# TABLE DE MATIERES

**LEXIQUE** ..... **1**

**POINTS-CLÉS** ..... **3**

**1.2.2. ENJEUX SUR L'ENVIRONNEMENT LÉGAL ET LÉGISLATIF LORS DE L'ADOPTION DE LA CHAÎNE DE BLOCS PAR UN ORGANISME PUBLIC** ..... **4**

1.2.2.1. LA CHAINE DE BLOCS ET LA GOUVERNANCE ..... 6
1.2.2.2. LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ..... 9
*1.2.2.2.1. Le projet de loi 64* ..... *9*
*1.2.2.2.2. Nature des renseignements personnels* ..... *11*
1.2.2.2.2.1. Renseignement personnel ..... 11
1.2.2.2.2.2. Renseignement personnel sensible ..... 12
1.2.2.2.2.3. Renseignement personnel dépersonnalisé ..... 15
1.2.2.2.2.4. Renseignement personnel anonymisé ..... 15
*1.2.2.2.3. Partage et communication de renseignements personnels* ..... *19*
1.2.2.2.3.1. Généralités relatives à la communication de renseignements par les organismes publics ..... 19
1.2.2.2.3.2. Communication de renseignements à l'extérieur du Québec ..... 20
*1.2.2.2.4. Droit à l'oubli et politiques de confidentialité* ..... *22*
1.2.2.2.4.1. Le droit à l'oubli et le droit à la rectification ..... 22
1.2.2.2.4.2. La situation canadienne ..... 24
1.2.2.2.4.3. La situation québécoise ..... 25
1.2.2.2.4.4. La compatibilité de ces droits à l'usage de la chaine de blocs ..... 27
1.2.2.2.4.5. Les politiques de confidentialité ..... 30
1.2.2.2.4.6. La nécessité potentielle d'une évaluation des facteurs relatifs à la vie privée ..... 31
*1.2.2.2.5. Le droit à la portabilité* ..... *33*
1.2.2.3. LA COMPATIBILITÉ DU DROIT DE LA PREUVE AVEC LA TECHNOLOGIE DE CHAÎNE DE BLOCS ..... 35

**BIBLIOGRAPHIE** ..... **37**

# LEXIQUE

**Bloc** : « Ensemble de données liées à des transactions, dont la validité doit être confirmée au moyen d'un mécanisme de validation pour qu'il puisse être intégré à une chaîne de blocs. »[1]

**Chaîne de blocs** : « Base de données distribuée et sécurisée, dans laquelle sont stockées chronologiquement, sous forme de blocs liés les uns aux autres, les transactions successives effectuées entre ses utilisateurs depuis sa création. »[2]

**Code de hachage** : « Code qui résulte de la transformation, au moyen d'une fonction de hachage cryptographique, d'un ensemble de données en une séquence alphanumérique de taille réduite, et qui permet d'identifier les données de départ sans y accéder. »[3]

**Empreinte numérique** : « Séquence de caractères alphanumériques de longueur fixe, qui représente le contenu d'un message sans le révéler, dont la valeur unique est produite par un algorithme de hachage. »[4]

**Hachage** : « Opération qui consiste à appliquer une fonction mathématique à un groupe de données de taille variable afin de générer un code unique de taille fixe, que l'on utilisera pour l'authentification et le stockage d'information. »[5]

**Mécanisme de validation** : « Mécanisme qui vise à assurer la validité des blocs ajoutés sur une chaîne de blocs ainsi que les transactions qu'ils contiennent. »[6]

**Noeud** : « Appareil informatique relié au réseau qui héberge une chaîne de blocs, destiné à relayer les transactions effectuées et à maintenir une copie complète ou partielle du registre distribué sur lequel ces transactions sont enregistrées. »[7]

---

[1] Office québécois de la langue française, « fiche terminologique : bloc », (2019), en ligne : *Office québécois de la langue française* < gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=26544746 >.

[2] Office québécois de la langue française, « fiche terminologique : chaîne de blocs », (2017), en ligne : *Office québécois de la langue française* < gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=26531717 >.

[3] Office québécois de la langue française, « fiche terminologique : code de hachage », (2019), en ligne : *Office québécois de la langue française* < gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=12399801 >.

[4] Office québécois de la langue française, « fiche terminologique : empreinte numérique », (2022), en ligne : *Office québécois de la langue française* < gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=8371028 >.

[5] Office québécois de la langue française, « fiche terminologique : hachage », (2021), en ligne : *Office québécois de la langue française* < gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=8367404 >.

[6] Office québécois de la langue française, « fiche terminologique : mécanisme de validation », (2019), en ligne : *Office québécois de la langue française* < gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=26552609 >.

[7] Office québécois de la langue française, « fiche terminologique : noeud », (2018), en ligne : *Office québécois de la langue française* < gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=26544969 >.

**Registre distribué** : « Registre simultanément enregistré et synchronisé sur un réseau d'ordinateurs, qui évolue par l'addition de nouvelles informations préalablement validées par l'entièreté du réseau et destinées à ne jamais être modifiées ou supprimées. »[8]

[8] Office québécois de la langue française, « fiche terminologique : registre distribué », (2018), en ligne : *Office québécois de la langue française* < gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=26544126 >.

# POINTS CLÉS

1. La première considération nécessaire à l'implantation d'une chaîne de blocs par un organisme public doit être le type de chaîne de blocs envisagé et ses modalités de gouvernance. C'est par cette analyse qu'un organisme public pourra déterminer si la technologie est adéquate pour l'entente envisagée et si l'infrastructure technologique nécessaire à la mise en œuvre de l'entente est réalisable. (Voir 1.2.2.2.1.)

2. Un organisme public souhaitant utiliser la technologie de la chaîne de bloc pour collecter et stocker les données et les renseignements personnels des citoyens du Québec devra identifier la nature de ces renseignements. Qu'ils s'agissent de renseignements personnels, de renseignements personnels sensibles, de renseignements dépersonnalisés ou de renseignements anonymisés, les organismes publics devront respecter les normes légales applicables à la collecte de ces différents types de renseignements. (Voir 1.2.2.2.2.)

3. Le droit à l'oubli (droit au déréférencement) est opposable aux tiers. Le droit à la rectification (droit à l'effacement) est opposable à l'organisme qui a effectué la collecte des renseignements (voir 1.2.2.2.4.1.).

4. Il n'existe pas au Québec de droit à l'oubli (droit au déréférencement) équivalent au droit européen. Un tel droit pourrait cependant s'appliquer au secteur privé dès l'entrée en vigueur du nouvel article 28.1 de la *Loi sur la protection des renseignements personnels dans le secteur privé* en septembre 2023. Rien ne laisse croire pour le moment que ce droit puisse être étendu aux organismes publics. Les organismes publics demeurent toutefois assujettis au droit à la rectification (droit à l'effacement) ce qui pourrait compliquer l'usage de la technologie de la chaîne de blocs en raison de sa caractéristique d'immuabilité. (Voir 1.2.2.2.4.)

5. L'usage de la technologie de chaîne de blocs n'est pas incompatible au droit à la portabilité qui entrera en vigueur en septembre 2024 au Québec. Or, les organismes publics devront être conscients des difficultés pratiques inhérentes à la chaîne de blocs relativement à la transmission de renseignements conservés sur la chaîne de blocs, et ce, afin de s'assurer d'être en mesure de répondre à leurs obligations légales. (Voir 1.2.2.2.4. et 1.2.2.2.5.)

### 1.2.2. ENJEUX SUR L'ENVIRONNEMENT LÉGAL ET LÉGISLATIF LORS DE L'ADOPTION DE LA CHAÎNE DE BLOCS PAR UN ORGANISME PUBLIC

L'implantation de la technologie de chaîne de blocs par les organismes publics a le potentiel de révolutionner la manière dont s'effectue la collaboration entre le secteur privé et les entités gouvernementales. L'adoption progressive de la technologie de chaîne de blocs par les organismes publics est hautement souhaitable, et ce, afin d'assurer l'efficience et la compatibilité de l'administration publique québécoise avec l'économie canadienne et mondiale. À ce titre, l'Institut sur la gouvernance numérique a récemment constaté la croissance rapide et significative de l'usage de la technologie de chaîne de blocs dans différents secteurs d'activités économiques. Ils arrivent à la conclusion qu'une part considérable du PIB mondial est susceptible de se retrouver sur les registres distribués au cours des cinq prochaines années : « [E]n 2027, 10% du PIB mondial pourrait être stocké dans les registres distribués »[9]. Toutefois, malgré les avantages inhérents de la technologie, il ne faut pas envisager sa mise en place comme une cassure et un remplacement intégral du système préexistant, mais plutôt comme un outil complémentaire permettant d'effectuer des gains en efficience et faciliter le traitement de certaines données par l'administration publique. Afin d'évaluer adéquatement les différentes finalités pour lesquelles la chaîne de blocs pourrait être utilisée conformément au droit québécois, il est également nécessaire comprendre les différents types de renseignements qu'un organisme public est susceptible de traiter.

Afin d'éviter la désuétude de cette analyse des impacts légaux et législatifs inhérents à l'implantation de la technologie de chaîne de blocs par les organismes publics, nos analyses relatives à la vie privée et à la protection des renseignements personnels tiennent compte des modifications au cadre législatif québécois qui découlent de la *Loi modernisant des dispositions législatives en matière de protection des renseignements*

[9] Institut de gouvernance numérique, *Registres distribués, l'évolution de la chaîne de blocs impacts, enjeux et potentiels pour le Québec*, Québec, 2019 à la p 11.

*personnels*[10]. Ainsi, l'analyse de ces dispositions sera effectuée à la fois selon le droit québécois actuel et selon les modifications à venir afin d'étayer les différentes considérations que devront envisager les organismes publics aux différentes étapes de l'entrée en vigueur des dispositions de la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels.*

[10] *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, LQ 2021 c 25.

### 1.2.2.1. LA CHAINE DE BLOCS ET LA GOUVERNANCE

L'adoption d'une chaîne de blocs par un organisme public commande une analyse minutieuse du type de chaîne de blocs dont la mise en place est envisagée. Autrement dit, l'encadrement normatif de l'usage de cette technologie pourra varier en fonction du type de chaîne de blocs précis utilisé. C'est pourquoi il est initialement nécessaire de comprendre certaines distinctions fonctionnelles et terminologiques. D'abord, il importe de ne pas confondre les registres distribués et la chaîne de blocs. Un registre distribué désigne une base de données répartie simultanément sur plusieurs serveurs de manière décentralisée[11] (comme exemple concret de registre distribué décentralisé, nous pouvons penser à la plateforme Ethereum). La chaîne de blocs constitue l'une des formes que peut prendre un registre distribué. Sommairement, la chaîne de blocs agit comme une feuille de calcul répartie entre les utilisateurs d'un réseau de poste-à-poste qui enregistre les transactions suivant l'ordre dans lequel elles ont été effectuées par les utilisateurs[12]. Chaque bloc est lié au précédent à l'aide d'un identificateur unique également appelé « hash ». Le procédé de hachage utilisé par la chaîne de blocs permet de transformer un document en une série de caractères alphanumériques :

> La blockchain fait appel à la technique de hachage qui permet de transformer un document et de le réduire sous format numérique. Le hash d'un message est un condensé cryptographique présenté par une séquence de caractères alphanumériques de longueur fixe, qui représente le contenu d'un message, sans le révéler et dont la valeur unique est produite par un algorithme de hachage. Le hachage est opéré à partir de la clé privée[13].

