directement atteinte à la protection des renseignements personnels de l'individu dans la mesure où leur fonction est limitée à la diffusion de la réponse à la demande. Ils peuvent toutefois constituer un inconvénient au moment de transmettre le résultat de la requête. En effet, ceux-ci peuvent être une source de nuisance pour les personnes aux alentours voire même pour la personne elle-même lorsque l'assistant vocal se déclenche involontairement. Cette source de nuisance représente également une atteinte à la confidentialité des données. Prenons l'exemple d'un individu qui introduit une requête à l'assistant vocal présent dans son téléphone. La réponse de l'assistant risque de rendre publique certaines informations que l'utilisateur aurait préféré garder secret, comme la lecture d'un message texte, ou d'un rendez-vous médical. Tout comme pour les microphones, les haut-parleurs de l'assistant vocal mettent en quelque sorte fin à la confidentialité des données puisque l'émission de la réponse se fera également à haute voix. Cette caractéristique technique soulève elle aussi la question de l'interaction avec l'homme dans un environnement public. Il semblerait que son utilisation autour de la voix ne soit pas encore pleinement adaptée à la volonté d'une société désireuse d'une meilleure protection de la vie privée contre l'intrusion des technologies[49].

[49] POULLET, Y., et HENROTTE, J-F., « La protection des données (à caractère personnel) à l'heure de l'Internet », dans *Protection du consommateur*, pratiques commerciales et T.I.C., coll. Commission Université-Palais, volume 109, Liège, Anthémis 2009, pp. 197-245 ; DETRAIGNE, Y., et ESCOFFIER, A.-M., *La vie privée à l'heure des mémoires numériques. Pour une confiance renforcée entre citoyens et société de l'information*, Rapport d'information n°441, senat.fr, 27 mai 2009, en ligne : < http://www.senat.fr/rap/r08-441/r08-441_mono.html#toc328 >.

Cependant, le rôle de l'assistant vocal ne se limite pas seulement à répondre à des requêtes, pour le rendre davantage attractif, les fabricants[50] ont chacun développé un écosystème[51] lui permettant d'interagir avec d'autres objets connectés.

c) L'intégration de l'assistant vocal dans son environnement au moyen de la connectivité

Pour fonctionner, l'assistant vocal est équipé d'un émetteur Wifi[52] lui permettant de capter le réseau internet domiciliaire ainsi que d'une antenne Bluetooth, tendant à faire disparaitre le recours au câble Ethernet[53] (i). L'assistant vocal se distingue également par sa capacité à s'associer avec d'autres appareils à proximité immédiate pour offrir à l'utilisateur un environnement entièrement connecté (ii).

i. Au réseau domiciliaire

La connexion sans fil, davantage prise en compte par les constructeurs[54], offre la possibilité pour l'utilisateur de pouvoir déplacer l'assistant vocal où bon lui semble dans son habitat sans avoir à se soucier de la présence d'une prise Ethernet. En s'affranchissant de la connexion filaire, l'utilisateur garde en main le contrôle de son environnement sans être contraint par l'installation

---

[50] C'est notamment le cas de Google avec sa gamme de produit Nest, en ligne : <https://store.google.com/ca/category/connected_home?hl=fr-CA >.

[51] Selon l'Office québécois de la langue française, l'écosystème informatique se définit comme étant un « (e)nsemble intégré du matériel et des ressources logicielles d'une organisation, considérés notamment du point de vue de leur complémentarité et de leur interopérabilité », OFFICE QUEBECOIS DE LA LANGUE FRANCAISE, « Grand dictionnaire terminologique : écosystème informatique », gdt.oqlf.gouv.qc.ca, 2018, en ligne : <http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=26544778 >. Cependant, dans le cadre de notre développement nous préférerons la notion de maison intelligente, que l'Office définit comme une « (h)abitation munie d'appareils électriques et électroniques connectés […] », OFFICE QUEBECOIS DE LA LANGUE FRANCAISE, « Grand dictionnaire terminologique : maison intelligente », gdt.oqlf.gouv.qc.ca, 2019, en ligne : <http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=8874598 >.

[52] Le terme, sans réel signification, se veut davantage comme un jeu de mots avec « Hi-Fi », DOCTOROW, C., « WiFi isn't short for 'Wireless Fidelity' », boingboing.net, en ligne : < https://boingboing.net/2005/11/08/wifi-isnt-short-for.html >.

[53] Ce terme désigne un protocole de réseau local basé sur des commutations de paquets et sur des câbles pour lier plusieurs machines entre elles, JOURNAL DU NET, « Ethernet : définition et fonctionnement », journaldunet.fr, 10 janvier 2019, en ligne : < https://www.journaldunet.fr/web-tech/dictionnaire-du-webmastering/1203383-ethernet-definition/ >.

[54] Les assistants vocaux les plus utilisés aujourd'hui se connectent par le biais d'un émetteur sans fil.

des différents objets connectés constituant, avec l'assistant vocal, la domotique[55]. Cette absence de port Ethernet dans les assistants vocaux illustre également une volonté de modernité et de liberté en passant à des appareils entièrement sans fil.

La mise en place d'une telle connectivité répond à une volonté d'intégrer l'assistant vocal à un environnement privé et de plus en plus connecté. Cette intégration passe dans un premier temps avec la connexion de l'assistant vocal au téléphone intelligent de l'utilisateur, puis dans un second temps par son interaction avec les autres objets connectés.

ii. Aux terminaux et objets disposant d'un accès à Internet

Avant toute utilisation de l'enceinte connectée, l'individu doit procéder au téléchargement d'une application sur son téléphone intelligent lui permettant d'effectuer les paramétrages qu'il souhaite de l'assistant vocal (partage ou non de la localisation, préférence en matière de fuseau horaire, volume etc.)[56]. Cette application aura davantage pour rôle de servir de centre de contrôle pour tous les appareils pouvant être reliés à l'assistant vocal. À travers cette application, l'utilisateur aura également un accès à tout l'historique des conversations avec l'assistant vocal. Selon les différents constructeurs, il est possible pour l'utilisateur de consulter et supprimer ces conversations depuis le téléphone intelligent. Nous précisons qu'une telle application ne vaut que pour les enceintes connectées. L'utilisation de l'assistant vocal intégré à un téléphone intelligent ou à une tablette ne requiert pas une telle installation. À la suite de l'installation de l'application, la personne pourra directement interagir avec l'assistant vocal en prononçant les mots clés ou par simple pression d'une touche de l'appareil.

Avec le temps, les entreprises ont su faire évoluer l'assistant vocal. Celui-ci est passé d'un simple outil de recherche vocal et d'exécution de tâches limitées à son intégration dans un véritable

[55] La domotique se définit comme un « [e]nsemble des techniques visant à intégrer à l'habitat tous les automatismes en matière de sécurité, de gestion de l'énergie, de communication, etc. », LAROUSSE, « Définitions : domotique », larousse.fr, en ligne : <https://www.larousse.fr/dictionnaires/francais/domotique/26402>.
[56] AMAZON, *Alexa Privacy and data handling overview,* white paper, en ligne : <https://d1.awsstatic.com/productmarketing/A4B/White%20Paper%20%20Alexa%20Privacy%20and%20Data%20Handling%20Overview.pdf >, p.6.

écosystème dont il constitue l'élément central. De nos jours, une multitude d'objets connectés ont fait leur apparition rendant l'habitat complétement obéissant à la voix de son propriétaire. En parcourant la page internet dédiée à l'assistant Google[57], nous découvrons que celui-ci peut être utilisé pour contrôler entièrement les pièces d'une maison, et même au-delà. Parmi les tâches qu'il est en mesure d'exécuter, l'assistant de Google peut gérer le système de sécurité, la température, le taux d'humidité dans le domicile. Mais également contrôler les appareils électroniques et électroménagers voire même lancer le démarrage de l'aspirateur intelligent.

L'assistant vocal a su se montrer utile dans la mesure où l'utilisateur dispose d'un objet pouvant exécuter certaines tâches en désignant ou nommant d'autres objets (ex : allumer la lumière, la télévision etc.)[58]. C'est par le biais de cet aspect que la notion de « assistant vocal » prend tout son sens. Tout comme, les objets connectés, l'assistant vocal a bénéficié d'une évolution que ce soit pour acquérir de nouvelles fonctionnalités ou interagir avec son utilisateur (apprentissage de nouveaux mots par exemple). Une évolution rendue possible grâce notamment à l'intelligence artificielle.

2. L'intelligence artificielle au service de l'assistant vocal

Si l'assistant vocal a su attirer et convaincre de son utilité, c'est en grande partie grâce à sa capacité d'apprentissage. Cette évolution permanente est rendue possible par l'intelligence artificielle. Évoquée pour la première fois par John McCarthy *et al*[59] lors de la conférence au Dartmouth college[60] en 1956, l'intelligence artificielle ne dispose pas à l'heure actuelle de définition

[57]GOOGLE, « Assistant Google : que peut-il faire ? », assistant.google.com, en ligne : <https://assistant.google.com/explore?hl=fr_ca >.
[58] MINKER, W., et NEEL, F., « Développement des technologies vocales », dans *Le travail humain*, vol. 65, 2002/3, en ligne : < https://www.cairn.info/revue-le-travail-humain-2002-3-page-261.htm#pa23 >, p.268.
[59] John McCarthy (1927-2011), PhD, mathématicien et informaticien, a présidé la Conférence de Dartmouth. Il est également à l'origine du langage de programmation Lisp, ENCYCLOPEDIA BRITANNICA, « Biography : John McCarthy », britannica.com, en ligne : < https://www.britannica.com/biography/John-McCarthy >.
[60]McCARTHY, J, et al., « A proposal for the Dartmouth summer research project on artificial intelligence », jmc.standford.edu, 31st august 1995, en ligne : < http://jmc.stanford.edu/articles/dartmouth/dartmouth.pdf >. La conférence de Dartmouth s'est déroulée sous la forme d'un atelier scientifique en réunissant une vingtaine de chercheurs, dont les organisateurs John McCarthy et Marvin Minsky.

officielle[61]. Marvin Minsky[62], un des pères fondateurs de l'intelligence artificielle, l'a défini comme étant « the science of making machines do things that would require intelligence if done by men»[63]. Dans un registre un peu plus récent, Yann Le Cun[64] apporte sa définition de l'intelligence artificielle comme « un ensemble de techniques permettant à des machines d'accomplir des tâches et de résoudre des problèmes normalement réservés aux humains et à certains animaux »[65].

La définition apportée par Yan Le Cun ne semble pas être plus précise. Selon le professeur Vermeys « (…) la notion même d'intelligence artificielle (IA) est galvaudée à un tel point qu'elle semble couvrir à la fois tout et rien »[66]. En effet, il semblerait qu'une telle approche de l'intelligence artificielle viendrait englober tout objet ou logiciel qui, dès lors a la capacité de réaliser une tâche ou une opération à la demande de l'homme, soit considérée comme étant intelligent[67]. Afin de mieux délimiter les contours de cette identification, Alan Turing a, en 1950, proposé de « réfléchir à la question : les machines peuvent-elles penser ? » [68] (notre traduction). C'est en tentant de répondre à cette question qu'il met en place le jeu d'imitation[69], qui, bien que non officiel, portera par la suite son nom, afin d'identifier si nous sommes en présence d'une machine dotée d'intelligence artificielle ou non[70].

---

[61]Selon l'Office, l'intelligence artificielle porte « sur la reproduction artificielle des facultés cognitives de l'intelligence humaine dans le but de créer des systèmes ou des machines capables d'exécuter des fonctions relevant normalement de celle-ci », OFFICE QUEBECOIS DE LA LANGUE FRANCAISE, « Grand dictionnaire terminologique : intelligence artificielle », 2017, en ligne <http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=8385376 >.

[62] Marvin Lee Minsky (1927-2016), PhD, mathématicien et informaticien, est le cofondateur avec John McCarthy du Groupe d'intelligence artificielle du MIT et co-organisateur de la Conférence de Dartmouth, ENCYCLOPEDIA BRITANNICA, « Biography : Marvin Minsky », britannica.com, en ligne : <https://www.britannica.com/biography/Marvin-Lee-Minsky#ref733635>.

[63] MINSKY, M., L., *Semantic information processing,* Cambridge, Mass., MIT Press, 1968, 440 p. ; Cette définition est également reprise par la CNIL dans son rapport de décembre 2017, COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES, *Comment permettre à l'homme de garder la main ? Rapport sur les enjeux éthiques des algorithmes et de l'intelligence artificielle,* cnil.fr, décembre 2017, en ligne : <https://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_garder_la_main_web.pdf >, p.16.

[64]Chercheur français considéré comme l'un des pionniers de l'apprentissage profond, WIKIPEDIA, « Yann Le Cun », en ligne : < https://docs.google.com/document/d/1liH9utlyETxvywBQAaXWRcK-l-qV9SCFTEVG0QJLktI/edit >.

[65] LE CUN, Y., « L'apprentissage profond : une révolution en intelligence artificielle », leçon inaugurale au Collège de France, février 2016, en ligne : < https://www.college-de-france.fr/media/yann-lecun/UPL4485925235409209505_Intelligence_Artificielle_____Y._LeCun.pdf >.

[66] VERMEYS, N., « La responsabilité civile du fait des agents autonomes », 2018, Vol. 30 n°3, *Les Cahiers de propriété intellectuelle*, p. 853.

[67] Ibid, pp.853-854.

[68] TURING, A.M., « Computing machinery and intelligence », Mind, Volume LIX, Issue 236, October 1950, p.433.

[69] Ibid.

[70] Le célèbre test de Turing repose ainsi sur une conversation entre un humain et une machine, généralement un ordinateur. Un examinateur suit la conversation, s'il ne parvient pas à opérer une différence entre la machine et l'humain à la fin d'un délai imparti alors la machine sera considérée comme dotée de l'intelligence artificielle.

Toutefois, toujours selon le professeur Vermeys, ce test de Turing ne suffirait lui non plus pour déterminer si une machine est intelligente ou non. Le professeur Vermeys de citer l'exemple des jeux vidéo pour en illustrer l'imprécision de ladite définition :

> « Même en admettant la définition classique voulant que l'intelligence artificielle représente la capacité pour une machine d'imiter l'intelligence humaine, voire même de se faire passer pour un être humain, il demeure que la notion d'IA regroupe des technologies aussi disparates que les personnages non-joueurs d'un jeu vidéo et les voitures autonomes, en passant par les agents intelligents tels Siri ou Alexa »[71] (références omises).

L'assistant vocal bénéficie, pour reprendre les termes officiels, à travers « l'amélioration du service », d'un apprentissage supervisé (a) lui permettant de fournir des réponses plus pertinentes et plus précises à l'utilisateur tout en étant contrôlé par l'humain. L'algorithme constitue le moteur de l'intelligence artificielle. Son absence rendrait alors impossible tout apprentissage intelligent d'une machine (b).

a) L'apport de l'apprentissage supervisé dans le fonctionnement de l'assistant vocal

Le fonctionnement de l'assistant vocal, dans son rôle de recherche du résultat, repose sur l'apprentissage supervisé (i) qui ne peut avoir lieu en l'absence d'une base de données nécessaire pour acquérir de nouvelles connaissances (ii).

i. L'identification de l'apprentissage intelligent de l'assistant vocal

L'apprentissage de l'assistant vocal lui offre la possibilité d'évoluer au fur et à mesure de ses interactions avec l'utilisateur, et comme nous le verrons, sous la supervision de son entraîneur. Cette idée renvoie à la question que Alan Turing s'était posé à ce propos[72]. L'intelligence

[71] VERMEYS, N., « La responsabilité civile du fait des agents autonomes », 2018, Vol. 30 n°3, *Les Cahiers de propriété intellectuelle*, p. 853.
[72] Précitée note 68.

artificielle de l'objet variera selon les besoins et l'utilisation qui en est faite de ce dernier. L'intelligence artificielle regroupe différents types d'apprentissage qui méritent ici d'être distingués afin d'éviter toute confusion du lecteur. L'apprentissage automatique, ou plus communément appelé « machine learning », se caractérise comme :

> « une des branches de l'intelligence artificielle. En utilisant l'informatique, nous concevons des systèmes qui peuvent apprendre des données d'une manière à être formées. Les systèmes peuvent apprendre et s'améliorer avec l'expérience et, avec le temps, affiner un modèle qui peut être utilisé pour prédire les résultats des questions sur la base de l'apprentissage précédent »[73] (nos traductions).

Le fonctionnement de l'assistant vocal repose sur l'utilisation d'algorithmes, dont la notion fera l'objet d'une définition ultérieurement, également appelé l'apprentissage supervisé, devant être différencié de l'apprentissage non supervisé et de l'apprentissage profond. Dans le premier cas, la machine est assistée de son entraîneur, bien souvent le programmeur, chargé de vérifier si elle a commis une erreur. Contrairement à l'apprentissage supervisé, l'absence de supervision conduit à ce que l'objet soit autonome dans sa prise d'action[74]. Comme nous le verrons, les fabricants améliorent sans cesse leurs produits. Cette amélioration passe donc par l'entraînement de l'assistant vocal qui exige donc un suivi de l'homme pour s'assurer de la pertinence du résultat choisi et évaluer sa compréhension de la parole humaine.

Si l'on reprend la citation de la Commission nationale de l'informatique et des libertés (ci-après la « CNIL ») portant sur la relation entre l'algorithme et les données[75], principalement la deuxième

---

[73] BELL, J., « Machine Learnings : Hands-On for Developers and Technical Professionals », onlinelibrary.wiley.com, 3 November 2014, en ligne : < https://onlinelibrary.wiley.com/doi/book/10.1002/9781119183464 >.

[74] ORACLE, « Qu'est-ce que l'apprentissage automatique ? », oracle.com, en ligne : < https://www.oracle.com/ca-fr/artificial-intelligence/what-is-machine-learning.html > ; Le troisième type d'apprentissage machine, l'apprentissage profond, ou « deep learning » est un autre mode d'apprentissage non supervisé de l'intelligence artificielle reposant sur un réseau de neurones artificiels. La présence de neurones ne signifie pas pour autant que l'intelligence artificielle se comporte véritablement comme un humain. En effet, la présence d'une multitude de couches, qui ne sont pas forcément interconnectées et la nécessité de recourir à des données en masse demandent une puissance informatique conséquente, qui représente à l'heure actuelle l'une des limites de l'apprentissage profond ; Voir également, VALIQUETTE, M-A., « Les différences entre intelligence artificielle, apprentissage machine et apprentissage profond », article de recherche, substance.etsmtl.ca, 23 octobre 2017, en ligne : < https://substance.etsmtl.ca/differences-intelligence-artificielle-apprentissage-machine-apprentissage-profond >.

[75] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES, *Comment permettre à l'homme de garder la main ? Rapport sur les enjeux éthiques des algorithmes et de l'intelligence artificielle,* cnil.fr, décembre 2017, en ligne : <https://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_garder_la_main_web.pdf >, p.18.

partie : « (…) Les données sans algorithmes sont muettes », nous en déduisons que pour qu'un assistant vocal puisse être entraîné en vue de produire un résultat, deux éléments indissociables l'un de l'autre sont exigés, un algorithme et des données en masse. Celles-ci sont stockées dans une base de données, sur des serveurs voire dans un nuage informatique, plus communément appelé le « cloud ». Par le biais de ces données entrant dans sa base, l'assistant vocal va pouvoir évoluer. Cette évolution est mentionnée par les fabricants aux utilisateurs[76].

ii. L'instruction et l'évolution de l'assistant vocal grâce à la base de données

Pour que l'apprentissage de l'assistant vocal puisse se faire, des données en quantité sont exigées. Ceux-ci seront stockées dans une base de données permettant à la fois à l'entraineur de parfaire l'apprentissage mais également de permettre à l'assistant de recueillir les informations nécessaires en réponse à la requête. Le recours à l'intelligence artificielle rend possible le traitement par l'assistant vocal d'un grand nombre de données, bien souvent volumineuses et nécessitant des outils performants pour y parvenir.

La base de données[77] se définit comme un « ensemble de données interreliées structurées selon certains critères en vue de permettre leur exploitation » [78]. D'un point de vue juridique, l'article 3 de la *Loi concernant le cadre juridique des technologies de l'information*[79] (ci-après la « LCCJTI ») apporte davantage de détails en définissant la notion de « document » comme :

> « [C]onstitué d'information portée par un support. L'information y est délimitée et structurée, de façon tangible ou logique selon le support qui la porte, et elle est intelligible sous forme de mots, de sons ou d'images. L'information peut être rendue au moyen de tout mode d'écriture, y compris d'un système de symboles transcriptibles sous l'une de ces formes ou en un autre système de symboles »[80].

---

[76] Voir l'extrait 3 de la politique de confidentialité de Google relative à l'amélioration du service, p.120.
[77] La base de données se différencie de la banque de données, regroupant des informations sur un sujet déterminé et accessible au public, OFFICE QUEBECOIS DE LA LANGUE FRANCAISE, « Grand dictionnaire terminologique : banque de données », gdp.oqlf.gouv.qc.ca, 2005, en ligne : <http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=8355655 >.
[78] OFFICE QUEBECOIS DE LA LANGUE FRANCAISE, « Grand dictionnaire terminologique : base de données », gdt.oqlf.gouv.qc.ca, 2006, en ligne : < http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=501757>.
[79] LRQ, c-1.1.
[80] Art. 3 al.1er LCCJTI.

S'agissant de la notion de « document technologique » telle que prévue à l'article 25 de cette même loi, celle-ci renvoie à « (…) tous les supports d'information, autres que le papier, créés par la science moderne et susceptibles d'être utilisés en preuve devant les tribunaux »[81]. La définition de « document technologique » ne bénéficie pas au sein de la LCCJTI d'une définition aussi précise[82] que celle de « document ». Selon le professeur Gautrais et M[e] Gingras, le « document technologique » se définit non pas par une définition mais plutôt une opposition « au document ''non-technologique'' c'est-à-dire à celui faisant appel au support papier ou à tout autre support physique de même nature »[83]. Et les auteurs de préciser que le document technologique constitue « un sous-ensemble faisant partie de la notion de document au sens de la Loi [LCCJTI] »[84]. Finalement, ils retiennent la définition émergeant de l'alinéa 4 de l'article 3 de la LCCJTI : « Les documents sur des supports faisant appel aux technologies de l'information visées au paragraphe 2° de l'article 1 sont qualifiés dans la présente loi de documents technologiques »[85] (nos soulignements). Ainsi, pour qu'un document acquiert la qualification de technologique, il doit recourir à un support, qui lui utilise une technologie de l'information[86].

À la lecture de ces différentes définitions, nous estimons que la base de données de l'assistant vocal doit être considérée comme étant un document technologique. Il ne s'agirait que d'une application de l'article 3 de la LCCJTI dont l'alinéa 3 dispose que :

> « (…) 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 ».

Pour appuyer nos propos, nous pouvons reprendre les quelques exemples de moyens de stockages de renseignements cités par le professeur Gautrais et M[e] Gingras pour illustrer le document

[81] FABIEN, C., « La preuve par document technologique », 2004, vol. 38 R.J.T. 533, p.537.
[82] GAUTRAIS, V., et GINGRAS P., « La preuve des documents technologiques », mai 2010, 22-2, Les cahiers de propriété intellectuelle 267-315, p. 273.
[83] Ibid.
[84] Ibid. p.274.
[85] Ibid. ; Art. 3 al.4 LCCJTI.
[86] GAUTRAIS, V., et GINGRAS P., « La preuve des documents technologiques », mai 2010, 22-2, Les cahiers de propriété intellectuelle 267-315.

technologique. Parmi ces exemples, nous pouvons citer la clé USB, un disque dur ou encore une disquette[87].

Quant au stockage des renseignements personnels issus de l'assistant vocal, les entreprises ont davantage recours à des *datacenters* [88] au sein desquels se trouvent les serveurs. Leur conservation peut également se faire dans un nuage informatique. Ceux-ci constituent un support faisant appel à des technologies issues de « la science moderne » nécessitant une connexion entre eux et l'assistant vocal pour échanger les renseignements personnels conservés à distance. Leur aspect physique réside dans les infrastructures, soit les abritant pour les serveurs, soit ayant une incidence fondamentale dans leur fonctionnement. Les nuages informatiques ne fonctionnant que de manière virtuelle, l'absence ou l'atteinte à leurs infrastructures peuvent remettre en cause la conservation des renseignements personnels, et plus précisément leur disponibilité, intégrité et confidentialité[89].

Une donnée se définit comme la « [r]eprésentation d'une information, codée dans un format permettant son traitement par ordinateur »[90]. Nous avons privilégié l'utilisation de la notion de « donnée » plutôt que celle de « renseignement » pour exposer la définition se conformant davantage à la réalité dans le traitement des informations par l'informatique.

---

[87] Ibid.

[88] Voir par exemple Google qui publie sur Internet la localisation de ses centres de données, GOOGLE, « Centres de données », google.com, en ligne : < https://www.google.com/about/datacenters/inside/locations/ >.

[89] L'intégrité, la confidentialité et la disponibilité sont les trois piliers de la sécurité de l'information. Voir VERMEYS, N. W., *Qualification et quantification de l'obligation de sécurité informationnelle dans la détermination de la faute civile*, papyrus.bib.umontreal.ca, Thèse de doctorat, Université de Montréal, Mars 2009, en ligne : < https://papyrus.bib.umontreal.ca/xmlui/bitstream/handle/1866/3663/12085490.PDF?sequence=2&isAllowed=y > ; Voir également HUBIN, J., POULLET, Y. et al, *La sécurité informatique, entre technique et droit,* Cahier du C.R.I.D., 14, 1998, Facultés Universitaires Notre-Dame de la Paix de Namur.

[90] OFFICE QUEBECOIS DE LA LANGUE FRANCAISE, « Grand dictionnaire terminologique : donnée », gdt.oqlf.gouv.qc.ca, 2004, en ligne : < http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=8358482 >.

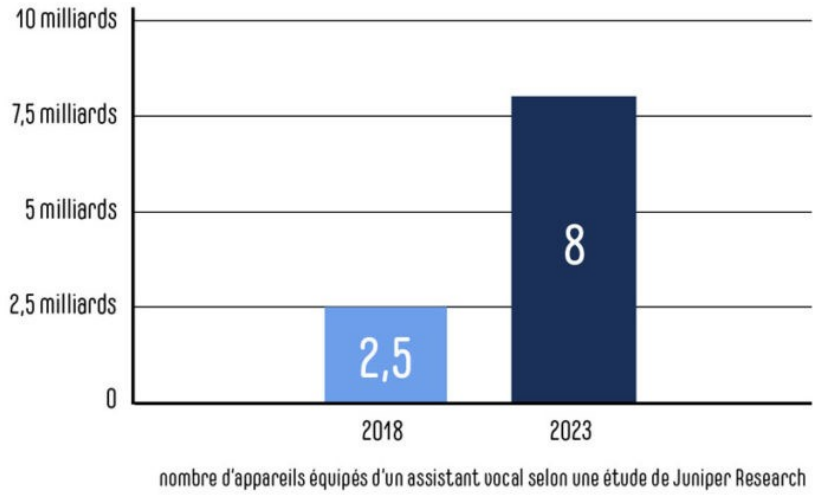


Figure 1. – Comparaison entre 2018 et 2023 du nombre d'appareils dotés d'un assistant vocal[91].

Tel qu'il appert de la figure 1 ci-dessus, le nombre d'appareils dotés d'un assistant vocal a augmenté de manière importante au cours des dernières années. Or, la multiplication des objets connectés intégrant un assistant vocal a concouru à une hausse de la collecte des données. Celles-ci sont devenues leur véritable source d'alimentation car le fonctionnement de l'assistant vocal repose exclusivement sur l'entrée et la sortie d'informations. Nous pouvons citer l'exemple de l'assistant Google Home qui, pour répondre à la requête, va chercher le résultat dans l'énorme base de données partagée avec le moteur de recherche et donc alimentée par les sites internet[92]. Aujourd'hui on affirme également que la donnée constitue « la matière première de cette révolution

[91] LOYER, C., *Juniper Research prédit 8 milliards d'appareils équipés d'un assistant vocal en 2023,* vokode.com, 14 février 2019, en ligne : < https://www.vokode.com/juniper-research-predit-8-milliards-dappareils-equipes-dun-assistant-vocal-en-2023/ >.

[92] Pour comprendre comment fonctionne la recherche par le biais du moteur de recherche Google, nous invitons le lecteur à consulter la page Google expliquant la manière dont son moteur fonctionne, GOOGLE AIDE SEARCH CONSOLE, « Comment fonctionne la recherche Google », support.google.com, en ligne : <https://support.google.com/webmasters/answer/70897?hl=fr >.

numérique. À ce titre, elle a été comparée au pétrole, ressource au cœur de la seconde révolution industrielle »[93], au point même de la considérer comme un véritable or noir numérique[94].

Cependant, l'assistant vocal ne recueille pas n'importe quel type de données. En effet, l'interaction avec l'utilisateur et son intégration dans un environnement domiciliaire connecté lui permettent d'obtenir des informations sur la vie privée des personnes se trouvant autour de lui. Ces informations, sensibles pour certaines, vont permettre aux fabricants de connaître toute la vie de l'utilisateur, ses habitudes, ses centres d'intérêts etc.

Ainsi, une donnée à caractère personnel[95], ou renseignement personnel selon les législations canadiennes, se définit comme un renseignement permettant d'identifier une personne[96]. Afin de garantir une certaine sécurité juridique face à l'évolution des technologies, la jurisprudence a estimé que « selon son sens clair, cette définition est indéniablement large »[97].

La jurisprudence a également apporté des précisions quant à la qualification de l'information comme renseignement personnel. En effet, selon la Cour fédérale un renseignement acquiert le caractère personnel dès lors qu'il existe une forte probabilité que l'individu puisse y être identifié[98]. Cette qualification est valable si le renseignement est pris seul ou en combinaison avec d'autres :

> « Ainsi, les renseignements, quels que soient leur forme et leur support, sont des renseignements « concernant » un individu s'ils « permettent » d'identifier l'individu ou « rendent possible » son identification, que ces renseignements soient utilisés seuls ou combinés avec des renseignements d'autres sources … »[99] (nos soulignements).

[93] INSTITUT MONTAIGNE, *Big data et objets connectés : Faire de la France un champion de la révolution numérique,* Rapport, institutmontaigne.org, avril 2015, en ligne : <https://www.institutmontaigne.org/ressources/pdfs/publications/rapport%20objets%20connecte%CC%81s(2).pdf >, p.11.
[94] Ibid. p.13.
[95] Terme employé par le Règlement Général de la Protection des Données.
[96] Art 2(1) LPRPDE ; art 2 LPRPSP ; art 54 Loi sur l'accès ; art 4 RGPD.
[97] *Dagg c. Canada (Ministre des Finances)*, [1997] 2 R. C. S 403, dissidents, par. 68.
[98] *Gordon c. Canada (Santé)*, 2008 CF 258.
[99] Ibid, par. 33.

Dans le cadre de l'utilisation de l'assistant vocal, et plus particulièrement lors d'une conversation orale, soit entre l'individu et l'assistant, soit entre deux personnes[100], les informations collectées peuvent également être qualifiées de renseignements personnels dès lors qu'elles sont susceptibles de concerner une tierce personne. C'est ce qu'il ressort de la décision *Morgan* c. *Alta Flights*[101]. Dans cette décision, il était question de l'enregistrement par le biais d'un dispositif d'écoute d'une conversation entre plusieurs personnes dans le but d'obtenir des informations pouvant servir une enquête visant une employée. L'enregistreur s'est révélé être défaillant et aucun renseignement n'a pu être collecté. À travers cette décision, la Cour fédérale reconnaît que le simple fait de vouloir recueillir un renseignement identifiant une personne, quand bien même il ne se trouve pas dans une forme consignée comme la conversation orale, constitue malgré tout un renseignement personnel[102].

L'émergence des donnés massive a sans nul doute contribué à l'utilisation de plus en plus importante de l'assistant vocal, et plus largement des objets connectés. Derrière cette notion, apparue pour la première fois en 1997[103], se cache des données dont leur taille est si importante que les techniques classiques de gestion des bases de données ne suffisent plus[104]. Selon Danièle Bourcier et Primavera De Filippi[105], le big data se caractériserait par le volume des données, leur variété et leur vitesse à laquelle elles sont produites. À ces caractéristiques s'ajoutent également

---

[100] BOURCIER, D. et DE FILIPPI, P. (dir), *Open Data & Big Data: nouveaux défis pour la vie privée*, Paris, Mare & Martin, 2016, p.106.

[101] *Morgan c. Alta Flights (Charters) Inc*., (2005) CF 421 ; COMMMISSARIAT A LA PROTECTION DE LA VIE PRIVEE, *Bulletin d'interprétation : Renseignement personnel*, priv.gc.ca, octobre 2013, en ligne : <https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/lois-sur-la-protection-des-renseignements-personnels-au-canada/la-loi-sur-la-protection-des-renseignements-personnels-et-les-documents-electroniques-lprpde/aide-sur-la-facon-de-se-conformer-a-la-lprpde/bulletins-sur-l-interpretation-de-la-lprpde/interpretations_02/ >.

[102] COMMMISSARIAT A LA PROTECTION DE LA VIE PRIVEE, *Bulletin d'interprétation : Renseignement personnel*, priv.gc.ca, octobre 2013, en ligne : < https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/lois-sur-la-protection-des-renseignements-personnels-au-canada/la-loi-sur-la-protection-des-renseignements-personnels-et-les-documents-electroniques-lprpde/aide-sur-la-facon-de-se-conformer-a-la-lprpde/bulletins-sur-l-interpretation-de-la-lprpde/interpretations_02/ >.

[103] COX, M., et ELLSWORTH, D., « Application-Controlled Demand Paging for Out-of-Core Visualization », Proceedings of the 8th IEEE Visualization Conference, Association for computing machinery, 1997 ; Voir également sur l'histoire du big data : PRESS, G., « A very short history of Big data », forbes.com, 9 may 2013, en ligne : <https://www.forbes.com/sites/gilpress/2013/05/09/a-very-short-history-of-big-data/#6bcfa3fe65a1 >.

[104] Ibid., et WHITE, T., « Hadoop : The definitive Guide, 2012 », cité par CENTRE DE RECHERCHE INFORMATIQUE DE MONTREAL, *Données massives et intelligence artificielle,* crim.ca, 11 juillet 2017, en ligne : < https://www.crim.ca/crim_uploads/documents/FICHE-BigData-IA-expertise-110717.pdf >.

[105] BOURCIER, D. et DE FILIPPI, P. (dir), *Open Data & Big Data: nouveaux défis pour la vie privée*, Paris, Mare & Martin, 2016, p.99.

celles de la visualisation, comme par exemple l'image ou le graphique, et la valeur des données[106], certaines vont se voir accorder plus d'importance que d'autres en fonction de la finalité recherchée par l'entreprise.

Les données massives vont permettre à l'assistant vocal, et donc à l'intelligence artificielle, de s'entraîner en traitant celles à sa disposition mais également de répondre à la requête de l'utilisateur. À l'occasion de la 38e conférence des commissaires à la protection des données personnelles et à la vie privée, il a été affirmé que :

> « The relation between artificial intelligence and big data is bi-directional: Artificial intelligence, through machine learning, needs a vast amount of data to learn: data in the realm of big data considerations. On the other direction, big data uses artificial intelligence techniques to extract value from big datasets »[107] (nos soulignements).

Le traitement de données en masse contribue à l'évolution de l'assistant vocal, que ce soit dans son apprentissage[108] ou dans sa faculté à proposer de nouvelles fonctionnalités et services à l'utilisateur. Comme pour chaque appareil connecté à Internet, l'assistant vocal dispose d'un système d'exploitation, Operating System ou OS. Ce système a pour principale fonction de gérer les ressources de l'appareil dans lequel se trouve l'assistant vocal, téléphone, ordinateur ou enceinte connectée par exemple. C'est à travers l'OS qu'une partie de l'évolution de l'assistant vocal va s'opérer. Une mise à jour va permettre de fournir une nouvelle interface graphique à l'utilisateur lui permettant de profiter des dernières nouveautés en matière d'avancée technologique.

C'est ainsi que Siri, l'assistant vocal d'Apple, a d'abord été en mesure de répondre à des services basiques (ajout d'un évènement dans le calendrier par exemple) avant de progressivement évoluer et proposer de nouvelles fonctionnalités devenant un véritable assistant ayant la capacité de se

---

[106] CENTRE DE RECHERCHE INFORMATIQUE DE MONTREAL, *Données massives et intelligence artificielle,* crim.ca, 11 juillet 2017, en ligne : < https://www.crim.ca/crim_uploads/documents/FICHE-BigData-IA-expertise-110717.pdf >.

[107] 38TH INTERNATIONAL CONFERENCE OF DATA PROTECTION AND PRIVACY COMMISSIONERS, *Artificial Intelligence, Robotics, Privacy and Data Protection,* Room Document, October 2016, en ligne : <https://edps.europa.eu/sites/edp/files/publication/16-10-19_marrakesh_ai_paper_en.pdf >.

[108] Voir le développement précédent relatif à l'apprentissage supervisé.

substituer à l'humain dans l'exécution de certaines tâches[109]. Dans le même temps cette mise à jour assure au fabricant que l'utilisateur continue toujours d'utiliser l'assistant vocal. Par conséquent, cette pratique lui garantit la collecte de plus en plus de renseignements personnels.

En plus de ces mises à jour, les utilisateurs ont la possibilité de personnaliser leur assistant vocal par le biais des compétences, ou « skills », mise en place par les fabricants. La figure ci-dessous illustre le nombre de compétences disponibles pour l'assistant vocal Alexa par pays.

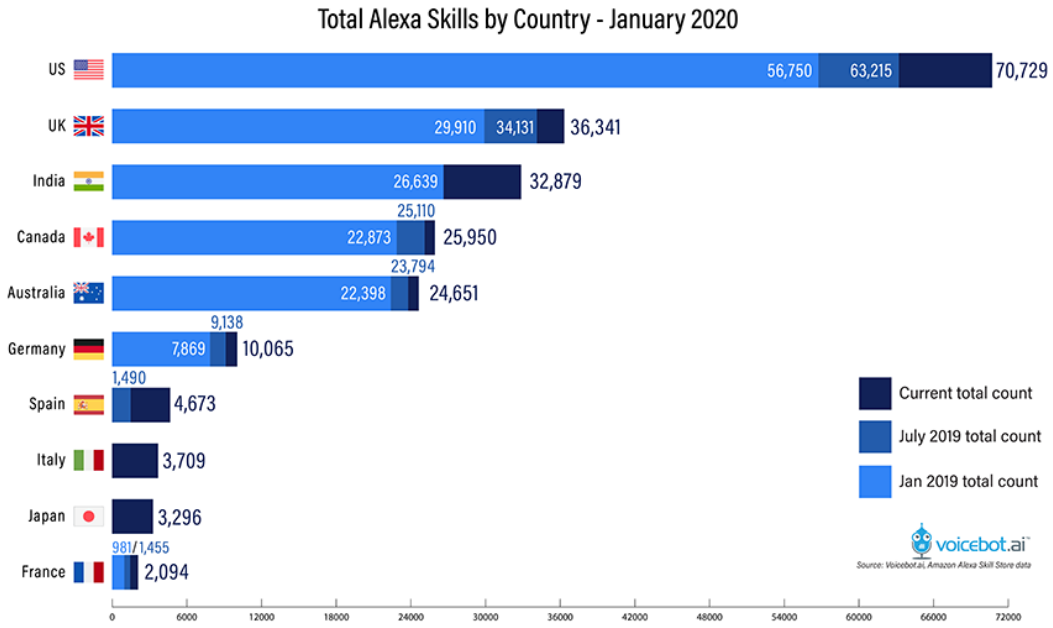


Figure 2. – Nombre de skills de l'assistant Alexa de Amazon par pays[110].

Ces compétences viennent encourager les personnes à davantage utiliser l'assistant vocal en transformant la manière d'interagir avec l'objet connecté. Parmi les skills, nous retrouvons des jeux pour enfants voire des histoires que l'assistant peut raconter.

[109] SANTOLARIA, N., *« Dis Siri » Enquête sur le génie à l'intérieur du smartphone,* Anamosa, 2016, pp.64-65.
[110] KINSELLA, B., « New Alexa skill data shows new U.S skills launched in 2019 fall to lowest level since 2016 », voicebot.ai, 17 January 2020, en ligne : < https://voicebot.ai/2020/01/17/new-alexa-skill-data-show-new-u-s-skills-launched-in-2019-fall-to-lowest-level-since-2016/ >.

Or, l'absence d'une réelle barrière dans l'interaction et le nombre conséquent de skills tendent à engendrer des enregistrements sonores de plus en plus important. En outre, la présence de plusieurs microphones sur certains modèles d'assistants vocaux favorise la collection de données en masse[111]. En effet, le recours à la voix nous empêche de réaliser qu'il n'existe aucun filtre ou écran entre nous et l'assistant vocal. Lié à l'apprentissage supervisé, notre comportement concourt à développer l'assistant vocal en lui fournissant les données nécessaires. Nous nous retrouvons alors être des acteurs de cette évolution mais dans le même temps nous dévoilons des éléments de notre vie privée.

Comme nous l'avons vu tout au long de cette première partie, une personne peut interagir avec l'assistant vocal pour commander une action ou obtenir une réponse à une recherche. Cette interaction est rendue possible à travers les caractéristiques techniques de l'assistant vocal et de son mode d'apprentissage. L'intelligence artificielle lui offre la possibilité de traiter un grand nombre de données contenues dans sa base de données. Cette interaction passe également par le TALN qui occupe une place essentielle dans le fonctionnement de l'assistant vocal en lui conférant à la fois la capacité de reconnaître la parole et les mots prononcés et répondre par le biais d'une voix de synthèse.

b) L'algorithme intelligent comme moteur de l'assistant vocal

Comme nous l'avons mentionné, l'intelligence artificielle s'articule autour de l'algorithme. Intégrée à l'assistant vocal, l'algorithme intelligent (i) va agir comme un véritable moteur pour produire le résultat demandé par l'utilisateur (ii).

[111] BOURCIER, D. et DE FILIPPI, P. (dir), *Open Data & Big Data: nouveaux défis pour la vie privée*, Paris, Mare & Martin, 2016.

i. La détermination de la notion de « algorithme intelligent »

La CNIL définit l'algorithme comme « une suite d'étapes permettant d'obtenir un résultat à partir d'éléments fournis en entrée »[112]. Toujours selon la CNIL, l'algorithme peut être auto-apprenant[113]. En d'autres termes, l'algorithme aura recours à l'apprentissage automatique[114] pour se développer de manière autonome. D'ailleurs l'Office québécois de la langue française (ci-après « l'Office ») renvoie le terme « intelligent » au domaine informatique. L'Office précise qu'est intelligent, la technologie possédante :

> « […] les ressources électroniques ou informatiques nécessaires pour traiter, de manière autonome, des données recueillies ou reçues, et pour pouvoir utiliser l'information afin de commander des actions »[115] (nos soulignements).

L'application de l'algorithme se caractérise par l'élaboration d'un logiciel conçu par le biais du langage informatique et exécuté par un ordinateur[116]. Dans la réalité, il s'agit principalement, pour vulgariser la chose, d'une boîte noire que, mis à part le programmeur, personne ne sait véritablement comment elle fonctionne[117].

La méconnaissance de l'élaboration et le fonctionnement de l'algorithme par l'utilisateur n'est pas sans incidence sur la protection de ses renseignements personnels. Ces informations ne lui sont pas révélées, et sont d'ailleurs absentes des politiques de confidentialité dans la rubrique relative à la collecte des données. Nous avons tenté de trouver un début d'information sur le fonctionnement

---

[112] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES, *Comment permettre à l'homme de garder la main ? Rapport sur les enjeux éthiques des algorithmes et de l'intelligence artificielle,* cnil.fr, décembre 2017, en ligne : <https://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_garder_la_main_web.pdf >, p.5. Cette définition est similaire à celle de la CEPEJ, COMMISSION EUROPEENNE POUR L'EFFICACITE DE LA JUSTICE, *Charte éthique européenne d'utilisation de l'intelligence artificielle dans les systèmes judiciaires et leur environnement,* adoptée lors de la 31e réunion plénière de la CEPEJ, Strasbourg, 3 et 4 décembre 2018.

[113] Ibid.

[114] Nous référons le lecteur à la partie I.B.2.b) sur l'apprentissage de l'assistant vocal.

[115] OFFICE QUEBECOIS DE LA LANGUE FRANCAISE, « Grand dictionnaire terminologique : intelligent », gdt.oqlf.gouv.qc.ca, 2007, en ligne : < http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=8374565>.

[116] COMMISSION NATIONALE DE L'INFORMATION ET DES LIBERTES, *Définition : Algorithme*, cnil.fr, en ligne : < https://www.cnil.fr/fr/definition/algorithme >.

[117] RICHARD, C., « Dans la boîte noire des algorithmes : Comment nous nous sommes rendus calculables », dans *Revue du crieur,* 2018/3, (n°11), en ligne : < https://www.cairn.info/revue-du-crieur-2018-3-page-68.htm#s1n7 >, p. 78.

de l'algorithme au sein d'un assistant vocal dans la politique de confidentialité du Google Home. Il s'avère que ladite politique ne fait aucunement état de la présence d'un algorithme. Cette absence ne fait guère d'illusion quant à la publication du code source, vulgairement comparé à une recette de cuisine. Sa publication serait de nature à divulguer de possible secrets commerciaux et/ou industriels. Par conséquent, ce genre d'information n'apparaît nullement sur Internet et n'est pas connu de l'utilisateur. D'ailleurs, la rédaction du code source nécessite la maîtrise de langages informatiques. Pour en faciliter la compréhension par le lecteur, nous avons repris dans la figure ci-dessous un exemple de code source « simple » afin de lui en donner un aperçu. La réalité s'avère bien plus complexe que cela car les multiples tâches pouvant être demandées à l'assistant vocal font appel à tout un programme permettant de mener à bien leur exécution.

```
/**
 * Simple HelloButton() method.
 * @version 1.0
 * @author john doe <doe.j@example.com>
 */
HelloButton()
{
  JButton hello = new JButton( "Hello, wor
  hello.addActionListener( new HelloBtnList

  // use the JFrame type until support for t
  // new component is finished
  JFrame frame = new JFrame( "Hello Button"
  Container pane = frame.getContentPane();
  pane.add( hello );
  frame.pack();
  frame.show();            // display the fra
}
```

Figure 3. – Exemple de code source[118].

[118] WIKIPEDIA, « Code source », wikipedia.org, en ligne : < https://fr.wikipedia.org/wiki/Code_source > ; Le code source est un fichier détaillant l'ensemble des instructions données en langage de programmation par le programmateur. JOURNAL DU NET, « Code source : définition, traduction », journaldunet.fr, 28 janvier 2020, en ligne : < https://www.journaldunet.fr/web-tech/dictionnaire-du-webmastering/1203623-code-source-definition-traduction/ >.

De plus, la publication du code binaire n'arrangerait en rien la compréhension du fonctionnement du logiciel par l'utilisateur. Celui-ci se veut comme la traduction du code source en une série de deux chiffres[119] (ou états) digne d'un film de Matrix.

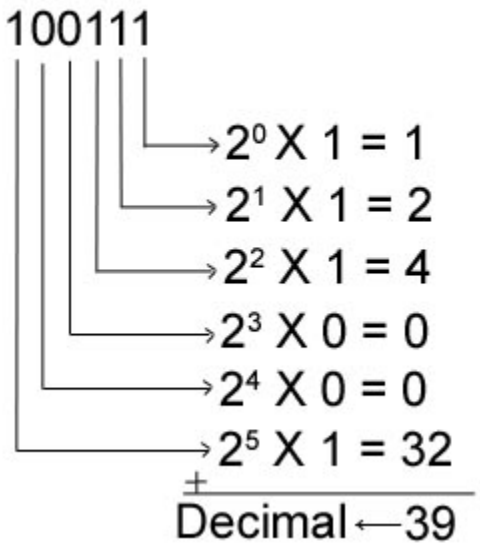


Figure 4. – Exemple d'un code binaire en haut à gauche et sa valeur décimale[120].

Nous présumons qu'un utilisateur lambda ne dispose pas de connaissances pointues dans le domaine de l'informatique, notamment dans la programmation. L'accès à un tel code se révèlerait être inutile puisqu'il est attendu de ces fabricants d'apporter des informations simples aux personnes afin qu'elles soient en mesure de comprendre le fonctionnement de l'objet.

Ce manque de transparence a pour conséquence de rendre le consentement vicié. En effet, si une personne n'est pas en mesure de comprendre le fonctionnement d'un objet, elle ne sera pas en capacité de fournir un consentement pleinement éclairé. Un manque d'éclaircissement qui démontre l'absence de transparence[121] autour du fonctionnement de l'assistant vocal.

---

[119] IONOS, « Le code binaire : pourquoi a-t-on besoin du système binaire ? », ionos.fr, 3 septembre 2019, en ligne : <https://www.ionos.fr/digitalguide/sites-internet/developpement-web/code-binaire/ >.

[120] FUTURA TECH, « Code binaire », futura-sciences.com, en ligne : < https://www.futura-sciences.com/tech/definitions/informatique-code-binaire-11934/ >.

[121] Ce principe est prévu à l'article 4.8 de l'annexe 1 de la LPRPDE ; Art. 5 du RGPD.

Bien que ce point soit développé ultérieurement, nous mentionnons que cette situation contrevient aux différentes dispositions législatives en vigueur au Canada et au Québec. L'article 4.3 de l'annexe 1 de la LPRPDE consacre le principe du recueil du consentement et précise que « [t]oute personne doit être informée de toute collecte, utilisation ou communication de renseignements personnels qui la concernent et y consentir […] » (nos soulignements). Le consentement est également énoncé aux articles 6 de la LPRPSP et 35 du C.c.Q.

Néanmoins, l'algorithme reste un élément essentiel garantissant le bon fonctionnement de l'assistant vocal. En son absence, l'assistant vocal se retrouvera dans l'incapacité de traiter la requête de l'utilisateur. Cela équivaudrait à être en possession d'ingrédients et ne pas avoir la recette indiquant les étapes à suivre pour arriver au résultat. L'assistant vocal n'aurait donc plus aucune utilité.

ii. La place occupée par l'algorithme intelligent

Inséré dans l'assistant vocal, l'algorithme a pour objectif de relier les différents mécanismes composant la reconnaissance vocale entre eux afin de faire parvenir le résultat de la requête ou d'engager l'action liée à la commande. Il s'agit plus précisément de connecter les briques technologiques[122] entre elles et de garantir leur bonne exécution.

Le caractère auto-apprenant de l'algorithme contribue à rendre l'assistant vocal plus intelligent et évolutif en ayant la capacité d'apprendre des usages et du vocabulaire employé par l'utilisateur. Dans le même temps, l'algorithme intelligent peut conduire le fabricant, et propriétaire de l'algorithme, a réalisé un profilage des utilisateurs. L'utilisation massive de l'assistant vocal, principalement dans le cadre de la maison intelligente, concourt à nourrir les entreprises de nos préférences et mode de vie leur permettant de mieux d'adapter leurs produits et services. Par exemple, un assistant vocal pourra suggérer à l'utilisateur de passer une commande d'ampoules

[122] Voir partie I.A.3. a) et notamment la figure 5.

intelligentes directement sur le site de vente du fabricant s'il détecte que celles déjà en place sont sur le point de ne plus fournir l'éclairage adéquat.

L'utilisation de l'algorithme poussée à l'extrême, peut être préjudiciable pour l'utilisateur, notamment en ce qui a trait au respect de sa vie privée[123]. Derrière ces assistants vocaux se trouve des entreprises[124] n'hésitant pas à sous-traiter l'analyse de ces enregistrements sonores tout en prenant le soin de ne pas mentionner la manière dont le service est amélioré[125].

Cette méthode a de quoi interpeller. En effet, les fabricants sont susceptibles d'obtenir des renseignements personnels pouvant dans certains cas être sensibles mais dont aucune mesure de sécurité n'est prévue dans le partage de ces informations avec des prestataires externes[126]. Tel que nous le verrons, cette situation va à l'encontre de la législation en matière de protection des renseignements personnels, principalement en ce qui concerne le transfert[127] des renseignements.

Toutefois, que l'assistant vocal intègre l'informatique en périphérie ou qu'il transmette les données au nuage informatique, son apprentissage reste limité et nécessite la supervision de l'homme. En effet, si l'on reprend la politique de confidentialité de Google, il est précisé que « … nous pouvons améliorer les résultats de recherche … » (nos soulignements). L'amélioration des résultats apportés

---

[123] Ibid. Nous reviendrons plus en détail, notamment en ce qui concerne la collecte des renseignements personnels, à la partie II.A.2.

[124] Ces entreprises, pour éviter d'être liées contractuellement aux utilisateurs, font appel à des tiers pour analyser les enregistrements même en l'absence de contrat les liant juridiquement, CASILLI A., « Derrière les assistants vocaux, des humains vous entendent », laquadratur.net, 18 mai 2018, en ligne : <https://www.laquadrature.net/2018/05/18/temoin_cortana/ > ; DAY, M., G. TURNER et N. DROZDIAK, « Amazon Workers Are Listening to What You Tell Alexa », bloomberg.com, 10 avril 2019, en ligne : <https://www.bloomberg.com/news/articles/2019-04-10/is-anyone-listening-to-you-on-alexa-a-global-team-reviews-audio >.

[125] Ibid.

[126] Ibid.

