INTRODUCTION

Dans la doctrine contemporaine, peut-être davantage dans les pays de *common law*, il est courant d'affirmer que le droit de la protection des renseignements personnels est à la croisée des chemins. Et face aux bouleversements technologiques que beaucoup considèrent comme étant, à juste titre, « révolutionnaires », il n'est d'autres choix que de changer le droit aussi. Suivant des degrés différents, plusieurs considèrent donc que **ce domaine en émergence, à l'instar du droit plus englobant qu'est le droit du cyberespace, est différent du droit traditionnel**[1]**. Le droit de la vie privée devrait par conséquent être au pire remanié, au mieux rebalancé**[2]**, certains principes étant désuets et d'autres sous-évalués**[3]**.**

Cette question sur le fait de savoir si à situation différente il importe d'apporter une solution différente est vieille comme le droit et se doit d'être traitée avec attention, pondération, retenue. Question que nous ne souhaitons pas considérer ici. En revanche, la doctrine à travers les âges a souvent mis de l'avant qu'il était de bon ton de trouver la solution qui était la moins dérangeante dans l'ordonnancement juridique qui bien souvent, comme dans le droit de la protection des renseignements personnels, a mis des siècles, des décennies à se matérialiser. Le droit est science de la réaction et gagne bien souvent à ne pas trop boule-

---

1 Laurence LESSIG, *Code and Other Laws of Cyberspace*, New-York, Basic Books, 2000. Frank EASTERBROOK, « Cyberspace and the Law of the Horse », (1996) *University of Chicago Legal Forum* 206 ; Laurence LESSIG, « The Law of The Horse – What Cyberlaw Might Teach », (1999) *Harvard Law Review* 501. Voir aussi David G. POST, « What Larry Doesn't Get : Code, Law, and Liberty in Cyberspace », (2000) 52 *Stan. L. Rev.* 1439, également en ligne : <http://cyber.law.harvard.edu/ilaw/Contract/Post_Full.html>. Vincent GAUTRAIS, « Libres propos sur le droit des affaires électroniques », (2006) *Lex Electronica*, en ligne : <http://www.lex-electronica.org/docs/articles_60.pdf>

2 Comme par exemple Daniel J. SOLOVE, *Understanding Privacy*, Cambridge et Londres, Harvard University Press, 2008.

3 Comme par exemple Andrew B. SERWIN, « Privacy 3.0 – The Principle of Proportionality », 2008, en ligne : <http://papers.ssrn.com/sol3/papers.cfm ?abstract_id=1089513>.

verser ce qui a mis du temps à grandir. Le doyen Cornu, sur la notion d'écrit électronique, avait eu cette parole pleine de sagesse selon laquelle :

> « Il serait préférable d'éviter la dénaturation inhérente à la fiction, lorsqu'un procédé plus neutre – et tout aussi ingénieux – permet d'obtenir un résultat équivalent.[4] »

Dans la même optique, le doyen Carbonnier considérait qu'il « fallait légiférer en tremblant ». C'est un peu selon cette approche que s'effectuera la présente analyse relativement à de nouveaux services de gouvernement en ligne.

Cela dit, et en l'absence de changements considérables de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*[5] et d'autres textes visant à protéger les renseignements personnels – notamment, à titre énonciatif et non limitatif – la *Loi concernant le cadre juridique des technologies de l'information*[6], la *Loi sur la Protection des renseignements personnels dans le secteur privé*[7] (L.R.Q. c. P-39.1), et la *Loi sur la protection des renseignements personnels et les documents électroniques*[8] (L.C. 2000, c. 5) – hormis les quelques changements assez ponctuels initiés en 2006[9] à la

---

4 Gérard CORNU, « L'imagination à bon droit ? », 2e conférence Albert-Mayrand, Montréal, Éditions Thémis, 1998, p. 15.

5 *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, L.R.Q., c. A-2.1, 2006, c. 22, en ligne : <http://canlii.org/fr/qc/legis/lois/lrq-c-a-2.1/derniere/lrq-c-a-2.1.html>.

6 *Loi concernant le cadre juridique des technologies de l'information,* L.R.Q.,c.C-1.1,enligne:<http://www.canlii.org///qc/legis/loi/c-1.1/20080818/tout.html>.

7 *Loi sur la Protection des renseignements personnels dans le secteur privé,* L.R.Q., c. P-39.1 en ligne : http ://www.canlii.org/fr/qc/legis/lois/lrq-c-p-39.1/derniere/lrq-c-p-39.1.html.

8 *Loi sur la protection des renseignements personnels et les documents électroniques* (plus connue sous l'acronyme PIPEDA), L.C. 2000, c. 5, en ligne : <http://www.canlii.ca/ca/loi/p-8.6/>.

9 *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, L.R.Q., c. A-2.1, 2006, c. 22. en ligne : <http://canlii.org/fr/qc/legis/lois/lrq-c-a-2.1/derniere/lrq-c-a-2.1.html>.

Loi sur l'accès – il est pourtant un constat à faire selon lequel de nouvelles questions se posent et il importe de concilier situations « nouvelles » et « vieux » droit.

Annonce des problématiques nouvelles

Nous le verrons dans la Partie préliminaire, que la tendance grandissante est que la perpétuation des services gouvernementaux d'une façon diligente et efficace exige de plus en plus une circulation[10] des renseignements personnels. De plus en plus souvent, émergent des situations selon lesquelles il est nécessaire – et non seulement utile – de se servir de ces derniers pour que le service soit tout simplement rendu. Le constat est simple : sans circulation, pas de service. Or, cette action de circulation est susceptible, au gré d'une interprétation par trop « rigoureuse » des lois sur la protection des renseignements personnels, de donner lieu à un encadrement que nous croyons passablement « lourd » quant au sens à donner à des termes tels que « **communiquer** », « **collecter** », « **transmettre** », « **détenir** », « **conserver** », « **utiliser** », etc. Bien sûr, nous le verrons dans la Partie 2, les lois sur la protection des renseignements personnels bénéficient d'une souplesse véritable. Néanmoins, les articles qui autorisent cette dernière sont souvent – ou parfois – difficiles à mettre en place ; mais également ils sont surtout inutiles dans la mesure où nous croyons qu'en plusieurs circonstances, ces hypothèses de protection par le droit ne sont pas réunies.

En ce qui a trait à la présente analyse, nous allons baser notre recherche sur trois situations différentes, représentant des niveaux d'intégration des technologies plus ou moins complexe, plus ou moins facile à interpréter quant à la réalisation des actions (telles que « communication », « collecte », « utilisation », etc.) encadrées par le droit.

La **première**, est celle où des renseignements personnels sont véhiculés de serveur à serveur, sous la responsabilité de ministè-

---

[10] Sur la notion de « circulation » telle que nous l'envisageons dans la présente étude, voir *Infra*, Partie préliminaire, Chapitre 1, Section 1, 1, B.

res ou organismes distincts, avec l'unique finalité d'identifier le citoyen qui veut accéder à un service exigeant ce niveau de sécurité[11]. Dans une telle situation, il est loisible de se demander si certaines opérations donnent lieu notamment à une « communication », à une « collecte », à une « utilisation », et par le fait même, à l'armada de mesures que les lois requièrent pour pareilles actions.