C'est par ce procédé cryptographique que la chaîne de blocs assure l'intégrité des informations qui y sont inscrites, car la tentative de corrompre l'information entraînerait une modification de l'identifiant unique du bloc ce qui serait conséquemment détecté par les nœuds du réseau et mènerait au rejet de l'entrée au registre. L'intérêt principal de la chaîne de blocs pour les organismes publics est qu'elle permet la tenue de registres infalsifiables et immuables. Du fait de sa nature, la technologie permet également aux

[11] Charlaine Bouchard, « Introduction : Qu'est-ce que la chaîne de blocs » dans Charlaine Bouchard, dir, *Comment la chaîne de blocs va transformer le droit?*, Montréal, Yvon Blais, 2020, 1 à la p 7.
[12] Raúl Zambrano, « Libérer le potentiel révolutionnaire de la technologie des chaînes de blocs pour le développement humain », Centre de recherche pour le développement international, Ottawa, 2017 à la p 22.
[13] « Fasicule 179 : Blockchain » au no 1, dans Dominique Legeais, dir, JCI Banque – Crédit – Bourse (QL).

participants du réseau d'accéder à la même source d'information puisque les empreintes numériques sont simultanément validées et transcrites sur l'ensemble des nœuds du réseau. Cette caractéristique inhérente à la chaîne de blocs réduit considérablement le risque d'erreur ou de fraude puisque les participants du réseau ont toujours accès à la source même des données et n'ont pas à procéder par l'envoi de copies. C'est d'ailleurs ce que réitère l'Institut de recherche en économie contemporaine : « La chaîne de blocs demeure encore aujourd'hui une technologie émergente, qui doit être validée par de multiples expérimentations et tests de la réalité ».[14]

Ensuite, une chaîne de blocs peut être publique ou privée et sans permission ou avec permission. La première distinction vise à circonscrire l'accès à l'information. Dans une chaîne de blocs publique, l'information est accessible à tous sans aucune restriction[15]. L'exemple le plus notable de ce type de chaîne de blocs est le système de paiement Bitcoin. Il s'agit d'une chaîne de blocs publique sans permission puisqu'elle est décentralisée, accessible à tous et permet les échanges de pair-à-pair. Ce type de chaîne de blocs pourrait éventuellement servir à différentes finalités pour les organismes publics advenant une adoption de masse de la technologie. Or, à l'heure actuelle, c'est plutôt les chaînes de blocs privées avec permission qui présentent un intérêt pour permettre aux organismes publics de tenir des registres et augmenter l'efficacité du traitement des données[16]. C'est par ailleurs, sur ce type de chaîne de blocs que sont basées les plateformes Entreprise Ethereum et Hyperledger. Les chaînes de blocs privées avec permission permettent de circonscrire l'accès au registre et également de restreindre les individus qui peuvent y inscrire des informations et les valider[17].

[14] Gilles L. Bourque et Éric N. Duhaime, « La révolution numérique au service du bien commun: la technologie des chaînes de blocs », INSTITUT DE RECHERCHE EN ÉCONOMIE CONTEMPORAINE, Québec, 2020, à la page 15.
[15] Louis Lehot, « United States: The Fourth Industrial Revolution: Legal Issues Around Blockchain», *mondaq* (7 décembre 2020) à la p 2.
[16] Young Ran Kim, « Blockchain Initiatives for Tax Administration » (2021) 4:69 UCLA L Rev 1 aux pp 42-43.
[17] White & Case « Beyond Bitcoin: The blockchain revolution in financial services », White & Case (7 mars 2016) à la p 5.

Enfin, il faut distinguer deux modèles de gouvernance en ce qui a trait à la répartition des nœuds et à l'administration d'une chaîne de blocs privée avec permission. Ce type de chaîne de blocs peut être utilisé selon un modèle de gouvernance pleinement privé ou selon un modèle de type consortium. La différence fondamentale entre une chaîne de blocs avec permission privée standard et celle de type consortium est essentiellement quant à la gouvernance et au degré de centralisation relatif au contrôle du registre :

> [A private blockchain] is controlled by a single entity or individual, where control is clearly centralised. [A consortium blockchain] is controlled by a group of approved individuals, where control is distributed among the different participants[18].

Ainsi, le modèle consortium est intéressant pour établir une collaboration entre plusieurs entités gouvernementales, car il permet d'assigner à la même chaîne de blocs privée des participants et des administrateurs qui émanent de différentes organisations[19]. Ce modèle assure du fait même une forme de décentralisation du réseau, puisque dans le cas du modèle consortium, le contrôle n'est pas concentré au sein d'un seul organisme. Quoi qu'il en soit, rappelons que les chaînes de blocs privées avec permission, qu'elles soient sous le contrôle d'un seul organisme ou suivant un modèle consortium, sont à favoriser pour la majorité des usages potentiels de la chaîne de blocs par les organismes publics puisqu'elles permettent de désigner les membres du réseau qui sont autorisés à inscrire des informations sur la chaîne de blocs et également ceux qui sont autorisés à lire l'information[20].

[18] José Miguel Moreira Moreno, *Blockchain and the right to be forgotten: A happy "marriage"*, mémoire de maîtrise en droit, Lund University, 2019 à la p 29.
[19] White & Case, *supra* note 17 à la p 5.
[20] Briseida Sofia Jiménez-Gómez, « Risks of blockchain for data protection: A European approach » (2020)

## 1.2.2.2. LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

L'enjeu le plus important que pose l'implantation d'une chaîne de blocs par les organismes publics est la protection des renseignements personnels et leurs modalités de partage. Deux considérations juridiques fondamentales s'imposent selon cette perspective. D'abord, la nature des renseignements personnels collectés (1.2.2.2.2.). Ensuite, les modalités de communication et l'obtention du consentement en fonction du destinataire des renseignements personnels (1.2.2.2.3.). Ces préoccupations doivent s'apprécier en considérant le contexte actuel de réforme de la législation en matière de renseignements personnels occasionnée par l'adoption de la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* (1.2.2.2.1.). Enfin, en conséquence de cette modernisation du cadre juridique québécois, il est également opportun d'évaluer la compatibilité de la chaîne de blocs au droit à l'oubli, au droit à la rectification (1.2.2.2.4.) ainsi qu'au droit à la portabilité (1.2.2.2.5.).

### 1.2.2.2.1. LE PROJET DE LOI 64

Le Québec traverse actuellement une modernisation de sa législation en matière de protection des renseignements personnels. L'adoption de la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* positionne le Québec comme chef de file en matière de protection des renseignements personnels, mais impose également un cadre rigoureux nécessitant des formalités de collecte strictes et une manipulation diligente des renseignements personnels des Québécois. La loi modifie notamment la *Loi sur les renseignements personnels dans le secteur privé* (ci-après « *Loi sur le secteur privé* »)[21] et la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (ci-après « *Loi sur l'accès* »)[22]. C'est principalement cette dernière qui énonce les obligations que doivent respecter les organismes publics en matière de traitement des renseignements personnels. De ce fait, les organismes publics qui souhaitent procéder à l'implantation d'une base de données avec l'usage d'une chaîne de blocs devront considérer avec diligence les

[21] *Loi sur les renseignements personnels dans le secteur privé,* RLRQ c P-39.1 [*Loi sur le secteur privé].*
[22] *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, RLRQ c A-2.1 [*Loi sur l'accès*].

formalités nécessaires à leur conformité juridique. À défaut du respect de leurs obligations, le nouvel article 159 de la *Loi sur l'accès* prévoit la possibilité d'imposer des sanctions pécuniaires pouvant atteindre 150 000$ à l'encontre des organismes publics qui manquent à leurs obligations[23].

La *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* a officiellement été adoptée le 21 septembre 2021. Or, les dispositions qu'elle renferme entreront en vigueur en trois étapes échelonnées sur une période de trois ans. L'entrée en vigueur de la plupart des dispositions de la loi sera le 22 septembre 2023[24]. Cependant, une exception est prévue à l'égard du droit à la portabilité que nous expliquons en détail à la section 1.2.2.2.5. Ce droit sera inscrit au nouvel article 84 de la *Loi sur l'accès* et entrera en vigueur le 22 septembre 2024[25]. La *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* prévoit également l'entrée en vigueur de certaines dispositions dès le 22 septembre 2022[26] dont les plus pertinentes traitent des procédures à suivre en cas d'incidents de sécurité[27].

| **ENTRÉE EN VIGUEUR DES MODIFICATIONS À LA *LOI SUR L'ACCÈS AUX DOCUMENTS DES ORGANISMES PUBLICS ET SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS*[28]** | | |
|---|---|---|
| **22 SEPTEMBRE 2022** | **22 SEPTEMBRE 2023** | **22 SEPTEMBRE 2024** |
| Articles : 8, 8.1, 43, 52.2, 59, 63.8 à 63.11, 67.2.1 à 67.2.3, 67.3, 94, 104, 107.1, 108, 109, 110.0.1, 110.0.2, 118, 120, 122, 122.1, 123, 125, 127, 127.1, 127.2, 129, 129.1, 130.2, 133, | Articles : 41.2, 47, 49, 50, 53, 53.1, 54, 55, 57, 59, 60, 63.3 à 63.7, 64, 64.1, 65, 65.0.1, 65.0.2, 65.1, 65.2, 67.2, 68, 68.1, 70, 70.1, 73, 79, 88.0.1, 88.1, 94, 98, 100, | Article : 84 |

[23] *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, *supra* note 10 art 69.
[24] *Ibid*, art 175.
[25] *Ibid*.
[26] *Ibid*.
[27] *Ibid*, art 15.
[28] Antoine Aylwin et Julie Uzan-Naulin, « Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels annotée », chronique de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (2021), en ligne : < https://www.fasken.com/fr/knowledge/projet-de-loi-64/2021/11/loi-sur-lacces-aux-documents-des-organismes-publics-et-sur-la-protection-des-renseignements >.

| | | |
|---|---|---|
| 134.1, 134.3, 134.4, 137.1, 137.2, 137.4, 139, 147, 149, 150, 151, 152, 155, 156 | 136, 137, 155, 158 à 162, 164.1, 164.2, 167, 174 | |

### 1.2.2.2.2. NATURE DES RENSEIGNEMENTS PERSONNELS

Les organismes publics qui songent à utiliser la chaîne de blocs pour effectuer des transactions devront déterminer si les renseignements qu'ils souhaitent traiter à l'aide de la technologie se prêtent adéquatement à son usage. Pour se faire, il est essentiel de comprendre la typologie des renseignements susceptibles d'être collectés et traités par les organismes publics, et ce, à la lumière des modifications législatives occasionnées par l'adoption du projet de loi 64. Quatre dispositions législatives sont nécessaires à la compréhension du régime juridique québécois actuel et à venir en matière de renseignements personnels. L'article 54 actuel de la *Loi sur l'accès* définit ce qu'est un renseignement personnel (1.2.2.2.3.1.). Prospectivement, la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* modifiera les articles 59, 65.1 et 73 de la *Loi sur l'accès*. C'est ainsi que l'article 59 renfermera désormais la définition d'un renseignement personnel sensible (1.2.2.2.3.2.). Pour leur part, les articles 65.1 et 73 de la loi distingueront le renseignement personnel dépersonnalisé (1.2.2.2.3.3.) et le renseignement anonymisé (1.2.2.2.3.4.).

#### 1.2.2.2.2.1. Renseignement personnel

La définition qu'a donnée le législateur à un renseignement personnel au Québec est très englobante et s'entend généralement d'un renseignement qui permet l'identification d'une personne :

> **54.** Dans un document, sont personnels les renseignements qui concernent une personne physique et permettent de l'identifier.[29]

Cette définition des renseignements personnels prévue à la *Loi sur l'accès* nous indique que, entre autres, la mention du nom, du prénom, de l'âge, de la date de naissance, de l'adresse de résidence ou de correspondance, le numéro de téléphone ou un numéro de

[29] *Loi sur l'accès*, *supra* note 22, art 54.

permis pourrait être qualifiée de renseignement personnel en cela que ce sont des renseignements portant sur une personne physique et qui ont pour effet de l'identifier.