[127] La LPRPDE prévoit implicitement au principe 4.1.3 de l'annexe 1 le transfert des renseignements. Le CPVP est venu apporter quelques précisions dans ses lignes directrices de Janvier 2009, COMMISSARIAT A LA PROTECTION DE LA VIE PRIVEE, *LPRPDE : Traitement transfrontalier des données personnelles, Lignes directrices,* priv.gc.ca, janvier 2009, en ligne : < https://www.priv.gc.ca/media/1994/gl_dab_090127_f.pdf >. Le RGPD prévoit au sein du chapitre V plusieurs dispositions encadrant le transfert des données vers des pays en dehors de l'UE, précité note 40 ; Voir également GRATTON, E., « Dealing with Canadian and Quebec Legal Requirements in the Context of Trans-border Transfers of Personal Information and Cloud Computing Services », dans *Développements récents en droit de l'accès à l'information et de la protection des renseignements personnels — les 30 ans de la Commission d'accès à l'information (2012)*, vol. 358, service de la formation continue, Barreau du Québec, Cowansville, Éditions Yvon Blais, 2012. Nous évoquerons plus en détail la notion de transfert à la page 104.

par les ingénieurs à l'assistant vocal concourt à son apprentissage tendant à le rendre plus intelligent et par conséquent, plus interactif.

Tout au long de ce développement, nous avons tenté de démontrer à la fois la puissance de l'algorithme et son exploitation dans l'analyse des données collectées par l'assistant vocal. Les fabricants se retrouvent alors en capacité d'adapter leurs produits et services en fonction de l'évolution de nos centres d'intérêts, préférences et consommation.

À travers cette supervision, il s'agit en réalité de s'assurer que l'assistant vocal a bien compris la requête qui lui a été introduite et qu'il a été en mesure d'y répondre correctement, tant par le choix des mots que par leur prononciation. Cette interaction par le biais du TALN est l'apport technologique nouveau embarqué par l'assistant vocal et qui le rend particulièrement utile. Le traitement automatique du langage naturel est donc l'objet de notre prochain développement.

3. Le recours au traitement automatique du langage naturel dans l'interaction homme-machine

Le TALN se trouve au cœur de l'interaction entre l'utilisateur et l'assistant vocal. Sa mise en place récente dans les objets connectés (a) a permis de mettre au point une nouvelle façon de les utiliser en consacrant entièrement l'interaction sur la voix humaine et de synthèse (b).

a) La mise en place du traitement automatique du langage dans l'assistant vocal[128]

Les progrès technologiques ont rendu possible la miniaturisation des composants nécessaires à la mise en place du TALN dans les objets connectés. Ces progrès ont également mis au jour de nouvelles techniques de transmission de l'information en décentralisant certains mécanismes. L'avantage d'un tel procédé est de permettre de réduire encore plus la taille de l'assistant vocal.

[128] La technicité de ce développement nous oblige à simplifier nos propos afin d'en faciliter la lecture. Nous invitons le lecteur à se référer à l'ouvrage complet sur le traitement automatique du langage naturel, notamment ce qui concerne la syntaxe : BOITE, R., et al, *Traitement de la parole,* Presses Polytechniques et universitaires romande, 2000, 488 p.

En effet, nous sommes passés de la Shoebox d'IBM, et ses dimensions semblable à une boîte à chaussure, à des objets pouvant rentrer dans nos poches, voire passer inaperçu au domicile.

Pour y parvenir, les fabricants vont essentiellement s'appuyer sur leurs serveurs stockant les données nécessaires pour fournir la réponse à la requête de l'utilisateur. Les enceintes connectées ou les téléphones intelligents dans lesquels se trouve l'assistant vocal ne serviront en réalité qu'à récupérer la demande introduite. Cette connexion à distance va permettre de séparer physiquement les briques technologiques[129] concourant à la réduction des dimensions de l'objet.

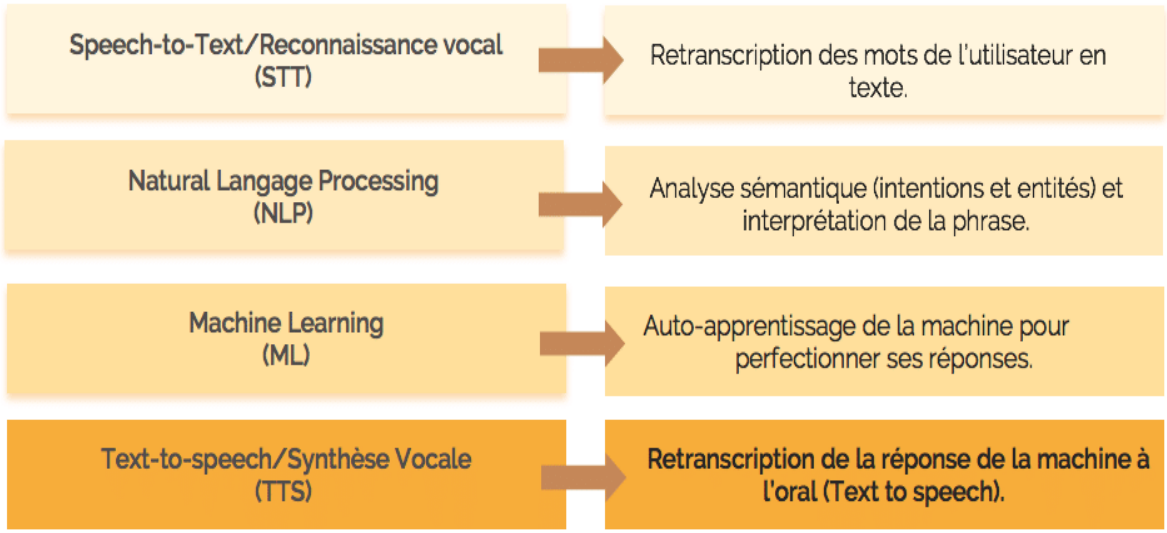


Figure 5. – Schéma représentant les différentes briques technologiques[130].

En d'autres termes, leur séparation physique rend possible l'utilisation de certaines voire d'une seule brique en fonction du produit ou service mis en place. Ainsi, le Speech-to-text (ci-après « STT ») peut seul trouver application au sein d'un ordinateur auprès d'une personne handicapée et dans l'incapacité de l'utiliser. Nous rappellerons au lecteur que la brique technologique NLP

[129] Une brique technologique est « un élément d'un produit ou d'un processus qui remplit une fonction ou qui dispose d'une propriété spécifique », GOTOS3, « Les briques technologiques deviennent des produits « tout-en-un » », gotos3.eu, 1 mars 2018, en ligne : < http://www.gotos3.eu/fr/nieuws/workshop-all-one-materialen > ; HADOPI et CSA, *Assistants vocaux et enceintes connectées : l'impact de la voix sur l'offre et les usages culturels et médias*, Rapport, mai 2019, p.20.

[130] ALIMI, J., « L'assistant vocal, l'interface homme-machine du futur », suricats-consulting.com, en ligne : < https://www.suricats-consulting.com/expertise-commerce-assistant-vocal/ >.

n'est autre que la traduction anglaise du TALN. Cette brique représente l'ensemble des mécanismes intervenant dans l'interaction entre l'homme et la machine[131].

Au moment de l'introduction de la requête, la parole[132] de l'utilisateur va être captée par le microphone qui la transforme en un signal électrique puis la transmettre à un préamplificateur chargé d'adapter le signal électrique. Ce signal est ensuite récolté par les analyseurs qui agissent comme porte d'entrée de la parole dans la machine[133]. Cette phase correspond à la brique technologique du STT. Si la parole est retranscrite à l'écrit et peut être lue par la machine, sa transmission entre les différents mécanismes se fait par les signaux électriques. Au cours de la phase de STT, l'assistant vocal va reconnaître les mots clés et les catégoriser selon leur unité lexicale. Les analyseurs vont par la suite transmettre ces signaux aux reconnaisseurs qui auront pour fonction de les analyser[134]. Nous passons alors à l'étape de l'analyse de la requête par la machine, et plus précisément à l'analyse sémantique de la phrase (Natural Language Understanding) par l'assistant vocal.

À ce stade, selon la machine et l'utilisation qui en est fait du TALN, il existe deux types de reconnaissance, celle du locuteur et celle de la parole. Le premier type sert essentiellement à reconnaître la personne qui parle dans une logique d'identification et d'authentification. Alors que le second type de reconnaissance est davantage axé sur la compréhension par la machine des paroles prononcées par le locuteur[135].

Les mots clés sont par la suite envoyés aux serveurs dans le but d'obtenir la réponse à la requête. L'assistant vocal, ayant bénéficié d'un apprentissage supervisé, saura détecter la bonne intention du locuteur. Autrement dit, Il est à même d'opérer une distinction entre une question et une commande d'action. La réponse choisie dans la base de données sera par la suite vérifiée par le Dialog Manager (ci-après « DM ») qui valide la réponse. Une fois la réponse validée, le DM

[131] BOLUS, D., « Les principales briques technologiques d'un bot », bot-trends.fr, 11 septembre 2018, en ligne : <https://www.bot-trends.fr/intelligence-artificielle-bot/ >.
[132] Les auteurs définissent la parole comme « une variation de la pression de l'air causée et émise par le système articulatoire », BOITE, R., et al, *Traitement de la parole,* Presses Polytechniques et universitaires romande, 2000, p.4.
[133] Ibid, pp.2-3.
[134] Ibid.
[135] Ibid.

transmet au Natural Language Generation (ci-après « NLG ») la décision de parler à l'utilisateur. La réponse est d'abord envoyée au module de synthèse vocale par le biais du Text-to-Speech (ci-après « TTS »), dont les synthétiseurs jouent le rôle de la parole artificielle[136]. Tout au long de ce processus, les codeurs vont s'assurer de la régulation du débit de la parole, lors de son stockage ou de sa transmission dans la machine[137].

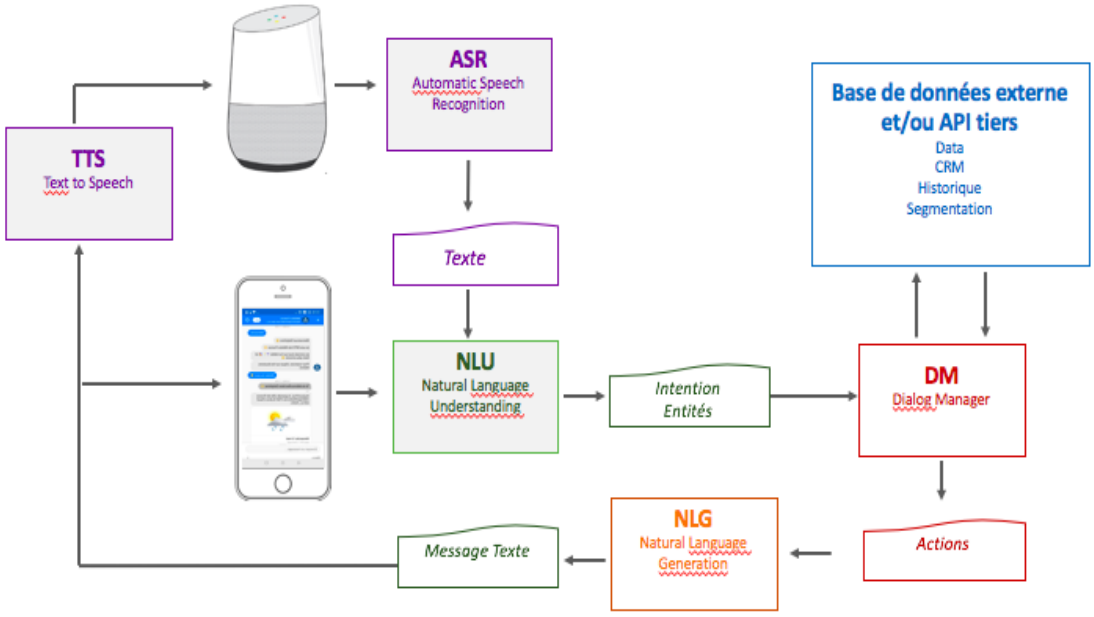


Figure 6. – Schéma illustrant le fonctionnement d'une commande vocale[138].

À travers ce développement, nous avons pu saisir l'organisation des différents mécanismes constituant le TALN au sein d'un assistant vocal. Si l'évolution technologique rend possible la séparation de ces différents mécanismes, comme la décentralisation de la base de données et le recours à la connexion sans fil pour la transmission des informations, la voix reste omniprésente tout au long de ce processus.

[136] Ibid.
[137] Ibid. pp.2-3.
[138] BOLUS, D., « Les principales briques technologiques d'un bot », bot-trends.fr, 11 septembre 2018, en ligne : < https://www.bot-trends.fr/intelligence-artificielle-bot/ >.

b) La voix, élément central au fonctionnement de l'assistant vocal

L'assistant vocal, comme son nom l'indique, est un assistant reposant uniquement sur l'utilisation de la voix. Le recours à la voix est d'autant plus crucial que « la parole est un vecteur d'information privilégié dans notre société d'où l'importance du traitement de la parole »[139].

Il offre à l'utilisateur une nouvelle expérience en n'utilisant que la voix, de l'activation à la réponse de l'assistant (i). Malgré l'utilisation de plus en plus importante de l'assistant vocal et la supervision humaine de son apprentissage, la compréhension du langage humain rencontre quelques limites techniques (ii), que nous pensons pertinent d'évoquer dans ce développement avant d'entamer la seconde partie.

i. L'activation simpliste de l'assistant vocal par le biais de mots d'éveil

L'utilisation simple avec pour seul outil la voix fait la popularité de l'assistant vocal. Il ne nécessite aucun prérequis, une personne de n'importe quel âge n'aura aucun mal à l'utiliser. Cela s'explique par le fait que :

> « la parole constitue le mode le plus naturel de communication entre personnes humaines, du fait que son apprentissage s'effectue dès l'enfance, ce qui est loin d'être le cas pour la maîtrise de la frappe au clavier, par exemple »[140].

Mais également parce que l'assistant vocal offre une certaine prouesse technologique :

> « En faisant converger le langage humain et le langage informatique sous les auspices de l'efficacité, l'interface vocale nous propulse dans un univers magique, où chacune de nos formules serait immédiatement suivies d'effets »[141].

[139] BOITE, R., et al, *Traitement de la parole,* Presses Polytechniques et universitaires romande, 2000, p.1.
[140] MINKER, W., et NEEL, F., « Développement des technologies vocales », dans *Le travail humain*, vol. 65, 2002/3, en ligne : < https://www.cairn.info/revue-le-travail-humain-2002-3-page-261.htm#pa23 >, p.267.
[141] SANTOLARIA, N., *« Dis Siri » Enquête sur le génie à l'intérieur du smartphone,* Anamosa, 2016, p.62.

En s'affranchissant de toutes les contraintes technologiques que peut poser un simple ordinateur, principalement à son installation et à l'utilisation d'un moteur de recherche classique, l'assistant vocal offre à son utilisateur une simplification de l'usage des technologies. Prenons l'exemple d'une recherche à effectuer sur Internet. Face aux nombreux résultats qu'une requête peut engendrer, il existe des opérateurs logiques facilitant la recherche (et, ou, sauf, guillemets etc.). Il est peu probable que toute personne navigante sur Internet ait une connaissance de ces opérateurs, et encore moins qu'elle sache les utiliser. La recherche sur ordinateur, pour obtenir les résultats les plus précis, doit se faire à partir de mots clés[142] pouvant être liés à ces opérateurs. La maîtrise de la recherche sur Internet peut pour certaines personne nécessité le suivi d'une formation. L'absence d'une telle connaissance aura pour tendance soit de compliquer la recherche, soit de décourager la personne de poursuivre sa recherche lorsqu'elle a du mal à trouver le résultat adéquat.

L'assistant vocal ne nécessite pas autant de maîtrise. Son activation simple commence par la prononciation de mots d'éveil comme « Ok Google » ou « Hey Siri » puis l'utilisateur entre sa requête. Il n'aura pas à se soucier de l'introduction de quelconque opérateur logique puisque selon le fonctionnement du TALN évoqué précédemment c'est la machine elle-même qui va s'occuper de la détection des mots clés. La simplicité d'utilisation de l'assistant vocal se traduit également par sa compréhension des termes employés par l'humain grâce au TALN. En effet, à travers le TALN :

> « (…) la prononciation d'un seul mot peut remplacer jusqu'à une dizaine de commandes élémentaires effectuées à l'aide de touches fonctions ou de souris et représente ainsi un effort mnémotechnique moindre »[143].

La réponse transmise par l'assistant vocal par le biais de la synthèse vocale offre à l'utilisateur la possibilité :

[142] HADOPI et CSA, *Assistants vocaux et enceintes connectées : l'impact de la voix sur l'offre et les usages culturels et médias*, Rapport, mai 2019, p.20.
[143] MINKER, W., et NEEL, F., « Développement des technologies vocales », dans *Le travail humain*, vol. 65, 2002/3, en ligne : < https://www.cairn.info/revue-le-travail-humain-2002-3-page-261.htm#pa23 >, p.267.

> « … d'avoir un accès immédiat à une information sans avoir à parcourir toute une arborescence hiérarchique de menus : il est toujours possible bien sûr d'utiliser des raccourcis clavier ou des langages de commande (…) »[144].

Toutefois, quand bien même les objets intégrant un assistant vocal sont de plus en plus nombreux, l'interaction entre l'utilisateur et l'assistant vocal est loin d'être une interaction où la compréhension de la parole par la machine est similaire à celle de l'homme. Le traitement automatique du langage naturel, bien qu'il soit à un stade avancé, continue de montrer certaines limites, notamment face à l'ambiguïté de la langue.

ii. Les limites techniques du TALN : l'exemple des faux positifs

L'évolution de la reconnaissance vocale illustre certes l'avancée majeure qu'a connu le traitement automatique du langage naturel, il n'en fait pas pour autant une technologie parfaite. En effet, le cas précité de notre couple américain ayant été enregistré à son insu après que l'assistant vocal s'est involontairement activé[145], est très révélateur de la survenance de ces faux positifs.

Si nous prenons la langue française, dont ses nombreuses règles grammaticales et ses exceptions font d'elle l'une des langues les plus difficiles à apprendre, il sera compliqué pour l'assistant vocal de comprendre les anaphores. En effet, la complexité de la langue rend plus difficile la segmentation en unité lexicale puisque la parole est « un signal continu sans marque de pause entre les mots, ce qui nécessite une segmentation »[146]. Cette difficulté à segmenter la requête peut être à l'origine de sa mauvaise interprétation par l'assistant vocal[147].

À cette difficulté s'ajoute une autre qui concerne davantage les différentes variétés d'une langue. Si l'on reprend la langue française, celle-ci va différer selon le pays dans lequel on se trouve, voire

---

[144] Ibid, p.28.
[145] RTBF, « Alexa, l'assistant vocal d'Amazon, envoie par erreur la conversation privée d'un couple à un collègue du mari », rtbf.be, 25 mai 2018, en ligne : < https://www.rtbf.be/info/insolites/detail_une-conversation-privee-envoyee-par-erreur-par-l-enceinte-connectee-d-amazon?id=9927755 >.
[146] MINKER, W., et NEEL, F., « Développement des technologies vocales », dans *Le travail humain*, vol. 65, 2002/3, en ligne : < https://www.cairn.info/revue-le-travail-humain-2002-3-page-261.htm#pa23 >, p.269.
[147] HADOPI et CSA, *Assistants vocaux et enceintes connectées : l'impact de la voix sur l'offre et les usages culturels et médias*, Rapport, mai 2019, p.20.

même en fonction de la région. Par exemple, le français parlé en France ne sera pas le même que celui au Québec. Cette différence compliquera le travail de l'assistant vocal qui aura du mal à comprendre la requête s'il ne prend pas en compte ces différentes variantes. Par exemple au Canada, le « football » renvoie à un sport collectif différent de celui que nous trouvons en dehors du continent nord-américain, appelé le « soccer ». Aussi, il existe des expressions propres à chaque pays qu'un assistant vocal ne parviendra peut-être pas à comprendre.

Ces difficultés de compréhension du langage sont de nature à limiter l'évolution du TALN. Des termes pouvant être un pronom ou un article selon l'usage qui en est fait par le locuteur ne seront pas forcément compris par la machine qui l'obligera alors à reformuler la requête[148]. La prononciation des homophones peut également induire en erreur l'assistant vocal. Par exemple les termes « Hockey » et « Ok » seront parfois confondus par la machine et pourront l'orienter vers un résultat erroné. Pour pallier ce problème, certains fabricants ont mis au point un assistant vocal pouvant prendre en charge les spécificités d'une langue. Par exemple, Amazon a rendu possible, par le biais d'une mise à jour, la prise en charge du français québécois[149].

En outre, le TALN rencontre une autre limite, celle des contraintes liées au contexte opérationnel[150]. En d'autres termes, l'assistant vocal ne sera pas capable de faire la différence entre les commandes qui lui sont destinées et l'échange que peut avoir un groupe de personnes. Notre exemple du couple et leur assistant de Amazon cité plus haut représente une parfaite illustration de cette limite que rencontre actuellement l'assistant vocal. Une limite qui peut dans des cas extrêmes être tournée en avantage. Nous pouvons prendre l'exemple de l'affaire d'un double meurtre aux États-Unis, pour laquelle la justice s'est intéressée à l'enregistrement sonore de la scène par l'assistant vocal Alexa[151]. L'enregistrement constitue ici un avantage puisqu'il permettra à la justice de rechercher la vérité sur les faits. Un avantage qui représente toutefois une exception dans

[148] MINKER, W., et NEEL, F., « Développement des technologies vocales », dans *Le travail humain*, vol. 65, 2002/3, en ligne : < https://www.cairn.info/revue-le-travail-humain-2002-3-page-261.htm#pa23 >, p.270.
[149] FORTIN, S., « Alexa veut séduire le Québec », lesoleil.com, 15 avril 2019, en ligne : <https://www.lesoleil.com/les-choix-de-la-redaction/alexa-veut-seduire-le-quebec-video-33011252346709f1a01053c9bee98c3c >.
[150] MINKER, W., et NEEL, F., « Développement des technologies vocales », dans *Le travail humain*, vol. 65, 2002/3, en ligne : < https://www.cairn.info/revue-le-travail-humain-2002-3-page-261.htm#pa23 >, p.268.
[151] GRUMIAUX, M., « Amazon sommé de transmettre des enregistrements d'un Echo suite à un double meurtre », clubic.com, 13 novembre 2018, en ligne : < https://www.clubic.com/alexa/actualite-847285-amazon-somme-transmettre-justice-enregistrement-echo-double-meurtre.html >.

la mesure où la demande de la transmission des enregistrements est formulée par la justice. Cette demande n'est pas systématique et concerne uniquement des faits particulièrement graves.

Pour tenter d'encadrer l'assistant vocal dans la collecte et le traitement des renseignements personnels, différentes dispositions législatives, constitutionnelles et internationales existent, dont les lois en matière de protection des renseignements personnels applicables aux entreprises privées. La jurisprudence a également été sollicitée pour tenter de faire évoluer le droit en interprétant ces dispositions au regard de l'évolution technologique afin de garantir leur effectivité.

B. La protection des renseignements personnels, une composante moderne de la vie privée

L'évolution technologique a contraint le juge à faire évoluer le droit à la vie privée pour maintenir l'effectivité des dispositions législatives et constitutionnelles les régissant notamment dans le cadre d'une utilisation massive des objets connectés dans le domicile de l'individu. Nous verrons que, pour y parvenir, le juge a d'abord mis au jour la notion de « vie privée informationnelle » avant de l'affiner avec l'aide de la doctrine pour mieux prendre en compte l'évolution socio-technologique de la société (1). Les lois qui en découlent ont permis de poser un cadre juridique plus précis aux entreprises afin de garantir la protection des renseignements personnels. Parmi ces balises, nous retrouvons certains principes fondamentaux que nous développerons ultérieurement (2).

1. Une protection constitutionnelle découlant du droit à la vie privée

Les garanties constitutionnelles du droit à la vie privée consacrées dans les chartes canadienne et québécoise constituent le fondement de la reconnaissance de la protection des renseignements personnels (a). L'évolution technologique a contraint le législateur à adopter un nouveau cadre juridique afin de mieux préserver le droit à la vie privée des individus. Cette construction du cadre juridique, passée par l'élaboration par le législateur de nouvelles lois propres à la protection des renseignements personnels, s'inspire notamment des textes internationaux (b).

a) Les dispositions constitutionnelles protégeant le droit à la vie privée

Le droit à la vie privée est un droit jouissant d'une protection à la fois au niveau national et au niveau international. Différents instruments juridiques internationaux consacrent explicitement un tel droit. Parmi ceux-ci, nous pouvons citer la Déclaration Universelle des Droits de l'Homme[152] (ci-après « DUDH »). Le droit à la vie privée est évoqué à l'article 12 et sa consécration dans la déclaration lui confère un caractère sacré en devenant l'un des fondements des droits de l'Homme[153]. Bien que la DUDH ne revêt pas de caractère contraignant, notamment envers les États non-signataires[154], le droit à la vie privée peut dans le cadre d'autres organisations internationales faire l'objet d'une obligation de respect lorsqu'un État souhaite y adhérer. Nous pouvons citer l'exemple de l'Union européenne. La Charte des droits fondamentaux de l'Union européenne[155] énonce à l'article 7 ce droit à la vie privée. L'adhésion à l'Union européenne se faisant uniquement si les conditions imposées, ou « critères de Copenhague »[156], sont respectées. Le traité sur l'Union européenne[157] prévoit parmi celles-ci la garantie par l'État candidat de la protection des droits de l'homme[158] énoncés dans la Charte, dont le respect de la vie privée.

Au Canada, différentes sources prévoient le droit à la vie privée. La Déclaration canadienne des droits énonce en son article premier le droit à la vie privée sous l'aspect du droit « à la vie, à la liberté, à la sécurité de la personne ainsi qu'à la jouissance de ses biens »[159]. Ce texte ne s'applique

[152] ORGANISATION DES NATIONS UNIES, *Déclaration Universelle des Droits de l'Homme,* Rés. AG 217 (III), Doc. Off. AG NU, 3e sess., supp. n°13, Doc. NU A/810 (1948).
[153] DETRAIGNE, Y., et ESCOFFIER, A.-M., *La vie privée à l'heure des mémoires numériques. Pour une confiance renforcée entre citoyens et société de l'information*, Rapport d'information n°441, senat.fr, 27 mai 2009, en ligne : <http://www.senat.fr/rap/r08-441/r08-441_mono.html#toc328 >.
[154] REY, B., *La vie privée à l'ère du numérique,* Lavoisier, coll. « Traitement de l'information », 2012, p.64.
[155] *Charte des droits fondamentaux de l'Union européenne*, 2000/C, journal officiel des Communautés européennes, 18 décembre 2000, 364/01. Elle dispose de la même valeur juridique que les traités, art. 6 alinéa 1er du Traité sur l'Union européenne.
[156] UNION EUROPEENNE, *Glossaire des synthèses : critères d'adhésion*, eur-lex.europa.eu, en ligne : < https://eur-lex.europa.eu/summary/glossary/accession_criteria_copenhague.html?locale=fr >.
[157] *Traité sur l'Union européenne,* version consolidée, C 326/13, 26 décembre 2012, journal officiel de l'Union européenne.
[158] Art. 2 et 49 du Traité sur l'Union européenne.
[159] *Déclaration canadienne des droits,* S.C. 1960, ch. 44.

toutefois que dans le champ des compétences fédérales[160]. Le droit à la vie privée est apparu avec le rapatriement de la Constitution en 1982[161]. La *Charte canadienne des droits et libertés*[162] (ci-après « la Charte canadienne ») prévoit implicitement le droit à la vie privée aux articles 7 et 8[163]. L'article 7 traite davantage des atteintes à la liberté, sécurité et à la vie de la personne par la justice[164]. L'article 8 consacre le droit à la vie privée à travers l'intégrité et la dignité de la personne en lui reconnaissant un droit à la sécurité[165]. Ce droit à la sécurité vaut également comme droit à la propriété puisqu'il est fait mention dans l'article des fouilles, perquisitions et des saisies, ce qui renvoie à l'idée d'une protection de la propriété privée, concept historique de la vie privée[166].

Au Québec, la *Charte des droits et libertés de la personne*[167] (ci-après « la Charte québécoise ») consacre explicitement le droit à la vie privée à son article 5, qui peut être complété par l'article 4. Cette disposition est complétée par celles du Code civil du Québec (ci-après le « C.c.Q. ». L'article 36 du C.c.Q. apporte certains éléments pouvant être considérés comme constituant une atteinte à la vie privée :

> « Peuvent être notamment considérés comme des atteintes à la vie privée d'une personne les actes suivants:

---

[160] PELLETIER, B., « Droit constitutionnel : la protection de la vie privée au Canada », revue juridique Thémis, 2001 35 R.J.T., p.490.
[161] THIBEAULT, A., *La surveillance électronique et métadonnées. Vers une nouvelle conception constitutionnelle du droit à la vie privée au Canada ?,* Mémoire de maîtrise, Université de Montréal, Mars 2015, en ligne : <https://papyrus.bib.umontreal.ca/xmlui/bitstream/handle/1866/12496/Thibeault_Alexandre_2015_memoire.pdf?sequence=2&isAllowed=y >, p.53.
[162] *Charte canadienne des droits et libertés*, Annexe B de la loi de 1982 sur le Canada (R-U), 1982, c 11.
[163] REITER, E. H., « Privacy and the Charter: Protection of people or places? », 2009, 88 R. du B. can., p.119 ; THIBEAULT, A., *La surveillance électronique et métadonnées. Vers une nouvelle conception constitutionnelle du droit à la vie privée au Canada ?,* Mémoire de maîtrise, Université de Montréal, Mars 2015, en ligne : <https://papyrus.bib.umontreal.ca/xmlui/bitstream/handle/1866/12496/Thibeault_Alexandre_2015_memoire.pdf?sequence=2&isAllowed=y > ; PELLETIER, B., « Droit constitutionnel : la protection de la vie privée au Canada », revue juridique Thémis, 2001 35 R.J.T., pp.504 et s.
[164] THIBEAULT, A., *La surveillance électronique et métadonnées. Vers une nouvelle conception constitutionnelle du droit à la vie privée au Canada ?,* Mémoire de maîtrise, Université de Montréal, Mars 2015, en ligne : <https://papyrus.bib.umontreal.ca/xmlui/bitstream/handle/1866/12496/Thibeault_Alexandre_2015_memoire.pdf?sequence=2&isAllowed=y > ; BROCHU, C., *Charte canadienne des droits et libertés,* LexisNexis, 2003.
[165] REITER, E. H., « Privacy and the Charter: Protection of people or places? », 2009, 88 R. du B. can., pp.122 et s. ; THIBEAULT, A., *La surveillance électronique et métadonnées. Vers une nouvelle conception constitutionnelle du droit à la vie privée au Canada ?,* Mémoire de maîtrise, Université de Montréal, Mars 2015, en ligne : <https://papyrus.bib.umontreal.ca/xmlui/bitstream/handle/1866/12496/Thibeault_Alexandre_2015_memoire.pdf?sequence=2&isAllowed=y >.
[166] *R* c. *Tessling,* 2004 CSC 67 (CanLII), [2004] 3 RCS 432, par. 16 ; BENYEKHLEF, K., *La protection de la vie privée dans les échanges internationaux d'informations,* Montréal, Thémis, 1993, p.39.
[167] *Charte des droits et libertés de la personne,* RLRQ c C-12.

> 1° Pénétrer chez elle ou y prendre quoi que ce soit;
> 2° Intercepter ou utiliser volontairement une communication privée;
> 3° Capter ou utiliser son image ou sa voix lorsqu'elle se trouve dans des lieux privés;
> 4° Surveiller sa vie privée par quelque moyen que ce soit;
> 5° Utiliser son nom, son image, sa ressemblance ou sa voix à toute autre fin que l'information légitime du public;
> 6° Utiliser sa correspondance, ses manuscrits ou ses autres documents personnels » (nos soulignements).

À la lecture de cet article, et plus particulièrement de son alinéa premier, nous comprenons que la liste énoncée n'est pas exhaustive. Le législateur renvoie donc au juge le soin d'y apporter les éléments nécessaires caractérisant une atteinte au droit à la vie privée.

Bien que la vie privée soit liée au bon fonctionnement de la société démocratique en étant indissociable de l'existence de l'individu et de l'exercice de ses droits et libertés[168], le droit à la vie privée est un droit ne bénéficiant pas d'une définition claire et précise. Comme le précisait le professeur Benyekhlef « […] la tentation de définir existe toujours, car beaucoup estiment que la simple énonciation du droit à la vie privée ne suffit pas pour assurer son respect »[169]. En effet, ni le législateur, ni la jurisprudence ne sont parvenus à l'heure actuelle à y apporter une définition permettant de mieux saisir cette notion. La jurisprudence européenne allant même jusqu'à affirmer que l'élaboration d'une définition ne saurait se faire au regard du caractère large de cette notion[170]. Cette position a été reconnue au Québec dans la décision *The gazette* c. *Valiquette* :

> « Qualifié comme l'un des droits les plus fondamentaux des droits de la personnalité (Duclos c. Aubry et Éditions Vice-Versa inc.), le droit à la vie privée échappe encore à une définition formelle »[171] (les soulignements sont dans l'original).

Cette absence de définition formelle tient à la « notion protéiforme » que constitue la vie privée[172]. Cet aspect protéiforme tend à compliquer la mise en place d'une véritable définition et confirme

---

[168] DETRAIGNE, Y., et ESCOFFIER, A.-M., *La vie privée à l'heure des mémoires numériques. Pour une confiance renforcée entre citoyens et société de l'information*, Rapport d'information n°441, senat.fr, 27 mai 2009, en ligne : <http://www.senat.fr/rap/r08-441/r08-441_mono.html#toc328 >.
[169] BENYEKHLEF, K., *La protection de la vie privée dans les échanges internationaux d'informations,* Montréal, Thémis, 1993, p.38.
[170] *Pretty c/ Royaume-Uni*, n°2346/03, §61, 29 avril 2002, CEDH.
[171] *The gazette* c. *Valiquette*, 1996 CanLII 6064 (QC CA).
[172] *R* c. *Tessling,* 2004 CSC 67 (CanLII), [2004] 3 RCS 432, par. 25.

dans le même temps que le droit à la vie privée n'est qu'une « constellation de valeurs concordantes et opposées de droits solidaires et antagonistes, d'intérêts communs et contraires » évoluant avec le temps et variant d'un milieu culturel à un autre »[173]. C'est en ce sens que l'honorable juge La Forest a jugé que :

> « (…) le droit général à la protection contre les fouilles, les perquisitions ou les saisies abusives garanti par l'art. 8 doit évoluer au rythme du progrès technologique et, par conséquent, nous assurer une protection constante contre les atteintes non autorisées à la vie privée »[174] (nos soulignements).

Cependant, le droit à la vie privée n'est pas un droit absolu[175]. Cette reconnaissance par l'honorable Michaud, juge en chef du Québec, confirme ce que l'honorable juge La Forest précisait :

> « Dans son commentaire fructueux sur le Quatrième amendement à la Constitution américaine, le professeur Amsterdam illustre admirablement cette situation en disant que, compte tenu du développement de la technologie moderne de l'écoute électronique, nous ne pouvons nous assurer d'être à l'abri de toute surveillance aujourd'hui que si nous nous retirons dans notre sous-sol, couvrons nos fenêtres, fermons les lumières et gardons un silence absolu »[176].

En d'autres termes, le droit à la vie privée ne constitue pas un droit inviolable, particulièrement à une époque où les technologies présentes dans notre quotidien sont de plus en plus gourmandes en renseignements personnels. En effet, il est admis par la jurisprudence que le droit à la vie privée « (…) est balisé par une série de limites et sa mise en œuvre appelle un équilibre avec d'autres droits fondamentaux »[177]. S'agissant de ces limites au droit à la vie privée, la Charte canadienne précise qu'elles doivent être issues d'une règle de droit et être raisonnables[178].

---

[173] *The gazette* c. *Valiquette*, 1996 CanLII 6064 (QC CA), reprenant le rapport du Rapport du Groupe d'étude, L'ordinateur et la vie privée, Ottawa, Ministère des Communications et de la Justice, 1972, p. 11 ; Voir VERONICA PEREZ ASINARI, M., et PALAZZI, P., *Défis du droit à la protection de la vie privée – Perspectives du droit européen et nord-américain,* Bruxelles, Brulyant, Cahiers du Centre de Recherches Informatiques et Droit, 2008.
[174] *R.* c. *Wong*, 1990 CanLII 56 (CSC), [1990] 3 RCS 36.
[175] *The gazette* c. *Valiquette*, 1996 CanLII 6064 (QC CA).
[176] *R*. c. *Wong*, 1990 CanLII 56 (CSC), [1990] 3 RCS 36 citant AMESTERDAM, A., G., *Perspectives on the Fourth Amendment*, (1974), 58 *Minn. L. Rev.* 848. p. 402.
[177] *The gazette* c. *Valiquette*, 1996 CanLII 6064 (QC CA).
[178] Art. 1er de la Charte canadienne.

La jurisprudence est venue compléter cette disposition dans la décision *Oakes*[179]. À travers cette décision, la Cour suprême a apporté des critères supplémentaires permettant d'apprécier le caractère raisonnable de l'atteinte à la vie privée. Ainsi, selon la Cour suprême l'atteinte peut se faire lorsqu'il existe un objectif réel et urgent et que des moyens proportionnels concourant à la réalisation de cet objectif portent une atteinte minime au droit visé.

Autrefois, il était question des atteintes à la vie privée impliquant des fouilles domiciliaires entraînant des saisies par les autorités compétentes. C'est dans ce contexte que le test de *Oakes* a été le plus souvent utilisé[180]. Il a été affirmé à propos du domicile que :

> « [l]e domicile est le lieu par excellence qui permet à tout individu d'exprimer sa personnalité de la façon qui lui convient, sans intrusion extérieure. Le domicile est le support physique de l'intimité de la personne humaine et, ne seraitce (sic) que pour cela, il doit être protégé. Nul ne doit y pénétrer sans y être invité »[181].

Lié historiquement au droit à la vie privée[182], le domicile constituait « l'ultime atteinte à la vie privée »[183]. Si la Cour suprême a estimé que l'article 8 de la Charte canadienne concerne également la personne, sa dignité et son intégrité[184], l'évolution de la société et l'émergence des technologies ont conduit le législateur et la jurisprudence à réadapter le droit à la vie privée, notamment en prenant en compte la protection des renseignements personnels. L'honorable juge La Forest a très justement rappelé qu'il n'existe plus à l'heure actuelle de véritable vie privée que si l'individu accepte de se couper physiquement et socialement du reste de la communauté[185].

---

[179] *R.* c. *Oakes*, 1986 CanLII 46 (CSC), [1986] 1 RCS 103.
[180] Nous verrons par la suite que cette jurisprudence a été reprise pour être appliquée au secteur privé et à la LPRPDE, voir partie II.B.2.c).ii.
[181] Ibid, par. 69.
[182] BENYEKHLEF, K., *La protection de la vie privée dans les échanges internationaux d'informations,* Montréal, Thémis, 1993, p.39.
[183] *R.* c. *Silviera*, [1995] 2 R.C.S. 297, par. 148.
[184] *Hunter et autres* c. *Southam inc.,* [1984] 2 R.C.S. 145 ; *R.* c. *Dyment* [1988] 2 R.C.S. 417 ; *R* c. *Tessling,* 2004 CSC 67 (CanLII), [2004] 3 RCS 432 ; PELLETIER, B., « Droit constitutionnel : la protection de la vie privée au Canada », revue juridique Thémis, 2001 35 R.J.T. ; THIBEAULT, A., *La surveillance électronique et métadonnées. Vers une nouvelle conception constitutionnelle du droit à la vie privée au Canada ?,* Mémoire de maîtrise, Université de Montréal, Mars 2015, en ligne : <https://papyrus.bib.umontreal.ca/xmlui/bitstream/handle/1866/12496/Thibeault_Alexandre_2015_memoire.pdf?sequence=2&isAllowed=y >.
[185] *R.* c. *Wong*, 1990 CanLII 56 (CSC), [1990] 3 RCS 36.

b) La reconnaissance de la protection des renseignements personnels comme une nouvelle dimension de la vie privée

Aujourd'hui, dans le cadre d'une société où l'information est qualifiée de « nouvel or noir numérique »[186] et face à la prolifération des technologies, la protection des renseignements personnels s'est avérée être essentielle afin de maintenir un certain degré de vie privée dans un environnement de plus en plus connecté.

Afin de définir la protection des renseignements personnels, il nous semble être pertinent de reprendre la définition apportée par M[es] Maria Veronica Perez Asinari et Pablo Palazzi. Ceux-ci définissent la protection des renseignements personnels comme étant une :

> « (…) garantie fondamentale nécessaire pour assurer, dans une société de l'information, le respect de l'ensemble des libertés tant individuelles que publiques et pour lutter contre tout risque de discrimination. Il s'agit d'offrir à l'individu une certaine maîtrise de son environnement informationnel et dès lors de la circulation de son image en même temps que de limiter les activités de traitement de l'information mises en place par les responsables de traitement tantôt, pour les personnes privées, au nom de leur liberté d'entreprendre ou d'association, tantôt pour l'État, au nom de l'intérêt général »[187] (nos soulignements).

Nous retrouvons les prémices de cette protection des renseignements personnels dans la jurisprudence de la Cour suprême. C'est ainsi que la Cour a jugé dans sa décision *R.* c. *Dyment* que la protection de l'information est consacrée au sein de la Charte canadienne des droits et libertés comme étant « (…) le droit à la vie privée en matière d'information »[188]. Et de rajouter concernant ce droit que :

---

[186] INSTITUT MONTAIGNE, *Big data et objets connectés : Faire de la France un champion de la révolution numérique,* Rapport, institutmontaigne.org, avril 2015, en ligne : <https://www.institutmontaigne.org/ressources/pdfs/publications/rapport%20objets%20connecte%CC%81s(2).pdf >, p.13.

[187] VERONICA PEREZ ASINARI, M., et PALAZZI, P., *Défis du droit à la protection de la vie privée – Perspectives du droit européen et nord-américain,* Bruxelles, Brulyant, Cahiers du Centre de Recherches Informatiques et Droit, 2008, p.41.

[188] *R.* c. *Dyment* [1988] 2 R.C.S. 417, par. 22 ; BENYEKHLEF, K., et TRUDEL, P., *Approches et stratégies pour améliorer la protection de la vie privée dans le contexte des inforoutes,* papyrus.bib.umontreal.ca, Mémoire présenté

> « (…) [d]ans la société contemporaine tout spécialement, la conservation de renseignements à notre sujet revêt une importance accrue. Il peut arriver, pour une raison ou pour une autre, que nous voulions divulguer ces renseignements ou que nous soyons forcés de le faire, mais les cas abondent où on se doit de protéger les attentes raisonnables de l'individu que ces renseignements seront gardés confidentiellement par ceux à qui ils sont divulgués, et qu'ils ne seront utilisés que pour les fins pour lesquelles ils ont été divulgués. Tous les paliers de gouvernement ont, ces dernières années, reconnu cela et ont conçu des règles et des règlements en vue de restreindre l'utilisation des données qu'ils recueillent à celle pour laquelle ils le font (…) »[189] (nos soulignements).

Dans la décision *R* c. *Plant*[190], la Cour suprême est venue préciser que l'intrusion dans des dossiers informatisés n'est pas susceptible de méconnaître l'article 8 de la *Charte des droits et libertés* lorsque les informations collectées ne portent pas sur la vie intime de la personne. La Cour suprême va même jusqu'à énoncer un certain nombre de facteurs à prendre en compte pour déterminer si nous sommes en présence d'une atteinte à la protection des renseignements personnels. C'est ainsi que :

> « (…) la nature des renseignements, celle des relations entre la partie divulguant les renseignements et la partie en réclamant la confidentialité, l'endroit où ils ont été recueillis, les conditions dans lesquelles ils ont été obtenus et la gravité du crime faisant l'objet de l'enquête, permet de pondérer les droits sociétaux à la protection de la dignité, de l'intégrité et de l'autonomie de la personne et l'application efficace de la loi »[191].

Dans cette même décision, la Cour apporte une nouvelle approche de l'attente raisonnable, celle du « biographical core », ou de « renseignements biographiques d'ordre personnel »[192]. Pour le professeur Benyekhlef cette approche se définit comme étant la faculté aux personnes de :

à la Commission de la culture de l'Assemblée nationale, Université de Montréal, Faculté de droit, Centre de recherche en droit public, 1997, en ligne : < https://papyrus.bib.umontreal.ca/xmlui/bitstream/handle/1866/71/0072.pdf?sequence=1&isAllowed=y >, p.14 ; Voir aussi BENYEKHLEF, K., « Les glissements du droit à la vie privée. De Feydeau à Facebook : de la comédie de mœurs à l'économie des données », dans V. GAUTRAIS, C. RÉGIS et L. LARGENTÉ (dir.), *Mélanges en l'honneur du professeur Patrick A. Molinari*, Montréal, Éditions Thémis, 2018, p.298.

[189] *R.* c. *Dyment* [1988] 2 R.C.S. 417, par. 22.

[190] *R.* c. *Plant*, 1993 CanLII 70 (CSC), [1993] 3 RCS 281.

[191] *R.* c. *Plant*, 1993 CanLII 70 (CSC), [1993] 3 RCS 281.

[192] Sur cette notion, voir THIBEAULT, A., *La surveillance électronique et métadonnées. Vers une nouvelle conception constitutionnelle du droit à la vie privée au Canada ?,* Mémoire de maîtrise, Université de Montréal, Mars 2015, en

> « (…) revendiquer une attente raisonnable en matière de vie privée informationnelle qu'à l'égard des renseignements personnels qui sont de nature biographique et qui révèlent des détails intimes sur leur mode de vie »[193].

Une telle prise de position par la Cour suprême, bien qu'elle ait pu rendre le concept de vie privée à une conception équivalente à « celle de la bourgeoisie du XIXe siècle »[194], peut sans doute s'expliquer par le manque d'anticipation des juges à l'égard de l'impact des technologies. Finalement, cette approche a fait l'objet d'une évolution par la Cour suprême[195], notamment en ce qui concerne la saisie et la fouille d'un téléphone intelligent[196] afin de prendre en compte l'impact du comportement des individus dans un monde davantage connecté. Une position qu'elle confirmera dans la décision *R.* c. *Fearon*, dont la juge Karakatsanis dissidente a déclaré :

> « Les appareils numériques personnels enregistrent non seulement nos renseignements biographiques, mais aussi nos conversations, nos photos, les sites sur le Web qui nous intéressent, les données concernant nos achats ainsi que nos loisirs. Notre empreinte numérique est souvent suffisante pour reconstituer les événements de notre vie, nos relations avec les autres, nos goûts et nos aversions, nos craintes, nos espoirs, nos opinions, nos croyances et nos idées. Nos appareils numériques sont en quelque sorte des fenêtres sur notre vie privée intérieure »[197].

Cette vie privée informationnelle[198] bénéficiera par la suite d'une protection renforcée par le législateur tant au fédéral qu'au provincial (i). La protection des renseignements personnels, pour

---

ligne :<https://papyrus.bib.umontreal.ca/xmlui/bitstream/handle/1866/12496/Thibeault_Alexandre_2015_memoire.pdf?sequence=2&isAllowed=y >, pp.77 et s.

[193] BENYEKHLEF, K., « Les glissements du droit à la vie privée. De Feydeau à Facebook : de la comédie de mœurs à l'économie des données », dans V. GAUTRAIS, C. RÉGIS et L. LARGENTÉ (dir.), *Mélanges en l'honneur du professeur Patrick A. Molinari*, Montréal, Éditions Thémis, 2018, p.299.

[194] BENYEKHLEF, K., « Les glissements du droit à la vie privée. De Feydeau à Facebook : de la comédie de mœurs à l'économie des données », dans V. GAUTRAIS, C. RÉGIS et L. LARGENTÉ (dir.), *Mélanges en l'honneur du professeur Patrick A. Molinari*, Montréal, Éditions Thémis, 2018, p.300.

[195] *R.* c. *Cole,* 2012 CSC 53 (CanLII), [2012] 3 RCS 34, par. 45 à 48.

[196] *R.* c. *Vu,* 2013 CSC 60 (CanLII), [2013] 3 RCS 657.

[197] *R.* c. *Fearon*, 2014 CSC 77 (CanLII), [2014] 3 RCS 621, par. 101 ; BENYEKHLEF, K., « Les glissements du droit à la vie privée. De Feydeau à Facebook : de la comédie de mœurs à l'économie des données », dans V. GAUTRAIS, C. RÉGIS et L. LARGENTÉ (dir.), *Mélanges en l'honneur du professeur Patrick A. Molinari*, Montréal, Éditions Thémis, 2018, p.306 ;

[198] *R.* c. *Dyment* [1988] 2 R.C.S. 417, par. 22 ; NADEAU, A-R., « La protection constitutionnelle de l'information : mythe ou réalité ? », dans *Développements récents en droit de l'accès à l'information (2002),* vol.173, service de la formation permanente du Barreau du Québec, 2002. ; REITER, E. H., « Privacy and the Charter: Protection of people or places? », 2009, 88 R. du B. can., p.129.

reprendre le terme moderne, est également consacrée comme principe fondamental dans certains textes juridiques internationaux et étrangers (ii).

i. Le cadre juridique de la protection des renseignements personnels au Québec et au Canada

Nous les avons évoqués tout au long de la première partie, différentes lois protégeant les renseignements personnels ont été adoptées au Québec et au Canada afin d'accompagner juridiquement l'évolution des technologies principalement dans le secteur privé.

Quelques mots doivent être dit au sujet de la *Loi sur la protection des renseignements personnels et des documents électroniques*[199]. Son principe étant de ne s'appliquer que dans les provinces n'ayant pas de loi spécifique portant sur le même champ d'application matériel[200]. À ce jour trois provinces disposent d'une loi en matière de protection de renseignements personnels essentiellement similaire à la LPRPDE[201], l'Alberta[202], la Colombie-Britannique[203] et le Québec[204]. Toutefois, il existe une exception à ce principe selon laquelle la LPRPDE continue malgré tout de s'appliquer dans ces provinces lorsque les transactions ont pour effet le transfert de renseignements personnels au-delà des frontières[205]. Pour être complet, nous ajouterons que cette loi s'applique également pour les entreprises fédérales telles que les banques, les sociétés de télécommunications

[199] *Loi sur la protection des renseignements personnels et les documents électroniques*, LC 2000, c 5.
[200] COMMISSARIAT A LA PROTECTION DE LA VIE PRIVEE, *Lois provinciales qui peuvent s'appliquer au lieu de la LPRPDE,* priv.gc.ca, mai 2020, en ligne : < https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/lois-sur-la-protection-des-renseignements-personnels-au-canada/la-loi-sur-la-protection-des-renseignements-personnels-et-les-documents-electroniques-lprpde/r_o_p/prov-lprpde/ >.
[201] Afin d'offrir une description complète des législations en matière de protection des renseignements personnels, nous mentionnerons seulement, car sans réel lien avec notre étude, que certaines provinces ont des lois protégeant uniquement les renseignements personnels dans le secteur de la santé ; Voir l'Ontario, *Loi de 2016 sur la protection des renseignements personnels sur la qualité des soins,* LO 2016, c 6, ann 2. ; Nouveau-Brunswick, *Loi sur l'accès et la protection en matière de renseignements personnels sur la santé,* LN-B. 2009, c P-7.05 ; Nouvelle-Ecosse, *Personal Health Information Act,* 2nd session, 61st General Assembly, Nova Scotia 59 Elizabeth II, 2010 ; Terre-Neuve-et-Labrador, *Personal Health Information Act*, SNL 2008, c P-7.01.
[202] *Personal Information Protection Act,* Statutes of Alberta, 2003, Chapter P-6.5.
[203] *Personal Information Protection Act,* Statutes of British-Columbia, 2003, Chapter 63.
[204] *Loi sur la protection des renseignements personnels dans le secteur privé,* RLRQ c P-39.1.
[205] COMMISSARIAT A LA PROTECTION DE LA VIE PRIVEE, *Survol de la LPRPDE,* priv.qc.ca, mai 2020, en ligne : < https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/lois-sur-la-protection-des-renseignements-personnels-au-canada/la-loi-sur-la-protection-des-renseignements-personnels-et-les-documents-electroniques-lprpde/r_o_p/prov-lprpde/ >.

et les compagnies de transport[206]. Pour la jurisprudence, la LPRPDE s'applique également aux entreprises présentes à l'étranger et dont le traitement à une incidence sur un citoyen canadien[207].

Si nous revenons vers le Québec, en plus de la LPRPSP, la province dispose dans son arsenal juridique de la *Loi concernant le cadre juridique des technologies de l'information*[208]. Cette loi novatrice en son temps se veut comme régulateur « [a]fin de clarifier l'applicabilité du régime juridique de droit commun aux documents électroniques et d'encadrer l'utilisation des TI (sic) »[209]. La cohérence du droit et son application aux technologies passent par la mise en place de plusieurs principes fondamentaux, à commencer par celui de la détermination du document, que nous avons examiné en première sous-partie. Le principe de la neutralité technologique « constitue une reconnaissance positive de la valeur juridique des documents sur support électronique »[210]. En vertu du principe, la valeur juridique d'un document doit être appréciée sans prendre en compte son support, technologique ou papier. L'équivalence fonctionnelle en constitue le corollaire de la neutralité technologique. Deux documents sur des supports différents mais ayant les mêmes informations pourront être interchangés à condition que l'intégrité de l'information soit préservée[211]. Pour vérifier l'intégrité du document, nous devons être en mesure de vérifier l'absence de toute altération de l'information et la fiabilité du support utilisé.

---

[206] COMMISSARIAT A LA PROTECTION DE LA VIE PRIVEE, *Lois provinciales qui peuvent s'appliquer au lieu de la LPRPDE,* priv.gc.ca, mai 2020, en ligne : < https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/lois-sur-la-protection-des-renseignements-personnels-au-canada/la-loi-sur-la-protection-des-renseignements-personnels-et-les-documents-electroniques-lprpde/r_o_p/prov-lprpde/ >.