Une **deuxième** hypothèse correspond à celle où, toujours pour des fins de permettre l'accomplissement d'un service au bénéfice de l'usager, un ministère ou organisme garde pour ce dernier des renseignements personnels le concernant. Par exemple, dans le quotidien des professeurs d'université au Canada, le réseau du CV Commun Canadien permet de conserver pour eux les renseignements qu'ils incluent dans leur curriculum vitae[12]. En pareille hypothèse, il importera de déterminer si une telle opération est consécutive de « communication », de « collecte », de « conservation », de « détention », d' « utilisation », etc.

Enfin, et ce sera notre **troisième** et dernier exemple, nous envisagerons l'hypothèse selon laquelle un organisme public entend favoriser l'hypothèse où des dépôts d'information, contenant potentiellement des renseignements personnels, seront effectués non pas par les organismes gérant un site mais par les usagers eux-mêmes. Plus précisément, nous considérons la situation selon laquelle un organisme visant à la promotion du tourisme d'une ville, d'une région, province ou pays incite les usagers intéressés à le faire à déposer des « témoignages » qui pourraient se traduire par la mise en ligne de textes, images, vidéos[13]. Aussi, et à supposer que certains de ces dépôts contiennent des renseignements personnels, du « déposant » ou d'autrui, il importera de déterminer si l'on est face à une « communication », « collecte », « conservation », « détention », « utilisation », etc., nécessitant l'intervention du droit.

---

11 *Infra*, Partie préliminaire, Chapitre 1, Section 1, 2, A.

12 *Infra*, Partie préliminaire, Chapitre 1, Section 1, 2, B.

13 *Infra*, Partie préliminaire, Chapitre 1, Section 1, 2, C.

Annonce de plan

Aussi, et afin de répondre à ces interrogations, nous commencerons notre étude en tentant de mettre sur table à la fois l'état des changements opérés par ceux-ci ainsi que les conséquences sur le droit applicable dans les circonstances. Et dans des développements préliminaires, nous tenterons de montrer que malgré les changements révolutionnaires imposés par la généralisation de l'« électronisation » des communications, le droit dispose d'une certaine dose de souplesse qui, en l'état actuel des choses nous apparaît tout à fait supportable par le droit positif (**Partie préliminaire**).

Cette souplesse du droit est d'abord et avant tout rendue possible grâce à l'interprétation juridique, qui, par essence, permet d'adapter le droit aux faits. Or, les nouvelles circonstances que nous décrirons dans la partie préliminaire doivent donner lieu à un changement dans la façon d'aborder les opérations de circulation des renseignements personnels précités dans l'annonce des problématiques nouvelles. Aussi, nous nous emploierons à développer l'interprétation qui est la plus en phase avec la mise en place de ces nouveaux services gouvernementaux en ligne et qui en bien des cas ne nécessite pas une lecture trop littérale des textes de lois (**Partie 1**).

Enfin, et toujours dans cette quête d'identification des éléments de souplesse disponibles dans les lois existantes afin de s'assurer que les services gouvernementaux soient en conformité au droit, sans avoir besoin de changer ce droit, nous développerons quelques propos sur les principales autorisations de circulation qui sont offertes dans les lois sur la protection des renseignements personnels. En revanche, si ces autorisations sont nombreuses, certaines sont difficiles à utiliser ou doivent l'être avec une relative parcimonie afin de ne pas dénaturer les fondements qui sont à leur origine (**Partie 2**).

Partie préliminaire

Changements relatifs à la circulation des RP

Nous sommes face à une révolution. Une révolution de l'ampleur de laquelle nous n'avons peut-être pas totalement conscience,[14] tant le phénomène est à la fois récent, à savoir le début des années 1990, et fondamental de par la profondeur des changements opérés, sans doute à cause de son caractère irrévocable également.

Pourtant les juristes jouent encore souvent le rôle d'un « Astérix gaulois » qui fait de la résistance dans l'analyse des faits et qui trouvent donc que le droit en a vu d'autres.

> « It seems passé today to speak of "the Internet revolution". In some academic circles, it is positively naïve. But it should not be. The change brought about by the networked information environment is deep. It is structural. It goes to the very foundations of how liberal markets and liberal democracies have coevolved for almost two centuries. »[15]

Souvent aussi, il est dit que le droit est un formidable outil d'adaptation aux faits. Certes. Si cela n'est pas faux, nous croyons pourtant qu'il s'agit de deux phénomènes qu'il importe de bien distinguer. Aussi, à la révolution des faits, il importe d'analyser le droit qui tente de les encadrer avec la retenue qui s'impose. Le droit dispose en effet de cette capacité de souplesse qui lui permet de passer outre les changements[16].

D'ailleurs, c'est exactement ce que nous constatons dans le cas précis qui nous intéresse : si les services de gouvernement en ligne ont besoin, pour que lesdits services puissent être donnés, qu'une certaine circulation des renseignements personnels soit assurée, il est selon nous assez clair que le droit permette d'opérer la transition du monde du papier au monde de l'électronique. En d'autres mots, de plus en plus de ces services gouvernemen-

---

14 Voir Michel SERRES, « Les nouvelles technologies : révolution culturelle et cognitive », conférence en ligne : <http://interstices.info/jcms/c_33030/les-nouvelles-technologies-revolution-culturelle-et-cognitive>.

15 Yochai BENKLER, *The Wealth of Networks – How Social Production Transforms Markets and Freedom*, New Haven et London, Yale University Press, 2006, p. 1.

16 Voir par exemple Frank EASTERBROOK, « Cyberspace and the Law of the Horse », (1996) *University of Chicago Legal Forum* 206.

taux – que nous appelons des « prestations en ligne »[17] (ci-après « PEL ») –, vont nécessiter une circulation des renseignements personnels. Aussi, le présent propos entend démontrer que l'analyse des différents outils juridiques (lois – jurisprudence – contrat) montre que certains d'entre eux – plus que d'autres – permettent d'opérer une transition harmonieuse entre le vieux droit et la nouvelle réalité. C'est donc cette révolution des faits (Chapitre 1) face à l'évolution du droit (Chapitre 2), que nous souhaitons traiter dans cette partie préliminaire.

[17] Cette notion de « prestations en ligne » est le terme utilisé tout au long de la présente étude pour identifier ce nouveau type de services gouvernementaux.

CHAPITRE 1
CHANGEMENTS FACTUELS RELATIFS À LA CIRCULATION DES RP : ILLUSTRATION D'UNE « RÉVOLUTION »

Aussi, face à l'importance des changements qui sont opérés par les « nouvelles » technologies, il importe au départ de partir des faits en décrivant, d'une part, ce qu'ils sont (Section 1) et, d'autre part, en identifiant les changements qui les caractérisent (Section 2).

SECTION 1 – ÉTATS DES LIEUX RELATIF À LA CIRCULATION DES PRESTATIONS EN LIGNE (PEL)

En bons juristes, ces faits vont d'abord nécessiter des définitions permettant de bien jauger l'ampleur du phénomène (1). Mais une partie de la difficulté d'analyse tient aussi au fait que les prestations en ligne peuvent prendre des formes particulièrement variées qu'il importe d'illustrer par quelques exemples (2).

1 – Définitions autour de la circulation des PEL

Commençons par les définitions. Les « prestations en ligne », qui constituent l'appellation que nous allons utiliser durant l'ensemble de nos travaux, méritent par conséquent une définition (A) qu'il importera de développer quelques lignes, en mettant l'accent sur le terme « circulation » qui ne jouit pas non plus d'une définition tout à fait unanime, tant du côté des juristes que des technologues ou des gestionnaires (2).