Puis, la jurisprudence de différentes décisions de la Commission d'accès à l'information du Québec (ci-après « CAI ») apporte quelques précisions quant à la notion de renseignement personnel. C'est dans l'affaire *Segal c. Centre de services sociaux de Québec*, en 1988, que la Commission a élaboré le test qui permet de déterminer ce qu'est un renseignement personnel au sens de la *Loi sur l'accès* : « […] un renseignement est personnel s'il fait connaître quelque chose à quelqu'un, s'il est en rapport avec une personne physique et que ce renseignement est susceptible de distinguer cette personne par rapport à quelqu'un d'autre »[30]. Ainsi, pour constituer un renseignement personnel au sens de la *Loi sur l'accès* le renseignement doit révéler quelque chose au sujet de l'individu visé[31]. En ce sens, même une information qui concerne indirectement une personne pourra être un renseignement personnel dans certaines circonstances[32]. C'est donc une analyse contextuelle qui doit être faite pour déterminer si un renseignement est susceptible de révéler des informations sur l'individu :

> [41] La question de savoir si un renseignement concerne une personne physique permet de l'identifier s'interprète donc selon le contexte et les faits de chaque situation. De la même façon que le nom d'une personne, seul, peut parfois ne pas constituer un renseignement personnel, un renseignement concernant un bien meuble ou immeuble peut, dans certaines situations, révéler ou faire connaître quelque chose (renseignement) ayant un rapport avec un individu (qui concerne) et être susceptible de distinguer cette personne par rapport à quelqu'un d'autre ou de reconnaître sa nature (permet d'identifier). [Nos soulignements][33]

### 1.2.2.2.2.2. Renseignement personnel sensible

La *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* ajoute la définition du renseignement personnel sensible à l'article 59 de la *Loi sur l'accès* en précisant que cette disposition s'applique à la loi dans son ensemble :

---

[30] *Segel c Centre de Services sociaux de Québec*, [1988] CAI 315; voir aussi *Chouquet c Fédération des Caisses Desjardins du Québec*, 2020 QCCAI 376 aux para 34-35.
[31] *J.C. c SSQ, société d'assurances générales inc.*, 2017 QCCAI 129 au para 37.
[32] *Ibid*.
[33] *Ibid*, au para 40.

> **59.** Un organisme public ne peut communiquer un renseignement personnel sans le consentement de la personne concernée. […]
>
> Pour l'application de la présente loi, un renseignement personnel est sensible lorsque, de par sa nature notamment médicale, biométrique ou autrement intime ou en raison du contexte de son utilisation ou de sa communication, il suscite un haut degré d'attente raisonnable en matière de vie privée. [Nos soulignements][34]

S'il est évident que les renseignements médicaux et biométriques seront d'ores et déjà considérés comme des renseignements personnels sensibles, nous constatons que le libellé de l'article offre une définition subjective de ce qu'est un renseignement personnel sensible. C'est pourquoi il sera nécessaire de porter une attention particulière à l'interprétation que donneront les tribunaux québécois à un renseignement « autrement intime ». À cet effet, les données financières des individus seront fortement susceptibles d'être interprétées comme des renseignements personnels sensibles[35]. Notons également d'une manière plus générale que la Cour suprême du Canada s'est prononcée à quelques reprises sur la nature sensible d'un renseignement personnel dans des affaires opposant deux considérations d'intérêt public soit, d'une part, la publicité des débats judiciaire et, d'autre part, le droit à la vie privée. C'est en pondérant ces « intérêts publics importants » que la Cour souligne la distinction dans l'affaire *Sherman (Succession) c. Donovan* :

> S'il porte essentiellement sur la protection de la dignité d'une personne, cet intérêt [la Cour reconnaît la menace à la dignité qu'entraîne la diffusion de renseignements privés dans le cadre de débats judiciaires comme un intérêt public important] sera miné dans le cas de renseignements qui révèlent quelque chose de sensible sur elle en tant qu'individu, par opposition à des renseignements d'ordre général révélant peu ou rien sur ce qu'elle est en tant que personne. [Nos soulignements][36]

Une lecture *a contrario* de cette affirmation donne un indice sur la nature d'un renseignement personnel sensible en l'opposant au renseignement personnel qui révèle « peu » sur la vie d'un individu. Dans le même ordre d'idée, la Cour suprême conclut dans

---

[34] *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, *supra* note 10, art 13.

[35] Antoine Aylwin et Julie Uzan-Naulin « On répond à vos questions – Modernisation des lois sur la protection des renseignements personnels 1/3 » (9 février 2022), en ligne : *Lexology* < lexology.com/library/detail.aspx?g=c7595fea-c082-4752-8bc9-b5251b77ea7f > ; Voir aussi Commissariat au lobbying du Canada, « Évaluation des facteurs relatifs à la vie privée pour le système de gestion de l'information de la Direction des enquêtes (SGIDE) » (10 mai 2022), en ligne : *Commissariat au lobbying du Canada* < lobbycanada.gc.ca/fr/rapports-et-publications/evaluation-des-facteurs-relatifs-a-la-vie-privee-pour-le-systeme-de-gestion-de-l-information-de-la-direction-des-enquetes-sgide/ >.

[36] *Sherman (Succession) c Donovan*, 2021 CSC 25 au para 75.

l'affaire *R. c. Cole*, que certains renseignements donnent lieu à une plus grande expectative de vie privée en raison de leur nature sensible. À cet effet, la Cour suprême précise que cet intérêt en matière de vie privée sera prépondérant lorsque «les renseignements pertinents concernent le cœur même des "renseignements biographique" ou "[a]utrement dit, plus les renseignements sont personnels et confidentiels" »[37] Si l'interprétation que feront les tribunaux québécois d'un renseignement personnel sensible au sens de l'article 53 de la *Loi sur l'accès* variera vraisemblablement de l'interprétation qu'en a fait la Cour suprême en opposant le droit à la vie privée au principe de publicité des débats judiciaires, il n'en demeure pas moins que ces extraits offrent des pistes de solutions envisageables. Certains soutiennent également l'hypothèse selon laquelle la définition de renseignement personnel sensible contenue au RGPD (Règlement général sur la protection des données) pourrait servir de source d'inspiration pour anticiper les renseignements qui seront considérés sensibles, bien qu'il ne faille pas sacraliser cette comparaison :

> L'article 9 du RGPD prévoit ce qui suit:
>
> 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 est interdit.
>
> S'il est possible de s'en inspirer, la définition du RGPD reflète une façon de penser européenne, et non nord-américaine. En conséquence, nous ne croyons pas que cette définition puisse servir de guide, bien que certains éléments seront considérés sensibles dans les deux lois. [Nos soulignements][38]

Quoi qu'il en soit, des exigences rigoureuses, notamment quant à l'obtention du consentement exprès, seront imposées aux organismes publics qui font la collecte de ce type de renseignements. Considérant, les défis inhérents à la chaîne de blocs en matière de traitement des renseignements personnels, les organismes publics qui songent à utiliser cette technologie pour le traitement de renseignements personnels sensibles devront s'assurer que la chaîne de blocs envisagée respecte les modalités spécifiques au traitement de ce type de renseignements prévues aux dispositions modernisées de la *Loi sur l'accès*.

[37] *R. c Cole*, 2012 CSC 53 au para 46.
[38] *Ibid*.

### 1.2.2.2.2.3. Renseignement personnel dépersonnalisé

En ce qui a trait au renseignement personnel dépersonnalisé, c'est l'article 65.1 modernisé de la *Loi sur l'accès* qui le définit à son deuxième alinéa :

> **65.1.** Un renseignement personnel ne peut être utilisé au sein d'un organisme public qu'aux fins pour lesquelles il a été recueilli. […]
>
> Pour l'application de la présente loi, un renseignement personnel est dépersonnalisé lorsque ce renseignement ne permet plus d'identifier directement la personne concernée. [Nos soulignements][39]

La compréhension de ce type de renseignement est hautement pertinente puisque la technologie de chaîne de blocs permet, par sa nature, la dépersonnalisation des renseignements. Effectivement, le hachage cryptographique constitue un exemple de procédé permettant d'obtenir une donnée dépersonnalisée. Or, cela n'a pas pour effet d'anonymiser la donnée dans la mesure où le code qui résulte du procédé de hachage peut tout de même être retracé vers l'individu à l'aide de la clé privée. La Commission d'accès à l'information a récemment offert sa propre définition d'un renseignement dépersonnalisé en expliquant que le cryptage de données n'a pas pour effet de dispenser les organismes de leurs obligations à l'égard des renseignements qu'ils traitent puisque le lien entre la donnée et l'individu existe toujours: « [Le renseignement personnel dépersonnalisé est un] renseignement dont les données d'identification sont remplacées par un code. Il est possible de retracer le lien entre le code et l'individu auquel on a attribué ce code puisque ce lien est conservé. » [Nos soulignements][40]

### 1.2.2.2.2.4. Renseignement personnel anonymisé

L'article 73 de la *Loi sur l'accès* prévoit qu'un renseignement personnel doit être détruit une fois que les fins pour lesquelles il a été recueilli par l'organisme public ont été atteintes. À la notion de destruction des renseignements personnels s'ajoutera, dès 2023, à l'article 73 de la *Loi sur l'accès*, la définition du renseignement personnel anonymisé qui constituera une alternative à la destruction:

---

[39] *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, *supra* note 10, art 20.

[40] Commission d'accès à l'information du Québec « Renseignements personnels », en ligne : *Commission d'accès à l'information du Québec* < cai.gouv.qc.ca/chercheurs/informations-complementaires/ >.

> **73.** Lorsque les fins pour lesquelles un renseignement personnel a été recueilli ou utilisé sont accomplies, l'organisme public doit le détruire ou l'anonymiser pour l'utiliser à des fins d'intérêt public, sous réserve de la *Loi sur les archives* ou de *Code des professions*.
>
> Pour l'application de la présente loi, un renseignement concernant une personne physique est anonymisé lorsqu'il est, en tout temps, raisonnable de prévoir dans les circonstances qu'il ne permet plus, de façon irréversible, d'identifier directement ou indirectement cette personne.
>
> Les renseignements anonymisés en vertu de la présente loi doivent l'être selon les meilleures pratiques généralement reconnues.[41]

Encore une fois, cette notion demeure quelque peu abstraite dans la mesure où la notion de « meilleures pratiques généralement reconnues » est évolutive, et ce, particulièrement en matière de technologies de l'information. Il importe de souligner que ce fardeau repose sur les organismes publics comme l'a souligné le ministre responsable du projet de loi 64 :

> [O]n lit, dans le contexte du troisième alinéa aussi de l'article, les renseignements anonymisés en vertu de la présente loi doivent l'être selon les meilleures pratiques généralement reconnues. Donc, c'est la formule consacrée pour dire : utilisez toutes les techniques possibles et les moyens technologiques possibles pour nous amener raisonnablement vers l'irréversibilité du renseignement. Donc, il y a une charge légale qui est imposée aux organismes qui est très élevée. [Nos soulignements][42]

Pour bien départager les différents types de renseignements, pensons concrètement aux activités d'une agence de sondage fictive opérant sur un site Internet. Afin de récupérer des données statistiques, l'agence offre aux citoyens des chèques-cadeaux contre leurs opinions sur divers sujets de société. Les citoyens, pour répondre aux batteries de questions, se voient offrir un code qui leur sert d'authentifiant sur le site Internet. Une fois les réponses récoltées, si les données sont juxtaposées au code d'utilisateur des participants, ces données seront des renseignements dépersonnalisés. A contrario, si le code d'utilisateur est supprimé après la saisie des données, rendant impossible l'identification du participant, il s'agira de renseignements anonymisés.

---

[41] *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, *supra* note 10, art 28.

[42] « Projet de loi 64, Loi modernisant des dispositions législatives en matière de protection des renseignements personnels » Québec, *Journal des débats de la Commission des institutions*, 42-1, vol 45, n° 135 (14 avril 2021) (Éric Caire) en ligne : *Assemblée nationale du Québec* < assnat.qc.ca/fr/travaux-parlementaires/commissions/ci-42-1/journal-debats/CI-210414.html >.