[207] *A.T. v. Globle24h.*com, 2017 CF 114 (CanLII), [2017] 4 RCF 310 ; CAMERON, A., « La portée globale de la législation canadienne en matière de protection de la vie privée : décision clé rendue par la Cour fédérale dans l'affaire Globe24h », dans *Bulletin de la protection de l'information et de la vie privée,* fasken.com, 28 février 2017, en ligne : < https://www.fasken.com/fr/knowledge/2017/02/privacyandinformationprotectionbulletin-20170228/#overview >.

[208] *Loi concernant le cadre juridique des technologies de l'information*, RLRQ c C-1.1 ; Nous n'aborderons pas tous les principes énoncés par cette loi mais seulement ceux que nous estimons essentiels de les mentionner.

[209] DE RICO, J-F., et, JAAR, D., « Le cadre juridique des technologies de l'information », dans *Développements récents en droit criminel (2008)*, service de la formation continue du Barreau du Québec, 2008 ; Nous invitons le lecteur à consulter le site internet lccjti.ca dédié exclusivement à la *Loi concernant le cadre juridique des technologies de l'information* ; Pour approfondir, voir TRUDEL, P., *Introduction à la loi concernant le cadre juridique des technologies de l'information*, Cowansville, Édition Yvon Blais, 2012.

[210] DE RICO, J-F., et, JAAR, D., « Le cadre juridique des technologies de l'information », dans *Développements récents en droit criminel (2008)*, service de la formation continue du Barreau du Québec, 2008 ; Nous invitons le lecteur à consulter le site internet lccjti.ca dédié exclusivement à la *Loi concernant le cadre juridique des technologies de l'information*.

[211] DE RICO, J-F., et, JAAR, D., « Le cadre juridique des technologies de l'information », dans *Développements récents en droit criminel (2008)*, service de la formation continue du Barreau du Québec, 2008 ; Nous invitons le lecteur à consulter le site internet lccjti.ca dédié exclusivement à la *Loi concernant le cadre juridique des technologies de l'information* ; Art. 2838 du CcQ ; Arts. 17 et s. de la LCCJTI.

Toutefois, l'avènement des technologies et la capacité de traitement des renseignements personnels à distance, remettant en cause par le même fait l'existence de frontières interétatiques, ont conduit à ce que leur protection soit érigé en un principe internationalement reconnu par différents textes que les législateurs fédéral et provincial se sont inspirés.

ii. La consécration internationale de la protection des renseignements personnels

Si la première trace de la protection des renseignements personnels dans la doctrine remonte à l'article de Warren et Brandeis[212] en l'évoquant indirectement par le biais de la vie privée, c'est l'élaboration des *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel* de l'Organisation de coopération et de développement économiques (ci-après « OCDE ») de 1980[213] qui a permis de jeter les bases de la protection des renseignements personnels dans le monde. En effet, les principes énoncés sont considérés comme des principes fondamentaux étant donné le rôle joué par l'OCDE dans la régulation de l'économie mondiale et le consensus qui en est sorti de ces lignes directrices. D'ailleurs, l'OCDE précise dans la préface de ses lignes directrices que :

> « (…) les pays Membres de l'OCDE ont jugé nécessaire d'élaborer des lignes directrices qui permettraient d'harmoniser les législations nationales relatives à la protection de la vie privée et qui, tout en contribuant au maintien de ces droits de l'homme, empêcheraient que les flux internationaux de données ne subissent des interruptions. Ces lignes directrices sont l'expression d'un consensus sur des principes fondamentaux qui peuvent être intégrés à la législation nationale en vigueur ou servir de base à une législation dans les pays qui ne sont pas encore dotés »214 (nos soulignements).

---

[212] WARREN, S., D., et BRANDEIS, L., D., « The right to privacy », 15 December 1890, Harvard Law Review, Vol. 4, No. 5, en ligne : < https://www.jstor.org/stable/1321160?seq=1#metadata_info_tab_contents >.

[213] ORGANISATION DE COOPERATION ET DE DEVELOPPEMENT ECONOMIQUES, *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnels*, Paris, 23 septembre 1980, en ligne : <https://www.oecd.org/fr/internet/ieconomie/lignesdirectricesregissantlaprotectiondelaviepriveeetlesfluxtransfrontieresdedonneesdecaracterepersonnel.htm >.

[214] Ibid.

Nos lois en matière de protection des renseignements personnels reposent en grande partie sur ces textes internationaux issus d'un consensus entre les pays membres ce qui leur confère une certaine légitimité. C'est ainsi que les professeurs Benyekhlef et Trudel décrivent ces principes fondamentaux :

> « Ces principes fondamentaux constituent, en quelque sorte, l'architectonique des diverses lois nationales de protection des renseignements personnels. Bien que ces instruments puissent diverger au plan de leur structure et de leur portée, l'interprète peut remarquer qu'ils s'articulent, malgré tout, autour d'un ensemble de règles communes (noyau dur) »[215].

Ces lignes directrices ont fait l'objet d'une révision en 1992 et en 2013 afin de mieux prendre en compte l'évolution des technologies, sans pour autant en changer l'objectif. C'est ainsi que l'OCDE évoque ce changement, particulièrement en ce qui concerne la circulation transfrontalière des renseignements personnels :

> « When the 1980 Guidelines were drafted, data flows largely constituted discrete point-to-point transmissions between businesses or governments. Today, data can be processed simultaneously in multiple locations; dispersed for storage around the globe; re-combined instantaneously; and moved across borders by individuals carrying mobile devices. Services, such as "cloud computing", allow organisations and individuals to access data that may be stored anywhere in the world »[216].

L'OCDE a également adopté des lignes directrices en 1992. Les *Lignes directrices régissant la sécurité des systèmes d'information*[217] sont venues compléter celles de 1980 en ce qu'elles visaient à encadrer, non pas le traitement des renseignements personnels, mais la sécurité des systèmes

---

[215] BENYEKHLEF, K., et TRUDEL, P., *Approches et stratégies pour améliorer la protection de la vie privée dans le contexte des inforoutes,* papyrus.bib.umontreal.ca, Mémoire présenté à la Commission de la culture de l'Assemblée nationale, Université de Montréal, Faculté de droit, Centre de recherche en droit public, 1997, en ligne : <https://papyrus.bib.umontreal.ca/xmlui/bitstream/handle/1866/71/0072.pdf?sequence=1&isAllowed=y>, p.16.

[216] ORGANISATION DE COOPERATION ET DE DEVELOPPEMENT ECONOMIQUES, *Recommendation of the Council concerning guidelines governing the protection of privacy and transborder flows of personal data (2013)*, C(80 58/FINAL, amendé le 11 juillet 2013, C (2013) 79, en ligne : < http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf >, p. 29.

[217] ORGANISATION DE COOPERATION ET DE DEVELOPPEMENT ECONOMIQUES, *Lignes directrices régissant la sécurité des systèmes d'information*, OCD/GD (92) 190, Paris, 1992, en ligne : <http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=OCDE/GD(92)190&docLanguage=Fr >.

réalisant le traitement. Elles ont depuis fait l'objet d'une révision en 2002[218] puis en 2015 avec la *Recommandation du Conseil sur la gestion du risque de sécurité numérique pour la prospérité économique et sociale*[219]. Ces différentes révisions tendent à accompagner l'évolution des technologies et l'émergence de nouvelles préoccupations comme celui de protéger l'individu. La protection de la personne n'était pas prévue dans les premières lignes directrices de l'OCDE en 1992 alors que nous la retrouvons dans celles de 2015. Cette absence s'explique par l'utilisation de plus en plus croissante d'appareils connectés, plus particulièrement de leur prolifération dans la vie privée de l'individu. Nous remarquons toutefois que le principe de sensibilisation des employés demeure l'une des mesures de sécurité pour limiter la survenance d'un incident impliquant des renseignements personnels. Nous reviendrons sur ce point ultérieurement.

Toujours sur le plan international, l'Organisation des Nations Unies a également mis en place les *Principes directeurs pour la réglementation des fichiers informatisés contenant des données à caractère personnel*[220]. Cependant, ce texte international, tout comme ceux de l'OCDE, bien qu'ils soulignent la bonne volonté des États signataires de s'engager dans leur mise en place, ne disposent pas de caractère contraignant[221]. Et comme leur intitulé l'indique, il ne s'agit que de recommandations aux États plutôt que de véritables règles de droit. Leur portée juridique reste donc assez limitée.

En Europe, le Conseil de l'Europe[222] a été la première organisation internationale à mettre en place un véritable droit de la vie privée avec l'article 8 de la *Convention européenne des droits de*

---

[218] ORGANISATION DE COOPERATION ET DE DEVELOPPEMENT ECONOMIQUES, *Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'informations : vers une culture de la sécurité*, 1037e session, Conseil de l'OCDE, 25 juillet 2002, en ligne : <https://www.oecd.org/sti/ieconomy/15582260.pdf >.

[219] ORGANISATION DE COOPERATION ET DE DEVELOPPEMENT ECONOMIQUES, *Gestion du risque de sécurité numérique pour la prospérité économique et sociale : Recommandation de l'OCDE et document d'accompagnement,* oecd.org, Paris, 1er octobre 2015, en ligne : <https://www.oecd.org/fr/internet/ieconomie/DSRM_French_final_Web.pdf>.

[220] ORGANISATION DES NATIONS UNIES, *Principes directeurs pour la réglementation des fichiers informatisés contenant des données à caractère personnel*, Assemblée générale des Nations Unies, New York, 14 décembre 1990, résolution 45/95.

[221] REY, B., *La vie privée à l'ère du numérique,* Lavoisier, coll. « Traitement de l'information », 2012, p.64.

[222] Pour éviter une éventuelle confusion du lecteur avec le Conseil européen et le Conseil de l'Union européenne, le Conseil de l'Europe est une organisation internationale, ou régionale pour certains, au même titre que l'UE. Alors que le Conseil européen est un des principaux organes de l'UE. Il est composé des chefs d'États et de gouvernements des pays membres. Le Conseil de l'UE, autre organe de l'UE, également appelé « conseil des ministres » regroupe tous les ministres des pays membres de l'UE en fonction des domaines politiques à traiter.

l'homme et des libertés fondamentales[223], duquel découle la protection des renseignements personnels[224]. Le Conseil de l'Europe a également mis en place la *Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel*[225]. Cette convention, toujours en vigueur, est le premier véritable outil juridique international dédié à la protection des renseignements personnels puisqu'il revêt un caractère contraignant envers les États membres. À cet effet, son article 1er énonce que :

> « Le but de la présente Convention est de garantir, sur le territoire de chaque Partie, à toute personne physique, quelles que soient sa nationalité ou sa résidence, le respect de ses droits et de ses libertés fondamentales, et notamment de son droit à la vie privée, à l'égard du traitement automatisé des données à caractère personnel la concernant («protection des données») » (nos soulignements).

Adoptée un an après les lignes directrices de l'OCDE, cette convention, par son caractère contraignant, a permis de mettre en place une véritable culture de la protection des renseignements personnels en Europe, qui sera d'ailleurs imitée par l'Union européenne[226]. Au sein de l'Union européenne, la protection des renseignements personnels a d'abord été prévue à l'article 8 de la *Charte des droits fondamentaux de l'Union européenne*[227] :

> « 1. Toute personne a droit à la protection des données à caractère personnel la concernant.
> 2. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification.
> 3. Le respect de ces règles est soumis au contrôle d'une autorité indépendante ».

---

[223] *Convention européenne des droits de l'homme et des libertés fondamentales,* Rome, 4 XI 1950.
[224] VERONICA PEREZ ASINARI, M., et PALAZZI, P., *Défis du droit à la protection de la vie privée – Perspectives du droit européen et nord-américain,* Bruxelles, Brulyant, Cahiers du Centre de Recherches Informatiques et Droit, 2008, p.35.
[225] *Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel,* Conseil de l'Europe, *Série des traités européens n°108*, Strasbourg, 28.I.1981.
[226] AILINCAI, M., A., *Le règlement général sur la protection des données. Aspects institutionnels et matériels,* colloque de Rennes 1, *Différents standards européen de protection des données ? A propos du droit de l'Union européen et du droit du Conseil de l'Europe,* 16 novembre 2018, pp. 1-2.
[227] *Charte des droits fondamentaux de l'Union européenne*, Nice, 7 décembre 2000, 2000/C 364/01.

Cette disposition vient renforcer la législation de l'UE déjà existante, particulièrement la *Directive relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données*[228]. Cette directive visait à instaurer un cadre juridique au sein de l'UE qui soit équivalent à celui mis en place par la Convention européenne au sein du Conseil de l'Europe. La directive sera par la suite remplacée par le *Règlement Général sur la Protection des Données*[229]. Ce texte novateur apporte des obligations et des droits nouveaux que nous avons pu évoquer dans la sous-partie précédente, tel que le droit à l'oubli ou la prise en compte de la biométrie comme une donnée personnelle sensible[230].

S'agissant de la biométrie, la Directive de 1995 prévoyait seulement le traitement des données personnelles en lien avec la santé et la vie sexuelle de la personne. Les données biométriques n'étaient donc nullement mentionnées. Cette absence peut sans doute s'expliquer par le contexte d'adoption de ladite Directive de 1995. Celle-ci a été adoptée à une époque où la reconnaissance vocale n'était encore qu'à ses premiers balbutiements. La reconnaissance vocale n'offrait pas la même efficacité que celle d'aujourd'hui pour être déployée à grande échelle. Et surtout, le TALN n'était pas encore accessible au grand public. C'est ainsi que le RGPD définit la donnée biométrique comme étant :

> « les données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique […] »[231].

Nous ne retrouvons pas de disposition équivalente au RGPD au sein du corpus législatif fédéral[232]. Du moins explicitement, puisque le CPVP affirme que ces lois prévoient implicitement la

---

[228] *Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données*, 24 octobre 1995, Journal Officiel n° L281 du 23 novembre 1995, p.0031-0050.

[229] *Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE*, 27 avril 2016, Journal Officiel n° L 119/1 du 4 mai 2016.

[230] DE TERWANGNE, C., et ROSIER, K., (dir), *Le Règlement Général sur la Protection des Données (RGPD/GDPR) : Analyse approfondie,* coll. Crids, Larcier, 2018, p. 258.

[231] Art. 4 du RGPD.

[232] *Loi sur la protection des renseignements personnels et les documents électroniques,* L.C. 2000, ch. 5. ; *Loi sur la protection des renseignements personnels,* L.R.C. (1985), ch. P-21.

qualification de renseignement personnel car les données biométriques concourent à l'identification d'une personne physique[233]. S'il n'existe aucun définition précise de la donnée biométrique[234], au Québec, seule la CAI apporte quelques indications sur ses caractéristiques dans son rapport sur la biométrie. Ainsi, ce type de donnée se définirait par toutes « informations personnelles intimes sur la composition de notre corps et sur notre comportement en général »[235]. Cette définition vient compléter l'apport de l'article 44 de la LCCJTI évoquant seulement les « caractéristiques ou des mesures biométriques ». Une approche similaire à celle de la CAI se retrouve au sein de la *Freedom of Information and Protection of Privacy Act* de la province de l'Alberta qui définit la donnée biométrique comme étant une « information derived from an individual's unique measurable characteristics ; »[236].

Pourtant, l'interprétation faite par les autorités gouvernementales ne constitue qu'une ligne directrice n'ayant aucun effet contraignant. Bien que la position ne soit pas majoritaire au sein de la doctrine, certains auteurs, dont M^e^ Éloïse Gratton, estiment qu'une donnée biométrique n'est pas nécessairement un renseignement personnel[237], principalement lorsqu'elle fait l'objet de mesure de chiffrement par l'algorithme[238]. Cette affirmation se confirme quand un tel renseignement est pris isolément d'un autre, dont l'association contribuerait à l'identification de la personne[239]. Pour le Groupe de travail *Article 29,* « (…) measures of biometric identification or their digital translation

[233] COMMISSARIAT A LA PROTECTION DE LA VIE PRIVEE, *Des données au bout des doigts,* priv.gc.ca, février 2011, en ligne : < https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/renseignements-sur-la-sante-renseignements-genetiques-et-autres-renseignements-sur-le-corps/gd_bio_201102/ >. Nous précisons qu'au moment de la rédaction du présent mémoire, le CPVP a annoncé qu'une mise à jour de son orientation au sujet de la biométrie est en cours ; Voir également : COMMISSARAIT A LA PROTECTION DE LA VIE PRIVEE, *Résumé de conclusions d'enquête en vertu de la LPRPDE n°2004-281 : Une organisation utilise la biométrie à des fins d'authentification,* priv.gc.ca, 3 septembre 2004, en ligne : < https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2004/lprpde-2004-281/ >.

[234] GAUTHIER, J.M., *Cadre juridique de l'utilisation de la biométrie au Québec : sécurité et vie privée,* papyrus.bib.umontreal.ca, Mémoire de maîtrise, Avril 2014, Centre de recherche en droit public, Faculté de Droit, Université de Montréal, en ligne : <https://papyrus.bib.umontreal.ca/xmlui/bitstream/handle/1866/11879/Gauthier_Julie_Mira_2014_memoire.pdf?sequence=2&isAllowed=y >, p. 28.

[235] CHASSE, M., *La biométrie au Québec : les enjeux,* cai.gouv.ca, document d'analyse, Commission d'accès à l'information, juillet 2002, en ligne : < https://www.cai.gouv.qc.ca/documents/CAI_DRA_biometrie_enjeux.pdf>.

[236] Art. 1 (b.1) *Freedom of Information and Protection of Privacy Act*, Revised Statutes of Alberta 2000, chapter F-25.

[237] GRATTON, E., *Understanding Personal Information : managing Privacy Risk*, LexisNexis, 2013, p. 32.

[238] GRATTON, E., « Chronique - Qu'est-ce qu'un renseignement personnel ? Le défi de qualifier les nouveaux types de renseignements » dans *Repères*, Janvier 2013, Éditions Yvon Blais, 2013.

[239] *Gordon* c. *Canada* (Santé), 2008 CF 258.

in a template form in most cases are personal data »[240]. Dans ce même document de travail, le Groupe de travail semble allait dans le sens de Me Gratton en affirmant que :

> « In cases where biometric data, like a template, are stored in a way that no reasonable means can be used by the controller or by any other person to identify the data subject, those data should not be qualified as personal data »[241].

Le RGPD apporte également de nouveaux concepts que nous avons mentionné précédemment, celle de la protection des données dès la conception, ou « privacy by design », et par défaut, également appelée « privacy by default »[242]. Alors que la protection par défaut implique une application une fois le produit ou service accessible au public[243], la protection des renseignements personnels dès la phase de conception prend en compte la protection et du respect de la vie privée dès la conception du produit ou du service. Pour Ann Cavoukian, la notion de protection par défaut regroupe sept principes fondamentaux[244] :

> « Proactive not reactive ; Preventive not remedial
> Privacy as the default setting
> Privacy embedded into design
> Full functionality
> End-to-end security
> Visibility and transparency
> Respect for user privacy »[245].

Ceux-ci pourraient s'appliquer à l'assistant vocal en s'alliant avec les principes fondamentaux régissant le traitement des renseignements personnels afin d'offrir une meilleure garantie du respect de la vie privée.

---

[240] GROUPE DE TRAVAIL ARTICLE 29, *Document de travail sur la biométrie,* 12168/02/EN, WP80, adopté le 1 août 2003, en ligne : < https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp80_en.pdf >, p.5.
[241] Ibid.
[242] Art. 25 du RGPD.
[243] ANNONYME, « Qu'est-ce que le privacy by design ? », donnees-rgpd.fr, 7 mai 2019, en ligne : < https://donnees-rgpd.fr/definitions/privacy-by-design/ >.
[244] CAVOUKIAN, A., « Privacy by design: The 7 foundational principles », ipc.on.ca, Information & Privacy Commissioner, Ontario, en ligne : < https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf>.
[245] Voir supra partie I.A.2.b. ii.

2. Les principes fondamentaux de la protection des renseignements personnels

Après avoir évoqué les différentes législations nationales et internationales garantissant une protection des renseignements personnels, nous allons dès à présent détailler les principes fondamentaux. Pour se faire, nous allons nous appuyer sur les principes énumérés dans l'annexe 1 de la LPRPDE, qui sont généralement les mêmes dans les autres lois et autres textes internationaux. Nous évoquerons les principes contribuant à la transparence du traitement (a), dont la responsabilité, la transparence et la détermination de la finalité, du consentement (b), des limitations au traitement, de la collecte à la conservation (c) et des droits accordés aux individus (d).

a) Les principes garantissant la transparence et la sécurité du traitement des renseignements personnels

Parmi les principes concourant à l'effectivité de la sécurité dans le traitement des renseignements personnels et tendant à offrir une certaine transparence, nous retrouvons la responsabilité (i), seulement prévue par la LPRPDE. Or, ce principe à lui seul ne saurait suffire, le législateur impose également à l'entreprise de déterminer à l'avance les finalités de la collecte des renseignements personnels (ii) permettant à l'utilisateur de l'assistant vocal d'avoir toutes les informations nécessaires pour consentir ou non à leur traitement. Enfin, la sécurité du traitement passe par l'instauration de différentes mesures de sécurité tant techniques qu'administratives ou organisationnelles (iii).

i. La responsabilité

Le premier de ces principes est celui de la responsabilité de l'organisation recueillant et traitant les renseignements personnels : « Une organisation est responsable des renseignements personnels

dont elle a la gestion et doit désigner une ou des personnes qui devront s'assurer du respect des principes énoncés »[246] (notre soulignement) au sein de l'annexe 1. Cette personne a pour mission de veiller au bon respect par son entreprise de la LPRPDE. Cette personne est qualifiée de responsable de la confidentialité, ou *chief privacy officer.* Cette fonction ne doit pas être confondue avec celui de délégué à la protection des renseignements personnels, ou *data protection officer* (ci-après « DPO »), tel que prévu par le RGPD[247]. La différence porte :

> « The DPO is more a regulatory requirement. This is the person who makes sure we follow the law. The CPO is more a strategist, answering questions and creating solutions on how we can add value back into the business, how privacy can be a competitive advantage and how privacy can help build trust with our customers »[248].

Si l'on revient à notre principe de responsabilité, celui-ci est également applicable à l'entreprise lorsqu'elle confie à un tiers le traitement des renseignements personnels qu'elle a récolté[249], y compris lorsque ledit tiers se trouve à l'étranger[250]. Il est à noter que la LPRPSP ne prévoit à l'heure actuelle aucune disposition relative à l'obligation de nommer un responsable du traitement des

---

[246] Art. 4.1 de l'annexe 1, LPRPDE.
[247] Art. 37 et s. du RGPD.
[248] COSEGLIA, J., « Coffee with privacy pros : DPO vs CPO. Lawyer vs Technician. The dualities of privacy », cpomagazine.com, 3 janvier 2019, en ligne : < https://www.cpomagazine.com/data-privacy/coffee-with-privacy-pros-dpo-vs-cpo-lawyer-vs-technician-the-dualities-of-privacy/ >.
[249] COMMISSARIAT A LA PROTECTION DE LA VIE PRIVEE, *Bulletin d'interprétation : Responsabilité,* priv.gc.ca, avril 2012, en ligne : < https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/lois-sur-la-protection-des-renseignements-personnels-au-canada/la-loi-sur-la-protection-des-renseignements-personnels-et-les-documents-electroniques-lprpde/aide-sur-la-facon-de-se-conformer-a-la-lprpde/bulletins-sur-l-interpretation-de-la-lprpde/interpretations_02_acc/ >.
[250] COMMISSARIAT A LA PROTECTION DE LA VIE PRIVEE, *Résumé de conclusions d'enquête en vertu de la LPRPDE n° 2008-394 : l'impartition des services de courriel de canada.com à une entreprise établie aux États-Unis suscite des questions parmi les abonnés*, priv.gc.ca, 19 septembre 2008, en ligne : < https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2008/lprpde-2008-394/ > ; COMMISSARIAT A LA PROTECTION DE LA VIE PRIVEE, *Résumé de conclusions d'enquête en vertu de la LPRPDE n° 2007-365 : Responsabilité d'institutions financières canadiennes dans la communication de renseignements personnels par SWIFT aux autorités des États-Unis,* priv.gc.ca, 2 avril 2007, en ligne : <https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2007/lprpde-2007-365/ > ; COMMISSARIAT A LA PROTECTION DE LA VIE PRIVEE, *Résumé de conclusions d'enquête en vertu de la LPRPDE n° 2006-333 : Une entreprise canadienne communique les renseignements personnels de ses clients à la société mère située aux États-Unis*, priv.gc.ca, 19 juillet 2006, en ligne : < https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2006/lprpde-2006-333/ > ; COMMISSARIAT A LA PROTECTION DE LA VIE PRIVEE, *Résumé de conclusions d'enquête en vertu de la LPRPDE n° 2005-313 : Un avis expédié aux clients d'une banque suscite des inquiétudes à propos de la USA PATRIOT Act,* priv.gc.ca, 19 octobre 2005, en ligne : <https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2005/lprpde-2005-313/ >.

renseignements personnels[251]. À cet effet, la Commission d'accès à l'information recommande que :

> « [L]a Loi sur le privé [LPRPSP] soit modifiée de façon à ce qu'elle prévoie la création de la fonction de responsable de l'accès et de la protection des renseignements personnels dans le secteur privé. Elle recommandait également que cette fonction puisse être déléguée, en tout ou en partie, à toute personne œuvrant dans l'entreprise »[252].

Aussi, l'obligation de responsabilité offrirait la possibilité aux citoyens qu'ils :

> « (…) puissent connaître comment celles-ci assurent concrètement la protection des renseignements personnels qu'ils leur confient et, surtout, qu'ils puissent savoir à qui s'adresser dans l'entreprise en cas de question ou d'insatisfaction à ce chapitre. À l'heure actuelle, leur seul recours est de déposer une plainte à la Commission, alors qu'un appel à la personne responsable auprès de l'entreprise aurait pu, dans bien des circonstances, régler la situation »[253].

Au-delà même du fait que l'absence d'un DPO au sein d'une entreprise est de nature à maintenir une certaine opacité dans le traitement des renseignements personnels, la CAI risque d'être paralysée par les plaintes pour non-respect de la législation. Cette fonction permettrait de mettre en place un règlement à l'amiable contribuant à limiter les recours juridiques et d'encourager les entreprises à déployer des efforts afin de préserver une relation d'affaires avec le consommateur tout en adoptant une politique davantage responsable de la protection des renseignements personnels. L'instauration d'une telle obligation permettrait, toujours selon la CAI, de mieux garantir la transparence lors de la collecte et l'utilisation des renseignements personnels[254]. Aussi, elle rentrerait en adéquation avec l'article 25 de la LCCJTI prévoyant l'obligation de confidentialité pour le responsable de l'accès au document.

---

[251] COMMISSION D'ACCES A L'INFORMATION, *Protection des renseignements personnels*, cai.gouv.qc.ca, en ligne : < http://www.cai.gouv.qc.ca/entreprises/protection-des-renseignements-personnels-1/ > ; Nous rappelons toutefois au lecteur qu'au moment de rédiger ce développement, le projet de loi n°64 portant modernisation de la loi sur l'accès et de la LPRPSP prévoira une telle obligation.
[252] COMMISSION D'ACCES A L'INFORMATION, *Rétablir l'équilibre,* Rapport quinquennal, cai.gouv.qc.ca, 2016, en ligne : < http://www.cai.gouv.qc.ca/documents/CAI_RQ_2016.pdf >, p. 76.
[253] COMMISSION D'ACCES A L'INFORMATION, *Rétablir l'équilibre,* Rapport quinquennal, cai.gouv.qc.ca, 2016, en ligne : < http://www.cai.gouv.qc.ca/documents/CAI_RQ_2016.pdf >, p. 76.
[254] COMMISSION D'ACCES A L'INFORMATION, *Rétablir l'équilibre,* Rapport quinquennal, cai.gouv.qc.ca, 2016, en ligne : < http://www.cai.gouv.qc.ca/documents/CAI_RQ_2016.pdf >, p. 76.

Bien que l'obligation de responsabilité ne soit pas prévue dans la LPRPSP, celle-ci prévoit tout de même celle de désigner un agent de renseignements personnels (ci-après « ARP »). L'ARP a pour rôle d'accueillir les demandes de personnes souhaitant exercer leurs droits d'accès et de rectification des renseignements personnels dont l'entreprise de l'ARP visée détient. Cette fonction se distingue de celle de DPO puisqu'il ne se contente pas d'assurer la conformité de son entreprise à la législation protégeant les renseignements personnels. Nous ne rentrerons pas davantage dans les conditions de mise en place de l'ARP[255] car non nécessaire à notre développement.

ii. La détermination de la finalité de la collecte et le principe de la transparence

Le deuxième principe est celui de la détermination de la finalité de la collecte. Avant de pouvoir collecter les renseignements personnels, l'entreprise doit porter à la connaissance de la personne les finalités qu'elle entend atteindre en traitant ses renseignements personnels. Ce principe de finalité est à la fois prévu à l'article 4.2 de l'annexe 1 de la LPRPDE et de manière moins évidente au sein de l'article 4 de la LPRPSP. Selon la LPRPDE, la détermination peut avoir lieu avant ou au moment de la collecte[256]. À titre de comparaison avec la LPRPDE, la LPRPSP prévoit que :

> « Toute personne qui exploite une entreprise et qui, en raison d'un intérêt sérieux et légitime, peut constituer un dossier sur autrui doit, lorsqu'elle constitue le dossier, inscrire son objet.
> Cette inscription fait partie du dossier »[257] (nos soulignements).

Le fait pour une entreprise de porter à la connaissance de l'individu les finalités qu'elle entend atteindre avec la collecte de ses renseignements personnels concourt à un certain degré de transparence de sa part. En effet, ce principe implique qu'une entreprise fasse « en sorte que des renseignements précis sur ses politiques et ses pratiques concernant la gestion des renseignements

[255] La désignation et le rôle de l'agent de renseignements personnels sont prévus aux articles 70 et s. de la LPRPSP.
[256] Art. 4.2 de l'annexe 1, *Loi sur la protection des renseignements personnels et les documents électroniques*¸ LC 2000, c 5.
[257] Art. 4, *Loi sur la protection des renseignements personnels dans le secteur privé,* RLRQ c P-39.1.

personnels soient facilement accessibles à toute personne »[258]. Ce principe contribue également à prévenir toute banalisation dans l'utilisation des renseignements en dehors des finalités pour lesquelles ils ont été collectés[259].

Toutefois, la simple publication par une entreprise d'informations peu précises quant à la finalité recherchée ne suffit pas pour satisfaire à ce critère de transparence. Selon le CPVP, l'information doit être suffisante pour avoir une idée précise du traitement[260], disponible[261] et rédigée en des termes claires et compréhensible[262] sur la manière dont l'entreprise assure la protection de la vie privée de l'individu.

iii. La mise en place de mesure de sécurité

L'instauration de mesures de sécurité est une obligation prévue à l'article 10 de la LPRPSP et au principe 4.7 de l'annexe 1 de la LPRPDE. Nous précisons que l'article 10.1 (1) de la loi fédérale impose à l'entreprise de déclarer toute atteinte aux mesures de sécurité pouvant entraîner un risque réel de préjudice grave à l'individu[263].

[258] Art. 4.8, de l'annexe 1, LPRPDE.
[259] DUASO CALES, R., *Principe de finalité, protection des renseignements personnels et secteur public : étude sur la gouvernance des structures en réseau,* papyrus.bib.umontreal.ca, Thèse de doctorat, Faculté de Droit, Université de Montréal, Université Panthéon-Assas II, 2011, en ligne : < https://papyrus.bib.umontreal.ca/xmlui/bitstream/handle/1866/12714/Duaso_Cales_Rosario_2011_these.pdf?sequence=2&isAllowed=y >, p.15.
[260] COMMISSARIAT A LA PROTECTION DE LA VIE PRIVEE, *Rapport des conclusions d'enquête en vertu de la LPRPDE n°2013-001 : Enquête sur les pratiques de traitement des renseignements personnels de WhatsApp inc.,* priv.gc.ca, 15 janvier 2013, en ligne : < https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2013/lprpde-2013-001/ >.
[261] COMMISSARIAT A LA PROTECTION DE LA VIE PRIVEE, *Résumé de conclusions d'enquête en vertu de la LPRPDE n°2006-348 : Communication inappropriée d'un diagnostic, mais la compagnie d'assurances maintient que ses politiques et ses pratiques concernant la protection des renseignements personnels sont transparentes,* priv.gc.ca, 14 août 2006, en ligne : < https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2006/lprpde-2006-348/ >.
[262] *Englander* c. *TELUS Communication Inc.,* 2004 CAF 287 ; COMMISSARIAT A LA PROTECTION DE LA VIE PRIVEE, *Rapport des conclusions d'enquête en vertu de la LPRPDE n°2013-003 : Des profils affichés sur le site de rencontre PositiveSingles.com se retrouvent sur d'autres sites Web de rencontres affiliés,* priv.gc.ca, 11 juillet 2013, en ligne : < https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2013/lprpde-2013-003/ >.
[263] Nous reviendrons sur cet article dans la partie II.B.2 sur l'obligation de notification des incidents de sécurité.

Ces dispositions énoncent explicitement l'obligation d'adopter des mesures de sécurité en fonction de la nature du renseignement personnel. L'utilisation de verbe « devoir » sous-entend que ce principe renferme une obligation de résultat[264]. L'annexe 1 de la LPRPDE apporte davantage de précision sur la mise en place de telles mesures de sécurité. C'est ainsi que l'article 4.7.3 prévoit des moyens d'ordre matériel, des mesures administratives et techniques. Et de rajouter la sensibilisation du personnel de l'entreprise comme mesure de sécurité efficace lorsque l'entreprise leur apporte une formation appropriée[265]. Le RGPD adopte une approche comparable en évoquant des mesures « techniques et organisationnelles »[266]. Parmi ces mesures de sécurité qu'une entreprise peut instaurer, et qui rejoint le principe de limitation de la collecte, celle de ne pas recueillir des renseignements personnels inutiles[267]. Dans le cas de la collecte d'un renseignement inapproprié à la finalité voulue ou effectuée par erreur, l'entreprise doit toutefois le conserver avant de le détruire selon la procédure qu'elle s'est fixée et tout en respectant le cadre légal[268].

La jurisprudence est également venue apporter quelques précisions sur l'interprétation à adopter des mesures de sécurité. Celle-ci a jugé que le bien-fondé de la mesure de sécurité doit être apprécié au regard du contexte d'utilisation des renseignements personnels et non pas en fonction de l'émergence de nouvelles techniques de sécurité[269]. En d'autres termes, les mesures de sécurité

---

[264] VERMEYS, N., W., *Responsabilité civile et sécurité informationnelle,* Cowansville, Yvon Blais, 2010, p. 107.
[265] COMMISSARIAT A LA PROTECTION DE LA VIE PRIVEE, *Rapport de conclusions d'enquêtes en vertu de la LPRPDE n°2011-001 : La collecte de données Wi-Fi par Google Inc.,* priv.gc.ca, 20 mai 2011, en ligne : < https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2011/lprpde-2011-001/ > ; COMMISSARIAT A LA PROTECTION DE LA VIE PRIVEE, *Rapport de conclusions d'enquêtes en vertu de la LPRPDE n°2012-009 : Des renseignements personnels sont communiqués sans consentement dans un message téléphonique laissé sur le lieu de travail d'une cliente,* priv.gc.ca, 8 août 2012, en ligne : < https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2012/lprpde-2012-009/ > ; COMMISSARIAT A LA PROTECTION DE LA VIE PRIVEE, *Résumé de conclusions d'enquête en vertu de la LPRPDE n°2002-54 : Un couple prétend qu'il y a eu communication inappropriée de leur dossier téléphonique à un tiers,* priv.gc.ca, 28 juin 2002, en ligne : < https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2002/lprpde-2002-054/ >.
[266] Art. 5 du RGPD.
[267] COMMISSARIAT A LA PROTECTION DE LA VIE PRIVEE, *Rapport de conclusions d'enquête en vertu de la LPRPDE n°2007-389 : TJX Companies Inc./ Winners Merchant International L.P.,* priv.gc.ca, 25 septembre 2007, en ligne : < https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2007/tjx_rep_070925/ >.
[268] COMMISSARIAT A LA PROTECTION DE LA VIE PRIVEE, *Rapport de conclusions d'enquêtes en vertu de la LPRPDE n°2011-001 : La collecte de données Wi-Fi par Google Inc.,* priv.gc.ca, 20 mai 2011, en ligne : < https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2011/lprpde-2011-001/ >.
[269] *Turner* c. *Telus Communications Inc.,* 2005 CF 1601 (CanLII).

doivent être proportionnelles à la sensibilité du renseignement faisant l'objet de la protection[270]. S'agissant des renseignements biométriques, selon le CPVP leur sensibilité dépendra du type de renseignements que l'entreprise entend collecter et de la technologie qui sera utilisée[271].

Nous constatons que les apports du CPVP sont considérables dans l'interprétation de ce principe alors même qu'ils sont quasi-inexistants du côté de la CAI en raison d'une absence d'obligation de notifier les incidents de sécurité ce qui laisse la libre discrétion aux entreprises de s'y soumettre[272]. Par conséquent, la CAI ne peut effectuer aucun suivi fiable des incidents et émettre des recommandations permettant de les prévenir.

b) Le consentement, un principe central dans la protection des renseignements personnels

Nous l'avons évoqué à de nombreuses reprises au sein de la précédente partie, le consentement « moteur de la protection des renseignements personnels »[273], est l'élément déclencheur du traitement des renseignements personnels[274]. Plus généralement, le consentement désigne un « accord de deux ou plusieurs volontés en vues de la conclusion d'un acte juridique »[275]. Sa présence centrale dans le principe de l'autonomie de la volonté[276] témoigne de l'importance qui lui

---

[270] COMMISSARIAT A LA PROTECTION DE LA VIE PRIVEE, *Rapport de conclusions d'enquêtes en vertu de la LPRPDE n°2014-003 : Une compagnie d'assurance révise ses mesures de sécurité à la suite d'une atteinte à la vie privée*, priv.gc.ca, 3 mars 2014, en ligne : < https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2014/lprpde-2014-003/ > ; COMMISSARIAT A LA PROTECTION DE LA VIE PRIVEE, *Rapport de conclusions d'enquêtes en vertu de la LPRPDE n°2012-009 : Des renseignements personnels sont communiqués sans consentement dans un message téléphonique laissé sur le lieu de travail d'une cliente*, priv.gc.ca, 8 août 2012, en ligne : < https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2012/lprpde-2012-009/ >.

[271] COMMISSARAIT A LA PROTECTION DE LA VIE PRIVEE, *Résumé de conclusions d'enquête en vertu de la LPRPDE n°2004-281 : Une organisation utilise la biométrie à des fins d'authentification,* priv.gc.ca, 3 septembre 2004, en ligne : < https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2004/lprpde-2004-281/ >.

[272] COMMISSION D'ACCES A L'INFORMATION, *Rétablir l'équilibre,* Rapport quinquennal, cai.gouv.qc.ca, 2016, en ligne : < http://www.cai.gouv.qc.ca/documents/CAI_RQ_2016.pdf >, pp.106-107.

[273] COMMISSION D'ACCES A L'INFORMATION, *Rétablir l'équilibre,* Rapport quinquennal, cai.gouv.qc.ca, 2016, en ligne : < http://www.cai.gouv.qc.ca/documents/CAI_RQ_2016.pdf >, p.89.

[274] CHASSIGNEUX, C., « Consentement manifeste et éclairé : politique de confidentialité sur Internet », 26 avril 2012, actes du 20e congrès AAPI 2012, Commission d'accès à l'information du Québec.

[275] CAIJ, « JurisBistro eDictionnaire : Dictionnaire de droit québécois et canadien, Consentement », dictionnaire.caij.qc.ca, édition révisée 2016, en ligne : <https://dictionnairereid.caij.qc.ca/recherche#q=consentement&t=edictionnaire&sort=relevancy&m=search >.

[276] LAZARO, C., et LE METAYER, D., « Le consentement au traitement des données personnelles : Perspective comparative sur l'autonomie du sujet », (2014) 48 RJTUM 765-815, 2014, p.787.

est accordé. Il constitue le point de départ de l'application du droit des obligations aux parties du contrat[277].

L'engagement contractuelle d'une personne est encadré par le droit des obligations. Tout d'abord, un mineur non émancipé[278] et un majeur protégé, sous curatelle[279] ou tutelle[280] ne pourront pas donner leur consentement. Lorsque ces conditions sont respectées, la personne capable de consentir doit ensuite être en mesure de le fournir en toute connaissance de cause. Ainsi, le consentement doit être à la fois libre, éclairé et réfléchi[281]. En d'autres termes, il s'agit d'apporter au cocontractant toutes les informations nécessaires lui permettant d'apprécier les risques probables et significatifs pouvant survenir lors de l'exécution du contrat[282]. Mais également pour éviter qu'une décision ne soit prise « sous l'effet de techniques de vente fort persuasives, sinon critiquables »[283], notamment par une personne vulnérable[284].

Ces conditions et le principe d'autonomie individuelle[285] se retrouvent d'ailleurs au sein de la *Loi sur la protection des renseignements personnels dans le secteur privé*[286]. En effet, l'article 14 de la loi précise que :

> « Le consentement à la collecte, à la communication ou à l'utilisation d'un renseignement personnel doit être manifeste, libre, éclairé et être donné à des fins spécifiques. Ce consentement ne vaut que pour la durée nécessaire à la réalisation des fins pour lesquelles il a été demandé.
> Un consentement qui n'est pas donné conformément au premier alinéa est sans effet » (nos soulignements).

[277] Ibid.
[278] Art. 153 du Code civil du Québec.
[279] Art. 281 et s. du Code civil du Québec.
[280] Art. 285 et s. du Code civil du Québec.
[281] BAUDOUIN, J-L., JOBIN, P-G., et al., *Les obligations,* 7e édition, Éditions Yvon Blais, 2013.
[282] Ibid.
[283] Ibid.
[284] Ibid.
[285] GUILMAIN, A., et GRATTON, E. « La protection des renseignements personnels dans le secteur privé au Québec : rétrospectives et perspectives », dans *Développements récents en droit à la vie privée (2019)*, vol. 465, service de la formation continue, Barreau du Québec, Montréal, Edition Yvon Blais, 2019, p.83.
[286] *Loi sur la protection des renseignements personnels dans le secteur privé,* RLRQ c P-39.1.

Quelques mots méritent d'être dit au sujet des conditions du consentement au regard de la LPRPSP. Pour M[e] Cynthia Chassigneux, le consentement doit être donné de manière non équivoque (manifeste) en l'absence de toute contrainte (libre) suivant des informations préalables (éclairé) relatives aux objectifs poursuivis (fins spécifiques) par le traitement de ses renseignements personnels[287].

À la différence de l'Union européenne où le consentement ne représente qu'une des six bases juridiques au traitement des renseignements personnels[288], au Canada, le consentement est l'unique base juridique à la licéité du traitement. Si le RGPD ne prévoit qu'un consentement explicite de la personne, il semblerait que l'annexe 1 de la LPRPDE autorise le recours à un consentement implicite :

> « 4.3.4
> La forme du consentement que l'organisation cherche à obtenir peut varier selon les circonstances et la nature des renseignements. Pour déterminer la forme que prendra le consentement, les organisations doivent tenir compte de la sensibilité des renseignements »[289] (nos soulignements).

Si le Commissariat à la protection de la vie privée reconnaît que le consentement explicite « est la forme de consentement la plus adéquate et respectueuse à utiliser dans toutes les circonstances »[290], le consentement implicite reste une option « acceptable dans des circonstances strictement

[287] CHASSIGNEUX, C., « Consentement manifeste et éclairé : politique de confidentialité sur Internet », 26 avril 2012, actes du 20[e] congrès AAPI 2012, Commission d'accès à l'information du Québec ; Voir également, COMMISSION D'ACCES A L'INFORMATION, *Rétablir l'équilibre,* Rapport quinquennal, cai.gouv.qc.ca, 2016, en ligne : < http://www.cai.gouv.qc.ca/documents/CAI_RQ_2016.pdf >, p.91.
[288] En vertu de l'article 6 du RGPD, les bases juridiques de la licéité du traitement sont : le consentement, l'exécution d'un contrat conclu par la personne concernée, application d'une obligation légale, nécessité de sauvegarde des intérêts vitaux de la personne, exécution d'une mission d'intérêt public, nécessité aux fins des intérêts légitimes poursuivis par le responsable du traitement.
[289] Art. 4.3.4 de l'annexe 1 de la LPRPDE.
[290] COMMISSARIAT A LA PROTECTION DE LA VIE PRIVEE, *Résumé de conclusions d'enquêtes en vertu de la LPRPDE n°2003-192 : Une banque n'obtient pas le consentement explicite de ses clients pour communiquer leurs renseignements personnels,* priv.gc.ca, 23 juillet 2003, en ligne : < https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2003/lprpde-2003-192/ > ;
COMMISSARIAT A LA PROTECTION DE LA VIE PRIVEE, *Résumé de conclusions d'enquête en vertu de la LPRPDE n°2003-203 : Un particulier laisse percer ses inquiétudes quant aux clauses de consentement sur un formulaire de demande de carte de crédit*, priv.gc.ca, 5 août 2003, en ligne : < https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2003/lprpde-2003-203/ >.

définies »[291]. M[es] Guilmain et Gratton estiment que le consentement implicite pourra être accepté dans le cadre des finalités essentielles à la collecte des renseignements personnels. Les entreprises doivent aussi permettre à l'individu de retirer son consentement pour ces fins secondaires. Le consentement explicite serait selon eux plus approprié pour les finalités non essentielles à la collecte[292]. Il s'agit, entre autres, des fins de marketing ou de sondage[293] résultant d'un achat d'un bien ou d'un service.

Ces propos doivent être nuancés dans la mesure où lesdites consentements, explicites et implicites, ne concernent que le recueil de renseignements personnels « classique ». Dans notre présent cas, et comme nous l'avons évoqué dans la partie précédente, la voix est qualifiée de renseignement personnel sensible[294]. Cette sensibilité a entrainé une contrainte dans l'obtention du consentement pour ces renseignements personnels. C'est ainsi que la LPRPDE dispose que « [e]n général, l'organisation devrait chercher à obtenir un consentement explicite si les renseignements sont susceptibles d'être considérés comme sensibles »[295]. Nous retrouvons une disposition similaire à l'article 10 de la LPRPSP. D'ailleurs le Commissariat à la protection de la vie privée a estimé que le consentement explicite était exigé de l'individu dans le cadre de la publicité ciblée découlant d'une activité de recherche en ligne sur des sites de santé[296]. Le CPVP rajoute qu'une personne raisonnable ne s'attendra pas à ce qu'une entreprise adapte la publicité en fonction des informations issus des renseignements personnels, notamment sensibles, recueillis sans son consentement explicite[297].

---

[291] Ibid.
[292] GUILMAIN, A., et GRATTON, E. « La protection des renseignements personnels dans le secteur privé au Québec : rétrospectives et perspectives », dans *Développements récents en droit à la vie privée (2019)*, vol. 465, service de la formation continue, Barreau du Québec, Montréal, Edition Yvon Blais, 2019, p.84.
[293] GUILMAIN, A., et GRATTON, E. « La protection des renseignements personnels dans le secteur privé au Québec : rétrospectives et perspectives », dans *Développements récents en droit à la vie privée (2019)*, vol. 465, service de la formation continue, Barreau du Québec, Montréal, Edition Yvon Blais, 2019, p.84.
[294] Voir supra I.A.3.b). i. dans laquelle nous mentionnons l'absence de définition dans les lois canadiennes et québécoises en matière de protection des renseignements personnels.
[295] Principe 4.3.6, Annexe 1, LPRPDE.
[296] COMMISSARIAT A LA PROTECTION DE LA VIE PRIVEE, *Rapport des conclusions en vertu de la LPRPDE n°2014-001 : L'utilisation par Google de renseignements sensibles sur l'état de santé aux fins de l'affichage de publicités ciblées soulève des préoccupations en matière de vie privée,* priv.gc.ca, 14 janvier 2014, en ligne : <https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2014/lprpde-2014-001/ >.
[297] COMMISSARIAT A LA PROTECTION DE LA VIE PRIVEE, *Résumé de conclusions d'enquêtes en vertu de la LPRPDE n°2002-42 (mise à jour) : Air Canada permet à 1% des membres Aéroplan de se « désister » des pratiques de partage d'information,* priv.gc.ca, 11 mars 2002, en ligne : < https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2002/lprpde-2002-042/ >.

Enfin pour terminer sur le principe du consentement, en vertu de la LPRPDE, et de son principe 4.3.8, l'utilisateur doit pouvoir tout au long du traitement de ses renseignements personnels garde la faculté de retirer son accord. Cette disposition n'est pas prévue par la LPRPSP. Néanmoins, celle-ci dispose que : « [c]e consentement ne vaut que pour la durée nécessaire à la réalisation des fins pour lesquelles il a été demandé »[298].

c) Les différentes limitations au traitement des renseignements personnels

Ces limitations se traduisent par deux principes. Tout d'abord l'entreprise doit se limiter dans la collecte des renseignements personnels à ceux qui lui sont nécessaires pour atteindre les finalités recherchées (i). Ensuite, elle ne doit se contenter d'utiliser que les renseignements collectés et limiter leur communication à des tiers. Enfin, la limitation de la collecte entraîne également une limitation dans la conservation puisque l'entreprise ne garderait que les renseignements personnels utiles (ii). Une telle pratique préviendrait la collecte et l'utilisation de renseignements inutiles, ce qui augmenterait les risques d'atteintes.

i. La limitation de la collecte, ou le critère de « nécessité »

La limitation de la collecte, ou de nécessité, est un principe qui :

> « [O]blige les entreprises à ne collecter que les renseignements personnels qui sont nécessaires à l'atteinte des fins visées par le traitement de ces renseignements et à effectuer cette collecte par le biais de moyens licites »[299].

[298] Art. 14, LPRPSP.
[299] DEZIEL, P-L., « Est-ce bien nécessaire ? Le principe de limitation de la collecte face aux défis de l'intelligence artificielle et des données massives », dans *Développements récents en droit de la vie privée (2019),* service de la formation continue du Barreau du Québec, 2019.

Ce principe est consacré dans l'annexe 1 de la LPRPDE comme étant le quatrième principe dans la protection des renseignements personnels. Son importance est d'ailleurs rappelée au point 4.4.3 de l'annexe 1 :

> « Ce principe est étroitement lié au principe de détermination des fins auxquelles la collecte est destinée (article 4.2) et à celui du consentement (article 4.3) ».

La LPRPSP évoque quant à elle la nécessité au sein de l'alinéa 1er de l'article 5 :

> « La personne qui recueille des renseignements personnels afin de constituer un dossier sur autrui ou d'y consigner de tels renseignements ne doit recueillir que les renseignements nécessaires à l'objet du dossier » (nos soulignements).

L'absence d'une définition claire et précise de la notion même de « nécessité » nous amène à nous référer à celle donner par l'Office de la langue française comme étant le : « [c]aractère de ce dont on absolument besoin »[300]. Ce manque de précision a poussé la CAI à intervenir pour tenter d'encadrer davantage ce principe.

Très tôt la Commission d'accès à l'information a adopté une approche stricte et littérale de la « nécessité »[301] du renseignement personnel en l'assimilant à quelque chose « d'indispensable »[302], « d'essentiel » ou même « primordial »[303]. Cette interprétation stricte et

---

[300] OFFICE QUEBECOIS DE LA LANGUE FRANCAISE, « Grand dictionnaire terminologique : nécessité », gdt.oqlf.gouv.qc.ca, 1974, en ligne : < http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=17584339>.

[301] DEZIEL, P-L., « Est-ce bien nécessaire ? Le principe de limitation de la collecte face aux défis de l'intelligence artificielle et des données massives », dans *Développements récents en droit de la vie privée (2019),* service de la formation continue du Barreau du Québec, 2019.

[302] *Syndicat des employées et employés professionnels et de bureau, section locale 57 et Caisse populaire St-Stanislas de Montréal*, 1998 CanLII 27651 (QC SAT) ; *Bellerose c. Université de Montréal,* [1986] C.A.I. 109 ; GRANOSIK, L., « Le critère de nécessité, dans Les 20 ans de la loi sur la protection des renseignements personnels », dans *Les 20 ans de la Loi sur la protection des renseignements personnels dans le secteur privé (2014)*, Vol. 392, service de la formation continue, Barreau du Québec, Cowansville, Yvon Blais, 2014, p.87.

[303] *Regroupement des comités logements et Association des locataires du Québec* c. *Corporation des propriétaires immobiliers du Québec*, Rapport d'enquête [1995] C.A.I. 370 (C.A.I.) ; GRANOSIK, L., « Le critère de nécessité, dans Les 20 ans de la loi sur la protection des renseignements personnels », dans *Les 20 ans de la Loi sur la protection des renseignements personnels dans le secteur privé (2014)*, Vol. 392, service de la formation continue, Barreau du Québec, Cowansville, Yvon Blais, 2014, p.87.

restrictive[304] de la notion de « nécessité » a certes l'avantage de protéger le droit à la vie privée[305], elle représente toutefois un obstacle pour les entreprises et leur intérêt économique dans le traitement des renseignements personnels[306].

Afin de mieux prendre en compte l'intérêt qu'ont les entreprises à traiter les renseignements personnels, une approche axée sur leurs besoins a vu le jour. L'interprétation relative et contextuelle ayant émergé dans la décision *Bellerose* c. *Université de Montréal*[307]. Il s'agit selon le professeur Déziel de ne plus adopter un positionnement voulant que le renseignement soit irremplaçable mais plutôt une interprétation au cas par cas en prenant en compte le contexte et « les circonstances particulières de chaque affaire »[308].