A – Définitions de PEL

Dans le cadre de cette quête définitionnelle de ce que sont les prestations en ligne offertes par les administrations publiques, il est d'abord un constat que nous voudrions proposer et ensuite identifier deux conséquences qui en découlent.

Relativement au constat, ces nouvelles façons de faire imposent une nouvelle vision : un **réseau** ne se gère pas comme une organisation en **silo** ; davantage, les organisations publiques proposent désormais des services où les renseignements personnels des citoyens n'ont plus le caractère **statique** d'antan. On est donc, par exemple, bien loin du ficher médical géré dans l'officine du médecin ou du fichier, où la protection de renseignements personnels sensibles passait par une « immobilisation » des données à un endroit unique sous le contrôle exclusif du gestionnaire des renseignements personnels.

Kenneth Kernaghan et Justin Gunraj soutiennent que l'adoption croissante par les administrations gouvernementales des technologies de l'information prédispose les organismes publics à changer leurs structures et leurs modes de gestion[18].

Un premier facteur de changement induit par les technologies de l'information est la pression engendrée par les lourds investissements et le mouvement conséquent pour une coopération plus intensive entre les organismes gouvernementaux. Par exemple, la sécurité coûte cher et il n'est pas anormal, dans le cadre d'une gestion saine des deniers publics, que ces derniers impartissent certains de leurs services soit à des tiers privés soit à des entités publiques spécialisées dans un service donné, qui vont gérer à l'occasion d'importantes quantités d'informations confidentielles.

Un second facteur favorisant cette distance d'avec le caractère statique des renseignements personnels tient au besoin accru d'expertise, de même que des capacités accrues de partager l'information. Cela porte à la création d'entités non ministérielles donnant lieu, au Canada, à la création d'« agences » se présentant comme des structures qui possèderaient des caractéristiques plus adaptées à l'accomplissement de fonctions horizontales.

Un troisième facteur de changement tient au déplacement d'une partie du niveau intermédiaire de gestion au profit d'une

---

[18] Kenneth KERNAGHAN and Justin GUNRAJ, « Integrating information technology into public administration : Conceptual and practical considerations, » (2004) 47 *Canadian Public Administration*, 525-546.

certaine « horizontalisation » de la hiérarchie administrative, de l'autorité et des contrôles. Conjugué avec l'accentuation des possibilités de dialogue direct avec les administrés, ce facteur induit des remises en cause des approches sur lesquelles se fondent les mécanismes de protection des renseignements personnels détenus par l'administration gouvernementale.

La généralisation des plates-formes de partage d'informations met à la portée des usagers et des administrations un ensemble de possibilités d'échange d'informations. Les internautes, citoyens, gestionnaires et agents de l'État sont en mesure de communiquer, partager et échanger des informations. Compte tenu de ce contexte, le cadre juridique relatif à l'information qui est nécessairement en possession de l'administration, devrait s'attacher à en régir les conditions d'accès par chaque agent de l'État plutôt que d'en interdire la circulation. Dans un État en réseau, l'enjeu n'est plus tellement de savoir si une information peut ou non être en possession de l'Administration mais plutôt si cette dernière a le droit d'y accéder et d'en faire usage pour prendre une décision dans une situation spécifique.

Les interactions dans le contexte des réseaux informatiques requièrent des modalités différentes de gestion des informations. Les administrations fonctionnant de plus en plus suivant une logique de réseau, les informations sont essentiellement circulantes, disponibles au moment où elles doivent l'être pour accomplir une prestation de service. Ces conditions de circulation accrue des informations nécessitent aussi des précautions car les potentialités d'accumulation et de couplage des informations sont plus considérables.

Cet état de fait nous entraîne à considérer deux conséquences directes. D'abord, la gestion de prestations en ligne amène à considérer ces services de manière globale, dans le sens où c'est par le biais d'un regard pluridisciplinaire impliquant à la fois l'œil d'un gestionnaire, d'un technologue et d'un juriste. Toujours selon cette approche globale, il importe de gérer l'information, et *a fortiori* les renseignements personnels, durant l'ensemble de leur « cycle de vie ». Ce concept neuf, ne provenant pas à l'origine du droit, a pourtant été inséré dans la *Loi concernant le cadre juri-*

dique des technologies de l'information relativement au maintien de l'intégrité[19]. Dans le cas qui nous intéresse, il peut assurément être utilisé pour bien montrer que la gestion des renseignements personnels est un processus qui concerne tant la gestion du site Internet in stricto sensu où ces derniers sont insérés – comprenons par là sa gestion technique – que derrière, là où ils sont accueillis, conservés, rendus accessibles suite à une demande d'accès, et éventuellement détruits.

Ensuite, et en raison même de la multiplication des interactions dans les réseaux, il est plus que jamais nécessaire de bien caractériser, au plan du droit, les situations juridiques impliquant un traitement d'information. C'est dans une telle perspective que la notion de « prestations en ligne » et le cadre juridique devant encadrer ces services prend tant d'importance.

Les prestations en ligne au sein d'un réseau se présentent comme des processus assurant des prestations pouvant concerner une pluralité d'entités, de ministères ou organismes publics. Ce sont des services qui, au sein d'un réseau procurent des interfaces de même que diverses fonctions afin de soutenir les échanges et partages d'informations.

Les prestations en ligne constituent la couche de services qui permettent de mettre en relation les citoyens et les diverses entités de l'Administration. Pour des motifs historiques et même en raison d'une certaine hésitation à généraliser le partage systématique d'informations, notamment les renseignements personnels, les principaux dépositaires d'informations au sein de l'appareil gouvernemental demeurent les ministères sectoriels ou les organismes publics disposant de grands répertoires de renseignements personnels. Les prestations en ligne viennent procurer des passerelles afin d'assurer la disponibilité d'informations adéquates à leur réalisation pour le bénéfice des « citoyens-usagers ».

Ces passerelles que constituent les prestations en ligne se présentent alors avec les caractéristiques des interfaces et des infrastructures de réseaux. Certaines supposent l'exercice de

[19] *Infra*, voir les développements sous la notion de « circulation ».

contrôles très intenses sur les informations traitées tandis que d'autres sont structurées comme des services de prestations intermédiaires, assurant le traitement des informations par l'usager lui-même ou encore à titre d'hébergeur, dépositaire ou simple transporteur. Il importe que le cadre juridique de la protection des renseignements personnels rende compte de cette importante évolution.

B – Définitions de « circulation »

Cette « nouvelle » administration électronique suppose la circulation accrue d'informations. La circulation de l'information se présente comme une donnée majeure du contexte dans lequel se déploie le gouvernement en ligne. L'information qui circule est de l'information qui se déplace, qui va d'un lieu à l'autre. Et de fait, l'avènement des services en ligne nécessite la circulation accrue de l'information. La circulation et le partage des informations permettent d'améliorer la qualité et la célérité des prestations.

La circulation de l'information concerne les multiples interactions qui caractérisent désormais la réalisation des interactions au sein des réseaux de communication. On a vu, au cours de la décennie 1990 se développer une tendance à postuler que le fait que l'information demeure au sein d'un organisme, ne circule pas, constitue un atout pour la protection de la vie privée. La circulation des renseignements personnels serait forcément suspectée de mettre en péril le droit des personnes à la confidentialité des renseignements personnels. Selon une certaine conception, les renseignements personnels doivent demeurer associés à l'établissement entendu comme lieu physique. Une telle conception s'accommode mal des tendances majeures découlant de la généralisation des environnements en réseaux. Le défi que posent ces environnements est celui de garantir la protection dans un contexte où les renseignements circulent. Un système de protection des renseignements personnels qui compterait sur le maintien de méthodes relevant d'un contexte technologique révolu pour assurer la protection de la vie privée des personnes est susceptible de se voir complètement dépassé

par les évolutions qui modifient les conditions de la gestion de l'information[20].