Exemple fictif :

| Répartition des participants de l'étude selon leur intention de vote | | | |
|---|---|---|---|
| **RENSEIGNEMENTS DÉPERSONNALISÉS** | | **RENSEIGNEMENTS ANONYMISÉS** | |
| **Code utilisateur** | **Parti politique** | **Participant** | **Parti politique** |
| **5MJ609** | Parti mauve | A | Parti mauve |
| **9HG198** | Parti brun | B | Parti brun |
| **7KD032** | Parti mauve | C | Parti mauve |
| **6MN569** | Ne sait pas | D | Ne sait pas |
| **3TH678** | Parti jaune | E | Parti jaune |

Ainsi, à l'inverse du renseignement personnel dépersonnalisé, le renseignement anonymisé perd en principe tout son caractère personnel : « […] lorsqu'il est anonymisé, techniquement, il n'est pas un renseignement personnel. Donc, on peut l'utiliser à des fins d'intérêt public. »[43] Ainsi, il n'y a plus d'enjeu d'accès, de rectification ou d'effacement d'un tel renseignement puisqu'il s'agit d'un renseignement qui répond, en principe, aux critères d'individualisation[44], de corrélation[45] et d'inférence[46]. Or, il est à noter que sous sa forme initiale, le nouveau libellé de l'article 73 de la *Loi sur l'accès* ne prévoyait pas la notion de raisonnabilité. À vrai dire, il peut même sembler paradoxal d'utiliser la notion de raisonnabilité et d'irréversibilité simultanément. Or, à cet effet, le ministre explique que l'ajout subséquent de la notion de raisonnabilité découle du fait qu'il est impossible de garantir qu'une donnée ait été anonymisée de manière irréversible, mais que dans la mesure du possible, c'est la cible à atteindre :

> Il y a des contextes où moi, je peux amener ce renseignement-là à une anonymisation irréversible, mais dans ce qui est raisonnable de faire, c'est-à-dire que… parce qu'il faut comprendre, là, puis ça, là-dessus, je veux être clair, dans un contexte x, un renseignement peut être désanonymisé Je ne nierai jamais ça. Puis prôner l'irréversibilité, c'est utopique. […] Donc, c'est pour ça qu'on veut amener… On garde la notion d'irréversibilité parce qu'il des contextes où ça peut s'appliquer, mais c'est pour ça qu'on ajoute aussi la notion de raisonnable, parce que, moi, dans un cas, je travaille dans un contexte qui est le mien, et dans ce contexte-là, moi, je dois amener l'anonymisation aussi loin ou, donc, aussi

[43] *Ibid*.
[44] Gouvernement du Québec « Destruction ou anonymisation », en ligne : *Québec* < quebec.ca/gouvernement/travailler-gouvernement/travailler-fonction-publique/services-employes-etat/conformite/protection-des-renseignements-personnels/anonymisation/destruction-ou-anonymisation > (« Il ne doit pas être possible d'isoler une personne ni de l'identifier directement ou indirectement. »).
[45] *Ibid* (« Il ne doit pas être possible de relier des ensembles de données distincts qui concernent une même personne. »).
[46] *Ibid* (« Il ne doit pas être possible de déduire de nouvelles informations sur une personne. »).

> proche de l'irréversibilité qu'il est raisonnable de me le demander. [Nos soulignements][47]

En ce sens, certains prétendent que les renseignements peuvent être anonymisés sur une chaîne de blocs par la destruction de la clé privée. Est-ce que, pour reprendre les propos du ministre, il s'agit d'une manière permettant de se rapprocher de l'irréversibilité? Comme nous l'expliquons lors de la section subséquente traitant du droit à l'oubli, nous ne sommes pas de cet avis. Nous croyons plutôt que la chaîne de blocs ne permet que l'atteinte d'un renseignement personnel dépersonnalisée. Autrement dit, il ne faut surtout pas confondre anonymat et pseudonymat. Dans ce dernier cas, contrairement au premier, le lien entre l'individu et les renseignements personnels est toujours présent. Rappelons enfin que l'anonymisation d'un renseignement est une alternative à la destruction des renseignements, et ce, lorsque l'intérêt public le justifie. En principe, l'obligation pour les organismes d'effacer un renseignement persiste lorsque cette finalité est absente. Les modalités d'anonymisation pourront également être précisées par règlements :

> Le projet de loi nº 64 est venu clarifier les options s'offrant aux entreprises et aux organismes lorsque la finalité pour laquelle des renseignements personnels sont recueillis a été atteinte. Ceux-ci auront deux options : procéder à la destruction du renseignement personnel ou anonymiser ce renseignement (afin de l'utiliser à des fins sérieuses et légitimes dans le cas des entreprises, ou à des fins d'intérêt public dans le cas des organismes publics). Les entreprises et les organismes ne pourront donc pas conserver de renseignements personnels indéfiniment, au cas où une nouvelle utilité se manifesterait. Précisons que, selon la loi, un renseignement est considéré comme anonymisé lorsqu'on peut raisonnablement prévoir, en tout temps, qu'il ne peut plus identifier une personne, que ce soit de façon directe ou indirecte, et ce, de manière irréversible. Le gouvernement déterminera par règlement des critères devant être respectés quant à l'anonymisation de renseignements. [Nos soulignements][48]

[47] *Journal de débats de la Commission des institutions*, *supra* note 42.

[48] Jérémie Wyatt et al., « Réforme des lois encadrant la protection des renseignements personnels : le projet de loi no 64 est maintenant adopté. » (10 novembre 2021), en ligne : *Norton Rose Fulbright* < nortonrosefulbright.com/fr-ca/centre-du-savoir/publications/8bde609b/reforme-des-lois-encadrant-la-protection-des-renseignements-personnels >.

### 1.2.2.2.3. PARTAGE ET COMMUNICATION DE RENSEIGNEMENTS PERSONNELS

#### 1.2.2.2.3.1. Généralités relatives à la communication de renseignements par les organismes publics

Les organismes publics ne peuvent en principe recueillir que l'information nécessaire à l'exercice de ses attributions par sa loi constitutive[49]. L'article 65.1 de la *Loi sur l'accès* modifié par l'article 20 de la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* prévoit ce qui suit :

> Un renseignement personnel ne peut être utilisé au sein d'un organisme public qu'aux fins pour lesquelles il a été recueilli, à moins du consentement de la personne concernée. Ce consentement doit être manifesté de façon expresse dès qu'il s'agit d'un renseignement personnel sensible.
>
> L'organisme public peut toutefois utiliser un renseignement personnel à une autre fin sans le consentement de la personne concernée dans les seuls cas suivants :
>
> 1° lorsque son utilisation est à des fins compatibles avec celles pour lesquelles il a été recueilli;
>
> 2° lorsque son utilisation est manifestement au bénéfice de la personne concernée;
>
> 3° lorsque son utilisation est nécessaire à l'application d'une loi au Québec, que cette utilisation soit ou non prévue expressément par la loi;
>
> 4° lorsque son utilisation est nécessaire à des fins d'étude, de recherche ou de production de statistiques et qu'il est dépersonnalisé.
>
> Pour l'application de la présente loi, un renseignement personnel est dépersonnalisé lorsque ce renseignement ne permet plus d'identifier directement la personne concernée.
>
> Un organisme public qui utilise des renseignements dépersonnalisés doit prendre les mesures raisonnables afin de limiter les risques que quiconque procède à l'identification d'une personne physique à partir de renseignements dépersonnalisés[50].

Cette disposition entrera en vigueur le 22 septembre 2023.

De plus, la *Loi sur l'accès* permet à un organisme public de communiquer un renseignement personnel à une personne ou à un organisme si la communication est

[49] *Loi sur l'accès*, *supra* note 22, art 64.
[50] *Ibid*, art 65.1 modifié par la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, *supra* note 10, art 20.

nécessaire à l'application d'une loi du Québec[51]. La communication est également permise lorsqu'elle est nécessaire à l'application d'une convention collective, d'un décret, d'un arrêté, d'une directive, d'un règlement qui établissent des conditions de travail[52]. Il en va de même pour une communication nécessaire à l'exercice d'un mandat ou à l'exécution d'un contrat de services ou d'entreprise confié à un organisme public[53]. Pour l'ensemble de ces situations, le consentement de la personne concernée n'est pas nécessaire lors de la communication des renseignements par l'organisme public.

### 1.2.2.2.3.2. Communication de renseignements à l'extérieur du Québec

Une considération inhérente à la technologie de chaîne de blocs est la nécessité pour les organismes publics qui envisagent son adoption de planifier la façon dont seront répartis les différents nœuds du réseau. Cette répartition pourrait entraîner des conséquences juridiques particulièrement importantes si certains nœuds du réseau sont situés à l'extérieur de la province de Québec. Cela pourrait notamment être le cas dans l'éventualité où des ententes sont conclues avec d'autres provinces, avec le gouvernement central, avec des entreprises privées ou avec les gouvernements d'autres États. L'article 70.1 de la *Loi sur l'accès* figure parmi les articles modifiés par le projet de loi *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels.* Sous sa nouvelle forme, des formalités significatives seront nécessaires à la communication de renseignements personnels à l'extérieur du Québec :

> **70.1.** Avant de communiquer à l'extérieur du Québec un renseignement personnel, un organisme public doit procéder à une évaluation des facteurs relatifs à la vie privée. Il doit notamment tenir compte des éléments suivants :
>
> 1° la sensibilité du renseignement;
>
> 2° la finalité de son utilisation;
>
> 3° les mesures de protection dont le renseignement bénéficierait;
>
> 4° le régime juridique applicable dans l'État où ce renseignement serait communiqué, notamment son degré d'équivalence par rapport aux principes de protection des renseignements personnels applicables au Québec.

[51] *Loi sur l'accès*, *supra* note 22, art 67
[52] *Ibid*, art 67.1
[53] *Ibid*, art 67.2

> La communication peut s'effectuer si l'évaluation démontre que le renseignement bénéficierait d'une protection équivalant à celle prévue à la présente loi. Elle doit faire l'objet d'une entente écrite qui tient compte notamment des résultats de l'évaluation et, le cas échéant, des modalités convenues dans le but d'atténuer les risques identifiés dans le cadre de cette évaluation.
>
> Il en est de même lorsque l'organisme public confie à une personne ou à un organisme à l'extérieur du Québec la tâche de recueillir, d'utiliser, de communiquer ou de conserver pour son compte un tel renseignement.
>
> Le présent article ne s'applique pas à une communication prévue au paragraphe 4° du deuxième alinéa de l'article 59 ou au paragraphe 1.1° du premier alinéa de l'article 68. Il ne s'applique pas non plus à une communication faite dans le cadre d'un engagement international visé au chapitre III de la Loi sur le ministère des Relations internationales (chapitre M-25.1.1), à une communication faite dans le cadre d'une entente visée au chapitre III.1 ou III.2 de cette loi ou à une communication prévue à l'article 133 de la Loi sur la santé publique (chapitre S-2.2).[54]

À la lumière des exigences du nouvel article 70.1 de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, l'usage de la technologie de chaîne de blocs pourrait être complexifié d'un point de vue juridique en fonction de la localisation des nœuds. En effet, puisque la technologie a pour effet de reproduire le registre sur l'ensemble des nœuds du réseau, il appert que la localisation d'un seul nœud à l'extérieur du Québec pourrait rendre impossible la mise en place d'un projet utilisant la chaîne de blocs si l'emplacement du nœud ne garantit pas une protection équivalant aux exigences québécoises. Il sera nécessaire pour arriver à cette conclusion de procéder à des évaluations des facteurs relatifs à la vie privée, et ce, dès qu'un seul nœud sera situé à l'extérieur du Québec. Dans la mesure où le critère d'équivalence serait satisfait, une entente écrite est également nécessaire.[55] Cela s'explique par l'obligation légale de protéger les renseignements personnels, et ce, même s'ils sont dépersonnalisés.

[54] *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, *supra* note 10, art 27.

[55] Jennifer Stoddart et Geneviève Laliberté « Le projet de loi 64 et l'exportation de données personnelles du Québec : des complications en vue » (17 août 2020), en ligne : *Fasken* < fasken.com/fr/knowledge/projet-de-loi-64/2020/08/17-the-exportation-of-personal-data-from-quebec >.

### 1.2.2.2.4. DROIT À L'OUBLI ET POLITIQUES DE CONFIDENTIALITÉ

#### 1.2.2.2.4.1. Le droit à l'oubli et le droit à la rectification

Il importe, en premier lieu, de définir et de distinguer le droit à l'oubli et le droit à la rectification. Le droit à l'oubli (le droit au déréférencement) désindexe l'information d'une personne sur un moteur de recherche sans pour autant supprimer la page Web d'origine. Lorsqu'on effectue une recherche à partir du nom d'une personne, la page Web continue d'exister sans toutefois être référencée par le moteur de recherche donné. Le droit à la rectification (droit à l'effacement) efface tout simplement une page Web et l'information de la personne contenue dans celle-ci. Toutefois, le lancement d'une recherche avec le nom de cette personne peut continuer de générer un résultat sur un moteur de recherche avec contenus archivistiques.