Toutefois, il semblerait que ces deux interprétations de la notion de « nécessité » ne soient pas adaptées à sa possible évolution :

> « Le critère du renseignement indispensable est très restrictif pour l'exercice des pouvoirs et devoirs des organismes publics [interprétation stricte et restrictive] alors que celui du renseignement utile ou requis privilégie, de façon très libérale, les besoins des organismes publics [interprétation relative et contextuelle] au détriment du droit fondamental des personnes à la protection de leur vie privée »[309].

---

[304] *Société de transport de la Ville de Laval* c. *X et al.*, 2003 CanLII 44085 (QC C.Q.), par.25 ; DEZIEL, P-L., « Est-ce bien nécessaire ? Le principe de limitation de la collecte face aux défis de l'intelligence artificielle et des données massives », dans *Développements récents en droit de la vie privée (2019),* service de la formation continue du Barreau du Québec, 2019.

[305] DEZIEL, P-L., « Est-ce bien nécessaire ? Le principe de limitation de la collecte face aux défis de l'intelligence artificielle et des données massives », dans *Développements récents en droit de la vie privée (2019),* service de la formation continue du Barreau du Québec, 2019 ; GRANOSIK, L., « Le critère de nécessité, dans Les 20 ans de la loi sur la protection des renseignements personnels », dans *Les 20 ans de la Loi sur la protection des renseignements personnels dans le secteur privé (2014)*, Vol. 392, service de la formation continue, Barreau du Québec, Cowansville, Yvon Blais, 2014, p.91.

[306] Ibid.

[307] *Bellerose* c. *Université de Montréal*¸ [1986] C.A.I. 109 ; DEZIEL, P-L., « Est-ce bien nécessaire ? Le principe de limitation de la collecte face aux défis de l'intelligence artificielle et des données massives », dans *Développements récents en droit de la vie privée (2019),* service de la formation continue du Barreau du Québec, 2019 ; GRANOSIK, L., « Le critère de nécessité, dans Les 20 ans de la loi sur la protection des renseignements personnels », dans *Les 20 ans de la Loi sur la protection des renseignements personnels dans le secteur privé (2014)*, Vol. 392, service de la formation continue, Barreau du Québec, Cowansville, Yvon Blais, 2014 ; COMMISSION D'ACCES A L'INFORMATION, *Rétablir l'équilibre,* Rapport quinquennal, cai.gouv.qc.ca, 2016, en ligne : <http://www.cai.gouv.qc.ca/documents/CAI_RQ_2016.pdf >, p.87.

[308] DEZIEL, P-L., « Est-ce bien nécessaire ? Le principe de limitation de la collecte face aux défis de l'intelligence artificielle et des données massives », dans *Développements récents en droit de la vie privée (2019),* service de la formation continue du Barreau du Québec, 2019.

[309] *Société de transport de la Ville de Laval* c. *X et al.*, 2003 CanLII 44085 (QC C.Q.), par.30.

C'est pourquoi, l'honorable juge Filion a dégagé dans la décision *Société de transport de la Ville de Laval* c. *X et al*.[310] une nouvelle interprétation en s'appuyant sur le test de *Oakes*, qualifiée par le professeur Déziel de « souple et dynamique »[311]. Dans cette décision, opposant un organisme public à une personne physique, dont elle a réclamé en application de l'article 64 de la *loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* la destruction des rapports médicaux, il a été question de l'interprétation de la notion de « nécessité » de la collecte d'un renseignement personnel. Selon cette interprétation, la nécessité doit d'abord être lue à la lumière de la finalité de la loi, qui est celle de la protection de la vie privée (interprétation restrictive). Ensuite la nécessité doit être appréciée en fonction des intérêts de l'entreprise ou de l'organisme public (interprétation contextuelle)[312]. Nous reproduisons ici le passage pertinent de la décision évoquant cette nouvelle interprétation :

> « La Cour est convaincue que la meilleure interprétation à donner de l'article 64 [de la loi sur l'accès] et la meilleure façon de s'assurer que son application favorise l'exercice des droits fondamentaux consiste à préciser l'exigence de nécessité en la développant autour des deux volets du critère de l'arrêt *Oakes* : l'objectif important et légitime d'une part et l'atteinte proportionnée d'autre part. Un renseignement sera donc nécessaire non pas lorsqu'il pourra être jugé absolument indispensable, ou au contraire simplement utile. Il sera nécessaire lorsque chaque fin spécifique poursuivie par l'organisme, pour la réalisation d'un objectif lié à ses attributions, sera légitime, importante, urgente et réelle, et lorsque l'atteinte au droit à la vie privée que pourra constituer la cueillette, la communication ou la conservation de chaque élément de renseignement sera proportionnelle à cette fin. Cette proportionnalité jouera en faveur de l'organisme lorsqu'il sera établi que l'utilisation est rationnellement liée à l'objectif, que l'atteinte est minimisée et que la divulgation du renseignement requis est nettement plus utile à l'organisme que préjudiciable à la personne. Autrement, le droit à la vie privée et à la confidentialité des renseignements personnels devra prévaloir »[313] (nos soulignements).

[310] *Société de transport de la Ville de Laval* c. *X et al.*, 2003 CanLII 44085 (QC C.Q.).
[311] DEZIEL, P-L., « Est-ce bien nécessaire ? Le principe de limitation de la collecte face aux défis de l'intelligence artificielle et des données massives », dans *Développements récents en droit de la vie privée (2019),* service de la formation continue du Barreau du Québec, 2019.
[312] DEZIEL, P-L., « Est-ce bien nécessaire ? Le principe de limitation de la collecte face aux défis de l'intelligence artificielle et des données massives », dans *Développements récents en droit de la vie privée (2019),* service de la formation continue du Barreau du Québec, 2019.
[313] *Société de transport de la Ville de Laval* c. *X et al.*, 2003 CanLII 44085 (QC C.Q.), par.44.

Cette nouvelle interprétation plus souple et dynamique[314] que les précédentes, offre la possibilité d'exercer une balance entre les intérêts de l'organisme ou l'entreprise et le droit à la vie privée de l'individu[315]. Les conditions d'application du test de *Oakes* nous renvoient au principe de détermination des finalités de la collecte des renseignements personnels évoqué plus haut.

Nous complétons ce principe en ajoutant qu'il est étroitement lié à la notion de « raisonnabilité » et de « pertinence »[316]. L'article 5 (3) de la LPRPDE prévoit que le traitement des renseignements personnels ne peut se faire que si une personne raisonnable estimerait acceptable dans les circonstances. Cette norme objective oblige l'entreprise à prendre en compte différents éléments tels que la nature du service offert et sa relation avec le client[317]. Pour s'assurer que les renseignements qu'elle collecte sont utiles, une entreprise doit respecter un certain nombre de critères. Ceux-ci ont été énoncés par le juge Perell dans la décision *Mountain Province Diamonds Inc*. v. *De Beers Canada Inc.* :

> « (…) the jurisprudence establishes that to determine whether an organization complies with s. 5(3) of PIPEDA, a four-part test is applied; namely: (1) Is the collection, use or disclosure of personal information necessary to meet a specific need?; (2) Is the collection, use or disclosure of personal information likely to be effective in meeting that need?; (3) Is the loss of privacy proportional to the benefit gained?; and (4) Is there a less privacy-invasive way of achieving the same end? »[318].

Cette décision reprend le test de *Oakes* pour l'appliquer à la LPRPDE. La LPRPSP quant à elle ne renferme pas de notion équivalente à celle de « raisonnable ». La CAI a pourtant évoqué dans son rapport quinquennal de 2016 que :

---

[314] DEZIEL, P-L., « Est-ce bien nécessaire ? Le principe de limitation de la collecte face aux défis de l'intelligence artificielle et des données massives », dans *Développements récents en droit de la vie privée (2019),* service de la formation continue du Barreau du Québec, 2019

[315] Nous ne développerons pas davantage ce point car cela nous amènerait à dépasser le cadre du présent travail, mais nous désirons porter à la connaissance du lecteur que cette interprétation souple et dynamique n'a pas été suivie par la CAI dans ses récentes décisions ; Voir notamment GRANOSIK, L., « Le critère de nécessité, dans Les 20 ans de la loi sur la protection des renseignements personnels », dans *Les 20 ans de la Loi sur la protection des renseignements personnels dans le secteur privé (2014)*, Vol. 392, service de la formation continue, Barreau du Québec, Cowansville, Yvon Blais, 2014, p.96 et s.

[316] GUILMAIN, A., et GRATTON, E. « La protection des renseignements personnels dans le secteur privé au Québec : rétrospectives et perspectives », dans *Développements récents en droit à la vie privée (2019)*, vol. 465, service de la formation continue, Barreau du Québec, Montréal, Edition Yvon Blais, 2019, p.115.

[317] Ibid., p.114.

[318] *Mountain Province Diamonds Inc*. v. *De Beers Canada Inc.,* 2014 ONSC 2026 (CanLII), par. 47.

> « Le droit au respect de la vie privée s'évalue notamment en considérant l'expectative de vie privée d'une personne raisonnable et bien informée, placée dans la même situation à l'égard d'un renseignement ».[319]

Une telle disposition vient donc *a priori* protéger l'utilisateur de l'assistant vocal de la collecte et l'utilisation de ses renseignements personnels autre que ceux qui sont nécessaires ou à des fins inacceptables même s'il a pu donner son consentement[320].

ii. La limitation de l'utilisation, de la communication et de la conservation des renseignements personnels

Bien que nous nous sommes attardés au principe de la limitation de la collecte, quelques mots devraient être dit concernant les limitations de communication, d'utilisation et de conservation. Nous les évoquons ensemble pour être en phase avec l'annexe 1 de la LPRPDE, qui d'ailleurs les énonce au principe 4.5 comme étant des interdictions à l'utilisation ou la communication des renseignements personnels en dehors des finalités pour lesquelles ils devaient être utilisés.

En vertu de ce principe, une entreprise doit porter à la connaissance de l'individu toutes les informations portant sur la durée et la procédure de conservation. À cet effet, l'article 4.5.4 précise que le principe 4.5 est « étroitement lié au principe du consentement (article 4.3), à celui de la détermination des fins auxquelles la collecte est destinée (article 4.2), ainsi qu'à celui de l'accès individuel (article 4.9) ».

En ce qui concerne la communication, la LPRPSP dispose que l'entreprise qui communique des renseignements personnels à l'extérieur du Québec doit adopter tous les moyens raisonnables permettant d'assurer que les renseignements ne seront pas réutilisés à d'autres fins et, ce, après

---

[319] COMMISSION D'ACCES A L'INFORMATION, *Rétablir l'équilibre,* Rapport quinquennal, cai.gouv.qc.ca, 2016, en ligne : < http://www.cai.gouv.qc.ca/documents/CAI_RQ_2016.pdf >, p.87 ; Voir *R.* c. *Wong*, [1990] 3 R.C.S. 36.
[320] GUILMAIN, A., et GRATTON, E. « La protection des renseignements personnels dans le secteur privé au Québec : rétrospectives et perspectives », dans *Développements récents en droit à la vie privée (2019)*, vol. 465, service de la formation continue, Barreau du Québec, Montréal, Edition Yvon Blais, 2019, p.116.

avoir obtenu le consentement de la personne visée[321]. L'absence de telles garanties doit contraindre le détenteur de ces renseignements d'opérer leur transfert[322]. L'article 17 renvoie aux articles 18 et 23 de la même loi pour ce qui est des exceptions au recueil du consentement dans le cadre d'un transfert en dehors de la province. Ces exceptions, que nous ne les listerons pas, visent essentiellement les cas d'assistance à l'exercice de la justice (art. 18) et de prospection commerciale ou philanthropique (art.23).

En outre, le transfert extra-provincial ne semble pas être clairement défini. En effet, pour M[es] Guilmain et Gratton, une distinction doit être faite entre la communication et le simple fait de confier les renseignements à un tiers, qui dans ce cas ne nécessite aucun consentement[323]. Selon eux, la qualification en une communication requerra comme préalable à tout transfert le consentement de l'individu sauf si l'entreprise parvient à se prévaloir d'une exception prévue aux articles 18 et 23. Une telle qualification n'est pas sans poser un problème pour l'entreprise car elle devra recueillir à nouveau le consentement des personnes. Cette contrainte supplémentaire irait à l'encontre des autres dispositions de la LPRPSP, dont l'article 20 autorisant les employés d'une entreprise ou les parties à un contrat de service d'accéder aux renseignements personnels sans le consentement de la personne intéressée.

Au niveau fédéral, la LPRPDE exige à l'article 4.1.3 que l'entreprise reste responsable des renseignements personnels, y compris lorsqu'elle procède à leur transfert en dehors du Canada. Lors de ce transfert, l'entreprise doit s'assurer par le biais, entre autres, d'un contrat que le tiers maintient un niveau de protection comparable des renseignement personnels. Le CPVP est venu préciser cette disposition en rappelant que « aucun contrat ni autre moyen ne peut avoir préséance sur les lois d'une administration étrangère »[324].

---

[321] Art. 17 de la LPRPSP ; COMMISSION D'ACCES A L'INFORMATION, *Rétablir l'équilibre,* Rapport quinquennal, cai.gouv.qc.ca, 2016, en ligne : < http://www.cai.gouv.qc.ca/documents/CAI_RQ_2016.pdf >, p.130.
[322] Art. 17 al. 3 de la LPRPSP.
[323] GUILMAIN, A., et GRATTON, E. « La protection des renseignements personnels dans le secteur privé au Québec : rétrospectives et perspectives », dans *Développements récents en droit à la vie privée (2019)*, vol. 465, service de la formation continue, Barreau du Québec, Montréal, Edition Yvon Blais, 2019, p.103.
[324] COMMISSARIAT A LA PROTECTION DE LA VIE PRIVEE, *Lignes directrices sur le transfert transfrontalier de renseignements personnels,* priv.gc.ca, janvier 2009, en ligne : < https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/aeroports-et-frontieres/gl_dab_090127/ > ; Ces lignes directrices ont fait l'objet d'une consultation de la part du CPVP à l'issue de laquelle il a été décidé qu'elles ne seraient pas modifiées, COMMISSARIAT A LA PROTECTION DE LA VIE PRIVEE, *Annonce : Le Commissariat tire ses conclusions suite*

S'agissant de la fin de l'utilisation des renseignements personnels, ce même principe prévoit la possibilité pour une entreprise de les « dépersonnaliser ». En d'autres termes, il est acceptable qu'une entreprise puisse recourir à la technique d'anonymisation des renseignements si elle ne souhaite pas les détruire. Il n'est pas inintéressant de faire un parallèle avec le RGPD. Celui-ci dispose à l'article 4 alinéa 5 que la pseudonymisation des données consiste au retrait des données tendant à identifier la personne concernée. Une telle disposition est absente de la LPRPSP[325]. La Commission d'accès à l'information rapporte seulement que l'article 12 de la LPRPSP cacherait une telle obligation de destruction lorsque :

> « L'utilisation des renseignements contenus dans un dossier n'est permise, une fois l'objet du dossier accompli, qu'avec le consentement de la personne concernée, sous réserve du délai prévu par la loi ou par un calendrier de conservation établi par règlement du gouvernement » (nos soulignements).

En vertu de cet article, l'entreprise, à défaut d'obtenir un consentement de l'intéressé, doit procéder à la destruction des renseignements personnels à l'issue de la réalisation de la finalité recherchée.

d) La reconnaissance de droits aux individus comme ultime contrôle de la protection des renseignements personnels

Le dernier rempart dans la protection des renseignements personnels se situe au niveau des droits accordés à l'individu. À travers leur exercice, notamment d'accès (i), de rectification et d'exactitude (ii), l'utilisateur garde un contrôle sur les renseignements personnels collectés par l'entreprise.

à la consultation sur les transferts aux fins de traitement, priv.gc.ca, 23 septembre 2019, en ligne : <https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/aeroports-et-frontieres/gl_dab_090127/>.

[325] COMMISSION D'ACCES A L'INFORMATION, *Rétablir l'équilibre,* Rapport quinquennal, cai.gouv.qc.ca, 2016, en ligne : < http://www.cai.gouv.qc.ca/documents/CAI_RQ_2016.pdf >, p.108.

i. Le droit d'accès aux renseignements personnels

Il s'agit du premier des droits reconnus aux individus, celui d'accéder aux renseignements personnels récoltés et détenus par l'entreprise. En vertu de l'article 4.9 de l'annexe de la LPRPDE : « [u]ne organisation doit informer la personne qui en fait la demande du fait qu'elle possède des renseignements personnels à son sujet, le cas échéant ». Ce principe se retrouve à l'article 27 de la LPRPSP avec une approche similaire, à savoir la prise de l'initiative de la demande d'accès par l'individu. Il ne revient donc pas à l'entreprise de proposer l'accès des renseignements personnels à la personne concernée. Le Code civil du Québec renferme également des dispositions portant sur le droit d'accès[326].

Cependant, l'exercice d'un tel droit n'est pas sans limite. En effet, la demande d'accès doit être formulée par écrit et comporter les précisions relatives aux renseignements à consulter[327]. En outre, dans le cas d'une transmission incomplète des renseignements par l'entreprise faisant suite à la demande d'accès, il appartiendra à l'individu d'apporter la preuve *prima facie* que la réponse n'a pas été exhaustive[328]. Aussi, l'accès aux renseignements comporte quelques exceptions qu'une entreprise peut se prévaloir parmi celles prévues par la LPRPDE[329].

Enfin, s'agissant de l'entreprise recevant la demande, elle dispose d'un délai de 30 jours pour y répondre[330] à compter du jour où celle-ci déclare comme complète la demande d'accès[331]. Il est à noter que l'absence de réponse de l'entreprise dans le délai imparti équivaut à un refus de donner suite à la demande ce qui ouvre la voie à une plainte de l'individu auprès du CPVP sur la base du principe 4.10 de l'annexe 1 de la LPRPDE ou de l'article 42 de la LPRPSP.

---

[326] Arts. 38 à 41 du C.c.Q.
[327] Art. 8 (1) de la LPRPDE ; Arts. 30 et 31 de la LPRPSP ; *Nammo* c. *TransUnion of Canada Inc.,* 2010 CF 1284.
[328] *Johnson* c. *Bell Canada,* 2008 CF 1086 (CanLII), [2009] 3 RCF 67.
[329] COMMISSARIAT A LA PROTECTION DE LA VIE PRIVEE, *Rapport de conclusions en vertu de la LPRPDE n°2009-022 : Un détaillant accepte d'améliorer ses mesures de protection à l'égard de ses enregistrements de vidéosurveillance,* priv.gc.ca, 9 juin 2009, en ligne : < https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2009/lprpde-2009-022/ >.
[330] Art. 8 (3) de la LPRPDE.
[331] COMMISSARIAT A LA PROTECTION DE LA VIE PRIVEE, *Résumé de conclusions d'enquête en vertu de la LPRPDE n°2006-334 : Une banque exige une pièce d'identité avant de répondre à une demande d'accès à des renseignements personnels,* priv.gc.ca, 21 février 2006, en ligne : < https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2006/lprpde-2006-334/ >.

ii. Le droit d'avoir des renseignements personnels exacts

En vertu de ce principe, les « (…) renseignements personnels doivent être aussi exacts, complets et à jour que l'exigent les fins auxquelles ils sont destinés »[332]. Cette disposition est équivalente à celle de l'article 11 de la LPRPSP.

Lors de nos recherches sur l'interprétation de ce principe, nous avons constaté que les juridictions ont essentiellement été saisis dans le cadre d'un litige relatif à l'évaluation d'un dossier de crédit ou à l'installation de caméras de surveillance. Du côté du CPVP, le constat est le même, l'émergence récente des assistants vocaux, et plus généralement des technologies qui le supporte (ex : téléphone intelligent) peuvent expliquer l'absence d'une telle interprétation du principe d'exactitude. Néanmoins, nous retiendrons de ce principe qu'un individu peut exercer son droit d'accès en vue de s'assurer que ses renseignements personnels sur lesquels l'entreprise se base pour prendre une décision sont bien complets au regard de la finalité recherchée. Cette possibilité de rectification, nous la retrouvons aux articles 8 et 30 de la LPRPSP.

À la lecture de cette sous-partie consacrée aux différentes dispositions garantissant une protection de la vie privée de l'individu, nous serions tentés d'affirmer que les technologies sont bien encadrées juridiquement. Or, dans le cadre de l'assistant vocal, ayant été rendu accessible au public dès 2011, dont l'évolution n'a cessé depuis, le cadre juridique que nous connaissons semble montrer ses limites au point de se retrouver être bouleversé.

Tout au long de cette première partie, nous nous sommes efforcés de présenter l'assistant vocal, ses caractéristiques techniques avec son système de fonctionnement intégrant le TALN et l'intelligence artificielle. Puis, nous avons défini et expliqué les dispositions constitutionnelles régissant le droit à la vie privée et les différents principes fondamentaux de la protection des renseignements personnels que l'assistant vocal rencontrera.

[332] Art. 4.6 de l'annexe 1 de LPRPDE.

La seconde partie du mémoire sera consacrée à l'incidence de l'assistant vocal sur la protection des renseignements personnels mais également sur les dispositions constitutionnelles du droit à la vie privée. Nous aborderons aussi l'inadéquation entre cette technologie et quelques-uns des régimes de responsabilité civile. Enfin nous terminerons cette partie par évoquer la nouvelle obligation légale de notification des incidents de sécurité et ses effets préventifs quant au respect des principes fondamentaux de la protection des renseignements personnels.

II. L'incidence de l'utilisation de l'assistant vocal sur le cadre juridique

Le droit constitutionnel actuel en matière de vie privée et les principes fondamentaux de la protection des renseignements personnels se sont trouvés être secoués par la commercialisation et la prolifération de l'assistant vocal (A). Son utilisation dans un cadre privé et le recours au TALN lui permettant de s'intégrer parfaitement dans la vie de l'individu ont eu pour incidence de mettre en lumière une autre inadéquation, celle des différents régimes de responsabilité civile prévus par le Code civil du Québec. Toutefois, cette inadéquation ne veut pas pour autant dire que l'assistant vocal est un véritable OVNI juridique échappant à toutes les règles de droit. Le législateur a su adopter un cadre juridique de la protection des renseignements personnels suffisamment large afin de pouvoir prendre en compte l'émergence des technologies, notamment en instaurant une obligation légale de notification des incidents de sécurité comportant des effets préventifs de leur survenance (B).

A. Une remise en cause de la protection des renseignements personnels par l'assistant vocal

La récente arrivée de l'assistant vocal est venue bousculer le droit constitutionnel actuel en matière de vie privée (1) et les principes fondamentaux de la protection des renseignements personnels (2).

1. L'atteinte aux dispositions constitutionnelles régissant le droit à la vie privée

Si la jurisprudence a pu mettre en application le test de *Oakes* aux dispositions de la LPRPDE, elle concernait principalement le domaine des affaires[333]. Le droit à la vie privée, tel qu'il est prévu par

[333] Voir par exemple *Mountain Province Diamonds Inc.* v. *De Beers Canada Inc.,* 2014 ONSC 2026 (CanLII).

les différents textes que nous avons présentés, apparaît comme étant inadapté au regard de l'essor des technologies intégrant le TALN. Leur démocratisation a eu pour conséquence de créer une certaine tension avec le droit à la vie privée[334]. La capacité de ces assistants vocaux à pouvoir collecter des renseignements personnels en masse et à les envoyer vers des structures de stockage où ils seront gardés indéfiniment, est de nature à remettre en cause ce concept de vie privée et des libertés individuelles[335].

Par ailleurs, la parfaite intégration de l'assistant vocal dans l'espace le plus privé de l'individu remet en cause cette notion de « domicile ». En effet, les fabricants de ces objets connectés, sous prétexte de l'amélioration du produit, sont en mesure d'analyser les renseignements collectés, de déduire certaines habitudes et de prédire la survenance d'un évènement. Comme nous le verrons lors de la détermination du gardien pour l'application de la responsabilité civile, il nous semble impossible de contraindre les habitants d'un logement équipé d'un assistant vocal, de restreindre leur parole lorsqu'ils s'y trouvent à proximité. Certains auteurs, comme le professeur Benoît Pelletier, n'hésitent d'ailleurs pas à qualifier cette intrusion de la part des entreprises de véritable « voyeurisme »[336] dans la sphère privée de l'utilisateur.

Les limites du traitement automatique du langage naturel représentent une preuve dans l'atteinte que peut constituer l'assistant vocal vis-à-vis de la vie privée, particulièrement lorsque celui-ci est utilisé dans le domicile. L'exemple impliquant l'assistant vocal Alexa d'Amazon dans l'interprétation erronée du mot d'éveil[337] nous parait être une bonne illustration de nos propos. Cet exemple met en lumière l'inadéquation entre le droit à la vie privée et une technologie ayant recours au TALN. Il était question de l'enregistrement d'une conversation d'un couple s'étant tenu à proximité d'Alexa avant qu'il ne soit envoyé à un de leur contact. Étant en présence d'un objet, dont les caractéristiques techniques le rendent quasi « invisible », nous sommes en droit de nous

[334] REY, B., *La vie privée à l'ère du numérique,* Lavoisier, coll. « Traitement de l'information », 2012, p.48.
[335] REY, B., *La vie privée à l'ère du numérique,* Lavoisier, coll. « Traitement de l'information », 2012 ; DETRAIGNE, Y., et ESCOFFIER, A.-M., *La vie privée à l'heure des mémoires numériques. Pour une confiance renforcée entre citoyens et société de l'information*, Rapport d'information n°441, senat.fr, 27 mai 2009, en ligne : <http://www.senat.fr/rap/r08-441/r08-441_mono.html#toc328 >.
[336] PELLETIER, B., « Droit constitutionnel : la protection de la vie privée au Canada », revue juridique Thémis, 2001 35 R.J.T., p.485.
[337] RTBF, « Alexa, l'assistant vocal d'Amazon, envoie par erreur la conversation privée d'un couple à un collègue du mari », rtbf.be, 25 mai 2018, en ligne : < https://www.rtbf.be/info/insolites/detail_une-conversation-privee-envoyee-par-erreur-par-l-enceinte-connectee-d-amazon?id=9927755 >.

interroger sur le caractère raisonnable que peut avoir l'utilisateur quant au respect de sa vie privée. Une personne interagissant avec l'assistant vocal s'attend elle à ce que ses renseignements personnels soient collectés et sa vie privée méconnue ? Il semblerait en apparence qu'une personne raisonnable ne s'attendra pas à ce qu'un assistant se déclenche et l'enregistre si le mot d'activation n'a pas été prononcé. Dans le cas contraire, l'intérêt de mettre en place un tel moyen d'activation nous interrogerait. La parole étant un mode de communication naturel[338], l'interaction avec l'assistant vocal se fera de manière instantanée et quasi fluide. L'utilisateur, par l'absence d'écran, ne se rendra pas, ou très peu, compte de la possible violation de sa vie privée. Ceci est d'autant plus vrai lorsque l'assistant vocal est intégré à un réseau d'objet connectés offrant, par exemple, une maison plus intelligente. Le fait pour une personne d'être complétement immergée dans son expérience l'empêchera de réaliser qu'une entreprise est en mesure de lui voler sa vie privée. Dans le cadre d'une expérience visant à sensibiliser les individus à l'usage de l'assistant vocal, l'artiste Lauren McCarthy a proposé à plusieurs personnes de se substituer à l'assistant vocal dans la réalisation des tâches demandées initialement faite par l'assistant vocal[339]. Cette expérience avait pour but de faire comprendre aux individus que le domicile constitue l'ultime rempart de notre vie privée et que celui-ci est en passe de céder par l'intrusion de l'assistant vocal.

Afin d'illustrer davantage nos propos sur la violation du domicile privée par l'assistant vocal, nous pouvons évoquer la publicité commerciale de la chaîne de restauration rapide Burger King aux États-Unis lors de l'évènement sportif du Superbowl en 2017. Au cours de cet évènement très suivi chez nos voisins américains, Burger King a réussi à faire activer les enceintes connectées de Google par le biais de son annonce télévisée[340]. À travers ces exemples, nous constatons que l'assistant

[338] MINKER, W., et NEEL, F., « Développement des technologies vocales », dans *Le travail humain*, vol. 65, 2002/3, en ligne : < https://www.cairn.info/revue-le-travail-humain-2002-3-page-261.htm#pa23 >, p.267.
[339] CHATELLIER, R., « Troqueriez-vous votre assistant domestique intelligent pour un être humain ? », linc.cnil.fr, 18 septembre 2017, en ligne : < https://linc.cnil.fr/fr/troqueriez-vous-votre-assistant-domestique-intelligent-pour-un-etre-humain >.
[340] TOWNSEND, T., « Burger King's new ad deliberately gets your Google Home to talk about burgers », vox.com, 22 april 2017, en ligne : < https://www.vox.com/2017/4/12/15274312/burger-king-ad-triggers-google-home > ; Nous pouvons également mentionner le cas de Google qui a toutefois déclenché involontairement l'assistant vocal par le biais de la publicité, OPAM, K., « Google's Super Bowl ad accidentally set off a lot of Google Homes », theverge.com, 5th February 2017, < https://www.theverge.com/2017/2/5/14517314/google-home-super-bowl-ad-2017 > ; Nous avons aussi trouvé le cas d'un présentateur de télévision ayant activé à distance les assistants vocaux des téléspectateurs, LIPTAK, A., « Amazon's Alexa started ordering people dollhouses after hearing its name on TV », theverge.com, 7 January 2017, en ligne : < https://www.theverge.com/2017/1/7/14200210/amazon-alexa-tech-news-anchor-order-dollhouse >.

vocal est un objet extrêmement intrusif dans la vie privée de son utilisateur. Son activation à distance par une tierce personne voire même via d'autres moyens technologiques, sans pour autant être en mesure d'opérer une distinction entre le locuteur, est de nature à remettre en cause l'existence la notion de « domicile » tel que l'a défini le professeur Pelletier comme étant un lieu physique protégeant l'individu de toute ingérence extérieure[341].

Cette situation soulève une autre question, celle de la détermination de la notion « d'expectative de vie privée ». Sachant que la vie privée n'est pas une notion ayant une définition formelle, il devient alors davantage compliqué de caractériser l'expectative de vie privée. Tout comme le droit à la vie privée, cette notion évolue en fonction de l'émergence des technologies. C'est donc au juge que revient la tâche d'assurer cette évolution. L'expectative de vie privée a vu le jour pour la première fois en 1984 dans la décision *Hunter et autres* c. *Southam Inc*[342] alors que le juge Dickson affirmait que :

> « Cette limitation du droit garanti par l'art. 8, qu'elle soit exprimée sous la forme négative, c'est-à-dire comme une protection contre les fouilles, les perquisitions et les saisies "abusives", ou sous la forme positive comme le droit de s'attendre "raisonnablement" à la protection de la vie privée, indique qu'il faut apprécier si, dans une situation donnée, le droit du public de ne pas être importuné [page160](sic) par le gouvernement doit céder le pas au droit du gouvernement de s'immiscer dans la vie privée des particuliers afin de réaliser ses fins et, notamment, d'assurer l'application de la loi »[343] (notre soulignement).

L'expectative de vie privée est devenue par la suite une « partie intégrante du droit constitutionnel canadien »[344]. À cet effet, elle a fait l'objet de précisions de la part de la Cour suprême pour déterminer les cas dans lesquels une personne pouvait se prévaloir de son droit à la vie privée en vertu de l'article 8 de la Charte canadienne. Dans la décision *R.* c. *Edwards*[345], le juge La Forest

[341] PELLETIER, B., « Droit constitutionnel : la protection de la vie privée au Canada », revue juridique Thémis, 2001 35 R.J.T., p.510.
[342] *Hunter et autres* c. *Southam Inc.,* [1984] 2 R.C.S. 145 ; BROCHU, C., *La Charte canadienne des droits et libertés*, LexisNexis, 2003.
[343] *Hunter et autres* c. *Southam Inc.,* [1984] 2 R.C.S. 145.
[344] PELLETIER, B., « Droit constitutionnel : la protection de la vie privée au Canada », revue juridique Thémis, 2001 35 R.J.T., p.513 citant Pierre TRUDEL, France ABRAN, Karim BENYEKHLEF et Sophie HEIN, Droit du cyberespace, Montréal, Éditions Thémis, 1997, 1296 p.
[345] *R.* c. *Edwards,* 1996 CanLII 255 (CSC), [1996] 1 RCS 128.

énonce que l'appréciation de l'attente raisonnable se fait au regard d'un ensemble de circonstances parmi lesquels :

> « (i) la présence au moment de la perquisition;
> (ii) la possession ou le contrôle du bien ou du lieu faisant l'objet de la fouille ou de la perquisition;
> (iii) la propriété du bien ou du lieu;
> (iv) l'usage historique du bien ou de l'article;
> (v) l'habilité à régir l'accès au lieu, y compris le droit d'y recevoir ou d'en exclure autrui;
> (vi) l'existence d'une attente subjective en matière de vie privée;
> (vii) le caractère raisonnable de l'attente, sur le plan objectif »[346].

Ces critères ont été repris pour être adaptés aux technologies. Dans la décision *R*. c. *Cole*[347], l'honorable juge McLachlin, juge en chef, a précisé au préalable que « [l]e critère de « l'ensemble des circonstances » s'intéresse au fond et non à la forme »[348]. En ce qui concerne leur application aux technologies, en l'espèce l'ordinateur, elle rapporte que les critères d'appréciation de l'attente raisonnable sont :

> « (1) l'examen de l'objet de la prétendue fouille; (2) la question de savoir si le demandeur possédait un droit direct à l'égard de l'objet; (3) la question de savoir si le demandeur avait une attente subjective en matière de respect de sa vie privée relativement à l'objet; (4) la question de savoir si cette attente subjective en matière de respect de la vie privée était objectivement raisonnable, eu égard à l'ensemble des circonstances »[349].

S'agissant de l'attente raisonnable à l'égard d'un assistant vocal, nos recherches jurisprudentielles ne nous ont pas permis d'aboutir à un résultat. À défaut, nous pouvons nous appuyer sur les différentes décisions rendues portant sur des cas d'écoutes téléphoniques[350] reprenant la notion de « attente subjective » précédemment citées. L'interception des communications téléphoniques peut

---

[346] *R*. c. *Edwards,* 1996 CanLII 255 (CSC), [1996] 1 RCS 128, par. 45.
[347] *R.* c. *Cole,* 2012 CSC 53 (CanLII), [2012] 3 RCS 34.
[348] *R*. c. *Cole,* 2012 CSC 53 (CanLII), [2012] 3 RCS 34, par. 40.
[349] *R*. c. *Cole,* 2012 CSC 53 (CanLII), [2012] 3 RCS 34, par. 40 ; Voir également : *R.* c. *Marakah*, 2017 CSC 59 (CanLII), [2017] 2 RCS 608 ; *R.* v. *Clarke,* 2017 BCCA 453 (CanLII).
[350] *R*. c. *Duarte,* [1990] 1 R.C.S. 30 ; *R.* c. *Wiggins*, [1990] 1 R.C.S. 62 ; *Strivastava* c. *Hindu Mission of Canada (Québec) Inc.*, 2001 CanLII 27966 (QC CA) ; *Ste-Marie* c. *Placements J.P.M. Marquis Inc.*, 2005 QCCA 312 (CanLII).

être comparée à l'utilisation d'un assistant vocal dans la mesure où nous sommes dans les deux cas en présence d'une technologie offrant la possibilité de discuter oralement à distance avec autrui, et dont la conversation peut être sauvegardée. La différence réside bien entendu dans l' « autrui », même si aujourd'hui des personnes ont tendance à accorder une certaine personnification à l'assistant vocal au point de l'intégrer au sein de leur vie privée[351]. Dans sa décision *Strivastava* c. *Hindu Mission of Canada (Québec) Inc.* la Cour d'appel a estimé que :

> « la question fondamentale en l'espèce est celle de savoir si la conversation est protégée et non le téléphone. En effet, je crois que l'emphase doit être mise sur l'attente subjective de la personne face à la conversation, son caractère raisonnable, ainsi que sur la nature de celle-ci. À défaut de quoi, il serait très difficile pour quelqu'un de prouver une expectative raisonnable de vie privée quant à tout élément intangible- (sic) ne pouvant être grevé d'un droit de propriété »[352] (le soulignement est dans l'original).

Dans cette affaire, il a été question de l'écoute des communications téléphoniques d'un prêtre d'un temple hindou sur la base de soupçons quant à l'exercice réel de ses fonctions. L'écoute de ses communications a révélé l'existence d'une relation amoureuse entre lui et une bénévole de ce même temple. Lors d'un vote à l'assemblée regroupant les décideurs du temple, le prêtre a été contraint de démissionner. Ensemble, ils engagent une action en dommages-intérêts pour atteinte à la vie privée[353].

Cette décision doit être lue en complément de celle rendue dans l'affaire *Ste-Marie* c. *Placements J.P.M. Marquis Inc*[354]. Dans les faits, Marquis a confié la construction d'un supermarché à Ste-Marie. Étant insatisfait de l'avancement du chantier, Marquis décide de placer sur écoutes les lignes téléphoniques qu'il a prêté à Ste-Marie. Ces écoutes révèlent la préparation d'un vol avec un tierce personne. Marquis décide de remettre l'enregistrement à la police, qui lance une enquête. Celle-ci

---

[351] Partie I.B.2.a) ; Voir également LACHANCE, F., *« O.K. Google, assiste-moi » Les parcours des utilisateurs et des familles qui domestiquent le Google Home,* papyrus.bib.umontreal.ca, Mémoire de maîtrise, Avril 2019, en ligne :<https://papyrus.bib.umontreal.ca/xmlui/bitstream/handle/1866/22464/Lachance_Francois_2019_memoire.pdf?sequence=2&isAllowed=y >.

[352] *Strivastava* c. *Hindu Mission of Canada (Québec) Inc.*, 2001 CanLII 27966 (QC CA), par. 71.

[353] *Strivastava* c. *Hindu Mission of Canada (Québec) Inc.*, 2001 CanLII 27966 (QC CA) ; BEAUREGARD, S., et GRANOZIK, L., « Les renseignements personnels et la responsabilité civile : à quel prix ? », dans Barreau du Québec, service de la formation continue, *Développements récents en droit de l'accès à l'information et de la protection des renseignements personnels,* Les 30 ans de la Commission d'accès à l'information (2012), vol. 358, Cowansville, éd. Yvon Blais, 2012, pp. 82-83.

[354] *Ste-Marie* c. *Placements J.P.M. Marquis Inc.*, 2005 QCCA 312 (CanLII).

n'aboutira à aucune accusation criminelle et Ste-Marie intente une action en dommages-intérêts pour violation de sa vie privée. Dans cette décision, la Cour d'appel énonce que « [e]n droit du travail, on a décidé déjà que l'interception de communications secrètes du salarié, lorsqu'elles ont lieu au travail, ne constitue pas toujours une violation de sa vie privée »[355] (nos soulignements). Il faut préciser que cette décision ne vaut que dans le cadre de relations contractuelles au travail, même si la nature des faits (interception de communications téléphoniques) est similaire à ceux dans l'affaire *Strivastava* c. *Hindu Mission of Canada (Québec) Inc.* Il ressort de ces jurisprudences que l'expectative de vie privée est déterminée en fonction de la nature de la conversation téléphonique et non pas sur l'utilisation du téléphone[356]. Néanmoins, il convient de garder à l'esprit qu'il ne s'agit que de cas de communication par téléphone. En d'autres termes, le téléphone lui-même ne peut s'activer de sa propre initiative et lancer un appel. Dans la décision *R.* c. *Wong*, le juge Lamer a précisé que :

> « [L]a question de savoir si une personne a une attente raisonnable en matière de respect de la vie privée ne peut être tranchée que dans le contexte factuel particulier de la surveillance, et non en fonction d'une notion générale de respect de la vie privée dans une société libre et démocratique dont une personne jouit en tout temps »[357] (notre soulignement).

Si, pendant de nombreuses années, la surveillance téléphonique visait essentiellement l'État, l'accès au grand public de l'assistant vocal, qu'il soit présent dans une enceinte connectée installée dans une maison voire dans une voiture, est susceptible de représenter une nouvelle évolution de cette notion d'expectative de vie privée. En effet, si des mots d'éveil ont été mis en place, c'est pour permettre à l'utilisateur d'activer l'assistant vocal quand bon lui semble. Nous serions donc tentés d'affirmer qu'un utilisateur, dès lors qu'il active l'assistant vocal, est conscient que sa vie privée peut être menacée.

---

[355] *Ste-Marie* c. *Placements J.P.M. Marquis Inc.*, 2005 QCCA 312 (CanLII), par. 21.
[356] *Strivastava* c. *Hindu Mission of Canada (Québec) Inc.*, 2001 CanLII 27966 (QC CA) ; *Ste-Marie* c. *Placements J.P.M. Marquis Inc.*, 2005 QCCA 312 (CanLII) ; BEAUREGARD, S., et GRANOZIK, L., « Les renseignements personnels et la responsabilité civile : à quel prix ? », dans Barreau du Québec, service de la formation continue, *Développements récents en droit de l'accès à l'information et de la protection des renseignements personnels,* Les 30 ans de la Commission d'accès à l'information (2012), vol. 358, Cowansville, éd. Yvon Blais, 2012, pp. 82-83.
[357] *R.* c. *Wong*, 1990 CanLII 56 (CSC), [1990] 3 RCS 36.

Cependant, il en va autrement lorsque ce même utilisateur interagit avec une autre personne à proximité de l'assistant vocal et qu'il s'active involontairement. Nous retrouvons encore une fois le fidèle exemple de notre couple américain. En reprenant leur cas, nous pouvons nous interroger sur la raisonnabilité de leur consentement lorsqu'ils échangent à côté de l'assistant vocal. Ont-ils pensé qu'ils allaient être enregistrés à la suite d'un faux positif de l'assistant vocal ? Auraient-ils du y penser avant d'engager la conversation ? Il serait selon nous difficile d'apporter une réponse positive à cette question auquel cas cela signifierait que les libertés individuelles, notamment d'expression, se retrouveraient être extrêmement limitées au sein même du domicile compte tenu de la puissance des microphones pouvant capter la parole à plusieurs dizaines de mètres.

D'ailleurs, la rédaction en des termes généraux des politiques de confidentialité nous amène à nous interroger sur la réelle prise de connaissance par les utilisateurs des conséquences de l'utilisation de l'assistant vocal sur leur vie privée. Si nous prenons la politique de l'assistant Google, nous remarquons que celle-ci renvoie vers la politique générale de confidentialité de l'entreprise, qui dans le même temps est commune à tous ses produits et services[358]. En outre, leur présence sur Internet obligerait l'utilisateur à aller les consulter sur le site du fabricant. Bien qu'une telle pratique a été confirmée dans la décision *Kranitz* c. *Rogers Cable Inc.*[359], une personne doit être en mesure de comprendre ce qu'elle lit. Selon nous, un utilisateur lambda ne saura pas adopter un raisonnement critique de la politique et se contentera seulement de suivre la position du fabricant.

À ce titre, nous estimons qu'il soit pertinent d'évoquer la décision *Mofo Moko* c. *eBay Canada Ltd.*[360] dans laquelle il a été question de la vente aux enchères d'un bien par un particulier sur la plateforme en ligne. Celle-ci a au cours des enchères suspendu la vente qui a causé un préjudice au vendeur et a fait valoir devant le juge la clause de résiliation de services prévue sur Internet et dont « l'utilisateur du site peut y avoir accès en cliquant sur un hyperlien »[361]. Au sujet de la clause, principalement en ce qui concerne sa rédaction, l'honorable Chantal Corriveau a déclaré que « la

[358] Voir JAAR, D., LACOSTE, E., et SENECAL, F., « Investir dans les renseignements personnels et leur protection », dans *Développements récents en droit de l'accès à l'information et de la protection des renseignements personnels — les 30 ans de la Commission d'accès à l'information (2012)*, vol. 358, service de la formation continue, Barreau du Québec, Cowansville, Éditions Yvon Blais, 2012, pp.193-194.
[359] *Kranitz* c. *Rogers Cable Inc.,* 2002 CanLII 49415 (ON SC).
[360] *Mofo Moko* c. *eBay Canada Ltd.,* 2016 QCCS 4669 (CanLII).
[361] Ibid, par. 25.

clause de résiliation d'eBay est très vague et générale. Sa rédaction n'est certainement pas des plus heureuses » (nos soulignements)[362].

Ainsi, à travers l'utilisation de l'assistant vocal, l'utilisateur place sa confiance entre les mains du fabricant pour respecter sa vie privée. Cependant, nos divers exemples ont mis en lumière le caractère intrusif de l'assistant vocal dans la vie privée de l'utilisateur, allant même jusqu'à son domicile. Pour continuer de préserver cette vie privée de l'utilisateur, nous pensons que cette notion d'expectative de vie privée doit elle aussi être revue. En effet, la jurisprudence, que nous avons évoqué précédemment[363], ne s'applique que pour le cas d'une interception téléphonique. À la différence du téléphone, et à moins d'être en présence d'un assistant vocal piraté à distance, les conversations ne sont pas écoutées instantanément. Elles sont d'abord conservées avant d'être utilisées. Il nous semble néanmoins opportun d'effectuer un parallèle entre la conservation des renseignements personnels issus de l'assistant vocal et celles des communications électroniques, orales ou écrites[364] provenant là aussi d'un téléphone, particulièrement quant à leur accès par un tiers, dont les autorités, et leur éventuelle interception.

Dans l'affaire *R.* c. *Société Telus Communications*[365]*,* il a été question de déterminer si la demande d'accès par les autorités à des messages textes conservés dans la base de données de l'entreprise et à ceux qui le seront, doit-elle être soumise en vertu du régime sur le mandat général prévu à l'article 487.01(1) du Code criminel. Cet article énonce qu'un tel mandat doit être délivré par un juge lorsque son absence assimilerait l'acte objet du mandat à une fouille, perquisition ou saisie. Cette disposition peut être utilisée à défaut d'autres dispositions législatives, que ce soit dans le code criminel ou dans une autre loi fédérale[366].

Au sujet de l'accès à des communications électroniques par le biais d'une base de données, la Cour suprême a précisé que l'interprétation des mots « intercepter une communication privée » doit se faire en :

---

[362] Ibid. par. 58 ; Voir également *Kranitz* c. *Rogers Cable Inc.,* 2002 CanLII 49415 (ON SC), par. 30.
[363] *Strivastava* c. *Hindu Mission of Canada (Québec) Inc.*, 2001 CanLII 27966 (QC CA) ; *Ste-Marie* c. *Placements J.P.M. Marquis Inc.*, 2005 QCCA 312 (CanLII).
[364] *R.* c. *Société Telus Communications*, 2013 CSC 16 (CanLII), [2013] 2 R.C.S. 3.
[365] Ibid.
[366] Art. 487.01 (1) *c*) du *Code criminel*, L.R.C. (1985), ch. C-46.

> « s'attachant à la prise de connaissance du contenu informationnel de la communication et aux attentes qu'avaient les interlocuteurs en matière de respect de la vie privée au moment de cette communication »[367].

Cette prise de connaissance, selon la Cour suprême, a lieu au cours du processus de transmission des renseignements personnels vers la base de données de l'entreprise. Elle ajoute également que l'interprétation formaliste du mot « intercepter » aurait :

> « essentiellement pour effet de rendre la partie VI [sur les atteintes à la vie privée] inutile en matière de protection du droit à la vie privée dans le cas des nouveaux moyens technologiques de communication textuelle électronique qui génèrent et sauvegardent des copies des communications privées dans le cadre du processus de transmission. Une interprétation étroite est en outre incompatible avec la formulation et l'objet de la partie VI qui accorde une protection étendue aux communications privées contre les ingérences non autorisées de l'État ».

La Cour suprême préconise donc une interprétation plus large de l'alinéa 487.01 (1) *c*) notamment pour éviter que :

> « (…) le mandat général ne soit pas utilisé comme mesure de premier recours, afin d'éviter que les autorités se soustraient aux exigences plus spécifiques ou rigoureuses en matière d'autorisation préalable, comme celles que l'on trouve à la partie VI »[368].

L'apparition extrêmement récente de l'assistant vocal semble porter un coup sévère à la notion de vie privée. La jurisprudence n'a pour l'heure pas eu l'occasion de se prononcer sur l'interprétation d'une telle notion au regard de cette nouvelle technologie, bien que nous ayons vu que différentes décisions, dont celles de la Cour suprême, en ce qui concerne l'interception des communications téléphoniques et la rédaction des conditions d'utilisation. Une émergence qui est venue bouleverser l'application des principes fondamentaux de la protection des renseignements personnels par les fabricants.

---

[367] *R.* c. *Société Telus Communications*, 2013 CSC 16 (CanLII), [2013] 2 R.C.S. 3.
[368] Ibid.

2. L'atteinte aux principes fondamentaux de la protection des renseignements personnels

Lors de la 36e Conférence internationale des commissaires à la protection de la vie privée et des données personnelles, il a été affirmé que « [t]he internet of things is here to stay »[369]. Ces objets connectés sont aujourd'hui bien implantés dans notre vie privée[370] au point que certaines personnes leur accordent une certaine personnalité[371]. Cette intrusion massive dans la sphère privée de l'individu n'est pas sans conséquence sur le respect par les entreprises des principes fondamentaux régissant la protection des renseignement personnels. À travers cette sous-partie nous mettrons en lumière l'absence de validité du consentement en raison d'une insuffisance des informations transmises par le fabricant à l'utilisateur de l'assistant vocal (a). Tout comme l'imprécision des termes des différentes législations régissant la protection des renseignements personnels (b). Aussi, nous aborderons les conséquences du mode de fonctionnement, notamment de la connectivité sans fil, de l'assistant vocal sur cette protection des renseignements personnels (c). L'absence de réelle mesures de sécurité prises par les entreprises est également de nature à bouleverser les principes fondamentaux, principalement en garantissant leur protection durant les différentes étapes de leur traitement (d). Enfin nous terminerons cette sous-partie en mettant en avant le manquement aux droits reconnus à l'utilisateur d'accéder et de modifier ses renseignements personnels détenus par les entreprises (e).

---

[369] 36TH INTERNATIONAL CONFERENCE OF DATA PROTECTION AND PRIVACY COMMISSIONERS, *Mauritius Declaration on the Internet of Things,* Balaclava, 14 October 2014, en ligne : <https://www.cai.gouv.qc.ca/documents/Mauritius-Declaration.pdf >, p.1.

[370] Nous avons cité différents exemples au sein de la première partie d'objets connectés qu'un assistant vocal peut contrôler, voir partie I.A.1.c. ii.

[371] Voir LACHANCE, F., *« O.K. Google, assiste-moi » Les parcours des utilisateurs et des familles qui domestiquent le Google Home,* papyrus.bib.umontreal.ca, Mémoire de maîtrise, Avril 2019, en ligne : <https://papyrus.bib.umontreal.ca/xmlui/bitstream/handle/1866/22464/Lachance_Francois_2019_memoire.pdf?sequence=2&isAllowed=y >.

a) Un consentement pas si libre et éclairé

Tout d'abord, et comme nous l'avons mentionné précédemment, le consentement de l'utilisateur, élément fondamental dans le traitement des renseignements personnels, apparaît comme n'étant pas juridiquement valide. En effet, l'utilisateur ne semble pas avoir pleinement connaissance de toutes les informations relatives aux raisons de la collecte. Ces finalités sont le plus généralement rédigées en des termes flous garantissant à l'entreprise la possibilité de collecter un grand nombre de renseignements[372]. De plus, la facilité avec laquelle il est possible d'activer l'assistant vocal met en lumière un autre problème juridique, celui de son utilisation par des personnes étant incapables de consentir, dont des enfants pouvant prononcer le nom de l'assistant en guise de premier mot[373]. Nous avons cité en première partie le cas d'une mère de famille qui a reçu plusieurs objets commandés par le biais de l'assistant vocal[374]. Il s'est avéré que cette commande a été faite par ses enfants mineurs. L'utilisation d'un assistant vocal par des enfants ne semble pas préoccuper les fabricants. Au contraire, certains d'entre eux ont même mis au point et commercialisé des assistants vocaux, des objets les intégrants et même des « skills » les poussant à interagir davantage avec eux.

Aussi, l'activation résultant d'un faux positif semblerait également engendrer l'enregistrement et la conservation des échanges aussi longtemps que l'utilisateur ne les supprime pas, comme le montre ci-dessous une partie de la lettre de Amazon répondant au sénateur américain Christopher A. COONS.

[372] COMMISSION D'ACCES A L'INFORMATION, *L'invasion des objets connectés : quelles sont les conséquences sur vos renseignements personnels ?,* cai.gouv.qc.ca, 24 avril 2015, en ligne : < https://www.cai.gouv.qc.ca/linvasion-des-objets-connectes-quelles-sont-les-consequences-sur-vos-renseignements-personnels/ > ; COMMISSION D'ACCES A L'INFORMATION, *Rétablir l'équilibre,* Rapport quinquennal, cai.gouv.qc.ca, 2016, en ligne : <http://www.cai.gouv.qc.ca/documents/CAI_RQ_2016.pdf >, p.91 ; PLOURDE, A., « Retour vers le futur : l'Internet des objets et la protection de la vie privée », dans *Développements récents en droit à la vie privée (2019)*, vol. 465, service de la formation continue, Barreau du Québec, Montréal, Edition Yvon Blais, 2019.

[373] LACHANCE, F., *« O.K. Google, assiste-moi » Les parcours des utilisateurs et des familles qui domestiquent le Google Home,* papyrus.bib.umontreal.ca, Mémoire de maîtrise, Avril 2019, en ligne : <https://papyrus.bib.umontreal.ca/xmlui/bitstream/handle/1866/22464/Lachance_Francois_2019_memoire.pdf?sequence=2&isAllowed=y >, pp.86 et s.

[374] CNEWS, « Ils utilisent l'assistant vocal Alexa pour commander pour 700 dollars de jouets », cnews.fr, 19 décembre 2019, en ligne : < https://www.cnews.fr/monde/2019-12-19/ils-utilisent-lassistant-vocal-alexa-pour-commander-pour-700-dollars-de-jouets >.