Lorsque l'information circule, elle passe d'un lieu à l'autre. Ces passages d'un lieu à l'autre s'effectuent selon des phases différentes. Mais dans le processus de circulation, l'information peut venir en possession d'une entité, voire d'une personne sans être connue de celles-ci. C'est que la circulation de l'information nécessite qu'elle passe entre les mains d'entités qui n'ont que la charge de l'acheminer ou de l'entreposer dans le cadre d'un processus d'acheminement. **Dans un réseau, l'information qui circule n'est pas nécessairement sous l'entier contrôle de l'entité qui se trouve à avoir la possession physique du support.**

La circulation de l'information se présente comme un processus au cours duquel l'information passe entre diverses mains. Ce processus doit être sécurisé de bout en bout, durant tout son « cycle de vie », expression qui a notamment été adoubée par la *Loi concernant le cadre juridique des technologies de l'information*[21]. Mais au plan du degré de maîtrise juridique, du contrôle de l'information, la circulation comporte des épisodes différents. Typiquement, une information est créée, puis transmise à une autre personne qui en reçoit communication. La circulation de l'information s'effectuera selon des phases au cours desquelles on peut reconnaître la transmission *via* un transmetteur, l'entreposage dans un répertoire mettant le message à la disposition de son destinataire et enfin, la communication au destinataire, lorsque celui-ci prend contrôle et connaissance du message.

---

[20] Pierre TRUDEL, *Améliorer la protection de la vie privée dans l'administration électronique : pistes afin d'ajuster le droit aux réalités de l'État en réseau*, Étude réalisée à la demande du Ministère des relations avec les citoyens et de l'immigration du Québec, Mars 2003, en ligne : <http://www.institutions-democratiques.gouv.qc.ca/acces-information/archives_en.htm>.

[21] *Loi concernant le cadre juridique des technologies de l'information*, L.R.Q., c. C-1.1, en ligne : <http://www.canlii.org///qc/legis/loi/c-1.1/20080818/tout.html>. La notion de « cycle de vie » est notamment utilisée aux articles 6, 12, 17, 46, 56, 64, 76.

Les prestations en ligne qui se développent dans la plupart des administrations publiques supposent le déploiement de services en ligne emblématiques des modes de circulation de l'information qui émergent désormais au sein des réseaux.

Notons à cet égard qu'il n'y a pas d'opposition entre circulation, mouvement de l'information et protection des renseignements personnels. Au contraire, c'est en constatant la nécessité de la faire circuler que des garanties sont apparues dans les lois[22]. François Rigaux évoquait même le fait que la circulation est la raison pour laquelle les lois ont été faites, et notamment la directive européenne sur la protection des renseignements personnels :

> « La nécessité de tenir en équilibre **deux intérêts divergents**, sans qu'aucun ne puisse, en principe, être sacrifié à l'autre, apparaît dans l'intitulé de la directive 95/46/CE du Parlement et Conseil des Communautés européennes du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.[23] » (nos soulignements)

---

[22] François RIGAUX, en ligne : <http://www.asmp.fr/travaux/gpw/internetvieprivee/rapport2/chapitr8.pdf> : « Les politiques législatives nationales tendent à la protection de la population de l'État à l'égard des traitements (automatisés ou non) de données à caractère personnel. La transnationalisation et la délocalisation de l'outil informatique, la facilité avec laquelle les données passent les frontières ont très tôt fait apparaître la nécessité de soumettre les États à des normes communes. »

[23] François RIGAUX, <http://www.asmp.fr/travaux/gpw/internetvieprivee/rapport2/chapitr8.pdf>. Une même perspective existe dans la *Loi fédérale sur la protection des renseignements personnels et les documents électroniques* (plus connue sous l'acronyme PIPEDA), L.C. 2000, c. 5, en ligne : <http://www.canlii.ca/ca/loi/p-8.6/>, où à l'article 3, on peut lire ceci : « 3. La présente partie a pour objet de fixer, dans une ère où la technologie facilite de plus en plus la circulation et l'échange de renseignements, des règles régissant la collecte, l'utilisation et la communication de renseignements personnels d'une manière qui tient compte du droit des individus à la vie privée à l'égard des renseignements personnels qui les concernent et du besoin des organisations de recueillir, d'utiliser ou de communiquer des renseignements personnels à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances. »

Ainsi, cette notion de « circulation » traduira dans la présente étude une double valeur : celle du « mouvement » de l'information tel que nous venons de le voir. Elle correspondra aussi à un terme volontairement englobant qui inclura des actions qui sont encadrées dans le cadre des différentes lois sur la protection des renseignements personnels tel que « transmission », « communication », « collecte », « utilisation », « conservation », etc. Et que nous devrons de définir plus tard[24].

2 – Illustrations relatives à ce changement

Ces différentes opérations liées à de « nouveaux services », que nous avons appelés des prestations en ligne, peuvent se matérialiser de bien des manières. Afin de présenter une vision assez fidèle de la situation, il est trois situations que nous aimerions présenter ici dans le cadre de ce paragraphe faisant état de la situation. En premier lieu, il est des services qui, pour des fins de sécurité, vont opérer des transferts de renseignements personnels pour s'assurer qu'une personne « X » soit bien celle qu'elle prétend être (A). Autre exemple, plusieurs services gouvernementaux offrent déjà la possibilité pour les usagers de « stocker » de l'information sur les serveurs des ministères et organismes, et ce, sans que ces derniers n'aient un contrôle direct sur le contenu ainsi gardé (B). Enfin, et dans une perspective très « web 2.0 » qui semble être vouée à un avenir très prometteur, le tout avec un degré supplémentaire d'innovation, il existe la possibilité pour les ministères et organismes de laisser aux citoyens de l'espace disponible pour « stocker » de l'information mais, de surcroît, cette information sera publiée et accessible à tout un chacun. Il s'agit donc bien là de contenu généré par les individus eux-mêmes, pour d'autres individus, et avec le rôle sinon passif, mais « non interventionniste » de l'État (C).

[24] *Infra*, Partie 1.

A – PEL et circulation de RP pour des fins d'identification

i) État de la situation factuelle

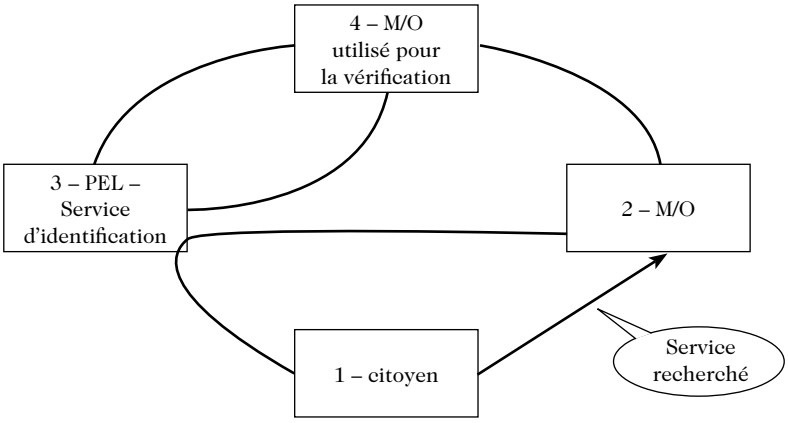
Notre première illustration correspond à une situation factuelle fictive mais qui risque de se développer grandement dans le futur : afin de rendre un service donné au citoyen, un ministère ou organisme demande au premier de s'identifier.