Considérant les similarités entre la réforme québécoise en matière de renseignements personnels et le *Règlement général sur la protection des données*, il est pertinent d'effectuer une analyse comparative de l'évolution du droit à l'oubli au sein de l'Union européenne. Les premières références au droit à l'oubli ont été prononcées dans le cadre de l'affaire *Google c. Agence espagnole de protection des données*.[56] Dans cette affaire, un résident espagnol de l'Union européenne avait formulé une plainte face au refus de Google de procéder au retrait de données à caractère personnel le concernant de leur moteur de recherche. Cette affaire est particulièrement d'intérêt puisqu'elle s'inscrit dans la suite d'événements ayant mené à l'adoption du *Règlement général sur la protection des données*. Dans l'affaire Google, la Cour conclut que la contestation relative à l'indexation des renseignements personnels de l'utilisateur était valable, et ce, même en l'absence de préjudices, dans la mesure où l'information diffusée n'était pas dans l'intérêt général du public :

> [92] La personne concernée pouvant, eu égard à ses droits fondamentaux au titre des articles 7 et 8 de la Charte, demander à ce que l'information en question ne soit plus mise à la disposition du grand public par son inclusion dans une telle liste de résultats, il y a lieu de considérer, ainsi qu'il ressort notamment du point 81 du présent arrêt, que ces droits prévalent, en principe, non seulement sur l'intérêt économique de l'exploitant du moteur de recherche, mais également sur

[56] CE, Google Inc. c Agencia Espanola de Protección de Datos, C131/12.

> l'intérêt de ce public à trouver ladite information lors d'une recherche portant sur le nom de cette personne. Cependant, tel ne serait pas le cas s'il apparaissait, pour des raisons particulières, telles que le rôle joué par ladite personne dans la vie publique, que l'ingérence dans ses droits fondamentaux est justifiée par l'intérêt prépondérant dudit public à avoir, du fait de cette inclusion, accès à l'information en question.[57]

Ce droit est maintenant bien imbriqué au cadre juridique de l'Union européenne puisque le législateur s'est assuré, à la suite de cette affaire, de consacrer ce droit de manière non équivoque à l'article 17 du *Règlement général sur la protection des données* : « la personne concernée a le droit d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, de données à caractère personnel la concernant et le responsable du traitement a l'obligation d'effacer ces données à caractère personnel dans les meilleurs délais […] »[58]. La réforme québécoise en matière de protection des renseignements personnels ayant calqué à de nombreux égards le *Règlement général sur la protection des données*, il est raisonnable d'émettre l'hypothèse que les tribunaux qui auront à se prononcer sur l'enjeu du droit à l'oubli se réfèrent prospectivement au droit européen, dont l'affaire Google, pour l'interprétation de la portée de ce droit au Canada, et ce, plus particulièrement après l'entrée en vigueur du nouvel article 28.1 de la *Loi sur la protection des renseignements personnels dans le secteur privé* le 22 septembre 2023.

Nous comprenons donc que l'immuabilité des données enregistrées sur une chaîne de blocs pourrait entraîner des conséquences particulières pour les organismes qui envisagent d'utiliser la technologie.

Les discussions entourant la naissance d'un « droit à l'oubli » au Québec se sont multipliées au cours de dernières années avec la prise de conscience collective de l'importance d'une protection adéquate des renseignements personnels et de la protection de la vie privée des Québécois. Un survol historique de l'évolution de ce droit et du droit à la rectification est hautement pertinent et permet d'envisager la manière dont ces droits pourraient potentiellement s'appliquer aux organismes publics et influencer leur capacité à adopter la technologie de chaîne de blocs pour le traitement de renseignements

[57] *Ibid*, au para 92.
[58] CE Règlement 2016/679 à l'art 17.

personnels. En ce sens, il importe de distinguer le droit de rectification qui est opposable à l'organisme qui a effectué la collecte de données et le droit à l'oubli qui est opposable aux tiers qui indexent les données[59]. De ce fait, il faut également comprendre que le droit à la rectification n'entraîne pas le droit à l'oubli :

> […] la Commission [d'accès à l'information du Québec] considère « le droit d'une personne de faire rectifier dans un dossier qui la concerne des renseignements inexacts, incomplets ou équivoques, n'est pas de l'ordre du "droit à l'oubli" qui vise à effacer des informations des espaces publics. » Le droit de rectification, prévu au Code civil du Québec et à la Loi sur le secteur privé, n'emporte donc aucunement un droit au déréférencement. [Nos soulignements][60]

### 1.2.2.2.4.2. La situation canadienne

Au Canada, les discussions portant sur l'applicabilité potentielle d'un droit à l'oubli remontent bien avant l'adoption de la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*. En 2016, le Commissariat à la protection de la vie privée du Canada avait procédé à la rédaction d'un rapport à la suite de leur consultation publique s'intitulant « Le droit à l'oubli peut-il s'appliquer dans le contexte canadien et dans l'affirmative comment ».[61] La conclusion du document de consultation publié par le Commissariat à la protection de la vie privée du Canada était qu'il n'existe pas de droit à l'oubli équivalant à l'Union européenne en soi au Canada, mais qu'il existe néanmoins des moyens prévus par le droit canadien afin de protéger la vie privée des Canadiens :

> Au Canada, il n'existe pas de loi sur le droit à l'oubli ou le droit à l'effacement en soi. Les gens s'adressent au Commissariat pour obtenir de l'aide lorsqu'ils tombent sur des sites Web qui affichent leurs renseignements personnels sans leur consentement. Le Commissariat surveille la conformité à la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE), qui établit les règles que doivent respecter les organisations du secteur privé lorsqu'elles traitent des renseignements personnels dans le cadre de leurs activités commerciales.[62]

---

[59] Marc-André Boucher, « Regard québécois sur le « droit à l'oubli » et la suppression de renseignements personnels en ligne » (20 juillet 2016), en ligne : *Fasken* < fasken.com/fr/knowledge/2016/07/intellectualpropertybulletin-20160720 >.
[60] *Ibid*. Voir aussi *C.L. c BCF Avocats d'affaires*, 2016 QCCAI 114 au para 65.
[61] Canada, Commissariat à la protection de la vie privée du Canada, *Réputation en ligne : que dit-on à mon sujet*, 2019.
[62] *Ibid*, aux pp 6-7.

Effectivement, la *Loi sur la protection des renseignements personnels et les documents électroniques* prévoit que les organisations sont autorisées à conserver les renseignements personnels qu'aussi longtemps que nécessaire pour réaliser les fins déterminées.[63]

### 1.2.2.2.4.3. La situation québécoise

Au Québec, la situation pourrait cependant être différente compte tenu de l'adoption de la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels.* Il est vrai que la jurisprudence actuelle est réticente à reconnaître l'existence d'un droit à l'oubli au Québec. À vrai dire, la Commission d'accès à l'information du Québec avait même écarté, en 2016, l'existence de ce droit dans une affaire de déréférencement qui présentait des similarités avec l'affaire Google exposée lors des paragraphes précédents. Dans l'affaire *C.L. c. BCF Avocats d'affaires*, une adjointe juridique qui avait quitté ses fonctions chez BCF avocat était toujours associée à ce cabinet par le moteur de recherche Google, et ce, malgré le retrait par BCF des informations d'emploi à son égard. La demanderesse souhaitait l'effacement complet de son lien antérieur à l'employeur d'Internet. Sommairement, la juge indique que BCF Avocats d'affaires devait effectivement procéder au retrait des informations sur le site Web (droit de rectification), mais que le cabinet avait répondu à ses obligations et que les droits ne pouvaient pas être exercés contre un tiers (droit à l'oubli). Ainsi, bien que la Commission ait souligné les obligations générales de l'ancien employeur de retirer les informations du site Web, la juge administrative a clairement distingué le « droit à l'oubli » des protections actuellement offertes par le droit positif québécois :

> [65] Le droit d'une personne de faire rectifier dans un dossier qui la concerne des renseignements inexacts, incomplets ou équivoques n'est pas de l'ordre du « droit à l'oubli » qui vise à effacer des informations des espaces publics. D'ailleurs, il n'est pas certain que ce droit, reconnu en Europe, trouve application au Québec. [Nos soulignements][64]

[63] *Loi sur la protection des renseignements personnels et les documents électroniques*, LC 2000 c 5 au principe 4.5.3.
[64] *C.L. c BCF Avocats d'affaires*, *supra* note 57 au para 65.

Cependant, depuis cette décision, il y a lieu de se demander si la volonté législative n'est pas plutôt la création, au Québec, d'une forme de droit à l'oubli similaire à celui présent en Europe. Il importe dès maintenant de préciser que la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* prévoit ce droit en visant précisément le secteur privé, et ce, sans prévoir d'équivalent dans la législation visant les organismes publics. Le nouvel article 28.1 de la *Loi sur la protection des renseignements personnels dans le secteur privé* qui entrera en vigueur en septembre 2022 offrira précisément un « droit à l'oubli » qui permettra à toute personne d'imposer aux entreprises de cesser la diffusion de leurs renseignements.[65] De plus, cette disposition prévoit que « les personnes concernées [aur]ont le droit de demander que leurs renseignements personnels cessent d'être diffusés ou soient désindexés ou réindexés lorsque la diffusion de celles-ci porte gravement atteinte à leur réputation ou à leur vie privée ».[66] Pour un organisme public, cela pourrait avoir de l'intérêt dans l'éventualité où une entente tripartite était conclue avec des entreprises du secteur privé ou si le droit à l'oubli n'en venait qu'à être étendu à eux. Or, il ne faut pas oublier, sans les confondre, que de manière plus générale, le *Code civil du Québec* prévoit également un « droit de rectification » qui permet à toute personne de demander que soit corrigé ou supprimé des renseignements personnels qui la concernent <u>en certaines circonstances</u> :

> **40.** Toute personne peut faire corriger, dans un dossier qui la concerne, des renseignements inexacts, incomplets ou équivoques; elle peut aussi faire supprimer un renseignement périmé ou non justifié par l'objet du dossier, ou formuler par écrit des commentaires et les verser au dossier.
>
> La rectification est notifiée, sans délai, à toute personne qui a reçu les renseignements dans les six mois précédents et, le cas échéant, à la personne de qui elle les tient. Il en est de même de la demande de rectification, si elle est contestée.[67]

[65] Éloïse Gratton et al., « Préserver un équilibre délicat : renforcer la protection des renseignements personnels dans le secteur privé tout en favorisant l'innovation et en soutenant l'économie numérique au Québec » (2020) à la p 12.
[66] *Ibid*.
[67] *Code civil du Québec*, RLRQ c C-1991, art 40.

Ce même droit est prévu spécifiquement dans la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* qui consacre le droit à la rectification :

> **89.** Toute personne qui reçoit confirmation de l'existence dans un fichier d'un renseignement personnel la concernant peut, s'il est inexact, incomplet ou équivoque, ou si sa collecte, sa communication ou sa conservation ne sont pas autorisées par la loi, exiger que le fichier soit rectifié.[68]

Ce droit est précisé dans l'affaire *V.-P. c. Commission de la santé et de la sécurité au travail* ou la Commission d'accès à l'information du Québec devait se prononcer sur la demande d'un employé qui souhaitait le retrait de certains documents contenus dans son dossier de travailleur. Dans cette décision, la Commission précise que le droit de rectification comprend la suppression des renseignements lorsque la collecte était ou n'est plus justifiée :

> [46] Toute personne peut s'adresser à un organisme public en vue de faire rectifier un renseignement inexact, incomplet ou équivoque détenue à son sujet. Celle-ci peut également requérir qu'un renseignement soit supprimé de son dossier si la loi ne permettait pas qu'il soit recueilli ou conservé par l'organisme.

#### 1.2.2.2.4.4. La compatibilité de ces droits à l'usage de la chaine de blocs

Ce tour d'horizon de l'application potentielle du « droit à l'oubli » et de l'application actuelle et certaine du droit à la rectification en droit québécois marque potentiellement un obstacle de taille à l'usage de la chaîne de blocs par les organismes publics et doit nécessairement être une considération lors de l'adoption de la technologie par un organisme public. Le prochain paragraphe permettra d'exposer les considérations juridiques et les difficultés qui opposent ces droits à la technologie de chaîne de blocs.