The answers to your questions are as follows:

1(a). How long does Amazon store the transcripts of user voice recordings?

We retain customers' voice recordings and transcripts until the customer chooses to delete them.

1(b). Do users have the ability to delete any or all of these transcripts?

Customers can review, listen to, and delete voice recordings associated with their account using the Voice History feature available in the Alexa app and the Alexa Privacy Hub, located at www.amazon.com/alexaprivacy. Customers can delete individual voice recordings, voice recordings from particular timeframes, or all of their voice recordings.

When a customer deletes a voice recording, we delete the transcripts associated with the customer's account of both of the customer's request and Alexa's response. We already delete those transcripts from all of Alexa's primary storage systems, and we have an ongoing effort to ensure those transcripts do not remain in any of Alexa's other storage systems. We do not store the audio of Alexa's response. However, we may still retain other records of customers' Alexa interactions, including records of actions Alexa took in response to the customer's request. And when a customer interacts with an Alexa skill, that skill developer may also retain records of the interaction. For example, for many types of Alexa requests – such as when a customer subscribes to Amazon Music Unlimited, places an Amazon Fresh order, requests a car from Uber or Lyft, orders a pizza from Domino's, or makes an in-skill purchase of premium digital content – Amazon and/or the applicable skill developer obviously need to keep a record of the transaction. And for other types of Alexa requests – for instance, setting a recurring alarm, asking Alexa to remind you of your anniversary, placing a meeting on your calendar, sending a message to a friend – customers would not want or expect deletion of the voice recording to delete the underlying data or prevent Alexa from performing the requested task.

Extrait 1. – Lettre du Vice-président de Amazon pour la politique publique en réponse au sénateur Christopher A. Coons[375].

Cette pratique serait contraire aux réglementations encadrant l'utilisation des renseignements personnels. En effet, plusieurs dispositions négligées par les fabricants méritent d'être rappelées, principalement en ce qui concerne le consentement et la collecte. Par exemple, le *Code civil du Québec* prévoit à l'article 35 :

[375] HUSEMAN, B., « Amazon Senator Coons Response Letter », scribd.com, 29 June 2019, en ligne : <https://fr.scribd.com/document/415372739/Amazon-Senator-Coons-Response-Letter#from_embed >.

> « Toute personne a droit au respect de sa réputation et de sa vie privée ; Nulle atteinte ne peut être portée à la vie privée d'une personne sans que celle-ci y consente ou sans que la loi l'autorise ».

Au Québec la *Loi sur la protection des renseignements personnels dans le secteur privé*[376] précise que le consentement doit être « manifeste, libre, éclairé et être donné à des fins spécifiques »[377]. La LPRPSP précise également que la collecte doit viser les renseignements nécessaires à la finalité recherchée par l'entreprise[378]. Cette collecte ne s'opère que :

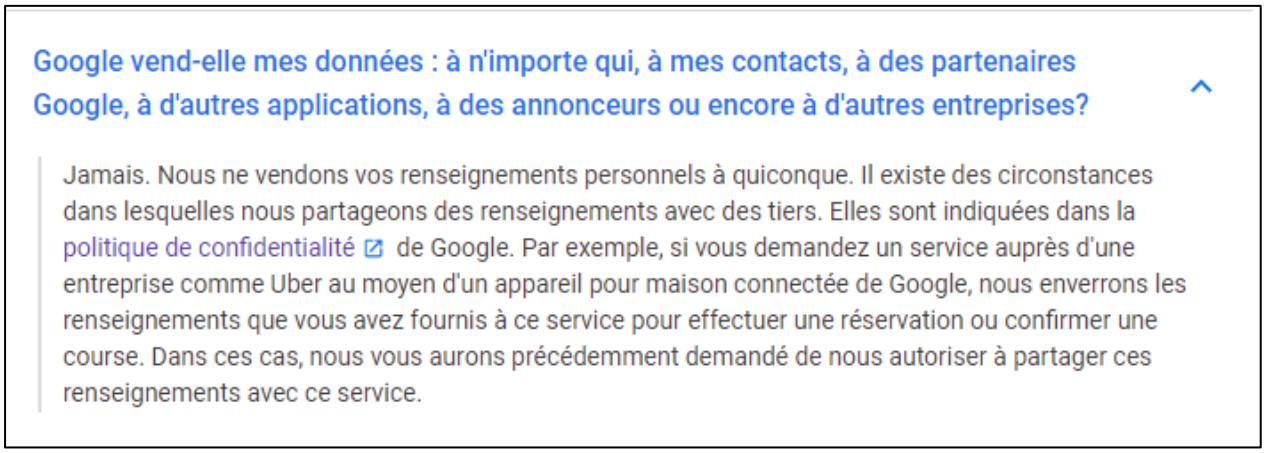
> « (…) si la finalité poursuivie est légitime, importante, urgente et réelle et si l'atteinte au droit à la vie privée consécutive à la collecte, la communication ou la conservation de chaque élément de renseignement est proportionnelle à cette finalité »[379].

Il ressort de ces articles que *a priori* la collecte des renseignements personnels ne doit se faire que si la personne concernée a donné son consentement ou si la loi autorise les entreprises à le faire. Or le problème de ces microphones, et plus généralement de l'assistant vocal, tient dans leur capacité à recueillir des données en masse et de manière continue. Ceci vaut non seulement après la prononciation du mot d'éveil et l'introduction de la requête mais également lors d'une erreur d'interprétation conduisant à l'enregistrement de l'utilisateur. La Commission d'accès à l'information a ainsi mis en garde contre l'atteinte à la protection des renseignements personnels par les objets connectés, dont les principes de collecte et de consentement sont souvent méconnus, pouvant résulter d'une utilisation massive[380]. En utilisant un assistant vocal, l'individu consent en apparence à ce que certains de ses renseignements personnels soient collectés par le fabricant, principalement ceux transmis par la requête. D'ailleurs ces fabricants précisent dans leurs politiques de confidentialité que certains renseignements sont collectés et peuvent être partagés

---

[376] *Loi sur la protection des renseignements personnels dans le secteur privé,* RLRQ c P-39.1 ; Voir également CHASSIGNEUX, C., « Consentement manifeste et éclairé : politique de confidentialité sur Internet », 26 avril 2012, actes du 20e congrès AAPI 2012, Commission d'accès à l'information du Québec. Nous évoquerons ce principe plus en détail dans notre seconde sous-partie.
[377] Art. 14 de la LPRPSP.
[378] Art. 5 de la LPRPSP.
[379] COMMISSION D'ACCES A L'INFORMATION, *La collecte de renseignements personnels,* cai.gouv.qc.ca, en ligne : < https://www.cai.gouv.qc.ca/la-collecte-de-renseignements-personnels/ >.
[380] COMMISSION D'ACCES A L'INFORMATION, *L'invasion des objets connectés : quelles sont les conséquences sur vos renseignements personnels ?,* cai.gouv.qc.ca, 24 avril 2015, en ligne : < https://www.cai.gouv.qc.ca/linvasion-des-objets-connectes-quelles-sont-les-consequences-sur-vos-renseignements-personnels/ >.

avec des entreprises tierces seulement lorsque l'utilisateur a recours à ses services par le biais de l'assistant vocal. Nous pouvons nous baser sur la politique de Google qui, pour le Google Home, prévoit une telle pratique.



Extrait 2. – Partie de la section « Services » de la politique de confidentialité du Google Home[381].

Cependant, ce consentement ne vaudrait selon nous que dans le cas où la personne utilise l'objet. En effet, notre exemple cité précédemment concernant notre couple d'américains constitue une parfaite illustration de la situation où l'utilisateur interagit dans son domicile avec un tiers et ne s'attend pas à ce qu'il soit enregistré. Dans cette hypothèse, nous estimons que le consentement n'est plus valable car l'intéressé n'avait pas l'intention d'utiliser son assistant vocal. N'étant pas informé de l'enregistrement, l'utilisateur sera alors placé dans une situation l'ignorant de l'atteinte à ses droits. Quant à ses renseignements personnels collectés, ils seront traités par la suite par des individus dont il ignore l'existence[382]. Cette information n'apparaît aucunement dans les politiques de confidentialité des fabricants. Ceux-ci se contentent simplement d'évoquer « l'amélioration du service » sans plus de détails pour justifier la collecte et l'utilisation des données[383].

[381] GOOGLE, « En savoir plus sur la sécurité et la confidentialité des données sur les appareils compatibles avec l'Assistant », support.google.com, en ligne : < https://support.google.com/googlenest/answer/7072285?hl=fr >.
[382] CASILLI A., « Derrière les assistants vocaux, des humains vous entendent », laquadratur.net, 18 mai 2018, en ligne : < https://www.laquadrature.net/2018/05/18/temoin_cortana/ >.
[383] Voir l'extrait 3 de la politique de confidentialité du Google Home relative à l'utilisation des données, p.120.

De plus, les informations relatives à la collecte, l'utilisation et la conservation des renseignements personnels se retrouvant sur Internet, l'utilisateur doit donc entreprendre de lui-même les démarches pour en prendre connaissance. Or, la recherche de ces politiques peut le décourager d'y accéder et, quand bien même il le fait, la lecture peut être longue et complexe ce qui entravera davantage l'accès à l'information[384].

b) Des législations en matière de protection de renseignements personnels dépassées par l'assistant vocal

L'assistant vocal met également en lumière le manque de précision ou l'inadéquation des termes employés par les lois de protection des renseignements personnels. Nous pensons plus précisément à la LPRPSP qui prévoit à plusieurs reprises la notion de « dossier ». Cette notion renvoie à l'idée de « tout ce qui est versé dans le dossier physique avec le nom de la personne concernée »[385] (notre soulignement). Les renseignements collectés ne sont pas forcément sauvegardés dans un dossier propre à chaque personne mais garder dans une base de données commune dans laquelle l'intelligence artificielle puise les informations nécessaires et pertinentes à la requête introduite par l'utilisateur.

Une tentative de vouloir interpréter cette notion à la lumière de l'article 3 de la LCCJTI a bien eu lieu[386]. En vertu de cet article, le dossier « peut être composé d'un ou plusieurs documents ». Pour le professeur Gautrais, cette disposition peut s'appliquer à la LPRPSP par le biais du principe de l'équivalence fonctionnelle, c'est-à-dire, en procédant à une application de la LCCJTI aux

[384] CHASSIGNEUX, C., « Consentement manifeste et éclairé : politique de confidentialité sur Internet », 26 avril 2012, actes du 20e congrès AAPI 2012, Commission d'accès à l'information du Québec ; Voir également, MCDONALD, A., M., et FAITH CRANOR, L., *The cost of reading privacy policies,* 2008, ISJLP, Vol. 4:3, en ligne : < https://pdfs.semanticscholar.org/4b51/2e2f5ff42ef00cccceca200d888676e6c506f.pdf >.

[385] DELWAIDE, K., et AYLWIN, A., « Leçons tirées de dix ans d'expérience : la loi sur la protection des renseignements personnels dans le secteur privé du Québec », dans *Développements récents en droit de l'accès à l'information (2005),* service de la formation permanente du Barreau du Québec, 2005.

[386] GAUTRAIS, V., et al., *Rapport auprès de la Commission d'accès à l'information (CAI),* 4 décembre 2015, Centre de recherche en droit public, en ligne : <https://www.gautrais.com/blogue/2015/12/04/rapport-aupres-de-la-commission-dacces-a-linformation/#_ftnref14 >.

documents et dossiers technologiques lorsque ceux-ci remplissent les mêmes fonctions que leur équivalent papier[387].

Cependant, de l'aveu même de la CAI, cette notion est aujourd'hui dépassée par l'émergence de l'Internet des objets[388]. Dans une société où l'information est devenue une ressource importante, celle-ci peut constituer une véritable porte d'entrée dans la vie privée de l'individu[389]. La personne les détenant pourra alors les réutiliser pour en émerger d'autres en agréant les données[390]. Les nouvelles données agrégées échapperont ainsi au consentement de la personne concernée. Le CPVP a d'ailleurs reconnu dans son document portant sur les accessoires intelligents[391] que :

> « (…) dans un monde où les accessoires informatiques et mobiles sont omniprésents, il devient de plus en plus difficile d'appliquer le principe de limitation de la collecte de renseignements personnels sous réserve du consentement donné à des fins déterminées »[392] (notre soulignement).

Cette affirmation est d'autant plus vraie pour l'assistant vocal, notamment à cause de l'utilisation entièrement vocale de l'objet et de la difficulté technique à limiter la collecte de la seule voix de l'utilisateur.

---

[387] ANNONYME, « Définition : Équivalence fonctionnelle », lccjti.ca, en ligne : <https://www.lccjti.ca/definitions/equivalence-fonctionnelle/#ancre1 >; Voir également la partie I.B.1. b) i.

[388] COMMISSION D'ACCES A L'INFORMATION, *Rétablir l'équilibre,* Rapport quinquennal, cai.gouv.qc.ca, 2016, en ligne : < http://www.cai.gouv.qc.ca/documents/CAI_RQ_2016.pdf >, pp.79-80.

[389] POULLET, Y., et HENROTTE, J-F., « La protection des données (à caractère personnel) à l'heure de l'Internet », dans *Protection du consommateur*, pratiques commerciales et T.I.C., coll. Commission Université-Palais, volume 109, Liège, Anthémis 2009, pp. 197-245.

[390] La technique de l'agrégation des données consiste en l'addition de différentes données afin d'aboutir à un résultat permettant d'obtenir une information sur un groupe de personnes, HAUTES ETUDES COMMERCIALES, « Données agrégées - définition », libguide.hec.ca, 30 octobre 2019, en ligne : <https://libguides.hec.ca/c.php?g=246665&p=2662506 >.

[391] COMMISSARIAT A LA PROTECTION DE LA VIE PRIVEE, *Les accessoires intelligents - Défis et possibilités pour la protection de la vie privée*, priv.gc.ca, janvier 2014, en ligne : < https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/recherche/consulter-les-travaux-de-recherche-sur-la-protection-de-la-vie-privee/2014/wc_201401/#heading-004-3 >.

[392] Ibid.

c) Un mode de fonctionnement allant à l'encontre des principes fondamentaux de la protection des renseignements personnels

Au-delà de son utilisation, le fonctionnement de l'assistant vocal remet en cause les principes fondamentaux de la protection des renseignements personnels. Cette remise en cause passe tout d'abord par sa connectivité sans fil poussant l'utilisateur à interagir et manipuler des objets connectés à l'assistant vocal (i) et se confirme à travers l'obligation qui lui est faite de divulguer davantage de renseignements personnels lors de la mise en route de celui-ci (ii).

i. Une connectivité sans fil encourageant l'atteinte à la protection des renseignements personnels

La technologie sans fil est réputée être plus à risque d'un piratage qu'une connexion filaire. Contrairement à une connexion sans fil, dont le piratage peut se faire à distance, dans le cadre d'une connexion au moyen d'un câble Ethernet un pirate doit se brancher physiquement sur le réseau pour être en mesure de le pirater[393]. En outre, l'émission d'ondes produites par le routeur ne peut être délimitée. Celles-ci varient en fonction de l'environnement physique pouvant restreindre la connexion à l'intérieur alors qu'au même moment une personne à l'extérieure peut profiter d'un meilleur signal en l'absence de tels obstacles[394]. Il est donc possible pour un pirate d'accéder à distance par le biais de cet assistant, qui aura alors le rôle de véritable porte d'entrée, non seulement sur le routeur émettant le Wifi mais également au contrôle des autres objets pouvant être liés à l'assistant vocal.

[393] PAUS, L., « WiFi ou Ethernet : Lequel est le plus rapide ? Le plus sûr ? », welivesecurity.com, 4 mai 2018, en ligne : < https://www.welivesecurity.com/fr/2018/05/04/wifi-ethernet-rapide/ >.
[394] Ibid.

L'arrivée prochaine du « WiFi certified 6 »[395], nom donné par la Wifi Alliance[396] pour évoquer la norme IEEE 802.11ax[397], contribuera indirectement à l'atteinte à la vie privée. En effet, en offrant une connexion plus rapide, et en vantant ses vertus, elle encourage les personnes à utiliser davantage les objets connectés. C'est d'ailleurs l'un des objectifs recherchés par la mise en place de cette nouvelle norme, la capacité d'un réseau à pouvoir supporter l'utilisation quotidienne et importante des objets connectés :

> « Wi-Fi CERTIFIED 6 devices meet the highest standards for security and interoperability, and enable lower battery consumption, making it a solid choice for any environment, including the Internet of Things (IoT) »[398] (nos soulignements).

En réalité cette nouvelle norme ouvre la voie à un recours de plus en plus important de la domotique, toujours plus gourmande en renseignements personnels, en faisant croire à l'utilisateur que les objets connectés seront reliés à Internet de manière fluide (interoperability) et en garantissant une protection des renseignements (security). Cet argument de marketing posera sans aucun doute le problème de l'atteinte à la vie privée puisque la maison intelligente offrirait aux entreprises la faculté de tout savoir sur ce qu'il se passe chez l'utilisateur. L'analyse des renseignements personnels peut également amener à la divulgation d'autres types de données émises par l'assistant vocal, parmi les autres objets connectés. Nous pensons tout particulièrement aux métadonnées qui se caractérisent par des informations portant sur la donnée principale (taille, localisation, date et heure de création etc.)[399], qui dans notre cas est le renseignement personnel. L'analyse des métadonnées pourrait servir par la suite aux entreprises en leur fournissant des informations permettant d'établir la survenance d'un évènement ou d'une activité[400] dans le

---

[395] WI-FI ALLIANCE, « Discover Wi-Fi: Wi-Fi certified 6 », wi-fi.org, en ligne : < https://www.wi-fi.org/discover-wi-fi/wi-fi-certified-6 >.

[396] Réseau d'entreprises visant à développer les standards du Wi-Fi et à offrir une interopérabilité en certifiant les équipements nécessaires. WI-FI ALLIANCE, « Discover Wi-Fi: Wi-Fi certified 6 », wi-fi.org, en ligne : < https://www.wi-fi.org/discover-wi-fi/wi-fi-certified-6 >.

[397] L'IEEE est une association professionnelle réunissant des acteurs dans les domaines de l'électroniques et technologiques. Elle élabore des normes techniques permettant d'accompagner l'évolution des technologies. L'une de ces normes, 802.11 porte sur les équipements dotés d'une antenne Wi-Fi. IEEE, « About IEEE », en ligne : <https://www.ieee.org/about/index.html >.

[398] Précitée note 400.

[399] OFFICE QUEBECOIS DE LA LANGUE FRANCAISE, « Grand dictionnaire terminologique : métadonnée », gdt.oqlf.gouv.qc.ca, 2020, en ligne : < http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=8869869 >.

[400] Pour approfondir, voir GINGRAS, P., et SENECAL, F., « Métadonnées : Plaidoyer pour des mal aimées et des incomprises », (2015) 74 Revue du Barreau, pp. 259 à 306.

domicile de l'utilisateur. Une telle pratique exposerait la vie privée de l'utilisateur déjà bien remise en cause par l'usage « normal » de l'assistant vocal.

L'utilisation massive et quotidienne de ces objets connectés engendrera des données sur l'utilisateur et son mode de vie qui pourront servir leurs fabricants. Le déploiement progressif de la nouvelle norme 802.11ax, ou Wifi 6, viendra renforcer le sentiment d'une :

> « (…) désensibilisation des citoyens, qui ne perçoivent plus les risques à l'égard de la protection des renseignements personnels ni l'impact que cette technologie peut avoir sur leur vie actuelle, mais aussi future. En effet, il est permis de penser, entre autres, aux enjeux concernant le stockage et à la conservation des caractéristiques et des mesures biométriques »[401].

L'attraction de l'utilisateur à l'assistant vocal, particulièrement lorsqu'il agit dans un environnement entièrement connecté lui offrant une expérience davantage personnalisable[402], concourrait à limiter l'exercice de ses droits.

ii. L'obligation de divulguer davantage de renseignements personnels par le biais de l'installation d'une application comme préalable à l'utilisation de l'assistant vocal

Ensuite, la remise en cause de ces principes se caractérise par l'imposition à l'utilisateur l'installation d'une application sur son téléphone intelligent. Elle a pour principale fonction de lui servir de centre de contrôle de l'assistant vocal. C'est ainsi que l'utilisateur peut consulter l'historique de ses conversations, modifier ses préférences de ses appareils reliés à l'assistant vocal, et surtout apporter des renseignements concernant le domicile (ex : l'adresse postale qui servira à l'envoi de la facture en cas d'achat effectué par le biais de l'assistant vocal).

[401] COMMISSION D'ACCES A L'INFORMATION, *Rétablir l'équilibre,* Rapport quinquennal, cai.gouv.qc.ca, 2016, en ligne : < http://www.cai.gouv.qc.ca/documents/CAI_RQ_2016.pdf >, p.102.
[402] BOURCIER, D. et DE FILIPPI, P. (dir), *Open Data & Big Data: nouveaux défis pour la vie privée*, Paris, Mare & Martin, 2016, p.110.

L'installation d'une telle application requiert énormément de renseignements personnels à fournir semblant *a priori* faire échec au test de *Oakes* lorsqu'il est appliqué en vertu de la LPRPDE[403]. En effet, alors même qu'en vertu de ce test, une balance devait être faite entre les intérêts de l'entreprise et la vie privée de l'individu, selon la CAI, la collecte des renseignements personnels par les objets connectés :

> « semble dépasser ce qui est nécessaire pour assurer l'offre de service de l'objet en question. De plus, l'interconnectivité croissante de ces objets fait craindre une augmentation considérable de la quantité de renseignements personnels collectés et par conséquent amplifie l'intrusion dans la vie privée des utilisateurs »[404] (nos soulignements).

Ainsi que l'affirmait M[e] Plourde, le test de *Oakes* est parfaitement adapté aux cas d'atteinte à la vie privée en dehors de l'environnement des objets connectés[405]. Cependant, les technologies comme l'assistant vocal rendent ce test inadapté. La capacité à recueillir massivement des renseignements personnels tout en couvrant cette pratique par la rédaction en des termes imprécis des finalités de la collecte, empêche l'utilisateur de déterminer justement quel renseignement a été nécessaire de celui qui ne l'est pas[406] même si une interprétation stricte de la « nécessité » a été adoptée par la CAI[407].

---

[403] *Société de transport de la Ville de Laval* c. *X et al.*, 2003 CanLII 44085 (QC C.Q.) ; *Mountain Province Diamonds Inc.* v. *De Beers Canada Inc.,* 2014 ONSC 2026 (CanLII) ; Voir aussi, PLOURDE, A., « Retour vers le futur : l'Internet des objets et la protection de la vie privée », dans *Développements récents en droit à la vie privée (2019)*, vol. 465, service de la formation continue, Barreau du Québec, Montréal, Edition Yvon Blais, 2019.

[404] COMMISSION D'ACCES A L'INFORMATION, *L'invasion des objets connectés : quelles sont les conséquences sur vos renseignements personnels ?,* cai.gouv.qc.ca, 24 avril 2015, en ligne : < https://www.cai.gouv.qc.ca/linvasion-des-objets-connectes-quelles-sont-les-consequences-sur-vos-renseignements-personnels/ >.

[405] PLOURDE, A., « Retour vers le futur : l'Internet des objets et la protection de la vie privée », dans *Développements récents en droit à la vie privée (2019)*, vol. 465, service de la formation continue, Barreau du Québec, Montréal, Edition Yvon Blais, 2019.

[406] PLOURDE, A., « Retour vers le futur : l'Internet des objets et la protection de la vie privée », dans *Développements récents en droit à la vie privée (2019)*, vol. 465, service de la formation continue, Barreau du Québec, Montréal, Edition Yvon Blais, 2019.

[407] *Regroupement des comités logements et Association des locataires du Québec* c. *Corporation des propriétaires immobiliers du Québec*, Rapport d'enquête [1995] C.A.I. 370 (C.A.I.).

d) L'absence de réelles mesures de sécurité garantissant la protection des renseignements personnels lors de l'utilisation de l'assistant vocal

Par cette pratique que nous démontrons tout au long de ce développement, les entreprises semblent ne pas adopter la bonne approche pour garantir la sécurité des renseignements personnels. En effet, comme l'a précisé le CPVP dans ses conclusions d'enquête n°2007-389 :

> « L'expérience de TJX/WMI illustre bien comment la conservation d'importantes quantités de renseignements de nature délicate peut constituer un danger, particulièrement si les renseignements n'ont aucune utilité légitime ou si on les conserve plus longtemps que nécessaire »[408] (notre soulignement).

Le CPVP précise également que les renseignements collectés par erreur alors que ceux-ci ne devraient pas l'être obligent l'entreprise à les conserver avant de les détruire tout en s'assurant par la suite de leur caractère inutilisable[409]. Nous nuançons ces propos du CPVP en rappelant qu'en l'état actuel des technologies, il est difficile voire impossible pour un assistant vocal de n'enregistrer par le biais de ses capteurs les seules paroles de l'utilisateur et non de celles d'un tiers conversant en même temps et à proximité. Bien que le législateur ait toujours la possibilité d'interdire à la vente une telle technologie, nous estimons qu'une telle action viendrait brider l'évolution technologique qui nuirait indirectement à la société. Nous pensons par ailleurs que l'utilisation de l'assistant vocal ne comporte pas que des inconvénients, même si tout au long de ce mémoire nous avons démontré l'inverse, mais peut être particulièrement utile pour certaines personnes comme celles atteintes d'un handicap.

En ce qui concerne la sécurité d'un point de vue plus général, l'assistant vocal est une technologie très récente et n'ayant pas bénéficiée d'une certaine maturité en termes de sécurité. Autrement dit,

---

[408] COMMISSARIAT A LA PROTECTION DE LA VIE PRIVEE, *Rapport de conclusions d'enquête en vertu de la LPRPDE n°2007-389 : TJX Companies Inc./ Winners Merchant International L.P.,* priv.gc.ca, 25 septembre 2007, en ligne : < https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2007/tjx_rep_070925/ >, par. 3.

[409] COMMISSARIAT A LA PROTECTION DE LA VIE PRIVEE, *Rapport de conclusions d'enquêtes en vertu de la LPRPDE n°2011-001 : La collecte de données Wi-Fi par Google Inc.,* priv.gc.ca, 20 mai 2011, en ligne : <https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2011/lprpde-2011-001/ >.

les entreprises n'ont pas eu suffisamment de temps pour développer des mesures de sécurité robustes. La mise en place d'une protection effective peut s'avérer être coûteuse et complexe à mettre en place à la fois pour l'entreprise[410] mais aussi pour le particulier[411] utilisant l'assistant vocal. Si les entreprises ont la possibilité d'engager massivement des moyens humains, financiers et matériels pour offrir un niveau de sécurité élevé, le réseau internet d'une personne ne pourra garantir un niveau de protection comparable pour contrer des attaques. Nous ne développerons pas dans ce développement toutes les techniques de piratages possibles de l'assistant vocal, mais seulement celles qui nous paraissent comme étant les plus marquantes dans la démonstration de sa vulnérabilité.

Cette insuffisance dans l'instauration des mesures de sécurité contraste avec le strict encadrement de l'utilisation des renseignements biométriques, notamment en Europe. Le RGPD prévoit en son article 9 l'interdiction du traitement des données biométrique :

> « Le traitement des données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique sont interdits »[412].

Cette réglementation ne vaut toutefois pas pour la personne qui fait un usage strictement privé des renseignements personnels[413]. À la différence d'une conversation téléphonique privée durant laquelle il est possible de demander au tiers de s'éloigner pour ne pas la perturber, le fabricant pourra profiter des renseignements personnels sensibles recueillis pour atteindre des finalités commerciales et marketing. En d'autres termes, les renseignements collectés vont servir

---

[410] Nous référons le lecteur vers la thèse du professeur Vermeys concernant les coûts économiques de la mise en place de mesures et contre-mesures pour garantir un niveau de sécurité acceptable, VERMEYS, N. W., *Qualification et quantification de l'obligation de sécurité informationnelle dans la détermination de la faute civile*, papyrus.bib.umontreal.ca, Thèse de doctorat, Université de Montréal, Mars 2009, en ligne : <https://papyrus.bib.umontreal.ca/xmlui/bitstream/handle/1866/3663/12085490.PDF?sequence=2&isAllowed=y>.

[411] REY, B., *La vie privée à l'ère du numérique,* Lavoisier, coll. « Traitement de l'information », 2012, p.166.

[412] Le paragraphe 2 de ce même article prévoit des exceptions à l'interdiction de traitement, parmi lesquelles nous retrouvons le consentement explicite de la personne.

[413] Art. 2 c) du RGPD ; Une telle disposition est également présente au sein de la LPRPDE à l'article 4 (2) b), et de manière implicite à l'article 10 de la LPRPSP en évoquant la condition d'exploitation d'une entreprise par une personne.

l'entreprise, en plus d'améliorer son produit, à émettre des annonces publicitaires en fonction du centre d'intérêt de l'individu identifié par le biais du traitement de ses informations sensibles et privées.

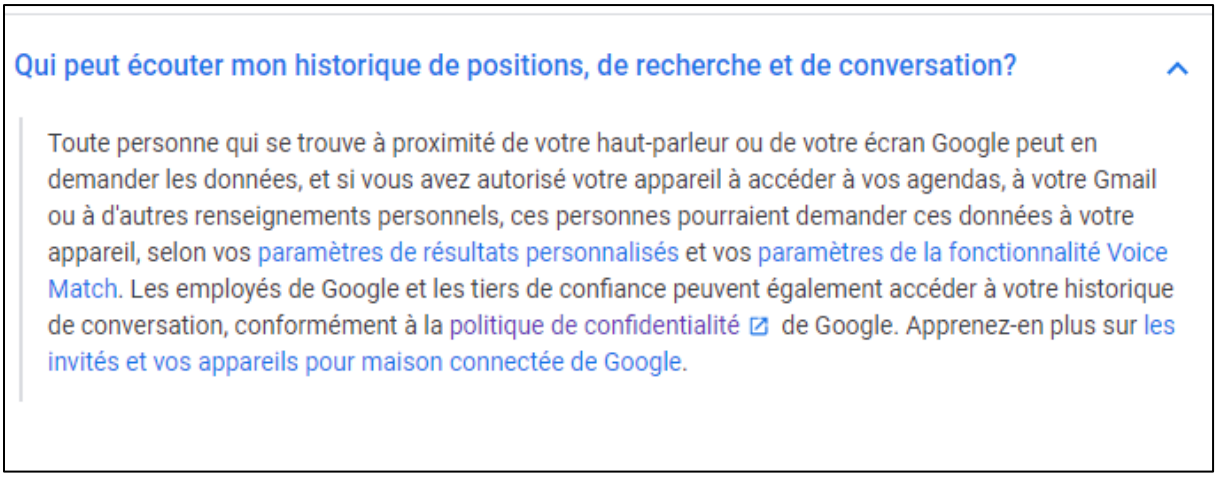
Le maniement simpliste de l'assistant vocal aboutit à la divulgation non intentionnelle d'informations sensibles portant sur le comportement de l'utilisateur et pouvant par la même occasion en révéler d'autres, notamment en ce qui concerne son corps[414] ou permettre l'identification de son entourage. Ces nouvelles informations seront alors qualifiées de renseignements personnels[415]. La collecte de ces renseignements se fait en l'absence de tout consentement de la part du tiers. L'activation simpliste de l'assistant vocal ouvre la porte à son fabricant, et généralement son entraîneur, à l'acquisition de renseignements personnels touchant des personnes au-delà du seul utilisateur. Un parallèle peut être fait avec une conversation téléphonique. Au cours de l'échange, il est possible d'entendre les personnes à proximité sans que celles-ci consentent à ce qu'elles soient écoutées. Cependant, il nous est impossible de mémoriser la conversation dans ses moindres détails. Alors que l'assistant vocal dispose de cette capacité et restitue ce qu'il a compris à son entraîneur qui bénéficiera de renseignements personnels supplémentaires[416].

---

[414] GAUTHIER, J.M., *Cadre juridique de l'utilisation de la biométrie au Québec : sécurité et vie privée,* papyrus.bib.umontreal.ca, Mémoire de maîtrise, Avril 2014, Centre de recherche en droit public, Faculté de Droit, Université de Montréal, en ligne : <https://papyrus.bib.umontreal.ca/xmlui/bitstream/handle/1866/11879/Gauthier_Julie_Mira_2014_memoire.pdf?sequence=2&isAllowed=y >.

[415] Tout dépend de l'usage qu'il en est fait de la voix. Pris individuellement, il est peu probable que la voix puisse servir à identifier formellement la personne ; Voir GRATTON, E., *Redefining Personal Information in the Context of the Internet,* papyrus.bib.umontreal.ca, Thèse de doctorat, Faculté de droit, Université de Montréal, Université Panthéon-Assas Paris II, Octobre 2012, en ligne : <https://papyrus.bib.umontreal.ca/xmlui/bitstream/handle/1866/19676/Gratton_Eloise_2012_these.pdf?sequence=4&isAllowed=y > ; Voir également *Gordon c. Canada*, précité note 104 ; DE TERWANGNE, C., et ROSIER, K., (dir), *Le Règlement Général sur la Protection des Données (RGPD/GDPR) : Analyse approfondie,* coll. Crids, Larcier, 2018, p. 262.

[416] CASILLI A., « Derrière les assistants vocaux, des humains vous entendent », laquadratur.net, 18 mai 2018, en ligne : < https://www.laquadrature.net/2018/05/18/temoin_cortana/ >.



Extrait 3. – Partie de la section « L'Assistant Google et ma vie privée » de la politique de confidentialité du Google Home[417].

En reprenant la politique de confidentialité du Google Home, il apparait clairement que toute personne proche de l'assistant vocal peut l'activer et introduire une requête. Aussi, Google précise que dans le cas d'une association de l'assistant vocal à certains services tels que Gmail, un tiers y aura également accès.

L'accessibilité de l'assistant vocal par différentes personnes remet en cause la protection des renseignements personnels en leur accordant un accès sans aucun contrôle aux données, notamment biométriques. Comme en témoigne l'extrait ci-dessous de la politique de confidentialité de Google n'importe quelle personne peut interagir avec l'assistant vocal à condition de prononcer le mot d'éveil. Cette pratique met également en lumière la faiblesse de l'identification du locuteur par l'assistant vocal en étant incapable de déterminer la personne qui s'adresse à lui et ainsi restreindre l'accès à certaines données. Chaque fabricant exige la création d'un compte via une application mobile. Or, le titulaire du compte ne fait pas de lui la seule personne autorisée à interagir avec l'assistant vocal.

[417] GOOGLE, « En savoir plus sur la sécurité et la confidentialité des données sur les appareils compatibles avec l'Assistant », support.google.com, en ligne : < https://support.google.com/googlenest/answer/7072285?hl=fr >.

Les invités et vos appareils pour maison connectée de Google

Toute personne invitée à votre domicile pourrait interagir avec vos appareils et vos services pour maison connectée de Google. Par exemple, toute personne se trouvant dans votre domicile, y compris un invité, peut activer le haut-parleur et afficher les appareils de votre domicile en disant « Ok Google », « Hey Google » ou en utilisant une autre méthode d'activation, comme effectuer un appui prolongé sur votre appareil. Pour mieux comprendre comment Google protège votre confidentialité lorsque vous utilisez nos appareils et nos services pour maison connectée, continuez à lire les explications ci-dessous et consultez la FAQ relative à la confidentialité Google Nest. Vous pouvez également en savoir plus sur l'Assistant Google et votre confidentialité.

Extrait 4. – Partie de la section « Google Home et votre confidentialité » de la politique de confidentialité du Google Home[418].

Ces éléments apparaissent explicitement sur le site de Google mais interrogent quant à la notion de « toute personne ». Celle-ci s'avère être beaucoup trop large et englobe plusieurs types de personnes, à commencer par les plus jeunes. Sa simplicité d'utilisation est à la fois un avantage pour des personnes, handicapées ou peu à l'aise avec les technologies, et un inconvénient, notamment lorsqu'il est utilisé par des mineurs.

Afin d'illustrer nos propos, nous pouvons prendre l'exemple de familles interrogées par François Lachance dans le cadre de son mémoire sur l'appropriation du Google Home[419]. Parmi celles rencontrées, certaines ont affirmé que l'usage répétitif de l'assistant vocal en présence de leur enfant a eu une incidence sur son apprentissage, notamment dans la prononciation de ses premiers mots[420].

Les fabricants ont bien conscience que des enfants ont un accès facile à leur assistant vocal. C'est dans cette optique que Amazon a mis en place une version spéciale de son enceinte Echo intégrant l'assistant vocal Alexa destinée aux enfants. En complément des « skills » disponibles pour divertir

[418] GOOGLE, « Les invités et vos appareils pour maison connectée de Google », support.google.com, en ligne : <https://support.google.com/googlenest/answer/7177221?hl=fr-ca >.
[419] LACHANCE, F., *« O.K. Google, assiste-moi » Les parcours des utilisateurs et des familles qui domestiquent le Google Home,* papyrus.bib.umontreal.ca, Mémoire de maîtrise, Avril 2019, en ligne : <https://papyrus.bib.umontreal.ca/xmlui/bitstream/handle/1866/22464/Lachance_Francois_2019_memoire.pdf?sequence=2&isAllowed=y >.
[420] Ibid. pp.86-87.

voire permettre à l'enfant d'interagir avec l'assistant vocal, la commercialisation d'un tel objet connecté aux enfants est de nature à porter une atteinte à leur vie privée.

En effet, les enfants utilisent des objets dont ils ne maîtrisent pas le système de fonctionnement ni les possibles conséquences de leur interaction sur la protection de leurs renseignements personnels. Or, l'utilisation simpliste de l'assistant vocal liée à sa personnification[421] tendent à effacer le sentiment d'être en face d'une simple machine. C'est ainsi que des enfants peuvent être amenés à jouer avec l'assistant vocal sans forcément s'en rendre compte[422] voire en profiter pour effectuer des achats à l'abri des regards des parents[423].

Or, comme nous l'avons évoqué précédemment, des personnes extérieures à l'entreprise commercialisant l'assistant vocal sont chargées d'écouter les enregistrements sonores[424]. De ce fait, le tiers analysant la conversation obtiendra un accès à un tel renseignement de nature confidentiel, et étant donné qu'il sera rattaché à un autre[425], il sera alors tout à fait possible d'identifier les personnes à proximité de l'utilisateur. Dans notre hypothèse, l'algorithme ne saura pas opérer un tri de la conversation entre ce qui relève de la qualification de « renseignement personnel » de ce qui ne l'est pas afin de le masquer pour empêcher toute divulgation.

La collecte de la voix, mode naturel de communication[426], est de nature à augmenter les risques « que les données biométriques soient captées à l'insu des individus »[427]. Tout comme la collecte,

---

[421] Ibid.
[422] CAREY, B., « The first Alexa toy is a $300 kitchen for kids, packed with dad jokes », cnet.com, 22 février 2020, en ligne : < https://www.cnet.com/news/first-amazon-alexa-toy-is-300-kidkraft-kitchen-for-kids/ >.
[423] CNEWS, « Ils utilisent l'assistant vocal Alexa pour commander pour 700 dollars de jouets », cnews.fr, 19 décembre 2019, en ligne : < https://www.cnews.fr/monde/2019-12-19/ils-utilisent-lassistant-vocal-alexa-pour-commander-pour-700-dollars-de-jouets >.
[424] CASILLI A., « Derrière les assistants vocaux, des humains vous entendent », laquadratur.net, 18 mai 2018, en ligne : < https://www.laquadrature.net/2018/05/18/temoin_cortana/ >.
[425] *Gordon* c. *Canada* (Santé), 2008 CF 258.
[426] MINKER, W., et NEEL, F., « Développement des technologies vocales », dans *Le travail humain*, vol. 65, 2002/3, en ligne : < https://www.cairn.info/revue-le-travail-humain-2002-3-page-261.htm#pa23 >, p.267.
[427] GAUTHIER, J.M., *Cadre juridique de l'utilisation de la biométrie au Québec : sécurité et vie privée,* papyrus.bib.umontreal.ca, Mémoire de maîtrise, Avril 2014, Centre de recherche en droit public, Faculté de Droit, Université de Montréal, en ligne : <https://papyrus.bib.umontreal.ca/xmlui/bitstream/handle/1866/11879/Gauthier_Julie_Mira_2014_memoire.pdf?sequence=2&isAllowed=y >, p. 86.

le stockage dans des serveurs à distance renforce le risque d'atteinte à ce genre de renseignement personnel[428] car l'individu n'aura pas de réel contrôle.

Le risque d'atteinte aux renseignements personnels par l'absence de mesures de sécurité adéquates est davantage renforcé par l'interaction de l'assistant vocal avec d'autres objets connectés reliés au réseau privé de leur utilisateur. Ceux-ci ne dépendant pas forcément du fabricant de l'assistant vocal, leur niveau de sécurité ne serait donc pas suffisamment robuste pour prévenir toute action malveillante. Les entreprises les commercialisant n'auront pas nécessairement la même vision voire les mêmes moyens pour garantir une sécurité optimale. Bien souvent la sécurité est négligée pour des raisons économiques et pour ne pas la répercuter sur le prix de l'objet[429]. L'utilisation de divers objets connectés ayant des niveaux de sécurité variés profiterait sans aucun doute à un pirate informatique qui aura la possibilité de s'y infiltrer par l'un de ces nombreux points d'accès qu'ils offrent et de corrompre le réseau[430]. Cette technique du « man in the middle » lui permettra par la suite d'intercepter les renseignements et leurs métadonnées pour ensuite les envoyer vers un serveur en vue de les récolter à l'abris des regards[431]. D'autres techniques, plus sophistiquées, et tout aussi dévastateur pour la vie privée de l'utilisateur et de ses renseignements personnels, existent. Parmi elles, celle de l'hameçonnage vocal, également appelée en anglais « vishing ». Cette nouvelle forme de piratage est apparue avec les technologies vocales comme le téléphone et se développe avec l'assistant vocal. Elle se présente comme une variante de l'hameçonnage classique, « phishing », consistant à obtenir des renseignements personnels en faisant croire à la victime qu'elle s'adresse à un tiers de confiance dans le but de lui usurper son identité[432]. L'hameçonnage vocal dans l'assistant vocal se caractérise par l'ajout d'un code dans le logiciel de l'assistant vocal

---

[428] COMMISSARIAT A LA PROTECTION DE LA VIE PRIVEE, *Des données au bout des doigts,* priv.gc.ca, février 2011, en ligne : < https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/renseignements-sur-la-sante-renseignements-genetiques-et-autres-renseignements-sur-le-corps/gd_bio_201102/ >.

[429] Voir notamment pour ce qui est de l'analyse économique du risque, VERMEYS, N. W., *Qualification et quantification de l'obligation de sécurité informationnelle dans la détermination de la faute civile*, papyrus.bib.umontreal.ca, Thèse de doctorat, Université de Montréal, Mars 2009, en ligne : <https://papyrus.bib.umontreal.ca/xmlui/bitstream/handle/1866/3663/12085490.PDF?sequence=2&isAllowed=y >, pp. 292 et s.

[430] CENTRE CANADIEN POUR LA CYBERSECURITE, « L'Internet des objets à la maison », pensezcybersecurite.gc.ca, 21 décembre 2018, en ligne : < https://www.pensezcybersecurite.gc.ca/cnt/rsks/ntrnt-thngs/hm-fr.aspx >.

[431] CALÉ, S., et TOUITOU, P., *La sécurité informatique : réponses techniques, organisationnelles et juridiques,* Hermès Sciences publications, Paris, 2007, p.82.

[432] OFFICE QUEBECOIS DE LA LANGUE FRANCAISE, « Grand dictionnaire terminologique : hameçonnage », gdt.oqlf.gouv.qc.ca, 2016, en ligne : < http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=8869710 >.

lors d'une mise à jour[433]. Les fabricants, ayant leur propre plateforme d'application, tels que Google ou Apple, vont vérifier la sécurité de l'application avant de la rendre disponible. Toutefois, les mises à jour publiées par la suite échappent à ce contrôle[434]. Le code malicieux installé, l'application, ou « skill », fera croire à l'utilisateur qu'une erreur a eue lieu et qu'il doit lancer une mise à jour comportant un correctif[435]. En réalité, le microphone reste activé sans que son utilisateur ne le sache. Une fois que le mot de passe prononcé aura confirmé le lancement de ladite mise à jour, le pirate n'aura plus qu'à accéder au compte de l'utilisateur[436]. Une autre variante de cet hameçonnage vocal consiste à modifier les mots clés des commandes vocales d'une « skill » afin de garder le microphone allumé tout en faisant croire à l'utilisateur que l'assistant est éteint après la prononciation du mot clé. Cette modification se fait par l'ajout à la commande vocale d'une suite de caractère imprononçable ou d'un laps de temps de silence. L'utilisateur pensant avoir fermé l'application se retrouvera être enregistré en continu car la commande vocale a été changée.

Enfin, la dernière technique que nous allons évoquer est qualifiée de « surfing attack ». Cette technique, aussi impressionnante qu'inquiétante offre la possibilité au pirate de prendre le contrôle de l'assistant vocal à partir de vibrations insonores. Les vibrations émises par le transducteur piézoélectrique[437] vont circuler sur la surface plate d'un meuble ayant des propriétés favorisant une telle circulation (ex : une table en bois) pour atteindre le téléphone, à condition bien entendu qu'il y soit posé. Sur une table et face à ces vibrations, le téléphone intelligent agit comme un mur captant ainsi toutes les ondes se dirigeant vers lui. Nous précisons que cette méthode a été testée

[433] AUCLERT, F., « Alexa et Google Home : de nouvelles failles exploitées par des pirates pour vous écouter », futura-science.com, 22 octobre 2019, en ligne : < https://www.futura-sciences.com/tech/actualites/objets-connectes-alexa-google-home-nouvelles-failles-exploitees-pirates-vous-ecouter-68518/ >.
[434] Ibid.
[435] CENTRE CANADIEN POUR LA CYBERSECURITE, « Cyberjournal numéro 11 », cyber.gc.ca, 11 juin 2017, en ligne : < https://cyber.gc.ca/fr/orientation/cyberjournal-numero-11-juin-2017 >.
[436] AUCLERT, F., « Alexa et Google Home : de nouvelles failles exploitées par des pirates pour vous écouter », futura-science.com, 22 octobre 2019, en ligne : < https://www.futura-sciences.com/tech/actualites/objets-connectes-alexa-google-home-nouvelles-failles-exploitees-pirates-vous-ecouter-68518/ >.
[437] Le transducteur est un « [d]ispositif activé par un système et qui retransmet son signal, souvent sous une autre forme, vers un second système », OFFICE QUEBECOIS DE LA LANGUE FRANCAISE, « Grand dictionnaire terminologique : transducteur », gdt.oqlf.gouv.qc.ca, 2012, en ligne : <http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=26522218 > ; Le transducteur piézolélectrique est un « type of electroacoustic transducer that convert the electrical charges produced by some forms of solid materials into energy », ANNONYME, « What is a transducer ? », americanpiezo.com, en ligne : < https://www.americanpiezo.com/piezo-theory/whats-a-transducer.html >.

sur les téléphones intelligents équipés d'un assistant vocal mais il ne fait aucun doute sur la possibilité d'utiliser cette technique sur des enceintes connectées.

Cette méthode du « surfing attack » exploite un défaut technique de l'assistant vocal qui se retrouve dans les téléphones intelligents et les enceintes connectées. En effet, dans notre développement sur le fonctionnement du traitement automatique du langage naturel, nous avons parlé du microphone qui converti le signal sonore en un signal électrique[438]. Il s'agit ni plus ni moins d'un transducteur. Dans le cadre de cette technique de piratage, l'assistant vocal reçoit directement un signal électrique sans avoir à convertir un quelconque signal sonore. La deuxième faille réside dans le caractère insonore des vibrations. En d'autres termes, il ne sera pas possible pour l'homme de déceler ces signaux. La seule possibilité pour lui de s'en apercevoir est de garder un œil sur son téléphone et de veiller à ce qu'il ne s'active pas. Ce cas peut être extrêmement préjudiciable si l'assistant vocal est activé par une personne à proximité, principalement quand on connaît la facilité par laquelle il est possible de le faire. Afin de mieux saisir l'impact d'un tel manque de sécurité, prenons l'hypothèse où un groupe de personnes assistent à une réunion et que l'une d'elles pose son téléphone sur la table. Un tiers malveillant pourra ensuite par le biais de la « surfing attack » le contrôler en activant l'assistant vocal, et ce, sans se faire repérer car les personnes seront occupées à interagir entre elles.

La vulnérabilité de l'assistant vocal illustre à quel point il reste tant d'effort à réaliser pour tenter d'atteindre un niveau de sécurité qu'une personne raisonnable est en droit de s'attendre. Des mesures que les entreprises tardent à appliquer en raison notamment des coûts qu'elles représentent[439]. Par ailleurs, tout comme pour la procédure de suppression des renseignements personnels décrite plus haut, l'utilisateur ne peut de lui-même s'assurer des mesures de sécurité prises par le fabricant. Cette « contrainte » l'oblige à suivre les affirmations des politiques de confidentialité car en « l'absence de processus obligatoires de vérification préalables à la mise en

[438] Voir supra partie I.A.3.a).
[439] PLOURDE, A., « Retour vers le futur : l'Internet des objets et la protection de la vie privée », dans *Développements récents en droit à la vie privée (2019)*, vol. 465, service de la formation continue, Barreau du Québec, Montréal, Edition Yvon Blais, 2019.

marché, il [l'utilisateur] n'a guère d'autre choix que de faire aveuglément confiance à ces énoncés »[440].

Nous terminons sur les mesures de sécurité par évoquer la négligence des entreprises à former adéquatement les personnes chargées d'écouter les enregistrements. Celles-ci ne sont recrutées que sur la base d'un examen de connaissance de leur langue maternelle. L'entreprise ne vérifie pas au travers d'une enquête de sécurité et / ou de personnalité si un candidat présente les compétences requises pour accéder et manipuler des renseignements personnels d'une certaine sensibilité[441]. Et cette « dresseuse d'IA » d'affirmer que « (…) sur plus d'une cinquantaine de pages d'instructions détaillées sur comment traiter les transcriptions, pas une seule ligne ne mentionnait le respect de la vie privée des utilisateurs »[442] (notre soulignement). Cette méthode de recrutement du personnel va à l'encontre du principe d'adoption de mesures de sécurité. Le défaut de formation constitue en vertu de la LPRPDE ou du RGPD un manquement grave. En outre, le manque de surveillance des employés lors de leur accès aux renseignements personnels peut ouvrir la voie à la commission de certaines fraudes, dont celle qualifiée de « fraude du président ». Cette technique reposait initialement sur l'envoi d'un courriel frauduleux signé par le président d'une entreprise à certains des employés leur demandant par exemple d'effectuer un transfert d'une somme importante d'argent vers un compte bancaire détenue par une personne malveillante. Aujourd'hui grâce aux technologies intégrant le TALN, une personne ayant accès aux enregistrements sonores d'un utilisateur peut les réutiliser en détournant la voix pour se faire passer pour le véritable utilisateur dans le cadre de cette fraude du président. Un tel procédé a été utilisé par des personnes se faisant passer pour Jean-Yves Le Drian, ancien ministre de la Défense et actuellement ministre de l'Europe et des Affaires étrangères[443]. Ces personnes sont même aller jusqu'à organiser des réunions par visioconférence tout en utilisant la voix du ministre[444]. Cette fraude, et plus globalement le vol

[440] PLOURDE, A., « Retour vers le futur : l'Internet des objets et la protection de la vie privée », dans *Développements récents en droit à la vie privée (2019)*, vol. 465, service de la formation continue, Barreau du Québec, Montréal, Edition Yvon Blais, 2019.
[441] CASILLI A., « Derrière les assistants vocaux, des humains vous entendent », laquadratur.net, 18 mai 2018, en ligne : < https://www.laquadrature.net/2018/05/18/temoin_cortana/ >.
[442] Ibid.
[443] GOUVERNEMENT, « Biographie : Jean-Yves Le Drian », gouvernement.fr, en ligne : <https://www.gouvernement.fr/ministre/jean-yves-le-drian >.
[444] AUDOUIN, C., « Arnaque au faux Le Drian » : l'avocate du ministre détaille le fonctionnement d'une escroquerie hors pair », franceinter.fr, 4 février 2020, en ligne : < https://www.franceinter.fr/arnaque-au-faux-le-drian-l-avocate-du-ministre-detaille-le-fonctionnement-d-une-escroquerie-hors-pair >.

d'identité, constitue une atteinte au principe 4.7.1 de la LPRPDE obligeant à prévenir tout vol ou réutilisation non autorisée de renseignement personnel[445].

e) L'atteinte à l'effectivité des droits reconnus à l'utilisateur dans la protection de ses renseignements personnels

L'atteinte aux droits reconnus à l'individu découle essentiellement de la conservation de ses renseignements personnels dans un pays étranger l'empêchant d'y avoir un réel accès (i). Cette situation offre notamment la possibilité pour les fabricants d'assistants vocaux de réutiliser les renseignements personnels à des fins de profilage (ii).

i. Une remise en cause de ses droits résultant de la conservation des renseignements personnels en dehors de son pays.

La transmission et la conservation des renseignements personnels dans des serveurs bien souvent localisés dans un pays étranger, ou virtuellement dans un nuage informatique, tendent à limiter l'effectivité à la fois des droits de l'individu d'y accéder, de les modifier et éventuellement de les supprimer. En effet, l'absence de possibilité pour l'utilisateur d'avoir un accès physique au lieu où sont conservés ses renseignements personnels, ou du moins à un recueil les consignant, l'oblige à se fier à l'honnêteté de l'entreprise dans l'exercice de ses droits. En outre, les renseignements personnels à l'étranger ne seront plus soumis à la législation du pays « émetteur » mais au pays « récepteur ». Pour tenter de lutter contre ces situations, les législations récentes intègrent des dispositions applicables à l'étranger. C'est notamment le cas du RGPD contenant des dispositions de portée extraterritoriale[446].