Conformément à un processus de sécurité bien légitime, mais également requis par le droit[25], le citoyen, bénéficiaire du service, s'exécute. Pour ce faire, l'organisme public concerné va demander à une identité indépendante, privée ou publique, qui correspond à ce que nous appelons un « service commun », de procéder à l'identification du citoyen. Ce processus va notamment s'effectuer en comparant les renseignements personnels du citoyen avec ceux qui existaient préalablement dans une autre banque de données gouvernementale « appartenant » à un autre organisme public. Ainsi, pour une simple opération de vérification d'identité, quatre intervenants sont requis : le citoyen **(1)** ; le ministère ou organisme (M/O) qui rend le service **(2)**, le « prestataire en ligne » (PEL) **(3)** et le ministère ou organisme (M/O) qui est responsable de la banque de données avec laquelle on va vérifier la véracité desdits renseignements personnels **(4)**.

---

[25] *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, L.R.Q., c. A-2.1, 2006, c. 22. en ligne : <http://canlii.org/fr/qc/legis/lois/lrq-c-a-2.1/derniere/lrq-c-a-2.1.html> et Art. 7 (3) à 7(3) i) de la *Loi sur la protection des renseignements personnels et les documents électroniques* (plus connue sous l'acronyme PIPEDA), L.C. 2000, c. 5, en ligne : <http://www.canlii.ca/fr/ca/legis/lois/lc-2000-c-5/derniere/lc-2000-c-5.html>.

Schéma 1



Sans être totalement limpide, il s'agit donc de la situation par laquelle un ministère qui pour assurer un service de sécurité à un citoyen, demande à un tiers de l'aider, tiers qui assure cette fonction en vérifiant l'identité de la personne concernée auprès d'une banque de données détenue par un autre ministère.

ii) État des conséquences sur le traitement juridique à y apporter

Mais cette simplicité relative n'est rien dès lors que l'on souhaite apporter à cette situation un traitement juridique rigoriste qui de surcroît est, selon nous, et comme nous le verrons dans les deux parties subséquentes, faux et préjudiciable.

Dans le cadre d'une première étape, le citoyen contacte le service d'identification pour s'identifier et celui-ci lui demande de consentir à ce que le ministère utilisé pour la vérification lui communique les renseignements personnels du citoyen – et ce en fonction d'une interprétation de l'article 59 de la *Loi sur l'accès*[26]. Suite à ce consentement, en deuxième lieu, la communication peut avoir lieu. Ces deux premières étapes sont généralement

[26] *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, L.R.Q., c. A-2.1, 2006, c. 22. en ligne : <http://canlii.org/fr/qc/legis/lois/lrq-c-a-2.1/derniere/lrq-c-a-2.1.html>.

nécessaires pour que l'usager puisse avoir un numéro d'identification. En troisième lieu, cette opération de consentement doit être faite une deuxième fois afin de s'assurer cette fois que le citoyen qui dispose d'un numéro d'identification est le bon. Ainsi, il pourra vérifier si le dossier qui est ouvert correspond bien à sa propre personne. Ensuite, et comme dans la plupart des sites Internet, en cinquième lieu, le citoyen doit consentir à des conditions d'utilisation de la plate-forme. En sixième lieu, un autre consentement (le quatrième) peut être requis pour que la communication entre le ministère opérant la vérification soit effectuée envers le ministère qui propose le service. Suite à ce consentement, en septième lieu, la communication peut avoir lieu. Le droit en général, et le contrat en particulier, qui peut donc être vu comme un outil facilitateur[27], perd cette finalité utilitaire en rendant au contraire le consentement diffus. L'usager, qui risque de ne pas toujours comprendre l'ensemble du processus, pourra légitimement se demander à quoi il consent vraiment.

Car, à bien y penser, plusieurs des étapes où les organisations publiques, dans un souci de respect du droit, deux fois plutôt qu'une, ne devraient pas être interprétées comme étant des opérations assujetties au contrôle des lois sur la protection des renseignements personnels. Davantage, et comme nous le verrons plus tard, à plusieurs reprises dans cette première illustration, la transmission d'information correspond davantage à une demande d'accès que l'usager, en contrôle des informations en cause, demande à un ministère ou organisme afin de bénéficier d'un service[28].

B – PEL et garde de RP : l'exemple des CV des professeurs d'université

i) État de la situation factuelle

Une autre situation, plus simple cette fois, peut également être trouvée dans l'hypothèse où un ministère et organisme offre

---

[27] Clare DALTON, « An Essay in the Deconstruction of Contract Doctrine », (1985) 94 *Yale Law Journal* 999.

[28] *Infra*, Partie 1.

aux citoyens ou à des particuliers de tous genres, un espace privé afin de permettre la satisfaction d'un service donné. Par exemple, les professeurs d'université du Canada disposent de la capacité de mettre leur *curriculum vitae* en ligne, et ce, dans l'objectif, d'une part, d'avoir une version en ligne qui puisse être facilement disponible pour des demandes de subvention futures et, d'autre part, afin de faciliter la visibilité des chercheurs. L'on peut notamment référer au site du FQRSC[29] ou au CV commun canadien[30].

ii) État des conséquences sur le traitement juridique à y apporter

Or, que ce soit pour les versions en ligne ou pour celles qui sont temporaires et non encore publiées, de certains de se demander si une telle opération est une collecte au regard des lois sur la protection des renseignements personnels[31]. En effet, en ce qui concerne le CV commun canadien, le contrat d'adhésion spécifie que l'organisme se contente d'héberger sur ses serveurs ces informations qui pourraient être physiquement vues comme des renseignements, assurément personnels, que l'organisme détient sous son contrôle et sa responsabilité, ne serait-ce qu'au niveau de l'accès à l'information :

> « Le système CVC utilise un logiciel qui surveille la transmission des données sur le réseau pour déceler toute tentative non autorisée de télécharger ou de modifier des renseignements ou de causer d'autres dommages. ….
>
> Ceux qui accèdent au système sans autorisation, ou qui abusent de leur autorité pour accéder à des renseignements personnels sans raison valable, sont exposés à une poursuite légale.

---

29 Fonds Québécois de Recherche sur la Société et la Culture en ligne : <http://www.fqrsc.gouv.qc.ca>.

30 Le CV commun canadien est en ligne : <http://www.commoncv.net/index_f.html>.

31 *Infra*, Partie 1, Chapitre 2, Section 2.