Rappelons d'abord que du fait de sa nature, la chaîne de blocs se caractérise par son immuabilité. Autrement dit, il n'est pas possible, en principe, de supprimer ou de modifier les informations sur la chaîne de blocs puisque cela aurait pour effet de détruire la chaîne

[68] *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, RLRQ c A-2.1, art 89.

de blocs[69]. Cette réalité s'applique également à la plupart des chaînes de blocs privées. À vrai dire, si une chaîne de blocs avec permission permet de restreindre l'accès aux données inscrites sur la chaîne de blocs, elle ne permet pas de les effacer ou de les modifier.[70] Si nous prenons l'exemple d'une chaîne de blocs construite avec Hyperledger, cette chaîne de blocs sera une base de données immuables et inaliénables puisque le retrait d'un bloc de la chaîne aurait pour effet de détruire la chaîne de blocs. De plus, comme le souligne l'organisme Hyperledger lui-même, l'usage d'une chaîne de blocs est justifié par la volonté de créer une base de données perpétuelle où l'information ne doit pas être effacée : « Blockchains can be used to record promises, trades, transactions or simply items we never want to disappear. Mirrored exactly across all nodes in a given network, it allows everyone in an ecosystem to keep a copy of the common system of record. Nothing can ever be erased or edited. » [Nos soulignements][71] Il est donc prioritaire pour les organismes de considérer le type de chaîne de blocs à utiliser ainsi que leurs limitations puisqu'elles pourraient ultimement avoir pour effet d'empêcher les organismes de se conformer à leurs obligations en matière de traitement des renseignements personnels. Cependant, tout n'est pas perdu puisque certaines solutions ont récemment été développées et pourraient permettre de pallier les exigences législatives quant à la rectification et l'effacement des renseignements. Par exemple, la société Accenture a récemment obtenu un brevet sur un procédé technologique qui permet de modifier les entrées effectuées à la chaîne de blocs et de substituer un bloc à un autre sans pour autant briser la chaîne de blocs:

> The feature of editability is provided by a new variation of the chameleon hash function. Modification of the blocks is enabled through the use of the chameleon hash key to unlock the link between the block that must be changed and its successor […] But, thanks to this mechanism, it is possible to substitute the existent block with a new one without breaking the chain, as it would happen traditionally. [Nos soulignements][72]

[69] Erik Källman, Blockchain v. Personal Data – A rising conflict Between Technology and the law, mémoire de maîtrise en droit, Tilburg University, 2019 à la p 20.
[70] Louis Bruno et al., « United States: The Data Privacy Block In The Chain: Blockchains And Immutability », *mondaq* (6 juin 2019) à la p 2.
[71] Hyperledger, « The HyperLedger Vision », en ligne (pdf) : *Hyperledger* < hyperledger.org/wp-content/uploads/2018/01/The-Hyperledger-Vision-4.pdf > à la p 3..
[72] Moreira Moreno, *supra* note 18 à la p 34.

À notre avis, considérant la malléabilité qu'exige la *Loi sur l'accès* et le *Code civil du Québec*, les organismes publics doivent s'assurer de la flexibilité de la solution envisagée, car la rigidité de la chaîne de blocs pourrait rapidement devenir une contrainte juridique insurmontable. En ce sens, rappelons que le simple cryptage d'une donnée n'a pas pour effet d'en faire une donnée anonymisée au sens du droit québécois. Bien au contraire, cette donnée demeure un renseignement personnel dépersonnalisé assujetti aux dispositions législatives de la *Loi sur l'accès*. La protection de cette donnée, c'est-à-dire la suite alphanumérique générée par le procédé de hachage cryptographique, demeure la responsabilité de l'organisme public qui l'a collectée. À cet égard, certains auteurs prétendent que le cryptage définitif et irréversible des données permettrait de répondre aux exigences législatives relatives au droit à l'oubli[73]. Ce procédé consiste à détruire la clé privée permettant d'accéder à la donnée cryptée. Or, nous sommes en désaccord avec cette approche et croyons que si le cryptage permet l'obtention d'une donnée dépersonnalisée au sens de la réforme québécoise des renseignements personnels, cela n'a pas pour effet d'en faire une donnée anonymisée. Si la nuance est subtile, il n'en demeure pas moins qu'une simple donnée dépersonnalisée demeure un renseignement personnel au sens de la loi.[74] De plus, il importe de réitérer que les risques de cyberattaques relatifs aux procédés de cryptographie asymétrique évoluent rapidement. Selon des études menées par la US National Institute of Standards and Technology, les méthodes de cryptage actuellement utilisées par la plupart des chaînes de blocs, considérées comme les plus sécuritaires, pourraient être vulnérables aux cyberattaques dans un avenir rapproché, et ce, en raison de l'arrivée imminente des ordinateurs quantiques :

> According to the NIST, elliptic curve cryptography will become ineffective. Worryingly, we are talking about the method used for the signature of cryptocurrencies, including the famous Bitcoin. Recent studies indicate that this method is highly vulnerable to attack by quantum computers, which, in a few years' time, could crack these codes in under 10 minutes. [Nos soulignements][75]

[73] Källman, *supra* note 69 à la p 22.
[74] *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, *supra* note 10, art 20.
[75] Eric Lavallée, « Canada : Artificial Intelligence And Blockchains Are Vulnerable To Cyberattacks » *mondaq* (21 août 2018) à la p 2.

Rappelons que puisque la distinction entre la donnée dépersonnalisée et la donnée anonymisée n'entrera en vigueur qu'en 2023, les tribunaux québécois n'ont pas encore eu à se prononcer sur la question. Or, les enjeux de cybersécurité identifiés ci-haut militent à notre avis en défaveur de la reconnaissance du cryptage comme une méthode permettant de donner lieu à l'anonymisation irréversible de données. Comme nous l'avons expliqué plus tôt, il s'agit plutôt d'une donnée dépersonnalisée, et ce, même si la clé privée permettant l'accès à une donnée cryptée est détruite.

### 1.2.2.2.4.5. Les politiques de confidentialité

Au plus tard en septembre 2022, les organismes publics devront avoir procédé à la création d'un comité sur l'accès à l'information et la protection des renseignements personnels[76] qui sera composé minimalement de « la personne responsable de l'accès aux documents, de celle responsable de la protection des renseignements personnels et de toute autre personne dont l'expertise est requise […] »[77]. Ce comité sera chargé d'élaborer des lignes directrices qui détaillent les procédures internes de traitement de renseignements personnels :

> 63.3. Un organisme public doit publier sur son site Internet des règles encadrant sa gouvernance à l'égard des renseignements personnels. Ces règles doivent être approuvées par son comité sur l'accès à l'information et la protection des renseignements personnels.
>
> Elles peuvent prendre la forme d'une politique, d'une directive ou d'un guide et doivent notamment prévoir les rôles et les responsabilités des membres de son personnel tout au long du cycle de vie de ces renseignements ainsi qu'un processus de traitement des plaintes relatives à la protection de ceux-ci. Elles incluent une description des activités de formation et de sensibilisation que l'organisme offre à son personnel en matière de protection des renseignements personnels.
>
> Ces règles incluent également les mesures de protection à prendre à l'égard des renseignements personnels recueillis ou utilisés dans le cadre d'un sondage […][78]

[76] *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, *supra* note 10, art 1.
[77] *Ibid*.
[78] *Ibid*, art 15.

La *Loi sur l'accès* modernisée ira plus loin en ce qui concerne les obligations de transparence des organismes qui utilisent un moyen technologique pour le traitement des renseignements personnels. Effectivement, ces entités auront l'obligation de mettre en place, en plus de modalités de gouvernance prévues à l'article 63.3 mentionné ci-haut, une politique de confidentialité expliquant les paramètres de conservation et destruction des renseignements personnels :

> 63.4. Un organisme public qui recueille par un moyen technologique des renseignements personnels doit publier sur son site Internet et diffuser par tout moyen propre à atteindre les personnes concernées une politique de confidentialité rédigée en termes simples et clairs. Il fait de même pour l'avis dont toute modification à cette politique doit faire l'objet.
>
> Un règlement du gouvernement peut déterminer le contenu et les modalités de cette politique et de cet avis.[79]

Évidemment, comme nous l'avons mentionné antérieurement et comme nous le détaillons dans la section subséquente sur le droit de la preuve, la technologie de chaîne de blocs est un moyen technologique au sens du droit québécois. Les organismes publics qui envisagent d'utiliser cette technologie devront prévoir leur politique de confidentialité en conséquence afin de se conformer à leurs obligations légales. Cela pourra représenter un défi dans la mesure où le libellé de l'article exige une politique rédigée en termes simples et clairs alors que la technologie est intrinsèquement complexe. De plus, comme l'indique le futur article 63.4 de la *Loi sur l'accès*, rappelons que c'est le comité sur l'accès à l'information et la protection des renseignements personnels qui sera chargé de procéder à l'approbation des politiques de confidentialité des organismes publics.

#### 1.2.2.2.4.6. La nécessité potentielle d'une évaluation des facteurs relatifs à la vie privée

La réforme de la *Loi sur l'accès* prévoit des formalités strictes que devront respecter les organisations qui procèdent au remplacement ou à des modifications de leurs procédés technologiques de traitement des données. En ce sens, l'une des obligations des organismes publics sera de consulter leur Comité sur l'accès à l'information et la protection des renseignements personnels pour les projets technologiques de traitement des

[79] *Ibid*.

renseignements personnels envisagés, et ce, dès septembre 2023, lors de l'entrée en vigueur de l'article 63.5 de la *Loi sur l'accès*. Les organismes qui envisagent la mise en place de la chaîne de blocs pour le traitement de renseignements personnels devront donc s'assurer d'impliquer ce Comité à leurs travaux afin de répondre à leurs obligations légales. Notons par ailleurs que le Comité devra être consulté dès le début des projets:

> 63.5. Un organisme public doit procéder à une évaluation des facteurs relatifs à la vie privée de tout projet d'acquisition, de développement et de refonte de système d'information ou de prestation électronique de services impliquant la collecte, l'utilisation, la communication, la conservation ou la destruction de renseignements personnels.
>
> Aux fins de cette évaluation, l'organisme public doit consulter, dès le début du projet, son comité sur l'accès à l'information et la protection des renseignements personnels.
>
> Cet organisme public doit également s'assurer que ce projet permet qu'un renseignement personnel informatisé recueilli auprès de la personne concernée soit communiqué à cette dernière dans un format technologique structuré et couramment utilisé.
>
> La réalisation d'une évaluation des facteurs relatifs à la vie privée en application de la présente loi doit être proportionnée à la sensibilité des renseignements concernés, à la finalité de leur utilisation, à leur quantité, à leur répartition et à leur support. [Nos soulignements][80]

De plus, comme l'indique le premier alinéa de l'article 63.5, les organismes qui envisagent la mise en place ou la refonte de leurs systèmes d'information, ce qui inclut à notre avis les projets de registres distribués, devront obligatoirement procéder à une évaluation des facteurs relatifs à la vie privée, et ce, même en l'absence de communication de renseignements personnels hors du Québec. Cette nouvelle disposition exige des organismes qu'ils anticipent, dès la genèse de leurs projets visant la manipulation de renseignements personnels, les risques inhérents à ceux-ci[81].

[80] *Ibid*.
[81] *Ibid*.

#### 1.2.2.2.5. LE DROIT À LA PORTABILITÉ

Le droit à la portabilité qui entrera en vigueur en septembre 2024 permettra à un individu de contraindre un organisme public à communiquer un renseignement à des tiers lorsque ce renseignement a été collecté à l'égard de l'individu qui effectue la demande et qu'il s'agit d'un renseignement personnel informatisé.