Cependant, l'application de telles dispositions relèvent avant tout de la bonne volonté du pays d'accueil de vouloir les appliquer aux entreprises présentes sur son territoire. Nous pouvons citer

[445] Nous précisons qu'une telle action malveillante est réprimée par l'article 403 (1) et (3) du *Code criminel*, L.R.C. (1985), ch. C-46.
[446] Nous pensons notamment au RGPD mettant en place le code de bonne conduite et les différents types de transfert selon les articles 40 et s.

l'exemple des États-Unis et de l'Union européenne. Seules les entreprises ayant adhérées au *Privacy Shield*[447] sont contraintes de respecter le RGPD lorsqu'elles font affaires avec un citoyen européen présent au sein de l'Union européenne[448]. S'agissant d'un individu présent au Québec, l'entreprise, étrangère ou non, en plus de devoir respecter la LPRPSP, doit également se conformer aux exigences de la LPRPDE puisqu'elle s'applique à l'international[449], ce qui n'est pas le cas de la loi québécoise[450].

Il n'existe donc à ce jour aucun moyen de contrôle par l'individu qu'une entreprise a effectivement fait droit à sa demande d'accès, de modification ou de suppression des renseignements personnels. Au contraire, il semblerait que les entreprises soient réticentes à vouloir réellement supprimer les renseignements lorsque l'utilisateur le requiert car ils constituent pour elles un investissement important[451]. Si l'on reprend le cas de notre Google Home, dont les renseignements personnels

---

[447] *EU-U.S. Privacy Shield framework principles issued by the U.S department of commerce*¸ 23 février 2016, en ligne : < https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004qAg >.

[448] Les États-Unis ont fait l'objet d'une première décision d'adéquation de la part de la Commission européenne dans le cadre du *Safe Harbor*. Cependant, la Cour de justice de l'Union européenne a invalidé cette décision dans l'affaire *Maximilian Schrems c/ Data Protection Commissioner*, C-362/14 du 6 octobre 2015, en ligne : < https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:62014CJ0362&from=FR >. Une nouvelle décision a été prise par la Commission européenne dans le cadre du *Privacy shield*, UNION EUROPEENE, *Décision d'exécution (UE) 2016/1250 de la Commission du 12 juillet 2016 conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à l'adéquation de la protection assurée par le bouclier de protection des données UE-États-Unis*, 12 juillet 2016, Journal officiel n°L207/1 du 1er août 2016, en ligne : < https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32016D1250&from=EN#d1e3041-1-1 >, avant d'être à son tour annulée par la CJUE, *Data protection commissionner c/ Facebook Ireland Ltd.,* et *Maximilian Schrems*, C-311/18 du 16 juillet 2020 ; Voir également, CASTETS-RENARD, C., *L'adoption du Privacy Shield sur le transfert des données personnelles,* 2016, Recueil Dalloz, p.1696.

[449] L'application de la LPRPDE à des entreprises étrangères émane de la jurisprudence, *A.T.* c. *Globle24.com*, 2017 CF 114 (CanLII), [2017] 4 RCF 310, par.52 ; *Lawson* c. *Accusearch Inc.*, 2007 CF 125 (CanLII), [2007] 4 RCF 314 ; COMMISSARIAT A LA VIE PRIVEE, *Rapport de conclusions d'enquête en vertu de la LPRPDE n°2018-002 : La réutilisation de millions de profils d'utilisateurs Facebook canadiens effectuée par une entreprise contrevient à la loi en matière de protection de la vie privée*, priv.gc.ca, 12 juin 2018, en ligne : < https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2018/lprpde-2018-002/ > ; GUILMAIN, A. et DOUVILLE, D., « La Loi sur la protection des renseignements personnels dans le secteur privé: quand s'applique-t-elle aux entreprises situées à l'extérieur du Québec? », fasken.com, 16 mai 2019, en ligne : <https://www.fasken.com/fr/knowledge/2019/05/van-the-quebec-private-sector-privacy-act/ >.

[450] La jurisprudence québécoise a tenté d'appliquer la LPRPSP à des entreprises étrangères en se fondant sur une approche large de la notion d'entreprise. *Firquet* c. *Acti-com*, 2018 QCCAI 245 (CanLII). Cependant, cette approche n'a été appliquée qu'aux entreprises étrangères disposant d'une représentation au Québec. *Serres floraplus inc*. c. *Norséco in.,* 2008 QCCS 1455 (CanLII) ; GUILMAIN, A. et DOUVILLE, D., « La Loi sur la protection des renseignements personnels dans le secteur privé: quand s'applique-t-elle aux entreprises situées à l'extérieur du Québec? », fasken.com, 16 mai 2019, en ligne : < https://www.fasken.com/fr/knowledge/2019/05/van-the-quebec-private-sector-privacy-act/ >.

[451] Voir notamment JAAR, D., LACOSTE, E., et SENECAL, F., « Investir dans les renseignements personnels et leur protection », dans *Développements récents en droit de l'accès à l'information et de la protection des renseignements*

collectés sont majoritairement conservés à l'étranger, l'entreprise rapporte sur la page internet dédiée à la suppression des données, une partie est reproduite ci-dessous, que la désinstallation de l'application mobile contrôlant l'assistant vocal n'entraîne pas une suppression automatique des informations.

Extrait 5. – Partie de la section « Suppression des données » de la page commune à tous les produits et service de Google [452].

Le passage surligné en gris nous appartient et a pour objet d'attirer l'attention du lecteur sur le fait qu'un lien renvoie vers une autre page décrivant la procédure à suivre pour procéder à la suppression d'une maison (intelligente), d'un profil (dans le cas de plusieurs utilisateurs de l'assistant) ou d'un des appareils connectés à l'assistant vocal. Nous constatons, que cette procédure ne vaut uniquement que pour l'utilisateur, aucune information concernant une éventuelle suppression des renseignements personnels par Google n'y figure. Pour la trouver, l'utilisateur doit approfondir ses recherches et se rendre encore une fois sur une autre page internet concernant tous les produits et services de l'entreprise. Nous constatons également que si Google énonce explicitement l'existence d'une « procédure visant à supprimer, de manière complète et sécurisée,

personnels — les 30 ans de la Commission d'accès à l'information (2012), vol. 358, service de la formation continue, Barreau du Québec, Cowansville, Éditions Yvon Blais, 2012, pp.193 à 213.

[452] GOOGLE, « En savoir plus sur la sécurité et la confidentialité des données sur les appareils compatibles avec l'Assistant », support.google.com, en ligne : < https://support.google.com/googlenest/answer/7072285?hl=fr >.

ces informations (…) »[453], aucun élément n'est en revanche donné sur la procédure en tant que telle. La suppression des renseignements personnels par l'utilisateur n'est donc qu'en partie effective, sinon trompeuse. Un utilisateur raisonnable ne s'attendra pas à, ou plutôt ne pensera pas, à devoir passer par toute cette procédure pour supprimer ses renseignements personnels. Une désinstallation supposerait pour l'utilisateur l'effacement des informations qui y sont présentes. Or, l'absence d'informations claires et précises sur la procédure à suivre peuvent lui porter préjudice.

Il convient de préciser qu'étant donné la capacité de l'assistant vocal à pouvoir enregistrer en continu son utilisateur, l'entreprise pourra au cours d'une demande d'accès à des renseignements personnels ne fournir que ceux qui ont été collectés lorsque l'utilisateur interagissait avec l'objet. Ce dernier n'aura donc pas connaissance que d'autres renseignements sont également stockés, et par conséquent ne pensera pas à en demander l'accès.

Nous l'avons rappelé dans la première partie, le stockage des renseignements personnels à distance tend également à limiter la garantie que ceux-ci ne feront pas l'objet d'une communication à un tiers. Il est difficile, voire impossible pour un individu de connaître précisément le détenteur de ses renseignements personnels ainsi que sa localisation. Pour tenter de contourner les règles juridiques contraignantes encadrant le transfert des données à l'étranger[454], notamment envers un tiers, les fabricants d'assistants vocaux n'hésitent pas à recourir, en dehors de tout cadre légal, aux services d'entreprises leur proposant de les assister dans l'amélioration du produit. Cette supervision humaine est totalement méconnue de l'utilisateur[455]. Dans l'interview donnée par Antonio Casilli à une ancienne « dresseuse d'IA », nous apprenons à propos de cette soi-disant « amélioration du produit » que :

> « Personnaliser les paramètres de confidentialité de services de ce genre requiert parfois des compétences en informatique qui dépassent l'utilisateur amateur, et des écrans de fumée font oublier que vous sacrifiez et marchandez votre vie privée à l'aide

[453] GOOGLE, « Supprimer vos activités », support.google.com, en ligne : <https://support.google.com/accounts/answer/465 >.
[454] Nous pensons notamment au RGPD mettant en place le code de bonne conduite et les différents types de transfert selon les articles 40 et s.
[455] CASILLI A., « Derrière les assistants vocaux, des humains vous entendent », laquadratur.net, 18 mai 2018, en ligne : < https://www.laquadrature.net/2018/05/18/temoin_cortana/ >.

> de formules comme « personnalisation du contenu », « optimisation des résultats », « amélioration de votre expérience et de nos services » » (nos soulignements).

Cette affirmation fait écho à ce que nous avons développé au sujet de l'absence de la publication du code source, ou à défaut de sa traduction binaire, de l'algorithme traitant les renseignements personnels, et plus précisément de la difficulté qu'un utilisateur aura à comprendre la conception d'un tel mécanisme s'il venait à être publié[456].

En outre, l'absence de contrôle sur le résultat découle en réalité de son utilisation même. Une diffusion à l'oral d'un résultat alors que l'utilisateur peut être occupé à réaliser d'autres tâches entraine une certaine baisse de jugement de sa part :

> « Nous allons perdre le réflexe de vérifier une information. Depuis plus de vingt ans sur le Web, pour une même question, il existe une multitude de résultats, ce qui alimente les débats et permet de se faire une opinion. Car la vérité est plurielle et cela, l'assistant vocal ne saura jamais le reproduire (…) »[457].

ii. Un manque d'effectivité contribuant à la réalisation de profilage de la part des entreprises

Pour tenter de remédier aux dérives importantes de l'utilisation des renseignements personnels dans la prise de décision à l'égard d'une personne physique, le RGPD a prévu des dispositions permettant de les encadrer :

> « La personne concernée a le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage[458], produisant des

[456] Voir partie I.A.2.a). i.
[457] TRAX MAGASINE, « Derrière les enceintes intelligentes, les oreilles des géants du web ? », citant Guillaume Champeau, traxmag.com, 7 janvier 2019, en ligne : < https://www.traxmag.com/derriere-les-enceintes-intelligentes-les-oreilles-des-geants-du-web/ >.
[458] Le profilage est défini comme « (…) toute forme de traitement automatisé de données à caractère personnel visant à évaluer les aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des aspects

effets juridiques la concernant ou l'affectant de manière significative de façon similaire »[459].

Dans le cadre de l'assistant vocal, le profilage résultant de l'analyse des requêtes ou du mode de vie d'un individu, s'opère lorsque celui-ci reçoit des annonces personnalisées[460]. Ce type d'information est de nature à influencer la prise de décision de l'intéressé puisqu'en cas d'achat faisant suite à une suggestion de l'assistant vocal, il se retrouvera alors lié contractuellement au vendeur. Pour l'entreprise, le profilage constitue un moyen lucratif en attirant la personne vers de nouveaux produits et services la poussant à dévoiler davantage de données. Cette méthode se fait le plus souvent de manière automatique par le biais donc de l'algorithme sans pour autant qu'une personne n'intervienne pour confirmer la décision de l'intelligence artificielle.

Cependant, au moment de l'installation de l'assistant vocal, l'utilisateur ne s'attend pas forcément à ce que le fabricant soit en mesure d'effectuer un tel profilage ciblé. Si l'on s'appuie sur la politique de confidentialité du Google Home, qui représente un très bon exemple tout au long de ce développement, nous constatons que le recours au profilage n'est prévu qu'implicitement en des termes généraux : « [e]n outre, c'est grâce aux données que tous les utilisateurs bénéficient gratuitement de nos services et se voient présenter des annonces pertinentes et utiles »[461].

Malgré cette interdiction du profilage, il existe une exception, celle du consentement explicite de l'utilisateur[462]. Le RGPD prévoit cette dérogation si la personne concernée puisse donner son consentement dans les conditions énoncées aux articles 4 et 7. Autrement dit, elle doit pouvoir être informée et consciente de l'usage qui en est fait de ses renseignements personnels. Son consentement doit théoriquement être donné en l'absence de toute contrainte. Or, l'utilisation d'un assistant vocal intégré à une enceinte connectée est soumis au préalable à l'installation d'une

---

concernant le rendement au travail de la personne concernée, sa situation économique, sa santé, ses préférences ou centres d'intérêt personnels, sa fiabilité ou son comportement, ou sa localisation et ses déplacements … », considérant n°71 du RGPD. Cette définition est également reprise à l'article 4 relatif aux définitions du RGPD.

[459] Art. 22 du RGPD.

[460] PESTANES, P. et GAUTIER, B., « Essor des assistants vocaux : Nouveau gadget pour votre salon ou fenêtre d'opportunité pour rebattre les cartes de l'économie du web ? », wavestone.com, 2017, en ligne : <https://www.wavestone.com/app/uploads/2017/09/Assistants-vocaux-04.pdf >.

[461] Voir l'extrait 3 de la politique de confidentialité du Google Home, p.120.

[462] BENSOUSSAN, A., (dir), *Règlement européen sur la protection des données, textes, commentaires et orientations pratiques,* Bruylant, lexing technologies avancées & droit, 2e édition, 2018.

application sur le téléphone intelligent de l'utilisateur. L'imposition d'une telle action est selon nous une forme nouvelle de contrainte sur le consentement. À défaut, l'individu ne pourrait pas interagir avec son assistant vocal de son enceinte connectée. Pour ce qui est de celui dans la tablette ou le téléphone intelligent, l'utilisateur est mis devant le fait accompli de la présence de l'assistant vocal sans passer par l'installation d'une application.

À l'heure actuelle ni la LPRPDE ni la LPRPSP ne prévoient pareille disposition concernant le profilage, ou tout de moins de manière explicite. Il faut aller voir du côté du CPVP qui est le seul a évoqué ce sujet. Dans le document relatif aux principes à l'équité dans le traitement de l'information[463], le CPVP préconise[464] qu'il soit interdit de procéder au profilage des individus du fait de l'absence d'une réelle transparence sur l'utilisation concrète qui est fait de leurs renseignements personnels. Cette interdiction serait, tout comme dans le RGPD, assortie d'une exception lorsque l'entreprise parvient à recueillir un consentement valable de la personne[465]. Mais à la différence du RGPD, cette interprétation émane d'une autorité ayant des pouvoirs limités pour faire respecter la LPRPDE. Le respect de cette interprétation reposera donc sur le principe de bonne foi de l'entreprise.

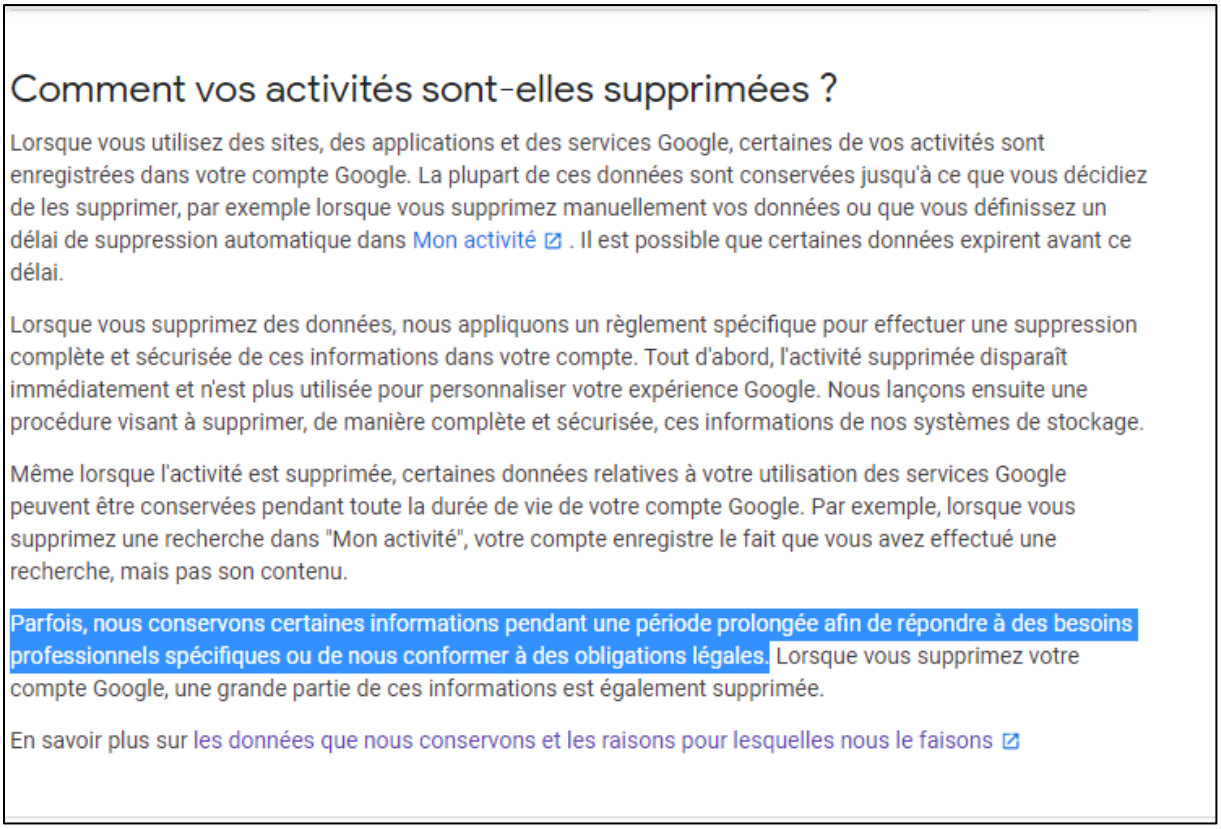
Pour parvenir à leurs fins, les entreprises rédigent à destination des utilisateurs, bien souvent ignorants de telles pratiques, des politiques de confidentialité en des termes généraux afin d'obtenir leur consentement à cette activité de profilage. Celle-ci doit, selon les textes, notamment européen, nécessiter un consentement en plus de celui donné pour l'utilisation de l'assistant vocal.

---

[463] CPVP, *Principes relatifs à l'équité dans le traitement de l'information de la LPRPDE,* priv.gc.ca, Mai 2019, en ligne : < https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/lois-sur-la-protection-des-renseignements-personnels-au-canada/la-loi-sur-la-protection-des-renseignements-personnels-et-les-documents-electroniques-lprpde/p_principle/ >.

[464] Nous rappellerons que les recommandations du Commissariat à la vie privée ne revêtent aucun caractère contraignant obligeant les entreprises à s'y conformer.

[465] COMMISSARIAT A LA PROTECTION DE LA VIE PRIVEE, *Position de principe sur la publicité comportementale en ligne,* priv.gc.ca, décembre 2015, en ligne : < https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/technologie/protection-de-la-vie-privee-en-ligne-surveillance-et-temoins/pistage-et-publicite/bg_ba_1206/ >.



Comment vos activités sont-elles supprimées ?

Lorsque vous utilisez des sites, des applications et des services Google, certaines de vos activités sont enregistrées dans votre compte Google. La plupart de ces données sont conservées jusqu'à ce que vous décidiez de les supprimer, par exemple lorsque vous supprimez manuellement vos données ou que vous définissez un délai de suppression automatique dans Mon activité . Il est possible que certaines données expirent avant ce délai.

Lorsque vous supprimez des données, nous appliquons un règlement spécifique pour effectuer une suppression complète et sécurisée de ces informations dans votre compte. Tout d'abord, l'activité supprimée disparaît immédiatement et n'est plus utilisée pour personnaliser votre expérience Google. Nous lançons ensuite une procédure visant à supprimer, de manière complète et sécurisée, ces informations de nos systèmes de stockage.

Même 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.

Parfois, nous conservons certaines informations pendant une période prolongée afin de répondre à des besoins professionnels spécifiques ou de nous conformer à des obligations légales. Lorsque vous supprimez votre compte Google, une grande partie de ces informations est également supprimée.

En savoir plus sur les données que nous conservons et les raisons pour lesquelles nous le faisons

Extrait 6. – Partie de la section « Suppression vos activités » de la page commune à tous les produits et service de Google[466]

Parmi ces « écrans de fumée », nous estimons qu'il est pertinent, bien que nous ayons déjà reproduit en première partie un extrait similaire mentionnant l'amélioration du service, de faire apparaître cet extrait, dont le passage surligné en bleu est le nôtre. La rédaction de ce passage a de quoi nous interpeller. Bien qu'il soit attendu d'une entreprise, dont il est question ici de Google, d'avoir une politique de confidentialité rédigée en des termes claires, ceux-ci doivent également être précis. Notre passage commence avec le terme « Parfois » et selon le dictionnaire *Le petit Robert*, cet adverbe a pour définition : « à certains moments, dans certains cas, de temps en temps »[467] (notre soulignement). L'usage de ce terme illustre le manque de précision dans la détermination du type d'informations collectées. Une imprécision que nous retrouvons avec

[466]GOOGLE, « Supprimer vos activités », support.google.com, en ligne : <https://support.google.com/accounts/answer/465 >.
[467]LE PETIT ROBERT, « Définition : Parfois », dictionnaire.lerobert.com, en ligne : <https://dictionnaire.lerobert.com/definition/parfois >.

l'emploi du terme « certaines ». En outre, la « période prolongée » ne nous apporte pas non plus davantage de précision sur la durée minimale et maximale de la conservation puisqu'il est mis en avant une conservation de manière occasionnelle de renseignements personnels aléatoires pouvant être supprimés par l'utilisateur. Une imprécision qui se retrouve enfin par les termes suivants « besoins professionnels spécifiques », et que l'on retrouve à différentes reprises dans les politiques de confidentialité sous l'expression « amélioration du produit ».

Le profilage met en lumière la puissance de l'algorithme puissance de l'algorithme et sa capacité à prédire certains évènements pouvant apparaître au cours de notre vie[468]. Afin de mieux illustrer nos propos, nous pouvons comparer cette technique aux témoins de connexion internet, plus communément appeler « cookies ». Le cookie, précisons-le dans le domaine de l'informatique, est un « [é]lément d'information qui est transmis par le serveur au navigateur lorsque l'internaute visite un site Web, et qui peut être récupéré par ce serveur lors de visites subséquentes »[469]. En d'autres termes, le témoin de connexion est un fichier texte installé dans l'ordinateur de l'utilisateur naviguant sur Internet[470]. Ce fichier va ensuite récolter un certain nombre de données qui permettront par la suite aux entreprises de connaître les préférences et les sites visités afin d'ajuster leurs annonces. D'un point de vue de la vie privée, les cookies agissent comme l'algorithme d'un assistant vocal en documentant l'activité de l'individu. De ce fait, les entreprises sauront adapter leurs contenus publicitaires en fonction des informations obtenues grâce à l'utilisateur, sans pour autant qu'il ne s'en rende compte. Sans rentrer dans le détail car n'étant pas dans le champ d'étude de notre présent développement, nous portons à la connaissance du lecteur que des régulations existent, principalement au sein de l'Union européenne, pour encadrer ces témoins de connexion Internet. C'est ainsi que la directive du 12 juillet 2002[471], complétée par celle du 19 décembre

---

[468] DEZIEL, P-L., « Les limites du droit à la vie privée à l'ère de l'intelligence artificielle : groupes algorithmiques, contrôle individuel et cycle de traitement de l'information », Les cahiers de propriété intellectuelle, Yvon Blais, vol. 30, n° 3, octobre 2018, en ligne : < https://www.lescpi.ca/articles/v30/n3/les-limites-du-droit-a-la-vie-privee-a-lere-de-lintelligence-artificielle-groupes-algorithmiques-controle-individuel-et-cycle-de-traitement-de-linformation/ >, pp.827-847.

[469] OFFICE QUEBECOIS DE LA LANGUE FRANCAISE, « Grand dictionnaire terminologique : témoin », gdt.oqlf.gouv.qc.ca, 2015, en ligne : < http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=2075216 >.

[470] RONAN, « Les cookies informatiques : amis ou ennemis ? », caragraph.fr, 2 février 2017, en ligne : <https://www.caragraph.fr/ficheArticle-Les-cookies-informatiques--amis-ou-ennemis--9.html >.

[471] *Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques),* Journal officiel n° L201, 31 juillet 2002, p.0037-0047, en ligne : < https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32002L0058&from=FR >.

2009[472], prévoit que l'utilisateur doit connaître les finalités de l'utilisation de ses renseignements provenant des témoins de connexion[473]. Au Canada, seul le Commissariat à la protection de la vie privée a émis des lignes directrices n'ayant pas force de loi concernant ces témoins de connexion invitant seulement a encadré un tel outil[474].

Cette illustration de la puissance de l'algorithme capable de constituer un véritable dossier sur la vie privée des personnes fait écho à ce qu'affirmait le professeur POULLET :

> « [L]'information représente pour ceux qui la détiennent un pouvoir vis-à-vis de ceux sur lesquels l'information est détenue. Celui qui détient l'information sur autrui peut adapter sa décision en fonction de la connaissance que l'information collectée et traitée lui donne d'autrui. Il prévoit son attitude et peut donc répondre à sa demande ou influencer celle-ci »[475] (nos soulignements).

Elle souligne dans le même temps l'importance que peut avoir l'algorithme dans le traitement des données. Ce traitement n'est rendu possible que par l'utilisation massive des technologies et leur facilité à s'intégrer au sein de notre environnement privé afin de récolter des données. Ainsi que le résume la CNIL dans son rapport : « [l]'algorithme sans données est aveugle. Les données sans algorithmes sont muettes »[476]. En d'autres termes, il est possible de limiter les effets pervers de l'algorithme intelligent en restreignant l'émission des données sans pour autant les rendre

---

[472] *Directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009 modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques, la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques et le règlement (CE) nº 2006/2004 relatif à la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs*, Journal officiel n° L337 du 18 décembre 2009, en ligne : < https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32009L0136&from=EN >.

[473] Art. 5 par. 3 de la directive 2002/58/CE.

[474] COMMISSARIAT A LA PROTECTION DE LA VIE PRIVEE, *Lignes directrices sur la protection de la vie privée et la publicité comportementale en ligne,* priv.gc.ca, décembre 2011, en ligne : < https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/technologie/protection-de-la-vie-privee-en-ligne-surveillance-et-temoins/pistage-et-publicite/gl_ba_1112/ > ; Ces lignes ont fait l'objet d'une mise à jour sans pour autant changer fondamentalement, COMMISSARIAT A LA PROTECTION DE LA VIE PRIVEE, *Position de principe sur la publicité comportementale en ligne,* priv.gc.ca, décembre 2015, en ligne : <https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/technologie/protection-de-la-vie-privee-en-ligne-surveillance-et-temoins/pistage-et-publicite/bg_ba_1206/ >.

[475] POULLET, Y., et HENROTTE, J-F., « La protection des données (à caractère personnel) à l'heure de l'Internet », dans *Protection du consommateur*, pratiques commerciales et T.I.C., coll. Commission Université-Palais, volume 109, Liège, Anthémis 2009, pp. 197-245.

[476] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES, *Comment permettre à l'homme de garder la main ? Rapport sur les enjeux éthiques des algorithmes et de l'intelligence artificielle,* cnil.fr, décembre 2017, en ligne : <https://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_garder_la_main_web.pdf >, p.18.

inaccessibles par l'algorithme. Une telle mesure porterait un coup sévère non seulement à l'évolution technologique mais également aux intérêts économiques de l'entreprise.

Le cas de Google est un bon exemple pour appuyer nos propos. Nous avons repris ci-dessous une partie de la politique de confidentialité de l'enceinte Google Home portant sur l'utilisation des données. Cette section tente d'expliquer la manière dont Google se sert des données récoltées pour améliorer ses services. Implicitement, Google reconnaît que des métadonnées peuvent être analysées en citant l'exemple de la circulation en temps réel, nécessitant de connaître la localisation de l'utilisateur.

Aussi cette politique apparaît comme étant inadaptée à la réalité du produit puisqu'il est question de récolter les données afin de mieux prévenir toute tentative d'accès à des sites web malveillants. Or, l'utilisation de l'assistant vocal ne requiert pas de visite de site internet ou d'utilisation d'un logiciel car l'expérience orale est entièrement liée à l'assistant lui-même. C'est lui qui est chargé par l'utilisateur d'aller chercher le résultat dans sa base de données. L'argument « amélioration du service » sans vraiment préciser de quel service il s'agit démontre que Google ne respecte pas les dispositions en vigueur, notamment en ce qui concerne le recueil du consentement.

Utilisation des données

Comment les données collectées sont-elles utilisées par Google ?

Avant tout, les données que nous recueillons nous permettent d'adapter nos services à vos besoins, et de les rendre plus rapides et plus intelligents. C'est ainsi que nous pouvons améliorer les résultats de recherche et fournir des informations de circulation en temps réel, par exemple. Les données nous aident également à vous protéger des logiciels malveillants, du hameçonnage et d'autres activités suspectes. Nous pouvons par exemple vous prévenir lorsque vous êtes sur le point de consulter des sites Web dangereux. En outre, c'est grâce aux données que tous les utilisateurs bénéficient gratuitement de nos services et se voient présenter des annonces pertinentes et utiles. Google Home s'améliore au fil du temps pour vous fournir des suggestions et des réponses plus adaptées et plus personnalisées. Pour en savoir plus, reportez-vous aux Règles de confidentialité de Google. Veuillez également lire les engagements de Google en matière de confidentialité dans la maison, notamment pour comprendre comment nous restreignons l'utilisation de certaines de vos données pour la personnalisation des annonces.

Extrait 7. – Partie de la section « Utilisation des données » de la politique de confidentialité du Google Home[477].

D'ailleurs, nous remarquons dans la politique de confidentialité du Google Home que Google renvoie à plusieurs reprises vers une autre politique plus générale concernant tous ses produits et services. Cette pratique nous interroge sur la réelle volonté de Google de protéger les renseignements personnels. Comme le souligne M[es] Jaar et Senecal, et Mme Lacoste :

> « Il ne s'agit plus de protéger des informations parce qu'elles sont qualifiées de « RP » [renseignement personnel] mais bien de protéger un investissement dans ces informations, parce que l'organisation y voit – et en crée – de la valeur »[478].

Nous retrouvons ici un autre point commun entre l'algorithme et le témoin de connexion Internet à des fins marketing. Google énonce dans cette section que « (…) c'est grâce aux données que tous les utilisateurs bénéficient gratuitement de nos services et se voient présenter des annonces pertinentes et utiles » (nos soulignements). Google se sert de ces données et par recoupement algorithmique parvient à identifier les centres d'intérêts et à orienter l'utilisateur vers les publicités compatibles. Le manque de précision quant au type de données utilisées pour recevoir ces annonces entretient le flou sur la conformité aux dispositions législatives protégeant les renseignements personnels. Cette opacité démontre une nouvelle fois une inadéquation entre la politique de confidentialité et le produit en question. Il n'est techniquement pas possible de faire passer des annonces par le biais de l'assistant vocal. Si tel est le cas, cela voudra dire qu'il restera toujours actif en les diffusant constamment.

Au regard de ce développement, il apparaît que la conception de l'assistant vocal n'a pas pris en compte l'intérêt de protéger les renseignements personnels. Cette protection est également insuffisante via les paramètres proposés à l'utilisateur. L'adoption récente de texte novateur tel que

---

[477] GOOGLE, « En savoir plus sur la sécurité et la confidentialité des données sur les appareils compatibles avec l'Assistant », support.google.com, en ligne : < https://support.google.com/googlenest/answer/7072285?hl=fr >.
[478] JAAR, D., LACOSTE, E., et SENECAL, F., « Investir dans les renseignements personnels et leur protection », dans *Développements récents en droit de l'accès à l'information et de la protection des renseignements personnels — les 30 ans de la Commission d'accès à l'information (2012)*, vol. 358, service de la formation continue, Barreau du Québec, Cowansville, Éditions Yvon Blais, 2012, p.194.

le RGPD ne saurait servir d'argument pour les fabricants d'assistants vocaux pour se défaire de la conformité à cette obligation. La possibilité de faire évoluer les logiciels de l'assistant vocal par le biais de mise à jour ou leur création et commercialisation toujours plus performant rendent possible l'intégration de la protection de la vie privée et des renseignements personnels dès la conception. À l'instar du constructeur Snips qui a su mettre en place un assistant vocal fonctionnant sur le principe de l'informatique en périphérie, ou « edge computing »[479].

La technique de l'informatique en périphérie offre la possibilité de traiter l'information à la périphérie du réseau (edge) par la machine connectée (computing). Contrairement à tous les assistants vocaux présent sur le marché et reliés au nuage informatique de leur fabricants pour s'alimenter en données, l'assistant vocal Snips intègre directement une base de données. Cette décentralisation du travail dans la recherche du résultat à la requête introduite offre davantage de respect de la vie privée de l'utilisateur puisque ses renseignements seront conservés directement dans la machine et ne feront donc pas l'objet d'un partage vers des serveurs pouvant être localisé dans un pays tiers[480]. Le recours à cette technique se révèle être prometteur en matière de protection des renseignements personnels.

L'assistant vocal bouleverse donc la protection des renseignements personnels. Les principes fondamentaux, à commencer par le consentement, doivent eux-aussi être réévalués[481] pour mieux prendre en compte cette technologie. Le C.c.Q. et ses régimes de responsabilité civile se trouve eux aussi être chamboulés par l'utilisation de l'assistant vocal. Pour garantir une effectivité continue de la protection de la vie privée, le législateur fédéral a modifié la LPRPDE afin d'y inclure une obligation de notification des incidents de sécurité qui, nous le verrons, peut avoir un effet préventif sur la protection des renseignements personnels.

---

[479] ANNONYME, « Le edge computing va rendre l'IA plus écologique, rapide et éthique », helloopenworld.com, 18 mai 2018, en ligne : < https://www.helloopenworld.com/objets-connectes-et-si-on-arretait-de-partager-la-data-6119 >.
[480] Ibid.
[481] GAUTRAIS, V., « Introduction générale : Le défi de la protection de la vie privée face aux besoins de circulation de l'information personnelle », Conférence organisée par le programme international de coopération scientifique, Ivry sur Seine, 5 juin 2003.

B. L'incidence de l'assistant vocal sur les régimes de responsabilité et l'obligation de notification des incidents de sécurité

En plus des lois en matière de protection des renseignements personnels et des dispositions constitutionnelles protégeant le droit à la vie privée, la commercialisation de l'assistant vocal a semble-t-il porter un coup sévère à l'effectivité des différents régimes de responsabilités civiles et contractuelle que nous connaissons au sein du *Code civil du Québec* (1). Pour tenter de remédier à ce problème, le législateur fédéral a entrepris une révision de la LPRPDE afin d'y inclure une nouvelle obligation, celle de la notification des incidents de sécurité. À travers cette obligation légale, les entreprises se retrouvent contrainte de se conformer au cadre juridique applicable aux renseignements personnels sous peine de faire l'objet d'une enquête pouvant nuire à sa réputation (2).

1. La détermination du régime de responsabilité découlant des limites techniques de l'assistant vocal

Reposant sur l'apprentissage supervisé, l'assistant vocal apprend de ses interactions avec l'utilisateur. Dans ce contexte, les échanges peuvent ne pas toujours être courtois et intelligent. Des personnes sont chargées d'analyser la bonne compréhension de la requête par la machine et interviennent pour corriger les éventuelles erreurs. Le cas du chatbot Tay de Microsoft en est un parfait exemple. Alors que son fabricant pensait mettre en place un agent conversationnel capable d'apprendre de lui-même au fil de ses interactions, il s'est avéré qu'il n'a pas su faire la différence entre des propos haineux et des propos plus bienveillants ou intelligents[482]. Une situation qui a contraint Microsoft de mettre fin à l'expérience de son chatbot.

Cette situation pose le problème de la reconnaissance de la responsabilité résultant de l'utilisation de l'assistant vocal et de ses interactions. En effet, si l'exemple cité concernant le couple américain,

[482] LIBERATION, « Microsoft muselle son robot « Tay » devenu nazi en 24 heures », liberation.fr, 25 mars 2016, en ligne : < https://www.liberation.fr/futurs/2016/03/25/microsoft-muselle-son-robot-tay-devenu-nazi-en-24-heures_1441963 >.

dont la conversation a été enregistrée et envoyée à un ami, a le mérite de mettre en lumière d'un point de vue technique les carences du TALN, sur le plan juridique la reconnaissance d'une éventuelle responsabilité n'est pas aussi évidente qu'il n'y paraît.

Le C.c.Q. prévoit différents régimes de responsabilités. Nous allons évoquer ceux qui pourraient s'appliquer selon les différents acteurs dans l'utilisation de l'assistant vocal, à savoir l'utilisateur et l'entreprise le commercialisant. Nous commencerons avec la responsabilité pour faute (a) avant de nous attarder sur celle découlant du fait d'un bien, en évoquant ses conditions de garde et d'autonomie (b). Nous verrons également le régime de la responsabilité d'un défaut de sécurité (c). Enfin, nous terminerons par nous interroger sur la pertinence d'appliquer le régime de la responsabilité contractuelle, notamment au regard de la difficulté à caractériser un éventuel vice pouvant ouvrir la voie vers la reconnaissance de la responsabilité du vendeur (d).

a) La responsabilité pour faute

Le premier de ces régimes est celui de la responsabilité pour faute énoncé à l'article 1457 du C.c.Q. Ce régime de responsabilité vise la réparation du préjudice[483] causé par une personne « douée de raison »[484]. Toute personne dispose d'une personnalité juridique lui permettant, par exemple, d'avoir un patrimoine, des droits et des obligations. L'assistant vocal ne possédant pas de personnalité juridique, quand bien même l'intelligence artificielle lui permettrait d'agir quasiment comme un humain, le régime de la responsabilité civile pour faute ne pourrait s'y appliquer directement.

Quid du régime de la responsabilité civile du fait des biens ?

[483] Le préjudice doit remplir différentes conditions pour que la victime puisse avoir droit à une quelconque réparation. Celui-ci doit avoir un caractère direct et certain résultant d'une activité licite. Le caractère futur du préjudice peut également être retenu dans certains cas, même s'il s'agit d'une simple probabilité. BAUDOUIN, J.-L., DESLAURIERS, P., et MOORE, B., *La responsabilité civile*, vol.1 : Principes généraux, 8e éd., Montréal, Éditions Yvon Blais, 2014.
[484] Art. 1457 du C.c.Q.

b) La responsabilité du fait d'un bien

Le C.c.Q. énonce que :

> « Le gardien d'un bien est tenu de réparer le préjudice causé par le fait autonome de celui-ci, à moins qu'il prouve n'avoir commis aucune faute »[485] (nos soulignements).

i. L'identification du gardien dans l'utilisation de l'assistant vocal

La notion de gardien a été précisée par la jurisprudence. Dans la décision, *Bolvin* c. *Montréal*[486] l'honorable Gatien Fournier précise au paragraphe 82 que :

> « La garde est donc, dans un sens large, une relation entre le responsable et l'objet, basée sur un pouvoir de surveillance, de contrôle et de direction, permettant au premier de prévenir le dommage pouvant être causé par le fait autonome du second » (nos soulignements).

Cette relation entre le responsable et l'objet doit être une « relation de pouvoir réel, concret et factuel du contrôle exercé par le gardien sur le bien afin qu'il puisse empêcher le bien de causer un dommage »[487]. Selon nous, il existerait différentes hypothèses dans l'utilisation de l'assistant vocal qui pourraient être soumis à un tel régime. Des situations qui amèneront sans doute à adopter des approches différentes de la notion de gardien. En effet, celle-ci varierait en fonction de la source du préjudice. Il conviendrait alors d'opérer une distinction entre le gardien de l'objet et celui de l'algorithme.

Si l'on suppose que l'assistant vocal a parfaitement fonctionné, de l'enregistrement de la requête à la transmission du résultat, il est possible que l'action demandée puisse porter préjudice à autrui.

---

[485] Art. 1465 du C.c.Q.
[486] *Bolvin* c. *Montréal (Ville de)*, 2015 QCCQ 1923 (CanLII).
[487] OLIVEIRA, S., *La responsabilité civile dans les cas de dommage causés par les robots d'assistance au Québec,* papyrus.bib.umontreal.ca, Mémoire de maîtrise, Université de Montréal, Avril 2016, en ligne : <https://papyrus.bib.umontreal.ca/xmlui/bitstream/handle/1866/16239/Oliveira_Sandra_2016_memoire.pdf?sequence=2&isAllowed=y >, p.84.

Cette action pourrait *a priori* entraîner la reconnaissance de la responsabilité civile de la personne au moment de l'interaction avec l'assistant vocal. C'est dans cette hypothèse que l'approche de l'utilisateur en tant que gardien devrait être privilégiée.

Cependant, au regard de l'émergence récente de l'assistant vocal, notamment de sa commercialisation au grand public en 2011, il nous paraît à l'heure actuelle difficile de clairement identifier le gardien. En effet, l'utilisation entièrement vocale de l'objet le rend facilement accessible par toute personne ayant la capacité de parler sans que celui-ci ne fasse la distinction entre les différents locuteurs. À travers leurs interactions, chaque personne se rend en quelque sorte gardien de l'objet.

Celle-ci aurait donc lieu si l'examen de l'assistant vocal au moment de son utilisation ne révélerait pas de dysfonctionnements particulièrement graves. Dans le cas contraire, il conviendrait d'adopter une autre approche de cette notion qui placerait alors le fabricant en tant que gardien, non pas de l'objet présent dans un domicile privé, mais de l'algorithme qu'il a lui-même conçu et développé. Nous privilégierons une telle approche selon deux types de scenarios, la transmission d'informations erronées de l'assistant vocal susceptible de causer un préjudice à son utilisateur et la collecte à son insu de renseignements personnels, deux cas résultant particulièrement des faux positifs.

En ce qui concerne, le premier cas de figure dans le cadre du fabricant en tant que gardien, nous pouvons prendre l'exemple d'un individu souhaitant obtenir des renseignements concernant le moyen d'avoir la peau lisse et introduit la requête de cette manière : « Je veux avoir la peau lisse » sans pour autant se préoccuper de la précision des termes employés et que son assistant vocal l'interprète comme « Je veux voir la police ». Les fabricants programment en général les assistants vocaux de sorte à contacter et envoyer certaines informations directement aux services d'urgences pour tenter de raccourcir le délai d'intervention des services de secours[488]. C'est ainsi que

[488] Une telle fonctionnalité est proposée dans les voitures qui active l'appel aux urgences en cas d'accident grave. Celle-ci est obligatoire au sein de l'Union européenne dans le cadre du *Règlement (UE) 2015/758 du Parlement européen et du Conseil du 29 avril 2015 concernant les exigences en matière de réception par type pour le déploiement du système eCall embarqué fondé sur le service 112 et modifiant la directive 2007/46/CE*, Journal officiel n° L123/77 du 19 mai 2015.

l'assistant vocal va mettre en relation les secours avec l'utilisateur voire dans certains cas leur demander d'intervenir directement[489]. Aussi, cette erreur d'interprétation entrainera l'enregistrement de l'environnement de son utilisateur. La demande d'intervention des secours par l'assistant vocal peut être confirmée par les pleurs d'un enfant pouvant être à proximité voire de ses cris en jouant et en les interprétant comme une situation grave. Dans ces hypothèses, à qui revient la responsabilité d'avoir dépêché les secours ? L'utilisateur peut-il se prévaloir de l'émergence d'un préjudice du fait de l'intervention des secours pour faire reconnaître la responsabilité du fabricant ? À ces questions, nous verrons dans le développement suivant que l'assistant vocal, notamment au regard de son manque d'autonomie, semble remettre en cause l'application d'un tel régime de responsabilité civile.

S'agissant de la collecte à l'insu de l'utilisateur, nous pouvons une nouvelle fois reprendre l'exemple de ce couple enregistré par l'assistant vocal. Le déclenchement non désiré est-il suffisant pour caractériser le « (…) pouvoir de surveillance, de contrôle et de direction » de l'algorithme par l'entreprise ? L'introduction d'une requête à haute voix, peut certes constituer un risque en remettant en cause la confidentialité des données[490], l'utilisateur ne saurait être reconnu comme ayant une part dans le partage des responsabilités au sens de l'article 1479 du CcQ car il en fait un usage normal de l'objet. Répondre par l'affirmative à cette question reviendrait à reconnaître que le couple devrait éviter de tenir une quelconque discussion à proximité de l'assistant vocal au sein même de leur domicile[491]. Cette affirmation aurait pour conséquence de limiter la liberté d'expression, surtout dans un cadre privé. Alors la garde appartiendrait-elle à l'entraîneur de l'intelligence artificielle qui n'a pas su préparer la machine à une telle situation puisqu'il semblerait exister des défauts caractérisés par les faux positifs ? La garde doit-elle appartenir au fabricant de l'objet dans lequel se trouve l'assistant vocal ou au fabricant de l'assistant vocal ? Il serait également extrêmement risqué de répondre par l'affirmative à cette question. L'affirmation tendrait

[489] S., P., « Un assistant domestique appel la police par erreur et vient au secours d'une victime de violences conjugales », jounaldugeek.com, 10 juillet 2017, en ligne : < https://www.journaldugeek.com/2017/07/10/google-home-appelle-la-police-par-erreur-et-vient-au-secours-dune-victime-de-violences-conjugales/ >.

[490] MINKER, W., et NEEL, F., « Développement des technologies vocales », dans *Le travail humain*, vol. 65, 2002/3, en ligne : < https://www.cairn.info/revue-le-travail-humain-2002-3-page-261.htm#pa23 >. Ces propos doivent être nuancés par l'existence d'une exception pour une personne privée traitant des renseignements personnels dans son domicile, ou dans le cadre d'une activité privée, Art. 2 c) RGPD ; art. 4 (2) b) LPRPDE ; art. 10 LPRPSP.

[491] Cette hypothèse encouragerait l'application de l'article 1479 du C.c.Q. lequel prévoit la responsabilité de la victime dans l'aggravation du préjudice qui irait alors à l'encontre de l'exemption accordée aux personnes physiques utilisant des renseignements personnels dans un cadre privé, notamment prévu par l'article 4 (2) de la LPRPDE.

à reconnaître indirectement aux fabricants un certain droit sur l'utilisation de l'assistant vocal, même après son achat par l'usager. Le fabricant pourrait alors selon son intérêt renforcer la surveillance dans le domicile privé de l'utilisateur pour s'assurer de la bonne utilisation de l'assistant vocal lui permettant par la suite d'apporter la preuve de l'absence d'une quelconque faute. Enfin, l'affirmation constituerait une limite à une telle approche de l'identification du gardien. Et pour ce qui est du respect de la vie privée, nous repasserons.

La nécessité d'une pareille approche de l'identification du fabricant comme gardien de l'algorithme s'explique principalement par le besoin de détenir un certain niveau de connaissances et de maîtrise du langage informatique, dont les figures 3 et 4 illustrent nos propos, pour élaborer un logiciel intelligent capable d'assister l'homme. Une telle maîtrise de la part du fabricant le qualifierait alors *de facto* gardien de l'algorithme intelligent. En outre, selon le professeur Vermeys l'opacité entourant le secret de fabrication de l'assistant vocal associé à son apprentissage en continue font obstacle à ce que son gardien (l'utilisateur de l'objet) puisse en avoir une maîtrise complète[492]. La notion de garde n'est donc pas simple à déterminer lorsqu'il s'agit de l'assistant vocal[493].

Un échec qui tend à se confirmer avec la tentative d'identification du caractère autonome de l'assistant vocal, nécessaire pour pleinement reconnaître la responsabilité du gardien du bien.

ii. L'absence de réelle autonomie de l'assistant vocal au sens de l'article 1465 du C.c.Q

Si le C.c.Q. ne définit pas la notion d'autonomie, la jurisprudence apporte deux critères pouvant l'apprécier : la création du préjudice par le bien sans que l'homme n'intervienne et le caractère mobile et dynamique du bien[494].

[492] VERMEYS, N., « La responsabilité civile du fait des agents autonomes », 2018, Vol. 30 n°3, *Les Cahiers de propriété intellectuelle*, p. 860.
[493] VERMEYS, N., « La responsabilité civile du fait des agents autonomes », 2018, Vol. 30 n°3, *Les Cahiers de propriété intellectuelle*, p. 860.
[494] OLIVEIRA, S., *La responsabilité civile dans les cas de dommage causés par les robots d'assistance au Québec,* papyrus.bib.umontreal.ca, Mémoire de maîtrise, Université de Montréal, Avril 2016, en ligne : <https://papyrus.bib.umontreal.ca/xmlui/bitstream/handle/1866/16239/Oliveira_Sandra_2016_memoire.pdf?sequence=2&isAllowed=y >, pp. 68 et s ; BAUDOUIN, J.-L., DESLAURIERS, P., et MOORE, B., *La responsabilité civile*, vol.1 : Principes généraux, 8e éd., Montréal, Éditions Yvon Blais, 2014.

S'agissant du premier critère, la faute doit être commise par le bien sans intervention humaine. Celui-ci doit disposer d'un certain degré d'autonomie de mouvement[495] pour agir à la place de l'homme. Il s'agit donc d'une autonomie de mouvement et non de parole, ou de pensée[496]. Nous pouvons prendre l'exemple d'un habitant demandant à son assistant vocal de programmer la température de son habitat à partir d'une heure précise et pour une durée déterminée à l'avance. Cette prise de décision ne résulte pas de l'assistant vocal mais bien de son utilisateur. L'intervention de l'homme est rendue nécessaire pour l'utiliser puisqu'un mot d'éveil doit être prononcé pour l'activer. Dans le cas de notre couple américain ayant eu une conversation à proximité de leur assistant vocal, celui-ci a envoyé la conversation non pas de son propre chef mais en pensant avoir entendu la demande de le faire. Malgré l'existence de ces faux positifs, l'assistant vocal ne se déclenche de sa propre initiative que très rarement, et encore moins pour décider seul d'une action.

Ensuite, concernant le second critère, celui de la mobilité du bien, l'assistant vocal est présent dans différents objets et terminaux mobiles. Il n'est pas lui-même en mouvement tel un robot. Son dynamisme se caractérise seulement par l'action d'une commande ou la réponse à une requête. Ce dynamisme résulte de l'activation de l'homme, qui a donc une implication dans l'activité de l'assistant vocal. Dans ces exemples cités précédemment, l'assistant vocal n'a aucune « motricité indépendante »[497] de l'homme. L'action de l'assistant vocal passe seulement par la connexion sans fil. Il ne dispose pas de moyens physiques lui offrant la possibilité d'être en mouvement tel une voiture autonome ou un robot dans une chaîne d'assemblage[498]. De ce fait, le régime de la responsabilité civile du fait des biens ne trouverait pas à s'appliquer à l'assistant vocal puisque les deux critères ne sont pas remplis.

c) La responsabilité du fabricant d'un défaut de sécurité du bien

[495] BAUDOUIN, J.-L., DESLAURIERS, P., et MOORE, B., *La responsabilité civile*, vol.1, Principes généraux, 8e édition, 2014.
[496] Ibid.
[497] VERMEYS, N., « La responsabilité civile du fait des agents autonomes », 2018, Vol. 30 n°3, *Les Cahiers de propriété intellectuelle*, p. 858.
[498] Ibid.

L'article 1468 du C.c.Q., en combinaison avec l'article 1469, prévoit la responsabilité du fabricant d'un défaut de sécurité du bien. Cette disposition, au regard des limites techniques du TALN, peut constituer une piste envisageable dans l'application de la responsabilité au fabricant de l'assistant vocal. Le défaut de sécurité se caractérise entre autres par :

> « (…) un vice de conception ou de fabrication du bien, d'une mauvaise conservation ou présentation du bien ou, encore, de l'absence d'indications suffisantes quant aux risques et dangers qu'il comporte ou quant aux moyens de s'en prémunir »[499] (nos soulignements).

Si le TALN a fait l'objet d'une évolution importante depuis ses débuts, les difficultés traduites par ses imperfections témoignent d'une nécessité de parfaire le système. Ces problèmes peuvent résulter tant d'une base de données incomplète[500] que d'un obstacle à pouvoir comprendre la complexité du langage naturel de l'homme[501]. Dans cette hypothèse, le régime de responsabilité du fait d'un défaut de sécurité ne trouverait pas à s'appliquer.

L'activation non désirée ne constitue pas le seul inconvénient susceptible d'entraîner un préjudice plus ou moins important à l'utilisateur. Nous l'avons mentionné dans ce développement, l'assistant vocal peut avoir du mal à interpréter correctement une requête en raison de la complexité de la langue ou d'un manque de maîtrise de l'objet de la part de l'utilisateur[502].

Mais au-delà même du TALN, c'est le système de l'assistant vocal qui peut faire l'objet d'un défaut de sécurité, notamment informatique[503]. Le piratage de l'assistant vocal par le biais du réseau internet privé reste toujours possible. Le risque est davantage important lorsque le pirate accède à

---

[499] Art. 1469 du C.c.Q.

[500] VERMEYS, N., « La responsabilité civile du fait des agents autonomes », 2018, Vol. 30 n°3, *Les Cahiers de propriété intellectuelle*, p. 862.

[501] MINKER, W., et NEEL, F., « Développement des technologies vocales », dans *Le travail humain*, vol. 65, 2002/3, en ligne : < https://www.cairn.info/revue-le-travail-humain-2002-3-page-261.htm#pa23 >.