> Vos renseignements personnels sont à l'abri de l'accès, de l'utilisation ou de la révélation non autorisée. Le système CVC sauvegarde vos renseignements personnels sur des ordinateurs placés dans un environnement sécure et avec accès contrôlé pour protéger contre l'accès, l'utilisation ou la révélation non autorisée. Toutes les données circulant entre le CVC et le matériel informatique des utilisateurs finaux, ou entre le CVC et le matériel informatique des organismes membres, sont encodées avec des technologies d'encryptage de 128 bits et sont transmises à l'aide du protocole SSL (Secure Socket Layer) »[32]

Un autre exemple, tout aussi illustratif d'une communication volontaire à un organisme public de renseignements personnels en dehors de toute obligation légale, mais où la possibilité de collecte est plus explicite, serait le cas du site du Fonds québécois de la recherche sur la nature et les technologies (FQRNT) qui mentionne, dans sa politique de confidentialité, que :

> « Si vous nous communiquez volontairement des renseignements personnels, par courriel ou au moyen d'un formulaire électronique, nous n'utiliserons que l'information requise pour permettre au personnel du Fonds de répondre à votre message ou de donner suite à votre demande. La correspondance électronique est traitée avec les mêmes mesures de confidentialité que les documents écrits.
>
> En conformité avec la **Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels**, si nous procédons à une collecte de renseignements personnels auprès de vous, vous serez informé :
>
> - De notre nom et de notre adresse ;
> - De l'usage auquel ce renseignement est destiné ;

[32] Le contrat d'adhésion au site du CV commun canadien en ligne : <https ://www.ccv-cvc.ca/pls/c3/c3.startup ?pLANGUAGE=2>.

- Des catégories de personnes qui auront accès à ce renseignement ;
- Du caractère obligatoire ou facultatif de la demande ;
- Des conséquences d'un refus de répondre à la demande ;
- Des droits d'accès et de rectification des renseignements prévus à la Loi. »[33]

On s'entend pourtant, que le service fourni tant par le Fonds québécois de la recherche sur la nature et les technologies que par le CV commun canadien n'est aucunement obligatoire et n'est aucunement requis par l'État pour sa bonne marche. Simplement, il s'agit d'un outil disponible relativement à une activité que le gouvernement en ligne souhaite soit valoriser, soit rendre plus visible. Il n'en demeure pas moins que la majorité de ces informations sont une nouvelle fois sous le contrôle de l'usager qui peut même les effacer presque totalement. Aussi, il est difficile de croire que cette capacité de contrôle distincte de celle, plus classique, que l'on peut trouver dans l'hypothèse d'un ministère gérant des renseignements personnels, ne puisse pas avoir une incidence sur la manière de comprendre le droit.

C – PEL et publication de RP : Exemple de site web 2.0 de promotion touristique

i) État de la situation factuelle

Enfin, la troisième situation que nous voulons présenter ici comme étant une bonne illustration de la nécessaire circulation de renseignements personnels tient là encore à une tendance selon laquelle le gouvernement en ligne entend mettre à contribution les usagers, les citoyens, en mettant en place des plates-formes où leurs avis pourront être entendus et lus par tout un chacun. Ainsi, et dans la lignée directe de ce qui se fait déjà sur ce

[33] La politique de confidentialité du site du Fonds québécois de la recherche sur la nature et les technologies (FQRNT) en ligne : <http://www.fqrnt.gouv.qc.ca/>.

que l'on appelle les réseaux sociaux (tels que *Facebook* – *MySpace* – *Youtube* – *Dailymotion* – voire aussi *Amazon* – etc.), il est tout à fait envisageable de voir, relativement à certaines priorités ciblées par un gouvernement, la mise en avant d'une structure où les citoyens seraient incités à « verser » du contenu volontairement au bénéfice du plus grand nombre. C'est par exemple, et conformément à l'annonce précitée, la tangente qu'entend suivre *Tourisme Québec* qui, fort justement, croit que les meilleurs « promoteurs » du Québec à l'étranger sont les québécois eux-mêmes[34].

Aussi, et en dépit d'une modération qui semble de mise en pareil cas[35], qu'elle soit faite *a posteriori* ou *a priori*, le site entend laisser un certain « espace de liberté » aux usagers, liberté certes encadrée mais inéluctable et qui aura sans aucun doute des incidences sur le plan de l'analyse juridique.

Au-delà de cet exemple en devenir, nous pourrons également étayer nos perspectives en regardant ce qui se fait ailleurs. En effet, les illustrations de sites gouvernementaux favorisant la promotion du tourisme sont légion, surtout, comme dans notre cas,

---

[34] Communiqué du Ministère du Tourisme du 17 novembre 2008 , « Concours Destination Québec- Le ministère du Tourisme lance un audacieux concours sur le Web 2.0 », en ligne : <http://www.bonjourquebec.com/mto/medias/communiques_pub/communique.asp ?no_comm=781&langue=francais&tri=date_comm&page=0> évoquait les éléments suivants : « Toujours à l'affût des nouvelles tendances en matière de marketing électronique, le ministère du Tourisme s'est lancé il y a un peu plus d'un an dans l'aventure du Web 2.0, aussi appelé Web participatif ou Web contributif. Le Ministère a déployé de nombreux efforts au cours des derniers mois pour développer un site contributif, sur lequel les internautes du Québec et d'ailleurs seront invités à partager leurs expériences et leurs aventures au Québec, en téléversant photos et vidéos de même qu'en créant des récits de voyage. Le site contributif sera lancé officiellement en janvier 2009. »

[35] Voir notamment le Journal *Les affaires*, « Agent de marketing web 2.0 : un nouveau job », 06 septembre 2008, en ligne : <http://www.lesaffaires.com/article/1/publication--lesaffaires/2008-09-06/482051/agent-de-marketing-web-20--un-nouveau-job.fr.html>.

lorsque l'on identifie des exemples tant au Québec[36], au Canada[37] ou à l'étranger[38]. Aussi, sur chacun de ces « espaces », l'on cherche à encourager les usagers à verser des documents, que ce soit des textes, images, vidéos relatant généralement leurs récits de voyage ou de vacances. Ces dépôts auront pour vertu présumée d'inciter des visiteurs du site en question à venir visiter non plus « virtuellement » mais pour de vrai, les villes, régions, provinces et pays que les sites tentent par ce biais de mousser. De par l'efficacité qui est souvent attachée à cette forme « web 2.0 » de publicité, nul doute que cette manière de faire devrait se généraliser.

ii) État des conséquences sur le traitement juridique à y apporter

En effet, ce contenu « téléversé » (pour reprendre l'expression du communiqué précité) est susceptible de poser des difficultés juridiques à plusieurs égards. En premier lieu, dès lors que le caractère illicite aura été effectivement porté à sa connaissance, il naîtra une obligation de diligence tel que convenu à l'article 22 de la *Loi concernant le cadre juridique des technologies de l'information*[39], et ce, même si l'application de ce niveau de diligence n'a donné lieu à aucune jurisprudence[40]. Mais tel n'est pas la ques-

---

36 Nous nous sommes par exemple inspirés du site de la ville de Montréal (<www.tourisme-montreal.org>).

37 Nous nous sommes par exemple inspirés de sites de Colombie-Britannique (<www.hellobc.com>), du Manitoba (<www.travelmanitoba.com> – <www.itsmymoment.ca>), de Nouvelle-Écosse (<www.novascotia.com>).

38 Nous nous sommes par exemple inspirés de sites anglais (<www.enjoyengland.com>), espagnol (<www.spain.info>), néerlandais (<www.holland.com>), suisse (<www.myswitzerland.com>), suédois (<www.communityofsweden.com>), autrichien (<www.coolaustria.com>), américain (<www.goseearizona.com>).

39 Article 22 de la *Loi concernant le cadre juridique des technologies de l'information,* L.R.Q., c. C-1.1, en ligne : <http://www.canlii.org///qc/legis/loi/c-1.1/20080818/tout.html>.