Bien que la chaîne de blocs ne soit pas *a priori* incompatible au droit à la portabilité, son usage pourrait entraîner des difficultés pratiques considérables susceptibles d'entraver la capacité des organismes publics à répondre à leurs obligations légales. Cela s'explique principalement par la difficulté pratique d'extraire des données de la chaîne de bloc :

> 84. L'organisme public donne communication d'un renseignement personnel à la personne qui a le droit de le recevoir en lui permettant de prendre connaissance du renseignement sur place pendant les heures habituelles de travail ou à distance et d'en obtenir une copie.
>
> À la demande du requérant, un renseignement personnel informatisé doit être communiqué sous la forme d'une transcription écrite et intelligible
>
> À moins que cela ne soulève des difficultés pratiques sérieuses, un renseignement personnel informatisé recueilli auprès du requérant, et non pas créé ou inféré à partir d'un renseignement personnel le concernant lui est, à sa demande, communiqué dans un format technologique structuré et couramment utilisé. Ce renseignement est aussi communiqué à sa demande à toute personne ou à tout organisme autorisé par la loi à recueillir un tel renseignement[82].

Dans un rapport sur la compatibilité de la technologie de chaîne de blocs au droit d'accès à l'information et au droit à la portabilité, la Commission nationale informatique et libertés a conclu qu'il n'existait aucune incompatibilité entre les caractéristiques inhérentes de la technologie de chaîne de blocs et ces droits. Selon la Commission, il suffit que l'organisme ait mis en place une structure facilitant la communication des renseignements aux requérants : « le responsable de traitement participant devra ainsi fournir une information concise, aisément accessible et formulée en termes clairs à la personne concernée avant de soumettre à validation des mineurs une donnée à caractère personnel »[83]. Si nous sommes

[82] Voir *Loi sur l'accès*, *supra* note 22, art 84; Voir aussi *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, *supra* note 10, art 30.

[83] France, Commission nationale informatique et libertés, *Premiers éléments d'analyse de la CNIL : Blockchain*, par Commission nationale informatique et libertés, 2018, en ligne: < cnil.fr/sites/default/files/atoms/files/la_blockchain.pdf > à la p 9.

d'accord avec leur conclusion, la mise en place d'une telle infrastructure entraîne des difficultés et nécessite une réflexion afin de déterminer si les gains en efficience que peut offrir la chaîne de blocs sont contrecarrés par les complexités occasionnées par la communication de renseignements à des tiers. Dans l'affirmative, l'usage d'une chaîne de blocs, bien que possible, ne serait pas souhaitable. À l'inverse, si un organisme conclut que les gains en efficience sont plus grands que les contraintes occasionnées par leur obligation potentielle de communiquer des renseignements à des tiers ou au requérant lui-même, les organismes publics, pour répondre à leurs obligations, devront mettre en place un processus leur permettant de transférer l'information de la chaîne de blocs vers un support adéquat pour la transmission des renseignements personnels aux tiers. Ce transfert de support technologique pourra nécessiter le respect de formalités strictes dont le non-respect pourrait avoir des conséquences en matière de preuve. Sur ce sujet, nous offrons davantage d'explications à la section 1.2.2.3.

### 1.2.2.3. LA COMPATIBILITÉ DU DROIT DE LA PREUVE AVEC LA TECHNOLOGIE DE CHAÎNE DE BLOCS

Une autre considération juridique relative aux chaînes de blocs se rapporte au droit de la preuve et à l'admissibilité d'un écrit qui est conservé sur ce type de registre distribué. À cet égard, nous arrivons à la conclusion que la chaîne de blocs est un excellent support qui répond aux exigences du droit positif québécois en matière de preuve. Afin de comprendre l'adaptabilité de la chaîne de blocs au droit de la preuve, la nature de la technologie impose de se référer à la *Loi concernant le cadre juridique des technologies de l'information*, et ce, conformément à l'article 2837 du *Code civil du Québec* :

> 2837. L'écrit est un moyen de preuve, quel que soit le support du document, à moins que la loi n'exige l'emploi d'un support ou d'une technologie spécifique.
>
> Lorsque le support de l'écrit fait appel aux technologies de l'information, l'écrit est qualifié de document technologique au sens de la *Loi concernant le cadre juridique des technologies de l'information*.[84]

Comme le souligne le juriste Jean-François De Rico, « l'écrit généré ou conservé sur une chaîne de blocs doit être qualifié de "document technologique" »[85] au sens de l'article 2837 du *Code civil du Québec.* Dans l'éventualité où un document contenu dans une chaîne de blocs devait être utilisé par un organisme public dans le cadre d'une procédure judiciaire, c'est la notion d'intégrité du document technologique qui permettrait d'établir la valeur de la preuve.[86] L'arrêt de principe relativement à l'intégrité d'un document technologique est l'affaire *Benisty c. Kloda*.[87] Sommairement, cette affaire explique que lors de la mise en preuve d'un document technologique, il n'y a pas de présomption d'authenticité du document qui découle de l'article 7 de la *Loi concernant le cadre juridique des technologies de l'information*. La Cour explique la distinction fondamentale entre une présomption d'intégrité et la présomption que le support technologique peut assurer l'intégrité du document :

---

[84] *Code civil du Québec*, *supra* note 67, art 2837.
[85] Jean-François De Rico, « Le droit de la preuve » dans Charlaine Bouchard, dir, *Comment la chaîne de blocs va transformer le droit*, Montréal, Yvon Blais, 2020, 1 à la p 139.
[86] *Ibid*.
[87] *Benisty c Kloda*, 2018 QCCA 608, aux para 99-101.

> [99] […] [L]es articles 2855 et 2874 C.c.Q. exigent la démonstration d'une preuve indépendante ou distincte d'authenticité du document mis en preuve. Or, un document technologique comprend généralement une documentation inhérente, comme des métadonnées, permettant d'identifier un auteur, la date de confection, ou encore la présence de modifications dans le document. Puisque ces métadonnées constituent une preuve inhérente du document technologique – et non pas une preuve indépendante ou distincte, tel que le requiert la première partie des articles 2855 et 28744 C.c.Q. – et qu'elles remplissent le même rôle qu'une preuve d'authenticité traditionnelle, le législateur dispense la partie de faire en plus telle preuve distincte.
>
> [100] Ainsi, **l'article 7 *L.c.c.j.t.i.* ne crée pas de présomption d'intégrité du document, mais seulement une présomption que la technologie utilisée par son support *permet d'assurer son intégrité*, ce que j'ai appelé la fiabilité technologique**. La nuance vient du fait qu'une atteinte à l'intégrité du document peut provenir de différentes sources; on peut penser, à titre d'illustration, que l'information peut être altérée ou manipulée par une personne sans que la technologie soit en cause.
>
> [101] Les articles 2855 et 2874 C.c.Q. indiquent qu'une preuve d'authenticité distincte est requise dans le cas visé au troisième alinéa de l'article 5 *L.c.c.j.t.i*, c'est-à-dire dans le cas où le support ou la technologie ne permet ni d'affirmer ni de dénier que l'intégrité du document est assurée. [Nos soulignements][88]

Ainsi, malgré la règle générale qui exige en principe une preuve distincte de l'authenticité lors de la présentation de l'élément de preuve, la plupart des documents technologiques permettent cette preuve par la présence de métadonnées,[89] ce qui est suffisant comme l'affirme l'indique la Cour: « Autrement dit, la dispense de prouver l'authenticité du document s'applique lorsque le support ou la technologie employée permet de constater que l'intégrité du document est assurée. »[90] En ce qui a trait à la technologie qui nous intéresse, la question à se poser n'est donc pas si la chaîne de blocs est présumée fiable, mais plutôt si ce support peut assurer l'intégrité du document. Comme nous l'expliquons dans les paragraphes suivants, la chaîne de blocs permet effectivement d'assurer l'intégrité des documents qu'elle conserve.

---

[88] *Ibid*, aux para 99-101.

[89] Les métadonnées sont un « Ensemble structuré de données accompagnant un ouvrage et servant notamment à en décrire le contenu et le format, à assurer son indexation dans les moteurs de recherche et les bases de données, et à faciliter la gestion des droits d'auteur qui y sont liés. » Elles sont composées de plusieurs éléments, dont le « titre, auteur, éditeur, ISBN, sujet, description, date de parution, langue, droits d'auteur, format, type de document, etc. ». Office québécois de la langue française, « fiche terminologique : métadonnées », (2015), en ligne : *Office québécois de la langue française* < https://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=26541384 >.

[90] *Ibid*, au para 103

# BIBLIOGRAPHIE

## LÉGISLATION

*Code civil du Québec*, RLRQ c C-1991.

*Loi constitutionnelle de 1867* (R-U), 30 & 31 Vict, c 3, reproduite dans LRC 1985, annexe II, nº 5.

*Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, LQ 2021 c 25.

*Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, RLRQ c A-2.1.

*Loi sur l'administration fiscale*, RLRQ c A-6.002.

*Règlement sur l'administration fiscale*, RLRQ c A-6.002., r 1.

*Loi sur l'Agence du revenu du Québec*, RLRQ c A-7.003.

*Loi sur la fiscalité municipale*, RLRQ c F-2.1.

*Loi sur la protection des renseignements personnels et les documents électroniques*, LC 2000 c 5.

*Loi sur la protection des renseignements personnels dans le secteur privé*, RLRQ c P-39.1.

*Loi sur la taxe de vente du Québec*, RLRQ c T-0.1.

*Loi sur le régime de rentes du Québec*, RLRQ c R-9.

*Loi sur les entreprises de service monétaires*, RLRQ c E-12.000001.

*Loi sur les impôts*, RLRQ c I-3.

*Règlement sur les impôts*, RLRQ c I-3., r 1.

*Loi sur les normes du travail*, RLRQ c N-1.1.

## JURISPRUDENCE

*Benisty c Kloda*, 2018 QCCA 608.

*Chouquet c Fédération des Caisses Desjardins du Québec*, 2020 QCCAI 376.

*C.L. c BCF Avocats d'affaires*, 2016 QCCAI 114.

*Google Inc. c Agencia Espanola de Protección de Datos*, C131/12

*J.C. c SSQ, société d'assurances générales inc.*, 2017 QCCAI 129.

*R. c Cole*, 2012 CSC 53

*Segel c Centre de Services sociaux de Québec*, [1988] CAI 315.

*Sherman (Succession) c Donovan*, 2021 CSC 25.

*V.-P. c Commission de la santé et de la sécurité au travail*, 2013 QCCAI 205.

## DOCTRINE

### Revues de droit

Alexopoulos, Charalampos et al., « How Blockchain Technology Changes Governement: A Systematic Analysis of Applications » (2021) 8:1 International Journal of Public Administration in the Digital Age 1.

Barban, Patrick, « Études conjointes de rapports relatifs à la blockchain (I) : rapport d'information sur les « chaînes de blocs » (2019) 184 Banque & Droit 50.

Ben-Ishai, Stéphanie et al., « Eligible Non-Participation in Canadian Social Welfare Programs » (2019) 64:3 RD McGill 499.

Clavin, James et al., « Blockchains for Governement : Use Cases and Challenges » (2020) 1:3 Digital Governement: Research and Practice 22.

Charalampos, Alexopoulos et al., « How Blockchain Technology Changes Government: A Systemic Analysis of Applications » (2021) 8:1 Int J Public Administration in the Digital Age 1.

De Charentenay, Simon, « Blockchain et Droit : Code is deeply Law » (2017) 39 Gaz Pal 15.

De Vauplane, Hubert, « Blockchain and Conflict of Laws » (2018) 2017:4 RTDF 50.

Drillon, Sébastien, « La révolution Blockchain : La redéfinition des tiers de confiance » (2017) 2016:4 RTD Com 893.

Gabison, Garry, « Policy Considerations for the Blockchain Technology Public and Private Applications » (2016) 19 SMU Sci & Tech L Rev 327.

Gaon, Aviv et Ian Stedman, « A Call to Action: Moving Forward with the Governance of Artificial Intelligence in Canada » (2019) 56:4 Alta L Rev 1137.

Jiménez-Gómez, Briseida Sofia, « Risks of blockchain for data protection: A European approach » (2020) 36 Santa Clara High Tech L J 281.

Kim, Young Ran, « Blockchain Initiatives for Tax Administration » (2021) 4:69 UCLA L Rev 1.

Lacoursière, Marc et Ivan Tchotourian, « Métamorphose technologique et institutions financières » (2019) 60 C de D 737.

Mockle, Daniel, « La gouvernance publique et le droit » (2006) 47 C de D 89.