[502] Voir aussi le mémoire de François LACHANCE que nous avons cité précédemment dans lequel il retranscrit les difficultés de certaines familles à interagir avec leur assistant vocal du fait de la mauvaise interprétation de la requête par celui-ci, LACHANCE, F., *« O.K. Google, assiste-moi » Les parcours des utilisateurs et des familles qui domestiquent le Google Home,* papyrus.bib.umontreal.ca, Mémoire de maîtrise, Avril 2019, en ligne : <https://papyrus.bib.umontreal.ca/xmlui/bitstream/handle/1866/22464/Lachance_Francois_2019_memoire.pdf?sequence=2&isAllowed=y >, p. 5 et pp. 39 et s.

[503] VERMEYS, N., « La responsabilité civile du fait des agents autonomes », 2018, Vol. 30 n°3, *Les Cahiers de propriété intellectuelle*, p. 864.

toute la domotique de l'utilisateur. Quand bien même le préjudice subi par ce dernier est important, la responsabilité du fabricant ou du programmeur, s'il est distinct du fabricant, ne sera pas automatiquement reconnue. En effet, toujours selon le professeur Vermeys :

> « (…) même si l'on reconnait la présence d'un tel défaut de sécurité dans le code d'un agent autonome, il importe de rappeler que le manufacturier de ce dernier, tout comme le développeur de l'algorithme, sera en mesure d'échapper à toute responsabilité s'il est en mesure de démontrer que ledit défaut de sécurité 'ne pouvait être connu, compte tenu de l'état des connaissances, au moment où il a fabriqué, distribué ou fourni »[504] (nos soulignements).

Alors que les dispositions du C.c.Q. exigent que le défaut de sécurité soit en deçà de ce qui est raisonnable, cette limite technique prévisible du TALN, l'utilisateur est informé par le biais de la politique de confidentialité d'une amélioration continue du produit[505], et ne représenteront pas en soi un défaut de sécurité pouvant causer un réel préjudice. Par conséquent, le régime de responsabilité du fait d'un défaut de sécurité serait inadapté à une telle technologie. L'évolution constante de son système de fonctionnement et sa capacité d'apprentissage vont sans doute corriger tous ces défauts. Aussi, étant une technologie très récente (rappelons que le premier assistant vocal a été commercialisé en 2011 avec l'iPhone 4S), il serait difficile de lui faire appliquer un tel régime juridique existant depuis plusieurs années. Nul ne sait ce que deviendra l'assistant vocal dans les prochaines années. L'évolution, telle qu'illustrée à l'annexe 1 du mémoire, nous laisse à penser que les progrès pourraient tôt ou tard émerger vers une maîtrise (quasi) parfaite du langage humain par l'assistant vocal et d'un système informatique plus respectueux de la vie privée et davantage sécurité d'un point de vue de la confidentialité des renseignements personnels.

d) La responsabilité contractuelle pour tenter de sauver le C.c.Q dans son application à l'assistant vocal

[504] VERMEYS, N., « La responsabilité civile du fait des agents autonomes », 2018, Vol. 30 n°3, *Les Cahiers de propriété intellectuelle*, p. 865.
[505] Voir l'extrait 3 de la politique de confidentialité du Google Home concernant l'utilisation des données.

En matière contractuelle la responsabilité du vendeur ne sera pas aussi simple à déterminer. L'existence d'un vice doit répondre à différentes caractéristiques pour reconnaître la responsabilité contractuelle du vendeur[506]. Dans le cadre de l'utilisation de l'assistant vocal par l'acheteur, il n'y a *a priori* aucun vice caché à l'utilisateur. D'ailleurs, il serait difficile de faire valoir l'existence d'un vice dans l'assistant vocal pour tenter de reconnaître la responsabilité du vendeur dans le cadre d'une relation contractuelle. Si l'on croit Jean-Louis Baudouin, Patrice Deslauriers et Benoît Moore :

> « Un vice mineur ne peut suffire à entraîner la responsabilité du vendeur. Le vice doit être de nature à rendre le bien impropre à l'usage auquel on le destine, ou à diminuer tellement son utilité que l'acheteur ne l'aurait pas acheté, ou n'aurait pas donné un si haut prix, s'il l'avait connu » [507] (nos soulignements).

Le fonctionnement de l'assistant vocal doit donc être réduit « (…) de manière importante en regard des 'attentes légitimes d'un acheteur prudent et diligent' » [508] pour que son utilisateur puisse tenter d'invoquer la responsabilité du vendeur. Cette situation où l'assistant dysfonctionne lors de l'interprétation de la requête peut certes être gênante pour l'individu, cela n'en fait pas un problème majeur dans l'exécution des tâches. La nécessité d'une constante amélioration est rappelée par le fabricant, comme nous l'avons déjà évoqué au sujet de Google.

La responsabilité du fabricant peut également venir d'une disposition législative autre que celles du Code civil du Québec, semblant être inadaptées à la protection des renseignements personnels[509]. Par exemple l'article 25 de la *Loi concernant le cadre juridique des technologies de l'information* renferme une obligation de confidentialité. En vertu de cet article :

---

[506] Le vice doit revêtir une certaine gravité, être caché, existant bien avant la vente ou au moment de celle-ci et ne pas être connu de l'acheteur, BAUDOUIN, J.-L., DESLAURIERS, P., et MOORE, B., « La responsabilité du fabricant et du vendeur – Le régime contractuel : étendue de la garantie de qualité », dans *La responsabilité civile*, vol.2 : Responsabilité professionnelle, 8e éd., Montréal, Éditions Yvon Blais, 2014.

[507] BAUDOUIN, J.-L., DESLAURIERS, P., et MOORE, B., « La responsabilité du fabricant et du vendeur – Le régime contractuel : étendue de la garantie de qualité », dans *La responsabilité civile*, vol.2 : Responsabilité professionnelle, 8e éd., Montréal, Éditions Yvon Blais, 2014.

[508] Ibid.

[509] LAFONT, I., *L'efficacité du régime de responsabilité civile comme mesure de contrainte au respect de l'obligation de sécurité des renseignements personnels,* papyrus.bib.umontreal.ca, Mémoire de maîtrise, Faculté de Droit, Université de Montréal, Novembre 2013, en ligne : <https://papyrus.bib.umontreal.ca/xmlui/bitstream/handle/1866/11222/Lafont_Isabelle_2013_memoire.pdf?sequence=2&isAllowed=y >.

> « La personne responsable de l'accès à un document technologique qui porte un renseignement confidentiel doit prendre les mesures de sécurité propres à en assurer la confidentialité »[510] (nos soulignements).

À cet effet, en vertu de l'article 25 de la LCCJTI, le responsable doit garantir la confidentialité des renseignements lorsqu'il se trouve en présence d'un document technologique comportant des renseignements confidentiels. L'obligation se traduit par la mise en place de mesures de sécurité garantissant la confidentialité des renseignements. Si la LPRPSP[511] n'énonce aucune mesure pouvant être prise, la LCCJTI, en plus d'évoquer l'obligation d'assurer la confidentialité, prévoit des mécanismes de contrôle d'accès par des personnes autorisées. Nous retrouvons des exemples de moyens de contrôle similaires au sein de la LPRPDE pouvant aider le responsable à mettre en œuvre les mesures de sécurité :

> « 4.7.3
> Les méthodes de protection devraient comprendre :
> a) des moyens matériels, par exemple le verrouillage des classeurs et la restriction de l'accès aux bureaux;
> b) des mesures administratives, par exemple des autorisations sécuritaires et un accès sélectif; et
> c) des mesures techniques, par exemple l'usage de mots de passe et du chiffrement »[512] (nos soulignements).

Nous rajouterons, qu'au sein de ce même principe, la sensibilisation du personnel à la confidentialité des renseignements personnels est également conseillée comme mesure pouvant être adoptée par une entreprise[513]. Nous retrouvons des dispositions quasi similaires au sein du RGPD à l'article 32 :

> « 1. Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré

[510] Art. 25 LCCJTI, LRQ, c-1.1.
[511] Art. 10 de la LPRPSP.
[512] Par. 4.7.3 ; Art. 4.7, annexe 1 de la LPRPDE.
[513] Par. 4.7.4 de l'annexe 1 de la LPRPDE. Cette sensibilisation passe par l'élaboration d'une politique de sécurité interne à l'entreprise, VERMEYS, N., *Responsabilité civile et sécurité informationnelle,* Cowansville, Yvon Blais, 2010, p.144.

> de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris entre autres, selon les besoins:
> a) la pseudonymsation et le chiffrement des données à caractère personnel ;
> b) des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ; (…) »[514] (nos soulignements).

Les législations en vigueur mettent donc en place une obligation de protection des renseignements personnels en les obligeant à adopter des mesures de sécurité assurant leur confidentialité. S'agissant des fabricants d'assistants vocaux, il ne fait aucun doute sur leur capacité, humaine, technique et financière à mettre en place des mesures fortes pour protéger la confidentialité des renseignements personnels. L'utilisateur pourra sans doute se baser sur ces dispositions, liées à celles du Code civil du Québec, en ce qui concerne la vie privée[515]. Pour faire réparer le préjudice subi de la violation de cette obligation encore faut-il qu'il sache, d'une part, qu'il a été enregistré à son insu, et, d'autre part, parvienne à faire un lien[516] entre l'enregistrement et l'existence d'un préjudice[517].

En outre, dans l'hypothèse où certains fabricants auraient recours à un prestataire de service, que ce soit pour le stockage des renseignements personnels ou leur traitement à des fins « d'amélioration des services », l'article 26 de la LCCJTI précise que le prestataire doit lui aussi prendre les mesures adéquates pour garantir la confidentialité des renseignements qu'il a sous sa garde. Cet article n'exonère pas le responsable, dans notre cas le fabricant, d'adopter de telles mesures[518].

---

[514] Art. 32 al.1er du RGPD.
[515] Art. 35 à 37 du C.c.Q.
[516] En matière de protection des renseignements personnels, la victime doit prouver « (1) que l'omission de l'entreprise de prendre des mesures de sécurité raisonnables a rendu objectivement réalisable son dommage et, ensuite, (2) que l'entreprise pouvait raisonnablement prévoir le préjudice subi », LAFONT, I., *L'efficacité du régime de responsabilité civile comme mesure de contrainte au respect de l'obligation de sécurité des renseignements personnels,* papyrus.bib.umontreal.ca, Mémoire de maîtrise, Faculté de Droit, Université de Montréal, Novembre 2013, en ligne : <https://papyrus.bib.umontreal.ca/xmlui/bitstream/handle/1866/11222/Lafont_Isabelle_2013_memoire.pdf?sequence=2&isAllowed=y >, p. 26.
[517] BAUDOUIN, J.-L., DESLAURIERS, P., et MOORE, B., *La responsabilité civile*, vol.1 : Principes généraux, 8e éd., Montréal, Éditions Yvon Blais, 2014.
[518] Selon le professeur VERMEYS, La simple omission d'adoption de mesures de sécurité visant à protéger les renseignements personnels peut constituer une faute et engager la responsabilité civile même s'il n'existe aucune violation, VERMEYS, N., *Responsabilité civile et sécurité informationnelle,* Cowansville, Yvon Blais, 2010, p.93.

L'activation de l'assistant vocal par la simple prononciation d'un mot d'éveil et son interaction avec l'utilisateur par le biais du TALN présentent l'avantage de faciliter son utilisation. Cependant, la simplicité d'accès remet en cause le respect de la vie privée, particulièrement dans le cas où un tiers interagit avec l'assistant vocal ne lui appartenant pas. Ce tiers aura la faculté d'accéder à des services ou applications pouvant dévoiler des renseignements personnels. Les limites techniques du TALN sont de nature à provoquer des effets juridiques, que l'utilisateur pourrait avoir du mal à établir dans l'optique d'obtenir une réparation. L'interaction avec l'assistant vocal vient mettre en lumière l'inadaptation du C.c.Q. dans sa fonction de réparation du préjudice puisque certaines conséquences juridiques ne seront pas ressenties par l'utilisateur[519]. Celui-ci, estimant avoir subi un préjudice dans la collecte de ses renseignements personnels et sans avoir forcément donné son consentement, se retrouvera dans l'impossibilité de faire reconnaître la responsabilité du fabricant de l'assistant vocal, l'absence d'un lien de causalité existe entre le dommage et le fait générateur[520] faisant défaut.

2. L'instauration d'une nouvelle obligation tendant à protéger les renseignements personnels, l'obligation de notification des incidents de sécurité

L'obligation de notifier les incidents de sécurité est une obligation ayant fait récemment son intégration dans la LPRPDE mais également dans d'autres textes internationaux (a). Bien que cette obligation se veut comme une mesure *a posteriori* de contrôle, elle cache en elle un effet préventif imposant aux entreprises d'adopter des mesures de sécurité efficace pour éviter la notification en cas de failles (b).

---

[519] LAFONT, I., *L'efficacité du régime de responsabilité civile comme mesure de contrainte au respect de l'obligation de sécurité des renseignements personnels,* Mémoire de maîtrise, Faculté de Droit, Université de Montréal, Novembre 2013, en ligne : <https://papyrus.bib.umontreal.ca/xmlui/bitstream/handle/1866/11222/Lafont_Isabelle_2013_memoire.pdf?sequence=2&isAllowed=y > ; Voir également BONNET, A., *La responsabilité du fait de l'intelligence artificielle,* Mémoire de Maîtrise, Banque des mémoires, Université Panthéon-Assas, Paris II, 2015, en ligne : <https://docassas.u-paris2.fr/nuxeo/site/esupversions/90fcfa29-62e4-4b79-b0b4-d1beacc35e86?inline >.

[520] Art. 1457 CcQ ; Voir également BAUDOUIN, J.-L., DESLAURIERS, P., et MOORE, B., *La responsabilité civile*, vol.1, Principes généraux, 8e édition, 2014.

a) Le cadre juridique de l'obligation de notification des incidents de sécurité

D'emblée nous précisons que la *Loi sur la protection des renseignements personnels dans le secteur privé* ne contient aucune disposition obligeant les entreprises à déclarer les incidents de sécurité dont ils sont victimes. Bien que son article 10 dispose qu'une organisation doit adopter des mesures de sécurité en prenant compte de la sensibilité du renseignement et que des recours existent, cette disposition n'est assortie d'aucun moyen de contrôle permettant d'effectuer un suivi des incidents et d'évaluer si l'entreprise a adopté les mesures nécessaires[521]. Nous retrouvons pareille situation avec la *Loi concernant le cadre juridique des technologies de l'information*. Les articles 25 et 26 de la loi prévoient seulement une obligation de confidentialité de la part du responsable du traitement (art. 25) et de son sous-traitant (art. 26).

Cette nécessité d'avoir une telle obligation de notification, la CAI l'a manifesté dès 2011 dans son rapport quinquennal en parlant de la consolidation de « (…) l'obligation d'adopter et de maintenir des mesures de sécurité efficaces et efficientes tout au long du cycle de vie des renseignements personnels »[522]. À cet effet, le gouvernement du Québec a émis des *Orientations gouvernementales pour un gouvernement plus transparent, dans le respect du droit à la vie privée et la protection des renseignements personnels*[523]. Parmi ces recommandations, le gouvernement préconise de « [o]bliger les organismes publics à gérer de façon transparente les incidents de sécurité portant sur des renseignements personnels »[524]. Pour y parvenir, le gouvernement entend intégrer au sein de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements*

[521] COMMISSION D'ACCES A L'INFORMATION, *Rétablir l'équilibre,* Rapport quinquennal, cai.gouv.qc.ca, 2016, en ligne : < http://www.cai.gouv.qc.ca/documents/CAI_RQ_2016.pdf >, pp.106-107.
[522] COMMISSION D'ACCES A L'INFORMATION, *Technologies et vie privée à l'heure des choix de société,* Rapport quinquennal, cai.gouv.qc.ca, juin 2011, en ligne : <https://www.cai.gouv.qc.ca/documents/CAI_RQ_2011.pdf >, p.37.
[523] SECRETARIAT A L'ACCES ET A LA REFORME DES INSTITUTIONS DEMOCRATIQUES, *Orientations gouvernementales pour un gouvernement plus transparent, dans le respect du droit à la vie privée et la protection des renseignements personnels*, institutions-democratiques.gouv.qc.ca, 2015, en ligne : < https://www.institutions-democratiques.gouv.qc.ca/transparence/documents/doc-orientations-gouv.pdf >.
[524] SECRETARIAT A L'ACCES ET A LA REFORME DES INSTITUTIONS DEMOCRATIQUES, *Orientations gouvernementales pour un gouvernement plus transparent, dans le respect du droit à la vie privée et la protection des renseignements personnels*, institutions-democratiques.gouv.qc.ca, 2015, en ligne : < https://www.institutions-democratiques.gouv.qc.ca/transparence/documents/doc-orientations-gouv.pdf >, orientation n°17, p.109.

personnels[525] une section encadrant la notification. À l'instar de la loi albertaine sur la protection des renseignements personnels prévoyant un tel mécanisme pour les entreprises du secteur privé[526], le Québec ne prévoit pas de notification automatique tout en omettant de préciser les cas devant faire l'objet d'une telle notification. Une telle modification de la LPRPSP viendrait selon la CAI maintenir une effectivité « essentiellement similaire à la LPRPDE »[527]. En effet, la LPRPDE prévoit depuis sa modification en 2018 l'obligation pour une entreprise de déclarer en vertu de l'article 10 toute atteinte causant un risque réel de préjudice grave à l'individu concerné. L'appréciation de ce « risque réel de préjudice grave » se fait en prenant en compte le degré de sensibilité du renseignement personnel et notamment la probabilité qu'il soit mal utilisé. Nous retrouvons une approche similaire au sein de la loi de l'Alberta [528].

Nous apportons quelques précisions supplémentaires concernant la LPRPSP, bien que la version actuellement en vigueur ne mentionne aucune obligation de notification, le projet de loi n°64 portant *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*[529] instaure cette obligation en cas de survenance d'un « incident de confidentialité ». Ce projet de loi définit un tel incident comme étant :

> « 1° l'accès non autorisé par la loi à un renseignement personnel;
> 2° l'utilisation non autorisée par la loi d'un renseignement personnel;
> 3° la communication non autorisée par la loi d'un renseignement personnel;
> 4° la perte d'un renseignement personnel ou toute autre atteinte à la protection d'un tel renseignement »[530].

L'obligation de notification viendrait selon la CAI :

---

[525] *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, RLRQ c A-2.1.
[526] Art. 34.1 (1), *Personal Information Protection Act,* Statutes of Alberta, 2003, Chapter P-6.5 ; AYLWIN, A., « L'obligation de notification en cas de violation de la confidentialité pour une entreprise du secteur privé », (2015) 74 R. du B., p.478.
[527] COMMISSION D'ACCES A L'INFORMATION, *Rétablir l'équilibre,* Rapport quinquennal, cai.gouv.qc.ca, 2016, en ligne : < http://www.cai.gouv.qc.ca/documents/CAI_RQ_2016.pdf >, p.106.
[528] Art. 19.1 (1), *Personal Information Protection Act,* Statutes of Alberta, 2003, Chapter P-6.5.
[529] ASSEMBLEE NATIONALE DU QUEBEC, *Projet de loi n°64 : Loi modernisant des dispositions législatives en matière de protection des renseignements personnels,* présenté par Mme Sonia LeBel, Ministre responsable des Institutions démocratiques, de la Réforme électorale et de l'Accès à l'information, première session, 42e législature, 2020.
[530] Ibid., p.12.

> « (…) responsabiliser les organismes publics et les entreprises quant à la nécessité de se doter d'un cadre de gouvernance relié à l'adoption et à la vérification régulière des mesures de sécurité mises en place afin d'évaluer si elles assurent efficacement la protection des renseignements personnels »[531].

La CAI a déjà tenu ces mêmes propos dans son rapport quinquennal de 2011 dans lequel elle précisait que l'obligation de notification va de pair avec celle de sécurité[532]. En outre, le projet de loi n°64 impose à l'entreprise de tenir un « registre des incidents de confidentialité », dont une copie pourra être transmise à la CAI si elle en fait la demande. Il s'agirait ni plus ni moins que d'un moyen de contrôle de la CAI sur les mesures mises en place par celle-ci et leur efficacité en fonction du préjudice subi. Un tel pouvoir de contrôle avait déjà été demandé par la CAI dans son rapport quinquennal

Au niveau international, l'OCDE a modifié ses lignes directrices de 1980[533] afin d'inclure l'obligation de notification[534] motivée par l'idée que « [r]equiring notification may enable individuals to take measures to protect themselves against the consequences of identity theft or other harms »[535]. L'OCDE adopte également une approche de la notification des incidents de sécurité basée sur l'atteinte grave aux renseignements personnels de l'individu. Selon l'OCDE, l'atteinte est celle « that puts privacy and individual liberties at risk »[536]. Cette approche permettrait de limiter « an undue burden on data controllers and enforcement authorities, for limited

---

[531] COMMISSION D'ACCES A L'INFORMATION, *Rétablir l'équilibre,* Rapport quinquennal, cai.gouv.qc.ca, 2016, en ligne : < http://www.cai.gouv.qc.ca/documents/CAI_RQ_2016.pdf >, p.107.
[532] COMMISSION D'ACCES A L'INFORMATION, *Technologies et vie privée à l'heure des choix de société,* Rapport quinquennal, cai.gouv.qc.ca, juin 2011, en ligne : <https://www.cai.gouv.qc.ca/documents/CAI_RQ_2011.pdf >, p.39.
[533] ORGANISATION FOR ECONOMIC COOPERATION AND DEVELOPMENT, *Guidelines governing the protection of privacy and transborder flows of personal data (2013)*, chapitre 1, C(80)58/Final, amendé le 11 juillet 2013 par C(2013) 79, en ligne : <http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf >.
[534] Ibid., art. 15 c).
[535] ORGANISATION FOR ECONOMIC COOPERATION AND DEVELOPMENT, *Chapter 2: Supplementary explanatory memorandum to the revised recommendation of the council concerning guidelines governing the protection of privacy and transborder flows of personal data (2013),* en ligne : <http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf >, p. 26.
[536] Ibid., p.27.

corresponding benefit »[537]. Dans le même temps une saisie « excessive notification to data subjects may cause them to disregard notices »[538].

Nous terminons notre revue du cadre juridique de l'obligation de notification avec le RGPD. La violation des renseignements personnels est définie comme :

> « (…) une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données »[539].

L'alinéa premier de l'article 33 prévoyant cette obligation se lit comme suit :

> « En cas de violation de données à caractère personnel, le responsable du traitement en notifie la violation en question à l'autorité de contrôle compétente conformément à l'article 55, dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques »[540] (nos soulignements).

Pour la CNIL, l'obligation doit répondre à deux conditions : (1) être en présence d'un traitement de renseignements personnels ; (2) que la violation, accidentelle ou illicite, porte atteinte à l'intégrité, la disponibilité ou la confidentialité du renseignement[541]. Nous noterons par ailleurs qu'une telle obligation n'est pas systématique lorsque survient la violation. Celle-ci doit entraîner atteinte aux droits et libertés de la personne pour contraindre le responsable du traitement à notifier à l'autorité de contrôle.

---

[537] Ibid.
[538] Ibid.
[539] Art. 4 du RGPD.
[540] Art. 33 al.1er du RGPD.
[541] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES, *Notifier une violation de données personnelles,* cnil.fr, 24 mai 2018, en ligne : < https://www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles > ; GROUPE DE TRAVAIL ARTICLE 29, *Lignes directrices sur la notification de violations de données à caractère personnel en vertu du Règlement (UE) 2016/679,* adoptée le 3 octobre 2017, version révisée et adoptée le 6 février 2018, en ligne : <https://www.cnil.fr/sites/default/files/atoms/files/wp250rev01_fr.pdf >, p.8.

Cette obligation de notification s'accompagne également d'une obligation de communication auprès de la personne concernée en application de l'article 34. Bien que les termes employés soient différents pour chaque obligation, il s'agit simplement que de synonymes. En effet, dans les lignes directrices du Groupe de travail « article 29 », nous constatons que les informations demandées à une entreprise dans le cadre d'une violation sont similaires que ce soit pour la notification ou pour la communication[542]. Nous croyons que l'utilisation de la notion de « notification » pour les autorités de contrôle renverrait davantage vers une volonté de contraindre l'entreprise à leur porter connaissance les faits pour le lancement d'une enquête plutôt que de les limiter à une simple transmission d'informations. C'est ainsi que l'Office québécois de la langue française définit en 1995 ladite notion comme étant le fait de « porter un acte juridique ou une décision à la connaissance des intéressés en observant des formes légales »[543].

b) L'effet préventif de l'obligation de notification dans la protection des renseignements personnels

L'obligation de notification comporte un double effet préventif, à la fois à l'égard des tiers, notamment en obligeant les entreprises à adopter des mesures de sécurité efficace pour prévenir tout acte malveillant (i), mais également en contribuant indirectement au respect des autres principes de la protection des renseignements personnels que nous avons eu l'occasion de mentionner (ii).

i. La prévention de l'obligation de notification vis-à-vis des tiers

Si l'obligation de notification des incidents de sécurité est avant tout une mesure *a posteriori* en complément de l'obligation de sécurité[544], la contrainte qui pèse sur les entreprises à devoir signaler

[542] GROUPE DE TRAVAIL ARTICLE 29, *Lignes directrices sur la notification de violations de données à caractère personnel en vertu du Règlement (UE) 2016/679,* adoptée le 3 octobre 2017, version révisée et adoptée le 6 février 2018, en ligne : <https://www.cnil.fr/sites/default/files/atoms/files/wp250rev01_fr.pdf >, pp. 16 et 23.
[543] OFFICE QUEBECOIS DE LA FRANCAISE, « Grand dictionnaire terminologique : notification », gdt.oqlf.gouv.qc.ca, 1995, en ligne : < http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=17486113 >.
[544] COMMISSION D'ACCES A L'INFORMATION, *Technologies et vie privée à l'heure des choix de société,* Rapport quinquennal, cai.gouv.qc.ca, juin 2011, en ligne : <https://www.cai.gouv.qc.ca/documents/CAI_RQ_2011.pdf >, p.39.

ces incidents les force à agir en amont en adoptant les mesures de sécurité adéquates pour protéger les renseignements personnels. L'adoption de mesures de sécurité est dans leur intérêt puisqu'elles leur évitent tout recours juridique de la part des individus portant sur la violation de leurs renseignements personnels émanant d'un tiers malveillant. Une telle action juridique serait de nature à porter sérieusement atteinte à leur réputation[545].

La prévention passe tout d'abord par l'analyse des risques susceptibles d'être encourues, notamment en prenant en compte le degré de sensibilité des renseignements personnels. Pour ce qui est des assistants vocaux, les renseignements collectés sont exclusivement la voix des utilisateurs et des personnes se trouvant à proximité lors de l'interaction. Il est bien connu que dans le domaine de la sécurité de l'information le « risque zéro » n'existe pas. Nous renvoyons à cet effet le lecteur à la sous-partie précédente dans laquelle nous évoquons les différentes, et non limitatives, techniques d'attaque d'une personne malveillante. Le responsable du traitement des renseignements personnels doit ainsi adopter toutes les mesures de sécurité qu'une personne raisonnable est en droit de s'attendre lors de l'utilisation de l'assistant vocal. L'analyse du risque passera donc par le suivi de l'évolution des règles de l'art, ou les « normes de l'industrie » et de « l'industrie des normes »[546] émises par des organismes externes tels que le CAI, le CPVP, la CNIL ou encore l'Organisation Internationale de normalisation. À titre préventif donc les entreprises doivent sans cesse évaluer les mesures de sécurité prises et les adapter si nécessaire.

La tenue obligatoire d'un registre des incidents de sécurité et sa communication aux autorités de contrôle peuvent également jouer un rôle dans la prévention de la survenance de l'incident. La transmission du registre répertoriant toutes les informations nécessaires permettant d'apprécier le niveau des mesures de sécurité au regard de la violation peut contraindre les entreprises à dévoiler certaines informations qu'elles aimeraient garder confidentielle pour ne pas en faire bénéficier aux concurrents. Aussi une communication du registre à l'autorité de contrôle aura pour avantage de prévenir la réalisation de futurs incidents de sécurité. Celles-ci seraient en capacité de mieux

[545] COMMISSION D'ACCES A L'INFORMATION, *Rétablir l'équilibre,* Rapport quinquennal, cai.gouv.qc.ca, 2016, en ligne : < http://www.cai.gouv.qc.ca/documents/CAI_RQ_2016.pdf >, p.107.

[546] VERMEYS, N. W., *Qualification et quantification de l'obligation de sécurité informationnelle dans la détermination de la faute civile*, papyrus.bib.umontreal.ca, Thèse de doctorat, Université de Montréal, Mars 2009, en ligne :<https://papyrus.bib.umontreal.ca/xmlui/bitstream/handle/1866/3663/12085490.PDF?sequence=2&isAllowed=y >, pp. 112 et s.

accompagner les entreprises dans l'élaboration des mesures de sécurité par le biais de la publication de documentations à l'instar de ce que fait le Commissariat à la protection de la vie privée avec les rapports d'enquêtes ou ses lignes directrices.

En outre, à travers cette obligation, c'est la formation des employés de l'entreprise qui est concernée. En effet, la sensibilisation fait partie intégrante de la prévention d'une violation car derrière chacune d'elle nous retrouvons une intervention humaine. C'est une des mesures obligatoires à instaurer en vertu de la LPRPDE[547] pour protéger les renseignements personnels. Pour les fabricants des assistants vocaux, une telle mesure permettra de développer une culture de la protection de la vie privée des utilisateurs. La mise en place de campagne de sensibilisation pourrait concourir à prévenir une quelconque intrusion dans leur base de données. En sensibilisant les employés, les fabricants pourront également communiquer publiquement et en toute transparence sur leur traitement des renseignements personnels. De ce fait, ils amélioreront leur réputation auprès de leurs consommateurs, qui auront accès à davantage d'information sur les méthodes de traitement et les procédures envisagées en cas d'incident de sécurité.

ii. Les effets de l'obligation de notification tendant à réaffirmer le respect des principes fondamentaux de la protection des renseignements personnels

L'obligation de notification amène également les entreprises à faire preuve de transparence dans la gestion des renseignements personnels en les obligeant indirectement à respecter les principes fondamentaux. La transparence dans les mesures de sécurité adoptées peut se caractériser en premier lieu par la publication d'une certification décernée par une autorité ou un organisme habileté à le faire. La certification est prévue par le RGPD aux articles 42 et 43. La *loi concernant le cadre juridique des technologies de l'information,* la loi sur l'accès ou la LPRPSP ne contiennent aucune dispositions similaires à celles du RGPD.

Les fabricants qui estiment respecter la protection de la vie privée des utilisateurs d'assistants vocaux pourront faire valoir leur label de bonne conduite pour tenter de convaincre les utilisateurs

[547] Art. 4.1.4 de l'annexe 1 de la LPRPDE.

que le traitement de leurs renseignements personnels respecte les règles en vigueur. Il serait erroné de dire que la certification vaut exemption d'application des législations en matière de protection des renseignements personnels. À cet effet, l'article 32 du RGPD précise, en complément de la possibilité de certification, que l'octroi de celle-ci ne vaut pas exemption à l'entreprise de se conformer au règlement de l'Union européenne. Nous précisons toutefois que l'attribution de la certification ne constitue pas un réel gage de confiance pour l'utilisateur d'un assistant vocal, dont son fabricant se situe dans un pays étranger. Nous pouvons citer l'exemple de la certification américaine *TRUSTe,* se basant sur une méthode peu exigeante, dont Arnaud Belleil affirme que :

> « Aux États-Unis, cette approche des *privacy seal* [certifications] se rattache à la démarche d'auto-régulation dans la mesure où les marques de confiance tendent à se substituer à une réglementation informatique et libertés qui n'est pas en vigueur »[548].

Cette certification manque en réalité d'une certaine fiabilité, notamment aux États-Unis :

> « Dans un esprit américain, assez éloigné des règlements et mentalités européennes, leur objet est pour l'essentiel de garantir que le site web a une politique sur les données personnelles et que cette politique fait l'objet d'une publication »[549] (nos soulignements).

Arnaud Belleil finit par résumer la situation des certifications américaines en disant que « il est possible d'être labellisé en faisant n'importe quoi si l'on informe le public que l'on fait n'importe quoi »[550].

Si l'on prend le cas de Google, comme celui des autres entreprises constituant le GAFAM[551], nous constatons l'absence de la présence d'une quelconque certification. Malgré le fait que l'obligation de notification constituerait un moyen efficace pour les obliger à communiquer sur leurs méthodes et procédures mises en place pour garantir la protection des renseignements personnels, leur

[548] BELLEIL, A., « La régulation économique des données personnelles ? », dans Legicom 2009/1 (N°42), ligne : <https://www.cairn.info/revue-legicom-2009-1-page-143.htm#s2n5 >, p.24.
[549] Ibid, p.25.
[550] Ibid.
[551] Acronyme donné à Google, Amazon, Facebook, Apple et Microsoft.

manque de conformité aux législations s'explique principalement par leur intérêt économique à récolter et utiliser les renseignements personnels pour en faire un profit, particulièrement par le biais des annonces ciblées.

En second lieu, la transparence passe par un meilleur respect des principes de collecte et d'utilisation des renseignements personnels. Nous avons eu l'occasion tout au long de ce travail de citer l'exemple d'une personne ayant été amenée à manipuler des renseignements personnels afin de vérifier la bonne compréhension et la retranscription écrite de la requête par l'assistant vocal [552]. À travers cet exemple, nous avons souligné l'absence de la mention à l'utilisateur qu'une entreprise tierce a accès à ses renseignements personnels. Si l'on émet l'hypothèse d'une atteinte à ces renseignements, sachant que personne n'est supposée connaître l'existence de cette entreprise, et que sur la base de ce témoignage aucune mesure de sécurité adéquate n'est prise (chiffrement des données, restriction d'accès etc.), il serait difficile pour les autorités de contrôle d'obtenir toutes les informations nécessaires leur permettant d'apprécier le niveau de sécurité adopté par le fabricant de l'assistant vocal. D'ailleurs, l'atteinte ne touchant que le tiers, l'absence de contrat avec le fabricant peut l'encourager à ne pas divulguer l'information au risque de perdre sa confiance et de remettre en cause l'attribution de la gestion des renseignements personnels. Dans le cas contraire, c'est au fabricant qu'appartiendrait le choix de notifier ou non aux autorités. Pour s'éviter une enquête pouvant donner lieu à une amende[553] et constituer une atteinte à sa réputation, le fabricant pourra opter pour l'option de minimiser la violation lors de la notification en cachant l'existence d'une quelconque relation avec l'entreprise tierce. Il s'agira dans cette hypothèse d'une des limites de l'obligation de notification qui est celle de l'insuffisance des informations apportées par l'entreprise à l'autorité de contrôle.

Une limite qui reste malgré tout relative puisque le fabricant n'est pas à l'abri d'une éventuelle dénonciation en interne. À l'image de cette « dresseuse d'IA » qui a décidé de mettre au jour la pratique de son entreprise. Une telle situation risquerait alors d'exposer la mauvaise pratique du

[552] CASILLI A., « Derrière les assistants vocaux, des humains vous entendent », laquadratur.net, 18 mai 2018, en ligne : < https://www.laquadrature.net/2018/05/18/temoin_cortana/ >.
[553] Rappelons que conformément à l'article 83 du RGPD, celle-ci peut atteindre 20 millions d'euros ou jusqu'à 4 % du chiffre d'affaire mondial de l'entreprise. Le projet de loi n°64 du Québec prévoit un montant pouvant aller jusqu'à 2 % du chiffre d'affaire ou 25 millions de dollars canadiens.

fabricant dans la collecte et l'utilisation des renseignements personnels. Pour prévenir ce genre de situation, le fabricant aurait tout intérêt à appliquer les différents principes de la protection des renseignements personnels ou il risquerait devoir rendre des comptes aux autorités de contrôle par le biais de cette obligation de notification.

Conclusion

L'évolution tout aussi moderne que rapide de l'assistant vocal a mis à mal les régimes juridiques de la vie privée et de la protection des renseignements personnels. Mais pas seulement, la jurisprudence, à l'image du test de *Oakes* et de son adaptation aux renseignements personnels[554], et les différents régimes de responsabilité civile se sont révélés être inadaptés à l'assistant vocal. Ceux-ci l'ont essentiellement été aux technologies conçues et largement utilisées ce qui a permis d'affiner avec le temps leur cadre juridique. C'est par exemple le cas d'une interception de communication téléphonique[555] ou l'accès à un ordinateur partagé pouvant être assimilé à une fouille au sens de la Charte canadienne[556].

L'assistant vocal est un phénomène nouveau dans le domaine de la protection des renseignements personnels et sa prolifération massive, aidée par son intégration dans différents terminaux mobiles et objets connectés, n'a pas laisser suffisamment de temps aux autorités étatiques de renforcer les législations actuelles afin de prévenir et réprimer toute atteinte à la vie privée. Signe d'un manque de contrôle du fait de sa récente commercialisation, l'assistant vocal lui-même embarquant le TALN est encore loin de garantir une parfaite maîtrise de la reconnaissance vocale. Ses nombreux cas de faux positifs et l'absence d'une sécurité robuste, bien que son utilité puisse être saluée en pensant particulièrement aux personnes en situation d'handicap, font de lui une technologie encore très vulnérable. Nous l'avons illustré tout au long de ce développement avec différents exemples de faits divers. La voix, qualifiée de renseignement personnel sensible, si elle est détournée par un tiers peut gravement porter préjudice à son propriétaire. Malgré la répression par le code criminel du vol d'identité[557], la conservation des renseignements personnels à l'étranger et leur réutilisation par des tiers sans en informer correctement l'utilisateur ne lui offrent pas la pleine garantie de l'effectivité de ses droits lui assurant par la même occasion du respect par l'entreprise des législations en vigueur.

---

[554] *Mountain Province Diamonds Inc*. v. *De Beers Canada Inc.,* 2014 ONSC 2026 (CanLII).
[555] *R*. c. *Duarte,* [1990] 1 R.C.S. 30 ; *R.* c. *Wiggins*, [1990] 1 R.C.S. 62 ; *Strivastava* c. *Hindu Mission of Canada (Québec) Inc.*, 2001 CanLII 27966 (QC CA) ; *Ste-Marie* c. *Placements J.P.M. Marquis Inc.*, 2005 QCCA 312 (CanLII).
[556] *R*. c. *Reeves,* 2018 CSC 56, [2018] 3 R.C.S. 531.
[557] Art. 402.2 (5) du *Code criminel*, L.R.C. (1985), ch. C-46.

Cette inadéquation est d'autant plus problématique que les utilisateurs sont les premiers acteurs à la fois de leur divulgation de renseignements personnels mais également de leur protection de leur vie privée. Reprenons un des principes les plus importants de la protection des renseignements personnels, celui du consentement. L'utilisateur va consentir à ce que des renseignements vont être collectés mais dans le même temps cette utilisation se fera au sein de son domicile, ou plus généralement dans un cadre privé. Le recours exclusivement au mode naturel de communication[558] et l'absence dans certains cas d'écrans permettant d'avoir un visuel sur les échanges et les résultats produits concourent à faire oublier à l'utilisateur qu'il interagit avec une machine. D'autant plus que les entreprises prennent le soin de les dotés d'un nom afin de leur accorder une certaine personnification favorisant leur domestication dans la vie privée des utilisateurs[559].

Ce « paradoxe de la vie privée »[560] n'est pas près de s'arrêter là. En effet, de nouveaux biens intègrent un assistant vocal à des fins commerciales et marketing, nous pouvons citer l'exemple des voitures[561] conduisant les entreprises à mettre en avant la faculté pour le conducteur de rester concentrer sur la route tout en lui offrant le pouvoir d'énoncer certaines commandes vocales. Alors même qu'il a été affirmé que :

> « Self determination is an inalienable right for all human beings. Personal development should not be defined by what business and government know about you. The proliferation of the internet of things increases the risk that this will happen »[562] (notre soulignement).

[558] MINKER, W., et NEEL, F., « Développement des technologies vocales », dans *Le travail humain*, vol. 65, 2002/3, en ligne : < https://www.cairn.info/revue-le-travail-humain-2002-3-page-261.htm#pa23 >, p.269.
[559] LACHANCE, F., *« O.K. Google, assiste-moi » Les parcours des utilisateurs et des familles qui domestiquent le Google Home,* papyrus.bib.umontreal.ca, Mémoire de maîtrise, Avril 2019, en ligne : <https://papyrus.bib.umontreal.ca/xmlui/bitstream/handle/1866/22464/Lachance_Francois_2019_memoire.pdf?sequence=2&isAllowed=y >, pp.26 et s.
[560] LAZARO, C., et LE METAYER, D., « Le consentement au traitement des données personnelles : Perspective comparative sur l'autonomie du sujet », (2014) 48 RJTUM 765-815, 2014, p.773.
[561] VITRÉ, P., « L'assistant vocal, nouvel ami des voitures ? », androidpit.fr, 4 octobre 2018, en ligne : <https://www.androidpit.fr/bmw-series-3-assistant-vocal >.
[562] 36TH INTERNATIONAL CONFERENCE OF DATA PROTECTION AND PRIVACY COMMISSIONERS, *Mauritius Declaration on the Internet of Things,* Balaclava, 14 october 2014, en ligne : <https://www.cai.gouv.qc.ca/documents/Mauritius-Declaration.pdf >, p.1.

Si le législateur fédéral a tenté de renforcer l'effectivité des principes fondamentaux en instaurant une obligation de notification des incidents de sécurité, celle-ci se révèle être insuffisante, principalement en raison d'un manque de clarté et de précision dans la rédaction des politiques de confidentialité obligeant l'utilisateur à se fier aux paroles de l'entreprise[563]. Cette pratique a surtout pour objectif de cacher la capacité technique de l'assistant vocal d'opérer une collecte massive des renseignements personnels par le biais des nombreux microphones qu'il comporte.

Selon nous, il devrait exister une présomption d'attente raisonnable de vie privée. Nous pouvons reprendre la théorie de l'obligation de moyens renforcée, soulevée par le professeur Crépeau[564], et reprise par le professeur Vermeys concernant la sécurité informationnelle[565]. L'obligation de moyen est assortie d'une présomption de faute. La présomption entraînerait un renversement du fardeau de la preuve qui sera à l'avantage du créancier et obligera le débiteur à démontrer qu'il a adopté les mesures raisonnables pour éviter le préjudice sans toutefois lui imposer une obligation de résultat[566]. Par analogie, nous pensons qu'une telle présomption d'expectative de vie privée pourrait permettre à l'utilisateur de l'assistant vocal de se décharger du fardeau de la preuve d'un comportement raisonnable, qui plus est dans un cadre privé, et de contraindre le fabricant à démontrer que les mesures adoptées ont permis d'éviter toute atteinte à la vie privée. À l'instar des politiques de confidentialité qu'une personne normale ne parviendrait pas lors de leur lecture à adopter un raisonnement critique sur leur légalité et qui devra donc s'y soumettre, la présomption pourrait trouver application à notre cas en raison de l'exigence de maîtriser la programmation informatique, qu'il n'est pas attendue d'un utilisateur raisonnable de détenir un quelconque niveau de connaissance. Par ailleurs, nous estimons que cette obligation devrait être appliquée à une pareille situation car cela déchargerait l'utilisateur d'une autre contrainte qui est celle de l'adoption par lui-même de mesures de sécurité alors même qu'il interagit *a priori* raisonnablement avec l'assistant vocal dans son domicile privé. Rejeter cette hypothèse reviendrait à ouvrir une possible

[563] PLOURDE, A., « Retour vers le futur : l'Internet des objets et la protection de la vie privée », dans *Développements récents en droit à la vie privée (2019)*, vol. 465, service de la formation continue, Barreau du Québec, Montréal, Edition Yvon Blais, 2019.
[564] CRÉPEAU, P-A., *L'intensité de l'obligation juridique,* Cowansville, Yvon Blais, 1989.
[565] VERMEYS, N. W., *Qualification et quantification de l'obligation de sécurité informationnelle dans la détermination de la faute civile*, papyrus.bib.umontreal.ca, Thèse de doctorat, Université de Montréal, Mars 2009, en ligne :<https://papyrus.bib.umontreal.ca/xmlui/bitstream/handle/1866/3663/12085490.PDF?sequence=2&isAllowed=y>.
[566] Ibid, p.107.

voie à la restriction de la liberté individuelle dans la sphère privée. L'individu serait alors contraint d'adapter son environnement privé en fonction de ses interactions avec l'assistant vocal.

Terminons par mentionner le cas des autorités de contrôle, le Commissariat à la protection de la vie privée et la Commission d'accès à l'information. Aux vues des législations et des pouvoirs limités qui leur sont confiés, nul doute que les entreprises auront moins de contraintes à respecter les lois en matière de protection des renseignements personnels. Contrairement à leurs homologues européens qui ont un pouvoir de sanction dissuasif en cas d'atteinte à la protection des renseignements personnels, le CPVP et la CAI ne disposent pas d'un tel pouvoir mais seulement celui de lancer des enquêtes non contraignantes, dont les résultats peuvent être rendus public.

Annexe

Annexe 1. – Schéma représentant l'évolution historique du TALN dans les technologies

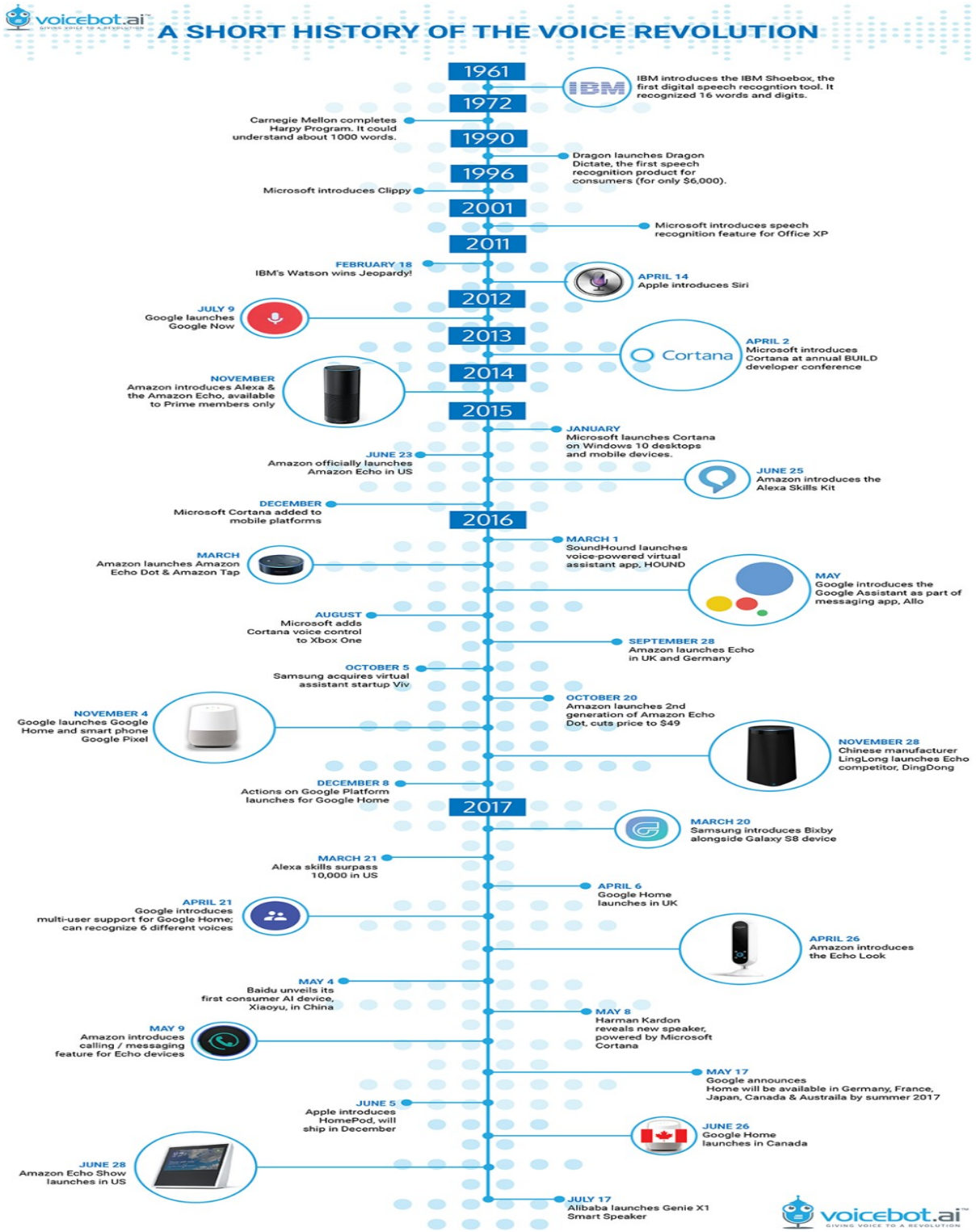


Table des législations

Textes du Canada

Charte canadienne des droits et libertés, Annexe B de la loi de 1982 sur le Canada (R-U), 1982, c 11.

Code criminel, L.R.C. (1985), ch. C-46.

Déclaration canadienne des droits, S.C. 1960, ch. 44.

Loi sur la protection des renseignements personnels, L.R.C. (1985), ch. P-21.

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

Textes de l'Alberta

Freedom of Information and Protection of Privacy Act, Revised Statutes of Alberta 2000, chapter F-25.

Personal Information Protection Act, Statutes of Alberta, 2003, Chapter P-6.5.

Texte de la Colombie-Britannique

Personal Information Protection Act, Statutes of British-Columbia, 2003, Chapter 63.

Texte du Nouveau-Brunswick

Loi sur l'accès et la protection en matière de renseignements personnels sur la santé, LN-B. 2009, c P-7.05.

Texte de la Nouvelle-Ecosse

Personal Health Information Act, 2nd session, 61st General Assembly, Nova Scotia 59 Elizabeth II, 2010.

Texte de l'Ontario

Loi de 2016 sur la protection des renseignements personnels sur la qualité des soins, LO 2016, c 6, ann 2.

Textes du Québec

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

Code civil du Québec, L.Q. 2020 c13.

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

Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, RLRQ c A-2.1.

Loi sur la protection des renseignements personnels dans le secteur privé, RLRQ c P-39.1.

Texte de Terre-Neuve-et-Labrador

Personal Health Information Act, SNL 2008, c P-7.01.

Législation du Conseil de l'Europe

Convention européenne des droits de l'homme et des libertés fondamentales, Rome, 4 XI 1950.

Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, Conseil de l'Europe, *Série des traités européens n°108*, Strasbourg, 28.I.1981.

Textes de l'Union européenne

Charte des droits fondamentaux de l'Union européenne, 2000/C, Nice, 7 décembre 2000, 2000/C, 364/01.

Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, 24 octobre 1995, Journal Officiel n° L281 du 23 novembre 1995, p.0031-0050.

Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques), Journal officiel n° L201, 31 juillet 2002, p.0037-0047.

Directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009 modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des

réseaux et services de communications électroniques, la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques et le règlement (CE) nº 2006/2004 relatif à la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs, Journal Officiel n° L337 du 18 décembre 2009.

Décision d'exécution (UE) 2016/1250 de la Commission du 12 juillet 2016 conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à l'adéquation de la protection assurée par le bouclier de protection des données UE-États-Unis, 12 juillet 2016, Journal officiel n°L207/1 du 1er août 2016.

Règlement (UE) 2015/758 du Parlement européen et du Conseil du 29 avril 2015 concernant les exigences en matière de réception par type pour le déploiement du système eCall embarqué fondé sur le service 112 et modifiant la directive 2007/46/CE, Journal Officiel n° L123/77 du 19 mai 2015.

Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, 27 avril 2016, Journal Officiel n° L 119/1 du 4 mai 2016.

Traité sur l'Union européenne, version consolidée, C 326/13, 26 décembre 2012, Journal Officiel de l'Union européenne.

Table des jugements

Jurisprudences du Canada

Jurisprudence de la Colombie-Britannique

Jurisprudence de l'Ontario

Kranitz c. *Rogers Cable Inc.,* 2002 CanLII 49415 (ON SC).

Mountain Province Diamonds Inc. v. *De Beers Canada Inc.,* 2014 ONSC 2026 (CanLII).

Jurisprudences du Québec

Bolvin c. *Montréal (Ville de)*, 2015 QCCQ 1923 (CanLII).

Bellerose c. *Université de Montréal,* [1986] C.A.I. 109.

Firquet c. *Acti-com*, 2018 QCCAI 245 (CanLII).

Mofo Moko c. *eBay Canada Ltd.,* 2016 QCCS 4669 (CanLII).

Regroupement des comités logements et Association des locataires du Québec c. *Corporation des propriétaires immobiliers du Québec*, Rapport d'enquête [1995] C.A.I. 370 (C.A.I.).

Serres floraplus inc. c. *Norséco in.,* 2008 QCCS 1455 (CanLII).

Société de transport de la Ville de Laval c. *X et al.*, 2003 CanLII 44085 (QC C.Q.).

Ste-Marie c. *Placements J.P.M. Marquis Inc.*, 2005 QCCA 312 (CanLII).

Strivastava c. *Hindu Mission of Canada (Québec) Inc.*, 2001 CanLII 27966 (QC CA).

Syndicat des employées et employés professionnels et de bureau, section locale 57 et Caisse populaire St-Stanislas de Montréal, 1998 CanLII 27651 (QC SAT).

The gazette c. *Valiquette*, 1996 CanLII 6064 (QC CA).

Jurisprudence de la Cour européenne des droits de l'Homme

Pretty c/ Royaume-Uni, n°2346/03, §61, 29 avril 2002, CEDH.

Jurisprudence de la Cour de justice de l'Union européenne

Maximilian Schrems c/ Data Protection Commissioner, C-362/14 du 6 octobre 2015.

Data protection commissionner c/ Facebook Ireland Ltd., et *Maximilian Schrems*, C-311/18 du 16 juillet 2020.

Jurisprudences du Conseil constitutionnel

Cons. const. n°71-44 DC du 16 juillet 1971, *Liberté d'association.*

Cons. const. n°99-416 DC du 23 juillet 1999, *Loi portant création d'une couverture maladie universelle*.