40 En effet, cet article n'a encore jamais donné lieu à de la jurisprudence au Québec quant à l'application de la diligence avec laquelle l'hébergeur de contenu doit agir. Mais compte tenu de la tendance observée dans plusieurs juridictions étrangères, il appert que le caractère illicite doit être suffisamment détaillé pour que naisse une telle obligation de diligence.

tion ici. Davantage, en second lieu, il s'agira de bien qualifier les opérations en cause notamment quant au traitement à apporter à la gestion des renseignements personnels. Car en effet, certains pourraient se demander si l'individu qui publie sur ladite plateforme du contenu incluant des informations confidentielles (tel que son nom, sa photo, son adresse, la photo ou vidéo de sa maison, etc.) a consenti à ce que celles-ci soient « publiées »[41], et ce, même si l'évidence semble montrer que le comportement de l'usager ne s'explique rationnellement que par une volonté de rendre publics les informations le concernant. Plus précisément, l'analyse subséquente nous permet de croire qu'un consentement peut être déduit de l'action même de l'usager[42]. La présence – ou non – de ce consentement aura notamment une importance réelle quant au fait de savoir si une collecte est faite de la part de l'hébergeur qui reçoit les renseignements personnels. Car préalablement à l'existence de ce consentement, l'on devra être en mesure de qualifier l'existence – ou non – de la collecte. Si elle existe – ce que nous ne croyons pas[43] –, alors la qualité du consentement pourra être évaluée.

SECTION 2 – Analyse autour des PEL

1 – Définition et influences du « web 2.0 » sur les PEL

Plusieurs des applications qui sont désormais disponibles dans les gouvernements en ligne sont largement inspirées, croyons nous, par ce qui est souvent dénommé comme étant le web 2.0. D'après Wikipedia, cette notion de « web 2.0 » est en effet la création de Darcy DiNucci, qui, en 1999, écrivait dans son article « Fragmented Future » :

> « The Web we know now, which loads into a browser window in essentially static screenfuls, is only an embryo of the Web

---

41 Dans le sens de la mise à la disposition du public.

42 *Infra*, Partie 2, Chapitre 1, Section 2.

43 *Infra*, Partie 1, Chapitre 2, Section 2.

> to come. The first glimmerings of **Web 2.0** are beginning to appear, and we are just starting to see how that embryo might develop. ... The Web will be understood not as screenfuls of text and graphics but as a transport mechanism, the ether through which interactivity happens. It will [...] appear on your computer screen, [...] on your TV set [...] your car dashboard [...] your cell phone [...] hand-held game machines [...] and maybe even your microwave »[44] (nos soulignements).

Cependant, le terme n'a refait surface qu'en 2003, puis a connu sa croissance de popularité quand O'Reilly Media et MediaLive ont, en 2004, organisé la première conférence Web 2.0. Dans leurs remarques d'ouverture, John Batelle et Tim O'Reilly ont précisé leur définition du « Web as Platform », qui consiste à ce que les logiciels et les applications informatiques soient construits avec le Web comme plateforme de base et non l'ordinateur – équipement lui-même. D'après eux, l'unique aspect de ce changement, est que « les clients sont en train de construire votre affaire pour vous »[45].

Par ailleurs, le 30 septembre 2005, Tim O'Reilly écrivait dans un article jugé par beaucoup comme fondateur du concept, intitulé « What Is Web 2.0 – Design Patterns and Business Models for the Next Generation of Software », les éléments suivants :

> « …there's still a huge amount of disagreement about just what « Web 2.0 means, with some people decrying it as a meaningless « marketing buzzword, and others accepting it as the new « conventional wisdom.
>
> « This article is an attempt to clarify just what we mean by Web 2.0.

---

44 Voir en ligne : <http://en.wikipedia.org/wiki/Web_2.0> et DiNucci, D. (1999). « Fragmented Future ». Print 53 (4) : 32.

45 Voir en ligne : <http://en.wikipedia.org/wiki/Web_2.0> et O'Reilly, Tim, and John Battelle, 2004. Opening Welcome : State of the Internet Industry. In . San Francisco, CA, October 5.

« In our initial brainstorming, we formulated our sense of Web 2.0 « by example :

Web 1.0		**Web 2.0**
DoubleClick	→	Google AdSense
Ofoto	→	Flickr
Akamai	→	BitTorrent
mp3.com	→	Napster
Britannica Online	→	Wikipedia
Personal websites	→	Blogging
evite	→	upcoming.org and EVDB
domain name speculation	→	search engine optimization
page views	→	cost per click
screen scraping	→	web services
publishing	→	Participation
content management systems	→	Wikis
directories (taxonomy)	→	tagging (« folksonomy »)
stickiness	→	Syndication

« The list went on and on. But what was it that made us identify « one application or approach as "Web 1.0" and another as « "Web 2.0" ? (The question is particularly urgent because the « Web 2.0 meme has become so widespread that companies « are now pasting it on as a marketing buzzword, with no real « understanding of just what it means. The question is « particularly difficult because many of those buzzword-« addicted startups are definitely *not* Web 2.0, while some of « the applications we identified as Web 2.0, like Napster and « BitTorrent, are not even properly web applications !) We « began trying to tease out the principles that are demonstrated « in one way or another by the success stories of web 1.0 and « by the most interesting of the new applications (…)

« Like many important concepts, Web 2.0 doesn't have a hard « boundary, but rather, a gravitational core. You can visualize Web 2.0 as a set of principles and practices that tie together a

> « veritable solar system of sites that demonstrate some or all of « those principles, at a varying distance from that core[46].

Dans cette même logique, Ian Davis écrivait :

> « web 2.0 is an attitude not a technology. It's about enabling and encouraging participation through open application and open services. » [47]

Ainsi, et malgré le flou inhérent associé à ce concept, les nouveaux services, tout comme le web 2.0, semble faire la part belle au rôle à jouer de l'usager, du citoyen, du consommateur, de l'internaute. Dans les cas qui sont les nôtres, l'usager dispose d'une capacité de **contrôle** de l'information qui le concerne sans précédent.

Le citoyen électronique est à bien des égards capable de **contrôler** un certain nombre d'information le concernant, à la différence de l'équivalent papier où il est strictement passif. Il importe donc de considérer le citoyen dans un environnement qui ne dispose peut-être pas des mêmes vulnérabilités que dans le monde du papier.

Ce qui paraît caractéristique du web 2.0 au plan du droit est le rôle plus actif que jamais tenu par l'usager.

Ces sites permettent aux internautes d'éditer et de modifier des contenus à leur guise. Dans d'autres cas de figure, on évoque la possibilité de combiner des applications et des contenus et synchroniser un site web avec d'autres[48]. Les sites de partage de contenus comme *YouTube* ou *Dailymotion* permettent aux inter-

---

[46] Tim O'Reilly, « What Is Web 2.0 – Design Patterns and Business Models for the Next Generation of Software » en ligne : <http://oreilly.com/web2/archive/what-is-web-20.html>.

[47] Ian DAVIS, « Talis, Web 2.0 and All That », (2005) en ligne : <http://iandavis.com/blog/2005/07/talis-web-20-and-all-that> (blogue).

[48] Mary MADDEN et Susannah FOX, « Riding the Waves of "Web 2.0" more than a Buzzword, but still not easily defined », Pew Internet, Backgrounder, <http ://www.pewinternet.org/pdfs\PIP_Web_2.0.pdf> ; Lis VEASMAN, « "Piggy Backing" on the Web 2.0 Internet : Copyright Liability and Web 2.0 Mashups », [2008] 30 *COMM/ENT* 311-337.

nautes de diffuser des contenus en ligne. Les sites de réseaux sociaux comme *Facebook* ou *Myspace* permettent aux individus de diffuser leur profil personnel de même que d'autres informations portant sur d'autres personnes[49].