Moerel, Lokke, « Blockchain & Data Protection… and Why They Are Not On A Collision Course », (2019) 6 European Rev of Private Law 825.

Rivière, Jean-Maxime, « Blockchain technology and IP – investigating benefits and acceptance in governments and legislations », (2018) 3:1 Junior Management Science 1.

Teperdjian, Raffi, « The puzzle of squaring blockchain with the general data protection regulation », (2020) 60 Jurimetrics J 253.

Tsakiridi, Sandy, « Blockchain and the GDPR – friend or foes? », (2020) 20:3 Privacy & Data Protection Journals 4.

Young, Steven, « Changing governance models by applying blockchain computing », (2018) 26 Cath U J L & Tech 53.

## Journaux, fils de presse et autres sources de nouvelles

Bradley, Dave et al., « Bitcoin network may move beyond currency: The blockchain ledger behind digital money is poised to change the future of global document registration », *The Lawyers Weekly* (14 août 2015).

Bruno, Louis et al., « United States: The Data Privacy Block In The Chain: Blockchains And Immutability », *mondaq* (6 juin 2019).

Buell, Todd, « Tax Administrations Urged To Start Small With Blockchain », *Law360 Tax Authority* (25 février 2020).

Buell, Todd, « Blockchain Assessment Likely by 2022, EU Tax Official Says », *Law360 Tax Authority* (25 mai 2021).

Collosa, Alfredo, « How Global Tax Administrations are Using Blockchain Technology », *Bloomberg Tax* (17 mars 2022).

Lavallée, Eric, « Canada: Artificial Intelligence And Blockchains Are Vulnerable To Cyberattacks », *mondaq* (21 août 2018).

Lehot, Louis, « United States: The Fourth Industrial Revolution: Legal Issues Around Blockchain», *mondaq* (7 décembre 2020).

Pearce, Aaron, « Canada: The Disruptive Power Of Blockchain From A Legal Perspective: Part 1: The Ontario Land Registry System », *mondaq* (28 juin 2021).

Stinson, Derek, « UK: Blockchain And GDPR: Walking On Thin Ice », *mondaq* (8 février 2022).

Stinson, Derek, « UK: Blockchain: Data Protection And Privacy», *mondaq* (29 décembre 2021).

Tisdale, Kirsten, « Digitally enabled governments can be more efficient in delivering services », *The Globe and Mail* (15 février 2019).

Wegrzyn, Kathleen et Eugenia Wang, « United States : Types Of Blockchain: Public, Private, Or Something In Between », *mondaq* (20 août 2021).

## Monographies

Buffet, Guillaume et al., *Comprendre la blockchain: Anticiper le potentiel de disruption de la blockchain sur les organisations* , U change, 2016.

De Filippi, Primavera et Aaron Wright, *Blockchain and the law: the rule of code*, Cambridge (Mass), Harvard University Press, 2019.

Grinhaus, Aaron, *A practical guide to Smart Contracts and Blockchain Law*, Toronto, LexisNexis, 2019.

Politou, Eugenia et al, *Privacy and Data Protection Challenges in the Distributed Era*, Suisse, Springer, 2022.

## Thèses et dissertations

Dauverchain, Mathieu, *Le consentement dans le contexte du traitement de données personnelles sur les sites de réseautage social*, mémoire de maîtrise en droit, Université Laval et Université de Paris-Sud Orsay, 2018.

Moreira Moreno, José Miguel, *Blockchain and the right to be forgotten : A happy "marriage"*, mémoire de maîtrise en droit, Lund University, 2019.

Källman, Erik, *Blockchain v. Personal Data – A rising conflict Between Technology and the law*, mémoire de maîtrise en droit, Tilburg University, 2019.

## Ouvrages collectifs

Bouchard, Charlaine, « Introduction : Qu'est-ce que la chaîne de blocs? » dans Charlaine Bouchard, dir, *Comment la chaîne de blocs va transformer le droit*, Montréal, Yvon Blais, 2020, 1.

Cofone, Ignacio N., « Online harms and the right to be forgotten » dans Ignacio N. Cofone, dir, *The right to be forgotten : A Canadian and Comparative Perspective*, New York, Routledge Focus, 2020, 1.

d'Anglejan-Chatillon, Alix et al, «Canada» dans Michael S. Sackheim, dir, The Virtual Currency Regulation Review, 3eéd, Londres, The Law Reviews, 2020, 78.

De Filippi, Primavera, « Repenser le droit à l'ère numérique : entre la régulation technique et la gouvernance algorithmique » dans V Gautrais & P E Moyse, dir, *Droit et Machine*, Éditions Thémis, 2017.

Scassa, Teresa, « A little knowledge is a dangerous thing: Information asymmetries and the right to be forgotten » dans Ignacio N. Cofone, dir, *The right to be forgotten : A Canadian and Comparative Perspective*, New York, Routledge Focus, 2020, 1.

Corrales, Marcelo et Karim Djemame « A Brokering Framework For Assessing Legal Risks in Big Data and the Cloud » dans Marcelo Corrales et al, dir, *Perspective in law, Business and Innovation Technology, Big Data and the Law*, Singapoure, Springer Nature, 2017, 187.

Forgó, Nikolaus et al, « The Principle of Purpose Limitation and Big Data » dans Marcelo Corrales et al, dir, *Perspective in law, Business and Innovation Technology, Big Data and the Law*, Singapoure, Springer Nature, 2017, 17.

Forgó, Nikolaus et al, « The Collection of Electronic Evidence in Germany: A Spotlight on Recent Legal Developements and Court Rulings » dans Marcelo Corrales et al, dir, *Perspective in law, Business and Innovation Technology, Big Data and the Law*, Singapoure, Springer Nature, 2017, 251.

Walch, Angela « Deconstructing "Decentralization": Exploring the Core Claim of Crypto Systems » dans Chris Brummer, dir, *Cryptoassets: Legal, Regulatory, and Monetary Perspectives*, New York, Oxford University Press, 2019, 39.

Yuriko, Haga, « Right to be Forgotten: A New Privacy Right in the Era of the Internet » dans Marcelo Corrales et al, dir, *Perspective in law, Business and Innovation Technology, Big Data and the Law*, Singapoure, Springer Nature, 2017, 97.

## Documents gouvernementaux

Canada, Conseil des technologies de l'information et des communications, *Rallier un consensus canadien : L'évolution de notre écosystème de la blockchain*, par Rosina Hamoni, Faun Rice et Ryan McLaughlin, 2019, en ligne: < ictc-ctic.ca/wp-content/uploads/2020/03/canada-blockchain-ecosystem-2019-frv2.pdf >.

CE, European Parliamentary Research Service and Technology, *Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law*, (Étude) par Michèle Finck, Brussels, Directorate-General for Parliamentary Research Services of the Secretariat of the European Parliament, 2019.

Québec, *Journal des débats de la Commission des institutions*, 42-1, vol 45, n° 135 (14 avril 2021) (Éric Caire) en ligne : *Assemblée nationale du Québec* < assnat.qc.ca/fr/travaux-parlementaires/commissions/ci-42-1/journal-debats/CI-210414.html >.

## Documentation internationale

OCDE, Direction de la Gouvernance publique, *Blockchain Unchained: Blockchain Technology and its Use in the Public Sector* (2018).

## Documents et rapports institutionnels

Bourque, Gilles L. et Éric N. Duhaime « La révolution numérique au service du bien commun : La technologie de chaîne de blocs » (2020), en ligne (pdf) : *Institut de recherche en économie contemporaine* < irec.quebec/ressources/publications/Note_recherche_IREC_ChainesdeBlocs_GBourque_ENDuhaime_Avr2020.pdf >.

Blockchain Research Institute, New directions for government in the second era of the digital age,Toronto, 2021.

Commissariat au lobbying du Canada, « Évaluation des facteurs relatifs à la vie privée pour le système de gestion de l'information de la Direction des enquêtes (SGIDE) », (2022).

Comptables professionnels agréés du Canada, Technologies des registres distribués / chaîne de blocs: Perspectives, 2019.

Aylwin Antoine et Julie Uzan-Naulin « Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels annotée », chronique de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, (2021), en ligne : <https://www.fasken.com/fr/knowledge/projet-de-loi-64/2021/11/loi-sur-lacces-aux-documents-des-organismes-publics-et-sur-la-protection-des-renseignements >.

Gratton, Éloïse et al., « Préserver un équilibre délicat : renforcer la protection des rensiegnements personnels dans le secteur privé tout en favorisant l'innovation et en soutenant l'économie numérique au Québec » (2020).

Institut de gouvernance numérique, Registres distribués, l'évolution de la chaîne de blocs impacts, enjeux et potentiels pour le Québec, Québec, 2019

Zambrano, Raúl, « Libérer le potentiel révolutionnaire de la technologie des chaînes de blocs pour le développement humain », Centre de recherche pour le développement international, Ottawa, 2017.

## Sites web

Aylwin, Antoine et Julie Uzan-Naulin, « On répond à vos questions – Modernisation des lois sur la protection des rensignements personnels 1/3 » (9 février 2022), en ligne : *Lexology* < lexology.com/library/detail.aspx?g=c7595fea-c082-4752-8bc9-b5251b77ea7f >.

Bohan, Anne-Marie et Rory O'Keeffe « What is blockchain and what are the legal challenges » (9 mai 2022), en ligne : *Lexology* < lexology.com/library/detail.aspx?g=761d2d1c-1178-47d9-9e76-2af9c58b193e >.

Indochine Counsel Business Law Practitionners, « Blockchains or databases, a discussion » (6 decembre 2021), en ligne : *Lexology* < lexology.com/library/detail.aspx?g=553b273e-0405-43aa-9ec3-92c16a6c800f >.

Neely, Robert et Joshua Butler, « Blockchain for government: are we there yet? » (17 septembre 2018), en ligne : *Lexology* < lexology.com/library/detail.aspx?g=dda32653-cb70-4876-b00c-e36e611546d6 >.

Office québécois de la langue française, « fiche terminologique : fonction de hachage cryptographique », (2019), en ligne : *Office québécois de la langue française* < gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=8354257 >.

Office québécois de la langue française, « fiche terminologique : hachage », (2021), en ligne : *Office québécois de la langue française* < gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=8367404 >.

Office québécois de la langue française, « fiche terminologique : identifiant de bloc », (2018), en ligne : *Office québécois de la langue française* < gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=26545131 >.

Office québécois de la langue française, « fiche terminologique : mécanisme de validation », (2019), en ligne : *Office québécois de la langue française* < gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=26552609 >.

Office québécois de la langue française, « fiche terminologique : métadonnées », (2015), en ligne : *Office québécois de la langue française* < https://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=26541384 >.

Office québécois de la langue française, « fiche terminologique : noeud », (2018), en ligne : *Office québécois de la langue française* < gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=26544969 >.

Office québécois de la langue française, « fiche terminologique : preuve d'activité », (2019), en ligne : *Office québécois de la langue française* < gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=26552693 >.

Office québécois de la langue française, « fiche terminologique : preuve de capacité », (2019), en ligne : *Office québécois de la langue française* < gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=26556506 >.

Office québécois de la langue française, « fiche terminologique : preuve de travail », (2018), en ligne : *Office québécois de la langue française* < gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=26544976 >.

Office québécois de la langue française, « fiche terminologique : preuve d'enjeu », (2018), en ligne : *Office québécois de la langue française* < gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=26545011 >.

Office québécois de la langue française, « fiche terminologique : registre distribué », (2018), en ligne : *Office québécois de la langue française* < gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=26544126 >.

Roy, Guillaume, « À quoi ressemblera l'identité numérique des Québécois » (13 février 2022), en ligne : *leQuotidien* < lequotidien.com/2022/02/13/a-quoi-ressemblera-lidentite-numerique-des-quebecois-7aac7f3e6e8ccbaa7a778eaea513c006 >.

Wei, Dominic et Joshua Chu « Application of blockchain technology in healthcare and life science – AI handling of patient data – Blockchain and the future of legal services » (31 mars 2022), en ligne : *Lexology* < lexology.com/library/detail.aspx?g=cb368aa5-0b82-4bf6-8c19-d67a64704833 >.