Références bibliographiques

Monographies et ouvrages collectifs

BAUDOUIN, J.-L., DESLAURIERS, P., et MOORE, B., *La responsabilité civile*, vol.1 : Principes généraux, 8e éd., Montréal, Éditions Yvon Blais, 2014.

BAUDOUIN, J.-L., DESLAURIERS, P., et MOORE, B., *La responsabilité civile*, vol.2 : Responsabilité professionnelle*,* 8e éd., Montréal, Éditions Yvon Blais, 2014.

BAUDOUIN, J-L., JOBIN, P-G., et al., *Les obligations,* 7e édition, Éditions Yvon Blais, 2013.

BENSOUSSAN, A., (dir), *Règlement européen sur la protection des données, textes, commentaires et orientations pratiques,* Bruylant, lexing technologies avancées & droit, 2e édition, 2018, 760 p.

BENYEKHLEF, K., *La protection de la vie privée dans les échanges internationaux d'informations,* Montréal, Thémis, 1993.

BOITE, R., et al, *Traitement de la parole,* Presses Polytechniques et universitaires romande, 2000, 488 p.

BOURCIER, D. et DE FILIPPI, P. (dir), *Open Data & Big Data: nouveaux défis pour la vie privée*, Paris, Mare & Martin, 2016, 269 p.

BROCHU, C., *Charte canadienne des droits et libertés,* LexisNexis, 2003.

CALÉ, S., et TOUITOU, P., *La sécurité informatique : réponses techniques, organisationnelles et juridiques,* Hermès Sciences publications, Paris, 2007, 282 p.

DE TERWANGNE, C., et ROSIER, K., (dir), *Le Règlement Général sur la Protection des Données (RGPD/GDPR) : Analyse approfondie,* coll. CRIDS, Larcier, 2018, 928 p.

GRATTON, E., *Understanding Personal Information : managing Privacy Risk*, LexisNexis, 2013, 515 p.

HUBIN, J., POULLET, Y. et al, *La sécurité informatique, entre technique et droit,* Cahier du C.R.I.D., 14, 1998, Facultés Universitaires Notre-Dame de la Paix de Namur, 260 p.

MINSKY, M., L., *Semantic information processing,* Cambridge, Mass., MIT Press, 1968, 440 p.

REY, B., *La vie privée à l'ère du numérique,* Lavoisier, coll. « Traitement de l'information », 2012, 297 p.

SANTOLARIA, N., *« Dis Siri » Enquête sur le génie à l'intérieur du smartphone,* Anamosa, 2016, 312 p.

VERMEYS, N., W., *Responsabilité civile et sécurité informationnelle,* Cowansville, Yvon Blais, 2010.

VERONICA PEREZ ASINARI, M., et PALAZZI, P., *Défis du droit à la protection de la vie privée – Perspectives du droit européen et nord-américain,* Bruxelles, Brulyant, Cahiers du Centre de Recherches Informatiques et Droit, 2008, 656 p.

Articles de doctrines

AILINCAI, M., A., *Le règlement général sur la protection des données. Aspects institutionnels et matériels,* colloque de Rennes 1, *Différents standards européen de protection des données ? A propos du droit de l'Union européen et du droit du Conseil de l'Europe,* 16 novembre 2018

AMESTERDAM, A., G., *Perspectives on the Fourth Amendment*, (1974), 58 *Minn. L. Rev.* 848.

AYLWIN, A., « L'obligation de notification en cas de violation de la confidentialité pour une entreprise du secteur privé », (2015) 74 R. du B., pp. 465-502.

BEAUREGARD, S., et GRANOZIK, L., « Les renseignements personnels et la responsabilité civile : à quel prix ? », dans Barreau du Québec, service de la formation continue, *Développements récents en droit de l'accès à l'information et de la protection des renseignements personnels,* Les 30 ans de la Commission d'accès à l'information (2012), vol. 358, Cowansville, éd. Yvon Blais, 2012.

BELL, J., « Machine Learnings : Hands-On for Developers and Technical Professionals », onlinelibrary.wiley.com, 3 November 2014, en ligne : < https://onlinelibrary.wiley.com/doi/book/10.1002/9781119183464 >.

BELLEIL, A., « La régulation économique des données personnelles ? », dans Legicom 2009/1 (N°42), pp. 143-151, en ligne : < https://www.cairn.info/revue-legicom-2009-1-page-143.htm#s2n5 >.

BENYEKHLEF, K., « Les glissements du droit à la vie privée. De Feydeau à Facebook : de la comédie de mœurs à l'économie des données », dans V. GAUTRAIS, C. RÉGIS et L. LARGENTÉ (dir.), *Mélanges en l'honneur du professeur Patrick A. Molinari*, Montréal, Éditions Thémis, 2018, pp. 291-319.

CAMERON, A., « La portée globale de la législation canadienne en matière de protection de la vie privée : décision clé rendue par la Cour fédérale dans l'affaire Globe24h », dans *Bulletin de la protection de l'information et de la vie privée,* fasken.com, 28 février 2017, en ligne : <https://www.fasken.com/fr/knowledge/2017/02/privacyandinformationprotectionbulletin-20170228/#overview >.

CASTETS-RENARD, C., « L'adoption du Privacy Shield sur le transfert des données personnelles », 2016, Recueil Dalloz, p.1696.

CAVOUKIAN, A., « Privacy by design: The 7 foundational principles », ipc.on.ca, Information & Privacy Commissioner, Ontario, en ligne : < https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf >.

CHASSIGNEUX, C., « Consentement manifeste et éclairé : politique de confidentialité sur Internet », 26 avril 2012, actes du 20e congrès AAPI 2012, Commission d'accès à l'information du Québec.

COX, M., et ELLSWORTH, D., « Application-Controlled Demand Paging for Out-of-Core Visualization », Proceedings of the 8th IEEE Visualization Conference, Association for computing machinery, 1997.

DELWAIDE, K., et AYLWIN, A., « Leçons tirées de dix ans d'expérience : la loi sur la protection des renseignements personnels dans le secteur privé du Québec », dans *Développements récents en droit de l'accès à l'information (2005),* service de la formation permanente du Barreau du Québec, 2005.

DE RICO, J-F., et, JAAR, D., « Le cadre juridique des technologies de l'information », dans *Développements récents en droit criminel (2008)*, service de la formation continue du Barreau du Québec, 2008.

DEZIEL, P-L., « Est-ce bien nécessaire ? Le principe de limitation de la collecte face aux défis de l'intelligence artificielle et des données massives », dans *Développements récents en droit de la vie privée (2019),* service de la formation continue du Barreau du Québec, 2019.

DEZIEL, P-L., « Les limites du droit à la vie privée à l'ère de l'intelligence artificielle : groupes algorithmiques, contrôle individuel et cycle de traitement de l'information », Les cahiers de propriété intellectuelle, Yvon Blais, vol. 30, n° 3, octobre 2018, en ligne : < https://www.lescpi.ca/articles/v30/n3/les-limites-du-droit-a-la-vie-privee-a-lere-de-lintelligence-artificielle-groupes-algorithmiques-controle-individuel-et-cycle-de-traitement-de-linformation/ >, pp.827-847.

FABIEN, C., « La preuve par document technologique », 2004, vol. 38 R.J.T. 533.

GAUTRAIS, V., « Introduction générale : Le défi de la protection de la vie privée face aux besoins de circulation de l'information personnelle », Conférence organisée par le programme international de coopération scientifique, Ivry sur Seine, 5 juin 2003.

GAUTRAIS, V., et GINGRAS P., « La preuve des documents technologiques », mai 2010, 22-2, Les cahiers de propriété intellectuelle 267-315.

GRANOSIK, L., « Le critère de nécessité, dans Les 20 ans de la loi sur la protection des renseignements personnels », dans *Les 20 ans de la Loi sur la protection des renseignements*

personnels dans le secteur privé (2014), Vol. 392, service de la formation continue, Barreau du Québec, Cowansville, Yvon Blais, 2014.

GRATTON, E., « Chronique - Qu'est-ce qu'un renseignement personnel ? Le défi de qualifier les nouveaux types de renseignements » dans *Repères*, Janvier 2013, Éditions Yvon Blais, 2013.

GRATTON, E., « Dealing with Canadian and Quebec Legal Requirements in the Context of Trans-border Transfers of Personal Information and Cloud Computing Services », dans *Développements récents en droit de l'accès à l'information et de la protection des renseignements personnels — les 30 ans de la Commission d'accès à l'information (2012)*, vol. 358, service de la formation continue, Barreau du Québec, Cowansville, Éditions Yvon Blais, 2012.

GUILMAIN, A., AYLWIN, A., et DELWAIDE, K., « Intelligence artificielle : priorité à la protection des renseignements personnels », ledevoir.com, 9 janvier 2018, en ligne : < https://www.ledevoir.com/opinion/idees/517082/intelligence-artificielle-priorite-a-la-protection-des-renseignements-personnels >.

GUILMAIN, A. et DOUVILLE, D., « La Loi sur la protection des renseignements personnels dans le secteur privé: quand s'applique-t-elle aux entreprises situées à l'extérieur du Québec? », fasken.com, 16 mai 2019, en ligne : < https://www.fasken.com/fr/knowledge/2019/05/van-the-quebec-private-sector-privacy-act/ >.

GUILMAIN, A., et GRATTON, E. « La protection des renseignements personnels dans le secteur privé au Québec : rétrospectives et perspectives », dans *Développements récents en droit à la vie privée (2019)*, vol. 465, service de la formation continue, Barreau du Québec, Montréal, Edition Yvon Blais, 2019.

JAAR, D., LACOSTE, E., et SENECAL, F., « Investir dans les renseignements personnels et leur protection », dans *Développements récents en droit de l'accès à l'information et de la protection des renseignements personnels — les 30 ans de la Commission d'accès à l'information (2012)*, vol. 358, service de la formation continue, Barreau du Québec, Cowansville, Éditions Yvon Blais, 2012, pp.193 à 213.

LAZARO, C., et LE METAYER, D., « Le consentement au traitement des données personnelles : Perspective comparative sur l'autonomie du sujet », (2014) 48 RJTUM 765-815, 2014.

LE CUN, Y., « L'apprentissage profond : une révolution en intelligence artificielle », leçon inaugurale au Collège de France, février 2016, en ligne : < https://www.college-de-france.fr/media/yann-lecun/UPL4485925235409209505_Intelligence_Artificielle_____Y._LeCun.pdf >.

MAZEAUD, V., « La constitutionnalisation du droit au respect de la vie privée », dans *Nouveaux cahiers du Conseil constitutionnel n°48 (dossier : Vie privée)*, juin 2015, pp.7 à 20.

McCARTHY, J, et al., « A proposal for the Dartmouth summer research project on artificial intelligence », jmc.standford.edu, 31st august 1995, en ligne : < http://jmc.stanford.edu/articles/dartmouth/dartmouth.pdf>.

MCDONALD, A., M., et FAITH CRANOR, L., « The cost of reading privacy policies », 2008, ISJLP, Vol. 4:3, en ligne : < https://pdfs.semanticscholar.org/4b51/2e2f5ff42ef00ccceca200d888676e6c506f.pdf >.

MINKER, W., et NEEL, F., « Développement des technologies vocales », dans *Le travail humain*, vol. 65, 2002/3, en ligne : < https://www.cairn.info/revue-le-travail-humain-2002-3-page-261.htm#pa23 >, pp.261 à 287.

NADEAU, A-R., « La protection constitutionnelle de l'information : mythe ou réalité ? », dans *Développements récents en droit de l'accès à l'information (2002),* vol.173, service de la formation permanente du Barreau du Québec, 2002.

PELLETIER, B., « Droit constitutionnel : la protection de la vie privée au Canada », revue juridique Thémis, 2001 35 R.J.T., pp. 485-522.

PESTANES, P. et GAUTIER, B., « Essor des assistants vocaux : Nouveau gadget pour votre salon ou fenêtre d'opportunité pour rebattre les cartes de l'économie du web ? », wavestone.com, 2017, en ligne : < https://www.wavestone.com/app/uploads/2017/09/Assistants-vocaux-04.pdf >.

PLOURDE, A., « Retour vers le futur : l'Internet des objets et la protection de la vie privée », dans *Développements récents en droit à la vie privée (2019)*, vol. 465, service de la formation continue, Barreau du Québec, Montréal, Edition Yvon Blais, 2019.

POULLET, Y., et HENROTTE, J-F., « La protection des données (à caractère personnel) à l'heure de l'Internet », dans *Protection du consommateur*, pratiques commerciales et T.I.C., coll. Commission Université-Palais, volume 109, Liège, Anthémis 2009, pp. 197-245.

REITER, E. H., « Privacy and the Charter: Protection of people or places? », 2009, 88 R. du B. can., 119-146.

ROCHELANDET, F., « I. Définition : vie privée et données personnelles », dans *Économie des données personnelles et de la vie privée,* cairn.info, 2010, en ligne : < https://www.cairn.info/Economie-des-donnees-personnelles-et-de-la-vie-pri--9782707157652-page-6.htm >.

RICHARD, C., « Dans la boîte noire des algorithmes : Comment nous nous sommes rendus calculables », dans *Revue du crieur,* 2018/3, (n°11), en ligne : < https://www.cairn.info/revue-du-crieur-2018-3-page-68.htm#s1n7 >, pp.68-85.

TURING, A.M., « Computing machinery and intelligence », Mind, Volume LIX, Issue 236, October 1950, pp. 433-460.

VALIQUETTE, M-A., « Les différences entre intelligence artificielle, apprentissage machine et apprentissage profond », article de recherche, substance.etsmtl.ca, 23 octobre 2017, en ligne : < https://substance.etsmtl.ca/differences-intelligence-artificielle-apprentissage-machine-apprentissage-profond>.

VERMEYS, N., « La responsabilité civile du fait des agents autonomes », 2018, Vol. 30 n°3, *Les Cahiers de propriété intellectuelle*, 851-880.

WARREN, S., D., et BRANDEIS, L., D., « The right to privacy », 15 December 1890, Harvard Law Review, Vol. 4, No. 5, en ligne : < https://www.jstor.org/stable/1321160?seq=1#metadata_info_tab_contents >, pp.193-220.

Thèses et mémoires

BONNET, A., *La responsabilité du fait de l'intelligence artificielle,* Mémoire de Maîtrise, Banque des mémoires, Université Panthéon-Assas, Paris II, 2015, en ligne : <https://docassas.u-paris2.fr/nuxeo/site/esupversions/90fcfa29-62e4-4b79-b0b4-d1beacc35e86?inline >.

DUASO CALES, R., *Principe de finalité, protection des renseignements personnels et secteur public : étude sur la gouvernance des structures en réseau,* papyrus.bib.umontreal.ca, Thèse de doctorat, Faculté de Droit, Université de Montréal, Université Panthéon-Assas II, 2011, en ligne : < https://papyrus.bib.umontreal.ca/xmlui/bitstream/handle/1866/12714/Duaso_Cales_Rosario_2011_these.pdf?sequence=2&isAllowed=y >.

GAUTHIER, J.M., *Cadre juridique de l'utilisation de la biométrie au Québec : sécurité et vie privée,* papyrus.bib.umontreal.ca, Mémoire de maîtrise, Avril 2014, Centre de recherche en droit public, Faculté de Droit, Université de Montréal, en ligne : <https://papyrus.bib.umontreal.ca/xmlui/bitstream/handle/1866/11879/Gauthier_Julie_Mira_2014_memoire.pdf?sequence=2&isAllowed=y >.

GRATTON, E., *Redefining Personal Information in the Context of the Internet,* papyrus.bib.umontreal.ca, Thèse de doctorat, Faculté de droit, Université de Montréal, Université Panthéon-Assas Paris II, Octobre 2012, en ligne : < https://papyrus.bib.umontreal.ca/xmlui/bitstream/handle/1866/19676/Gratton_Eloise_2012_these.pdf?sequence=4&isAllowed=y >.

LACHANCE, F., *« O.K. Google, assiste-moi » Les parcours des utilisateurs et des familles qui domestiquent le Google Home,* papyrus.bib.umontreal.ca, Mémoire de maîtrise, Avril 2019, en ligne : < https://papyrus.bib.umontreal.ca/xmlui/bitstream/handle/1866/22464/Lachance_Francois_2019_memoire.pdf?sequence=2&isAllowed=y >.

LAFONT, I., *L'efficacité du régime de responsabilité civile comme mesure de contrainte au respect de l'obligation de sécurité des renseignements personnels,* papyrus.bib.umontreal.ca, Mémoire de maîtrise, Faculté de Droit, Université de Montréal, Novembre 2013, en ligne : <https://papyrus.bib.umontreal.ca/xmlui/bitstream/handle/1866/11222/Lafont_Isabelle_2013_memoire.pdf?sequence=2&isAllowed=y >.

OLIVEIRA, S., *La responsabilité civile dans les cas de dommage causés par les robots d'assistance au Québec,* papyrus.bib.umontreal.ca, Mémoire de maîtrise, Université de Montréal, Avril 2016, en ligne : < https://papyrus.bib.umontreal.ca/xmlui/bitstream/handle/1866/16239/Oliveira_Sandra_2016_memoire.pdf?sequence=2&isAllowed=y >.

THIBEAULT, A., *La surveillance électronique et métadonnées. Vers une nouvelle conception constitutionnelle du droit à la vie privée au Canada ?,* Mémoire de maîtrise, Université de Montréal, Mars 2015, en ligne : < https://papyrus.bib.umontreal.ca/xmlui/bitstream/handle/1866/12496/Thibeault_Alexandre_2015_memoire.pdf?sequence=2&isAllowed=y >.

VERMEYS, N. W., *Qualification et quantification de l'obligation de sécurité informationnelle dans la détermination de la faute civile*, papyrus.bib.umontreal.ca, Thèse de doctorat, Université de Montréal, Mars 2009, en ligne : < https://papyrus.bib.umontreal.ca/xmlui/bitstream/handle/1866/3663/12085490.PDF?sequence=2&isAllowed=y >.

Rapports et documents gouvernementaux

ASSEMBLEE NATIONALE DU QUEBEC, *Projet de loi n°64 : Loi modernisant des dispositions législatives en matière de protection des renseignements personnels,* présenté par Mme Sonia LeBel, Ministre responsable des Institutions démocratiques, de la Réforme électorale et de l'Accès à l'information, première session, 42e législature, 2020.

BENYEKHLEF, K., et TRUDEL, P., *Approches et stratégies pour améliorer la protection de la vie privée dans le contexte des inforoutes,* papyrus.bib.umontreal.ca, Mémoire présenté à la Commission de la culture de l'Assemblée nationale, Université de Montréal, Faculté de droit, Centre de recherche en droit public, 1997, en ligne : < https://papyrus.bib.umontreal.ca/xmlui/bitstream/handle/1866/71/0072.pdf?sequence=1&isAllowed=y >.

CENTRE DE RECHERCHE INFORMATIQUE DE MONTREAL, *Données massives et intelligence artificielle,* crim.ca, 11 juillet 2017, en ligne : < https://www.crim.ca/crim_uploads/documents/FICHE-BigData-IA-expertise-110717.pdf >.

CHASSE, M., *La biométrie au Québec : les enjeux,* cai.gouv.ca, document d'analyse, Commission d'accès à l'information, juillet 2002, en ligne : < https://www.cai.gouv.qc.ca/documents/CAI_DRA_biometrie_enjeux.pdf>.

COMMISSARIAT A LA PROTECTION DE LA VIE PRIVEE, *Annonce : Le Commissariat tire ses conclusions suite à la consultation sur les transferts aux fins de traitement,* priv.gc.ca, 23 septembre 2019, en ligne : < https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/aeroports-et-frontieres/gl_dab_090127/>.

COMMMISSARIAT A LA PROTECTION DE LA VIE PRIVEE, *Bulletin d'interprétation : Renseignement personnel*, priv.gc.ca, octobre 2013, en ligne : < https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/lois-sur-la-protection-des-renseignements-personnels-au-canada/la-loi-sur-la-protection-des-renseignements-personnels-et-les-documents-electroniques-lprpde/aide-sur-la-facon-de-se-conformer-a-la-lprpde/bulletins-sur-l-interpretation-de-la-lprpde/interpretations_02/ >.

COMMISSARIAT A LA PROTECTION DE LA VIE PRIVEE, *Bulletin d'interprétation : Responsabilité,* priv.gc.ca, avril 2012, en ligne : < https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/lois-sur-la-protection-des-renseignements-personnels-au-canada/la-loi-sur-la-protection-des-renseignements-personnels-et-les-documents-electroniques-lprpde/aide-sur-la-facon-de-se-conformer-a-la-lprpde/bulletins-sur-l-interpretation-de-la-lprpde/interpretations_02_acc/ >.

COMMISSARIAT A LA PROTECTION DE LA VIE PRIVEE, *Des données au bout des doigts,* priv.gc.ca, février 2011, en ligne : < https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/renseignements-sur-la-sante-renseignements-genetiques-et-autres-renseignements-sur-le-corps/gd_bio_201102/ >.

COMMISSARIAT A LA PROTECTION DE LA VIE PRIVEE, *Les accessoires intelligents - Défis et possibilités pour la protection de la vie privée*, priv.gc.ca, janvier 2014, en ligne : < https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/recherche/consulter-les-travaux-de-recherche-sur-la-protection-de-la-vie-privee/2014/wc_201401/#heading-004-3 >.

COMMISSARIAT A LA PROTECTION DE LA VIE PRIVEE, *Lignes directrices sur la protection de la vie privée et la publicité comportementale en ligne,* priv.gc.ca, décembre 2011, en ligne : < https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/technologie/protection-de-la-vie-privee-en-ligne-surveillance-et-temoins/pistage-et-publicite/gl_ba_1112/ >.

COMMISSARIAT A LA PROTECTION DE LA VIE PRIVEE, *Lignes directrices sur le transfert transfrontalier de renseignements personnels,* priv.gc.ca, janvier 2009, en ligne : < https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/aeroports-et-frontieres/gl_dab_090127/ >.

COMMISSARIAT A LA PROTECTION DE LA VIE PRIVEE, *Lois provinciales qui peuvent s'appliquer au lieu de la LPRPDE,* priv.gc.ca, mai 2020, en ligne : < https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/lois-sur-la-protection-des-renseignements-personnels-au-canada/la-loi-sur-la-protection-des-renseignements-personnels-et-les-documents-electroniques-lprpde/r_o_p/prov-lprpde/ >.

COMMISSARIAT A LA PROTECTION DE LA VIE PRIVEE, *Position de principe sur la publicité comportementale en ligne,* priv.gc.ca, décembre 2015, en ligne : < https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/technologie/protection-de-la-vie-privee-en-ligne-surveillance-et-temoins/pistage-et-publicite/bg_ba_1206/ >.

COMMISSARIAT A LA PROTECTION DE LA VIE PRIVEE, *Principes relatifs à l'équité dans le traitement de l'information de la LPRPDE,* priv.gc.ca, mai 2019, en ligne : < https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/lois-sur-la-protection-des-renseignements-personnels-au-canada/la-loi-sur-la-protection-des-renseignements-personnels-et-les-documents-electroniques-lprpde/p_principle/ >.

COMMISSARIAT A LA PROTECTION DE LA VIE PRIVEE, *Rapport de conclusions d'enquête en vertu de la LPRPDE n°2007-389 : TJX Companies Inc./ Winners Merchant International L.P.,* priv.gc.ca, 25 septembre 2007, en ligne : < https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2007/tjx_rep_070925/ >.

COMMISSARIAT A LA PROTECTION DE LA VIE PRIVEE, *Rapport de conclusions en vertu de la LPRPDE n°2009-022 : Un détaillant accepte d'améliorer ses mesures de protection à l'égard de ses enregistrements de vidéosurveillance,* priv.gc.ca, 9 juin 2009, en ligne : < https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2009/lprpde-2009-022/ >.

COMMISSARIAT A LA PROTECTION DE LA VIE PRIVEE, *Rapport de conclusions d'enquêtes en vertu de la LPRPDE n°2011-001 : La collecte de données Wi-Fi par Google Inc.,* priv.gc.ca, 20 mai 2011, en ligne : < https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2011/lprpde-2011-001/ >.

COMMISSARIAT A LA PROTECTION DE LA VIE PRIVEE, *Rapport de conclusions d'enquêtes en vertu de la LPRPDE n°2012-009 : Des renseignements personnels sont communiqués sans consentement dans un message téléphonique laissé sur le lieu de travail d'une cliente,* priv.gc.ca, 8 août 2012, en ligne : < https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2012/lprpde-2012-009/ >.

COMMISSARIAT A LA PROTECTION DE LA VIE PRIVEE, *Rapport des conclusions d'enquête en vertu de la LPRPDE n°2013-001 : Enquête sur les pratiques de traitement des renseignements personnels de WhatsApp inc.,* priv.gc.ca, 15 janvier 2013, en ligne : < https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2013/lprpde-2013-001/ >.

COMMISSARIAT A LA PROTECTION DE LA VIE PRIVEE, *Rapport des conclusions d'enquête en vertu de la LPRPDE n°2013-003 : Des profils affichés sur le site de rencontre PositiveSingles.com se retrouvent sur d'autres sites Web de rencontres affiliés,* priv.gc.ca, 11 juillet 2013, en ligne : < https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2013/lprpde-2013-003/ >.

COMMISSARIAT A LA PROTECTION DE LA VIE PRIVEE, *Rapport des conclusions en vertu de la LPRPDE n°2014-001 : L'utilisation par Google de renseignements sensibles sur l'état de santé aux fins de l'affichage de publicités ciblées soulève des préoccupations en matière de vie privée,* priv.gc.ca, 14 janvier 2014, en ligne : < https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2014/lprpde-2014-001/ >.

COMMISSARIAT A LA PROTECTION DE LA VIE PRIVEE, *Rapport de conclusions d'enquêtes en vertu de la LPRPDE n°2014-003 : Une compagnie d'assurance révise ses mesures de sécurité à la suite d'une atteinte à la vie privée*, priv.gc.ca, 3 mars 2014, en ligne : < https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2014/lprpde-2014-003/ >.

COMMISSARIAT A LA PROTECTION DE LA VIE PRIVEE, *Rapport de conclusions d'enquête en vertu de la LPRPDE n°2018-002 : La réutilisation de millions de profils d'utilisateurs Facebook canadiens effectuée par une entreprise contrevient à la loi en matière de protection de la vie privée*, priv.gc.ca, 12 juin 2018, en ligne : < https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2018/lprpde-2018-002/ >.

COMMISSARIAT A LA PROTECTION DE LA VIE PRIVEE, *Résumé de conclusions d'enquêtes en vertu de la LPRPDE n°2002-42 (mise à jour) : Air Canada permet à 1% des membres Aéroplan de se « désister » des pratiques de partage d'information,* priv.gc.ca, 11 mars 2002, en ligne : < https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2002/lprpde-2002-042/ >.

COMMISSARIAT A LA PROTECTION DE LA VIE PRIVEE*, Résumé de conclusions d'enquête en vertu de la LPRPDE n°2002-54 : Un couple prétend qu'il y a eu communication inappropriée de leur dossier téléphonique à un tiers,* priv.gc.ca, 28 juin 2002, en ligne : < https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2002/lprpde-2002-054/ >.

COMMISSARIAT A LA PROTECTION DE LA VIE PRIVEE, *Résumé de conclusions d'enquêtes en vertu de la LPRPDE n°2003-192 : Une banque n'obtient pas le consentement explicite de ses clients pour communiquer leurs renseignements personnels,* priv.gc.ca, 23 juillet 2003, en ligne : < https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2003/lprpde-2003-192/ >.

COMMISSARIAT A LA PROTECTION DE LA VIE PRIVEE, *Résumé de conclusions d'enquête en vertu de la LPRPDE n°2003-203 : Un particulier laisse percer ses inquiétudes quant aux clauses de consentement sur un formulaire de demande de carte de crédit,* priv.gc.ca, 5 août 2003, en ligne : < https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2003/lprpde-2003-203/ >.

COMMISSARAIT A LA PROTECTION DE LA VIE PRIVEE, *Résumé de conclusions d'enquête en vertu de la LPRPDE n°2004-281 : Une organisation utilise la biométrie à des fins d'authentification,* priv.gc.ca, 3 septembre 2004, en ligne : < https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2004/lprpde-2004-281/ >.

COMMISSARIAT A LA PROTECTION DE LA VIE PRIVEE, *Résumé de conclusions d'enquête en vertu de la LPRPDE n° 2005-313 : Un avis expédié aux clients d'une banque suscite des inquiétudes à propos de la USA PATRIOT Act,* priv.gc.ca, 19 octobre 2005, en ligne : < https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2005/lprpde-2005-313/ >.

COMMISSARIAT A LA PROTECTION DE LA VIE PRIVEE, *Résumé de conclusions d'enquête en vertu de la LPRPDE n° 2006-333 : Une entreprise canadienne communique les renseignements personnels de ses clients à la société mère située aux États-Unis*, priv.gc.ca, 19 juillet 2006, en ligne : < https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2006/lprpde-2006-333/ >.

COMMISSARIAT A LA PROTECTION DE LA VIE PRIVEE, *Résumé de conclusions d'enquête en vertu de la LPRPDE n°2006-334 : Une banque exige une pièce d'identité avant de répondre à une demande d'accès à des renseignements personnels,* priv.gc.ca, 21 février 2006, en ligne : <https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2006/lprpde-2006-334/ >.

COMMISSARIAT A LA PROTECTION DE LA VIE PRIVEE, *Résumé de conclusions d'enquête en vertu de la LPRPDE n°2006-348 : Communication inappropriée d'un diagnostic, mais la compagnie d'assurances maintient que ses politiques et ses pratiques concernant la protection des renseignements personnels sont transparentes,* priv.gc.ca, 14 août 2006, en ligne : <https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2006/lprpde-2006-348/ >.

COMMISSARIAT A LA PROTECTION DE LA VIE PRIVEE, *Résumé de conclusions d'enquête en vertu de la LPRPDE n° 2007-365 : Responsabilité d'institutions financières canadiennes dans la communication de renseignements personnels par SWIFT aux autorités des États-Unis,* priv.gc.ca, 2 avril 2007, en ligne : < https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2007/lprpde-2007-365/ >.

COMMISSARIAT A LA PROTECTION DE LA VIE PRIVEE, *Résumé de conclusions d'enquête en vertu de la LPRPDE n° 2008-394 : l'impartition des services de courriel de canada.com à une entreprise établie aux États-Unis suscite des questions parmi les abonnés*, priv.gc.ca, 19 septembre 2008, en ligne : < https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2008/lprpde-2008-394/ >.

COMMISSARIAT A LA PROTECTION DE LA VIE PRIVEE, *Survol de la LPRPDE,* priv.qc.ca, mai 2020, en ligne : < https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/lois-sur-la-protection-des-renseignements-personnels-au-canada/la-loi-sur-la-protection-des-renseignements-personnels-et-les-documents-electroniques-lprpde/r_o_p/prov-lprpde/ >.

COMMISSARIAT A LA PROTECTION DE LA VIE PRIVEE, *LPRPDE : Traitement transfrontalier des données personnelles, Lignes directrices,* priv.gc.ca, janvier 2009, en ligne : <https://www.priv.gc.ca/media/1994/gl_dab_090127_f.pdf >.

COMMISSION D'ACCES A L'INFORMATION, *L'invasion des objets connectés : quelles sont les conséquences sur vos renseignements personnels ?,* cai.gouv.qc.ca, 24 avril 2015, en ligne : <https://www.cai.gouv.qc.ca/linvasion-des-objets-connectes-quelles-sont-les-consequences-sur-vos-renseignements-personnels/ >.

COMMISSION D'ACCES A L'INFORMATION, *La collecte de renseignements personnels,* cai.gouv.qc.ca, en ligne : < https://www.cai.gouv.qc.ca/la-collecte-de-renseignements-personnels/>.

COMMISSION D'ACCES A L'INFORMATION, *Protection des renseignements personnels*, cai.gouv.qc.ca, en ligne : < http://www.cai.gouv.qc.ca/entreprises/protection-des-renseignements-personnels-1/ >.

COMMISSION D'ACCES A L'INFORMATION, *Rétablir l'équilibre,* Rapport quinquennal, cai.gouv.qc.ca, 2016, en ligne : < http://www.cai.gouv.qc.ca/documents/CAI_RQ_2016.pdf >.

COMMISSION D'ACCES A L'INFORMATION, *Technologies et vie privée à l'heure des choix de société,* Rapport quinquennal, cai.gouv.qc.ca, juin 2011, en ligne : <https://www.cai.gouv.qc.ca/documents/CAI_RQ_2011.pdf >.

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES, *Comment permettre à l'homme de garder la main ? Rapport sur les enjeux éthiques des algorithmes et de l'intelligence artificielle,* cnil.fr, décembre 2017, en ligne : <https://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_garder_la_main_web.pdf >.

COMMISSION NATIONALE DE L'INFORMATION ET DES LIBERTES, *Définition : Algorithme*, cnil.fr, en ligne : < https://www.cnil.fr/fr/definition/algorithme >.

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES, *Notifier une violation de données personnelles,* cnil.fr, 24 mai 2018, en ligne : < https://www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles >.

DETRAIGNE, Y., et ESCOFFIER, A.-M., *La vie privée à l'heure des mémoires numériques. Pour une confiance renforcée entre citoyens et société de l'information*, Rapport d'information n°441, senat.fr, 27 mai 2009, en ligne : < http://www.senat.fr/rap/r08-441/r08-441_mono.html#toc328 >.

GAUTRAIS, V., et al., *Rapport auprès de la Commission d'accès à l'information (CAI),* 4 décembre 2015, Centre de recherche en droit public, en ligne : <https://www.gautrais.com/blogue/2015/12/04/rapport-aupres-de-la-commission-dacces-a-linformation/#_ftnref14 >.

HADOPI et CSA, *Assistants vocaux et enceintes connectées : l'impact de la voix sur l'offre et les usages culturels et médias*, Rapport, mai 2019.

INSTITUT MONTAIGNE, *Big data et objets connectés : Faire de la France un champion de la révolution numérique,* Rapport, institutmontaigne.org, avril 2015, en ligne : <https://www.institutmontaigne.org/ressources/pdfs/publications/rapport%20objets%20connecte%CC%81s(2).pdf >.

SECRETARIAT A L'ACCES ET A LA REFORME DES INSTITUTIONS DEMOCRATIQUES, *Orientations gouvernementales pour un gouvernement plus transparent, dans le respect du droit à la vie privée et la protection des renseignements personnels*, institutions-

democratiques.gouv.qc.ca, 2015, en ligne : < https://www.institutions-democratiques.gouv.qc.ca/transparence/documents/doc-orientations-gouv.pdf >.

Documents internationaux

36TH INTERNATIONAL CONFERENCE OF DATA PROTECTION AND PRIVACY COMMISSIONERS, *Mauritius Declaration on the Internet of Things,* Balaclava, 14 October 2014, en ligne : < https://www.cai.gouv.qc.ca/documents/Mauritius-Declaration.pdf >.

38TH INTERNATIONAL CONFERENCE OF DATA PROTECTION AND PRIVACY COMMISSIONERS*, Artificial Intelligence, Robotics, Privacy and Data Protection,* Room Document, October 2016, en ligne : < https://edps.europa.eu/sites/edp/files/publication/16-10-19_marrakesh_ai_paper_en.pdf >.

COMMISSION EUROPEENNE*, Pratique anticoncurrentielle : La Commission ouvre une enquête sectorielle sur l'internet des objets pour les consommateurs,* communiqué de presse, 16 juillet 2020, Bruxelles, en ligne : <https://ec.europa.eu/commission/presscorner/detail/fr/ip_20_1326 >.

COMMISSION EUROPEENNE POUR L'EFFICACITE DE LA JUSTICE, *Charte éthique européenne d'utilisation de l'intelligence artificielle dans les systèmes judiciaires et leur environnement,* adoptée lors de la 31e réunion plénière de la CEPEJ, Strasbourg, 3 et 4 décembre 2018.

GROUPE DE TRAVAIL ARTICLE 29, *Document de travail sur la biométrie,* 12168/02/EN, WP80, adopté le 1 août 2003, en ligne : < https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp80_en.pdf >.

GROUPE DE TRAVAIL ARTICLE 29, *Lignes directrices sur la notification de violations de données à caractère personnel en vertu du Règlement (UE) 2016/679,* adoptée le 3 octobre 2017, version révisée et adoptée le 6 février 2018, en ligne : <https://www.cnil.fr/sites/default/files/atoms/files/wp250rev01_fr.pdf >.

ORGANISATION DE COOPERATION ET DE DEVELOPPEMENT ECONOMIQUES, *Gestion du risque de sécurité numérique pour la prospérité économique et sociale : Recommandation de l'OCDE et document d'accompagnement,* oecd.org, Paris, 1er octobre 2015, en ligne : <https://www.oecd.org/fr/internet/ieconomie/DSRM_French_final_Web.pdf>.

ORGANISATION DE COOPERATION ET DE DEVELOPPEMENT ECONOMIQUES, *Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'informations : vers une culture de la sécurité*, 1037e session, Conseil de l'OCDE, 25 juillet 2002, en ligne : <https://www.oecd.org/sti/ieconomy/15582260.pdf >.

ORGANISATION DE COOPERATION ET DE DEVELOPPEMENT ECONOMIQUES, *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de*

caractère personnels, Paris, 23 septembre 1980, en ligne : < https://www.oecd.org/fr/internet/ieconomie/lignesdirectricesregissantlaprotectiondelaviepriveeetlesfluxtransfrontieresdedonneesdecaracterepersonnel.htm >.

ORGANISATION DE COOPERATION ET DE DEVELOPPEMENT ECONOMIQUES, *Lignes directrices régissant la sécurité des systèmes d'information*, OCD/GD (92) 190, Paris, 1992, en ligne : <http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=OCDE/GD(92)190&docLanguage=Fr >.

ORGANISATION DE COOPERATION ET DE DEVELOPPEMENT ECONOMIQUES, *Recommendation of the Council concerning guidelines governing the protection of privacy and transborder flows of personal data (2013)*, C(80 58/FINAL, amendé le 11 juillet 2013, C (2013) 79, en ligne : < http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf >.

ORGANISATION FOR ECONOMIC COOPERATION AND DEVELOPMENT, *Chapter 2: Supplementary explanatory memorandum to the revised recommendation of the council concerning guidelines governing the protection of privacy and transborder flows of personal data (2013),* en ligne : < http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf>.

ORGANISATION FOR ECONOMIC COOPERATION AND DEVELOPMENT, *Guidelines governing the protection of privacy and transborder flows of personal data (2013)*, chapitre 1, C(80)58/Final, amendé le 11 juillet 2013 par C(2013) 79, en ligne : <http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf >.

ORGANISATION DES NATIONS UNIES, *Déclaration Universelle des Droits de l'Homme,* Rés. AG 217 (III), Doc. Off. AG NU, 3e sess., supp. n°13, Doc. NU A/810 (1948).

ORGANISATION DES NATIONS UNIES, *Principes directeurs pour la réglementation des fichiers informatisés contenant des données à caractère personnel*, Assemblée générale des Nations Unies, New York, 14 décembre 1990, résolution 45/95.

UNION EUROPEENE, *Décision d'exécution (UE) 2016/1250 de la Commission du 12 juillet 2016 conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à l'adéquation de la protection assurée par le bouclier de protection des données UE-États-Unis*, 12 juillet 2016, Journal officiel n°L207/1 du 1er août 2016, en ligne : < https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32016D1250&from=EN#d1e3041-1-1 >.

UNION EUROPEENNE, *Glossaire des synthèses : critères d'adhésion*, eur-lex.europa.eu, en ligne : < https://eur-lex.europa.eu/summary/glossary/accession_criteria_copenhague.html?locale=fr >.

U.S DEPARTMENT OF COMMERCE, *EU-U.S. Privacy Shield framework principles issued by the U.S department of commerce*¸ 23 février 2016, en ligne : < https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004qAg >.

Articles de presse

ALIMI, J., « L'assistant vocal, l'interface homme-machine du futur », suricats-consulting.com, en ligne : < https://www.suricats-consulting.com/expertise-commerce-assistant-vocal/ >.

ANNONYME, « Le edge computing va rendre l'IA plus écologique, rapide et éthique », helloopenworld.com, 18 mai 2018, en ligne : < https://www.helloopenworld.com/objets-connectes-et-si-on-arretait-de-partager-la-data-6119 >.

ANNONYME, « Qu'est-ce que le privacy by design ? », donnees-rgpd.fr, 7 mai 2019, en ligne : < https://donnees-rgpd.fr/definitions/privacy-by-design/ >.

AUCLERT, F., « Alexa et Google Home : de nouvelles failles exploitées par des pirates pour vous écouter », futura-science.com, 22 octobre 2019, en ligne : < https://www.futura-sciences.com/tech/actualites/objets-connectes-alexa-google-home-nouvelles-failles-exploitees-pirates-vous-ecouter-68518/ >.

AUDOUIN, C., « Arnaque au faux Le Drian » : l'avocate du ministre détaille le fonctionnement d'une escroquerie hors pair », franceinter.fr, 4 février 2020, en ligne : < https://www.franceinter.fr/arnaque-au-faux-le-drian-l-avocate-du-ministre-detaille-le-fonctionnement-d-une-escroquerie-hors-pair >.

BOLUS, D., « Les principales briques technologiques d'un bot », bot-trends.fr, 11 septembre 2018, en ligne : < https://www.bot-trends.fr/intelligence-artificielle-bot/ >.

CAREY, B., « The first Alexa toy is a $300 kitchen for kids, packed with dad jokes », cnet.com, 22 février 2020, en ligne : < https://www.cnet.com/news/first-amazon-alexa-toy-is-300-kidkraft-kitchen-for-kids/ >.

CASILLI A., « Derrière les assistants vocaux, des humains vous entendent », laquadratur.net, 18 mai 2018, en ligne : < https://www.laquadrature.net/2018/05/18/temoin_cortana/ >.

CHATELLIER, R., « L'espion qui me logeait : assistants vocaux et objets connectés dans la maison », linc.cnil.fr, 10 avril 2018, en ligne : < https://linc.cnil.fr/fr/lespion-qui-me-logeait-assistants-vocaux-et-objets-connectes-dans-la-maison >.

CHATELLIER, R., « Troqueriez-vous votre assistant domestique intelligent pour un être humain ? », linc.cnil.fr, 18 septembre 2017, en ligne : < https://linc.cnil.fr/fr/troqueriez-vous-votre-assistant-domestique-intelligent-pour-un-etre-humain >.

CNEWS, « Ils utilisent l'assistant vocal Alexa pour commander pour 700 dollars de jouets », cnews.fr, 19 décembre 2019, en ligne : < https://www.cnews.fr/monde/2019-12-19/ils-utilisent-lassistant-vocal-alexa-pour-commander-pour-700-dollars-de-jouets >.

COSEGLIA, J., « Coffee with privacy pros : DPO vs CPO. Lawyer vs Technician. The dualities of privacy », cpomagazine.com, 3 janvier 2019, en ligne : < https://www.cpomagazine.com/data-privacy/coffee-with-privacy-pros-dpo-vs-cpo-lawyer-vs-technician-the-dualities-of-privacy/ >.

DAY, M., G. TURNER et N. DROZDIAK, « Amazon Workers Are Listening to What You Tell Alexa », bloomberg.com, 10 avril 2019, en ligne : <https://www.bloomberg.com/news/articles/2019-04-10/is-anyone-listening-to-you-on-alexa-a-global-team-reviews-audio >.

DOCTOROW, C., « WiFi isn't short for 'Wireless Fidelity' », boingboing.net, en ligne : <https://boingboing.net/2005/11/08/wifi-isnt-short-for.html >.

FONTAINE, P., et LEPESQUEUR, B., « Découvrez l'iPhone 4S et son étonnant assistant vocal Siri », 01net.com, 12 décembre 2011, en ligne : < https://www.01net.com/actualites/decouvrez-l-and-039-iphone-4s-et-son-etonnant-assistant-vocal-siri-video-543854.html >.

FORTIN, S., « Alexa veut séduire le Québec », lesoleil.com, 15 avril 2019, en ligne : <https://www.lesoleil.com/les-choix-de-la-redaction/alexa-veut-seduire-le-quebec-video-33011252346709f1a01053c9bee98c3c >.

FUTURA TECH, « Code binaire », futura-sciences.com, en ligne : < https://www.futura-sciences.com/tech/definitions/informatique-code-binaire-11934/ >.

GEOFFRAY, « [Infographie] Histoire de l'Internet des objets au fil du temps », meilleure-innovation.com, 11 août 2014, en ligne : < https://www.meilleure-innovation.com/infographie-internet-objets/ >.

GRUMIAUX, M., « Amazon sommé de transmettre des enregistrements d'un Echo suite à un double meurtre », clubic.com, 13 novembre 2018, en ligne : <https://www.clubic.com/alexa/actualite-847285-amazon-somme-transmettre-justice-enregistrement-echo-double-meurtre.html >.

IONOS, « Le code binaire : pourquoi a-t-on besoin du système binaire ? », ionos.fr, 3 septembre 2019, en ligne : < https://www.ionos.fr/digitalguide/sites-internet/developpement-web/code-binaire/ >.

JOURNAL DU NET, « Code source : définition, traduction », journaldunet.fr, 28 janvier 2020, en ligne : < https://www.journaldunet.fr/web-tech/dictionnaire-du-webmastering/1203623-code-source-definition-traduction/ >.

JOURNAL DU NET, « Ethernet : définition et fonctionnement », journaldunet.fr, 10 janvier 2019, en ligne : < https://www.journaldunet.fr/web-tech/dictionnaire-du-webmastering/1203383-ethernet-definition/ >.

KINSELLA, B., « New Alexa skill data shows new U.S skills launched in 2019 fall to lowest level since 2016 », voicebot.ai, 17 January 2020, en ligne : < https://voicebot.ai/2020/01/17/new-alexa-skill-data-show-new-u-s-skills-launched-in-2019-fall-to-lowest-level-since-2016/ >.

KUMPARAK, G., « The original Siri app gets pulled from the App store, servers to be killed », techcrunch.com, 4 October 2011, en ligne : < https://techcrunch.com/2011/10/04/the-original-siri-app-gets-pulled-from-the-app-store-servers-killed/ >.

LIBERATION, « Microsoft muselle son robot « Tay » devenu nazi en 24 heures », liberation.fr, 25 mars 2016, en ligne : < https://www.liberation.fr/futurs/2016/03/25/microsoft-muselle-son-robot-tay-devenu-nazi-en-24-heures_1441963 >.

LIPTAK, A., « Amazon's Alexa started ordering people dollhouses after hearing its name on TV », theverge.com, 7 January 2017, en ligne : <https://www.theverge.com/2017/1/7/14200210/amazon-alexa-tech-news-anchor-order-dollhouse>.

LOYER, C., « Juniper Research prédit 8 milliards d'appareils équipés d'un assistant vocal en 2023 », vokode.com, 14 février 2019, en ligne : < https://www.vokode.com/juniper-research-predit-8-milliards-dappareils-equipes-dun-assistant-vocal-en-2023/ >.

MUTCHLER, A., « Voice assistant timeline: A short history of the voice revolution », voicebot.ai, 14th July 2017, en ligne : < https://voicebot.ai/2017/07/14/timeline-voice-assistants-short-history-voice-revolution/ >.

OPAM, K., « Google's Super Bowl ad accidentally set off a lot of Google Homes », theverge.com, 5th February 2017, < https://www.theverge.com/2017/2/5/14517314/google-home-super-bowl-ad-2017 >.

ORACLE, « Qu'est-ce que l'apprentissage automatique ? », oracle.com, en ligne : <https://www.oracle.com/ca-fr/artificial-intelligence/what-is-machine-learning.html >.

PAUS, L., « WiFi ou Ethernet : Lequel est le plus rapide ? Le plus sûr ? », welivesecurity.com, 4 mai 2018, en ligne : < https://www.welivesecurity.com/fr/2018/05/04/wifi-ethernet-rapide/ >.

PINOLA, M., « Speech Recognition Through the Decades: How we Ended Up With Siri », pcworld.com, 2nd November 2011, en ligne : <https://www.pcworld.com/article/243060/speech_recognition_through_the_decades_how_we_ended_up_with_siri.html >.

PRESS, G., « A very short history of Big data », forbes.com, 9th may 2013, en ligne : <https://www.forbes.com/sites/gilpress/2013/05/09/a-very-short-history-of-big-data/#6bcfa3fe65a1 >.

RONAN, « Les cookies informatiques : amis ou ennemis ? », caragraph.fr, 2 février 2017, en ligne : < https://www.caragraph.fr/ficheArticle-Les-cookies-informatiques--amis-ou-ennemis--9.html >.

RTBF, « Alexa, l'assistant vocal d'Amazon, envoie par erreur la conversation privée d'un couple à un collègue du mari », rtbf.be, 25 mai 2018, en ligne : <https://www.rtbf.be/info/insolites/detail_une-conversation-privee-envoyee-par-erreur-par-l-enceinte-connectee-d-amazon?id=9927755 >.

S., P., « Un assistant domestique appel la police par erreur et vient au secours d'une victime de violences conjugales », jounaldugeek.com, 10 juillet 2017, en ligne : <https://www.journaldugeek.com/2017/07/10/google-home-appelle-la-police-par-erreur-et-vient-au-secours-dune-victime-de-violences-conjugales/ >.

TRAX MAGASINE, « Derrière les enceintes intelligentes, les oreilles des géants du web ? », citant Guillaume Champeau, traxmag.com, 7 janvier 2019, en ligne : <https://www.traxmag.com/derriere-les-enceintes-intelligentes-les-oreilles-des-geants-du-web/ >.

TOWNSEND, T., « Burger King's new ad deliberately gets your Google Home to talk about burgers », vox.com, 22 april 2017, en ligne : < https://www.vox.com/2017/4/12/15274312/burger-king-ad-triggers-google-home >.

VERSET, J-C., « Les enceintes intelligentes seront-elles nos futurs majordomes numériques ? », rtbf.be, 26 juillet 2018, en ligne : < https://www.rtbf.be/info/medias/detail_les-enceintes-intelligentes-seront-elles-nos-futurs-majordomes-numeriques?id=9981502 >.

VITRÉ, P., « L'assistant vocal, nouvel ami des voitures ? », androidpit.fr, 4 octobre 2018, en ligne : < https://www.androidpit.fr/bmw-series-3-assistant-vocal >.

WHITE, T., « Hadoop : The definitive Guide, 2012 », cité par CENTRE DE RECHERCHE INFORMATIQUE DE MONTREAL, *Données massives et intelligence artificielle,* crim.ca, 11 juillet 2017, en ligne : < https://www.crim.ca/crim_uploads/documents/FICHE-BigData-IA-expertise-110717.pdf >.

Sites internet

AMAZON, « Alexa Privacy and data handling overview », white paper, en ligne : <https://d1.awsstatic.com/productmarketing/A4B/White%20Paper%20%20Alexa%20Privacy%20and%20Data%20Handling%20Overview.pdf >.

ANNONYME, « Définition : Équivalence fonctionnelle », lccjti.ca, en ligne : <https://www.lccjti.ca/definitions/equivalence-fonctionnelle/#ancre1 >.

ANNONYME, « What is a transducer ? », americanpiezo.com, en ligne : <https://www.americanpiezo.com/piezo-theory/whats-a-transducer.html >.

APPLE, « Apple Launches iPhone 4S, iOS 5 & iCloud », apple.com, Apple Newsroom, 4 October 2011, en ligne : <https://www.apple.com/newsroom/2011/10/04Apple-Launches-iPhone-4S-iOS-5-iCloud/ >.

APPLE, « Contrôler votre domicile avec Siri », support.apple.com, en ligne : <https://support.apple.com/fr-ca/HT208280 >.

CAIJ, « JurisBistro eDictionnaire : Dictionnaire de droit québécois et canadien, Consentement », dictionnaire.caij.qc.ca, édition révisée 2016, en ligne : <https://dictionnairereid.caij.qc.ca/recherche#q=consentement&t=edictionnaire&sort=relevancy&m=search >.

CENTRE CANADIEN POUR LA CYBERSECURITE, « Cyberjournal numéro 11 », cyber.gc.ca, 11 juin 2017, en ligne : < https://cyber.gc.ca/fr/orientation/cyberjournal-numero-11-juin-2017 >.

CENTRE CANADIEN POUR LA CYBERSECURITE, « L'Internet des objets à la maison », pensezcybersecurite.gc.ca, 21 décembre 2018, en ligne : <https://www.pensezcybersecurite.gc.ca/cnt/rsks/ntrnt-thngs/hm-fr.aspx >.

DEFENSE ADVANCED RESEARCH PROJECTS AGENCY, < www.darpa.mil >.

ENCYCLOPEDIA BRITANNICA, < www.britannica.com >.

GOOGLE,< www.support.google.com >.

GOTOS3, « Les briques technologiques deviennent des produits « tout-en-un » », gotos3.eu, 1 mars 2018, en ligne : < http://www.gotos3.eu/fr/nieuws/workshop-all-one-materialen >.

GOUVERNEMENT, < www.gouvernement.fr >.

HAUTES ETUDES COMMERCIALES, < www.libguide.hec.ca >.

HUSEMAN, B., « Amazon Senator Coons Response Letter », scribd.com, 29 June 2019, en ligne : < https://fr.scribd.com/document/415372739/Amazon-Senator-Coons-Response-Letter#from_embed >.

IBM, < www.ibm.com >.

IEEE, < www.ieee.org >.

LAROUSSE, < www.larousse.fr >.

LE PETIT ROBERT, < www.dictionnaire.lerobert.com >.

OFFICE QUEBECOIS DE LA LANGUE FRANCAISE, < www.gdt.oqlf.gouv.qc.ca >.

WI-FI ALLIANCE, < www.wi-fi.org >.

WIKIPEDIA, < www.wikipedia.org >.