Il existe une tendance, aussi bien dans le déploiement des services gouvernementaux en ligne que dans le développement de l'offre de services et de fonctions sur Internet, vers une implication plus marquée de l'usager. Cette implication concerne aussi bien la production d'informations que les interactions qui prennent place à l'occasion de divers évènements de vie. Ces tendances font en sorte que chaque usager devient plus ou moins un acteur interconnecté en réseau. Il lui incombe de plus en plus de connaître et de gérer les divers types d'enjeux et risques inhérents à une telle démultiplication des interactions dans lesquelles il est désormais engagé.

L'environnement du web 2.0 s'inscrit en dehors d'un modèle dans lequel une entité centrale assume seule les responsabilités, le cadre juridique se trouve caractérisé par un ensemble de risques répartis entre un nombre indéterminé d'acteurs de dimensions et de statuts différents. Si les risques qu'implique le web 2.0 ne sont pas nécessairement nouveaux, ils semblent désormais se poser à une échelle différente. Le rôle accru de l'usager contribue à déplacer et à démultiplier les lieux où se manifestent des risques et enjeux dont plusieurs peuvent présenter des dimensions juridiques. En raison du rôle actif qu'il tient, l'usager lui-même prend des décisions, adopte des pratiques dont doivent forcément tenir compte les autres acteurs. Les décisions que prend l'usager sont, plus que dans l'Internet de première génération, susceptibles d'emporter des conséquences pour les tiers.

Par dessus tout, les environnements web utilisés couramment afin de permettre les interactions entre les usagers et les multiples services avec lesquels ils peuvent entrer en relation, sont régis par les commandes des usagers. C'est à ces derniers que

---

[49] Steven JAMES, « Social Networking Sites : Regulating the Online "Wild West"of Web 2.0 », [2008] 2 *Ent. L.R.* 47-50.

revient le pouvoir de décider s'ils souhaitent appeler à eux un document et s'ils souhaitent expédier un fichier à quelqu'un d'autre.

Dans cet environnement, il existe des lieux qui accueillent les usagers et leur proposent diverses fonctions. Ces lieux ne prétendent pas exercer un contrôle sur l'information qui y est traitée par les usagers.

2 – Caractéristiques principales des PEL

A – Tendance à une circulation croissante des RP

Conformément à une expression désormais reconnue, avec de telles prestations en ligne, on consacre le passage de la gestion d'information en silo à une gestion en réseau. La circulation des renseignements personnels est donc inhérente à une gestion contemporaine, et ce, sans que cela soit vu comme une atteinte au droit. Ce changement est opéré par des exigences d'efficacité, de facilité, de sécurité du traitement des RP. Une circulation qui n'est d'ailleurs pas antinomique avec les premiers textes internationaux où l'on met clairement en perspective que protection des renseignements personnels ne s'oppose pas à leur circulation. Cette « non opposition » apparaît d'ailleurs dès le début dans les lignes directrices de l'OCDE[50] – texte dont s'inspirent les lois québécoises sur la protection des renseignements personnels – où justement, la protection des renseignements personnels était rendue nécessaire du fait du caractère inévitable de leur circulation. La circulation impliquait donc une série de garanties ; garanties qui ne devaient pas empêcher la circulation.

Ainsi, et conformément aux trois illustrations précédentes, la circulation non seulement s'impose pour qu'un service soit rendu mais une circulation accrue devra être faite si l'on souhaite qu'il soit de meilleur qualité. À cet égard, il est possible de citer plusieurs auteurs américains qui dans le cadre d'une étude pluridis-

---

[50] Voir le texte de François RIGAUX à cet égard en ligne : <http://www.asmp.fr/travaux/gpw/internetvieprivee/rapport2/chapitr8.pdf>.

ciplinaire évoquent la nécessité d'un changement de perspective dans ce sens :

> « In many cases it is only by making better use of the information that is collected, and by retaining what is necessary to hold data users responsible for policy compliance that we can actually achieve greater information accountability"[51]. »

Selon ces auteurs qui évoquent une réalité américaine certes différente que la nôtre au Québec, ils considèrent notamment que le contrôle quant à la circulation des renseignements personnels devrait se faire davantage *a posteriori* et moindrement *a priori*. En effet, et d'une manière comparable à celle qui prévaut en matière fiscale, ils privilégient une solution où le contrôle s'opérerait non pas avant la circulation des renseignements personnels mais après. Comme pour le contribuable qui remplit une déclaration de revenus, les utilisateurs de renseignements personnels pourraient les utiliser mais devraient faire face à un contrôle *a posteriori* sur simple demande d'un organisme en charge de ce contrôle[52].

Ce propos prospectif indique les pistes à l'égard de l'interprétation à donner à ce droit « ancien » confronté à une réalité nouvelle afin qu'elle se fasse en accord avec la réalité qui est celle d'une gestion gouvernementale en réseau. En effet, une telle interprétation doit être faite en concordance avec la réalité inhérente qu'est celle de ces nouvelles prestations en ligne.

---

[51] Daniel J. Weitzner, Harold Abelson, Tim Berners-Lee, Joan Feigenbaum, James Hendler, et Gerald Jay Sussman, *Information Accountability*, en ligne : <http://dspace.mit.edu/bitstream/handle/1721.1/37600/MIT-CSAIL-TR-2007-034.pdf;jsessionid=5C55BCE830931159A076383961472C6A?sequence=2>.

[52] Daniel J. WEITZNER, Harold ABELSON, Tim BERNERS-LEE, Joan FEIGENBAUM, James HENDLER, et Gerald Jay SUSSMAN, *Information Accountability*, en ligne : <http://dspace.mit.edu/bitstream/handle/1721.1/37600/MIT-CSAIL-TR-2007-034.pdf;jsessionid=5C55BCE830931159A076383961472C6A?sequence=2>. Voir notamment la section 4.

B – Tendance au contrôle accru de l'usager

Une autre caractéristique importante, majeure, qui semble pouvoir être déduite des trois illustrations que nous avons exposées, est que l'usager dispose d'une certaine capacité de contrôle sans doute sans précédent dès lors que l'on la compare à celle qui prévaut dans les environnements papier. Et avec les tendances découlant des modèles associés au web 2.0, les prestations en ligne se présentent de plus en plus comme des interfaces permettant à l'usager de « gérer » l'information qui le concerne.

La circulation de renseignements personnels entre organismes publics ou entre entités privées et publiques est assujettie à un régime juridique spécifique visant à garantir que les échanges sont justifiés et sont effectués dans le respect des droits des personnes concernées.

Cet état de fait nécessite de qualifier adéquatement les situations afin d'éviter la mise en place d'encadrements juridiques inutilement lourds et possiblement porteurs d'effets pervers liberticides.

Ainsi, lorsqu'un usager accède à une interface afin de réaliser une transaction, il pourra devoir « accéder » à des renseignements personnels le concernant (comme dans le cadre de la situation 1 préalablement décrite et relative à la méthode d'authentification d'identité du citoyen aux fins de permettre l'accès à un service déterminé)[53]. Il pourra aussi verser lui-même des renseignements personnels qu'il pourra ultérieurement utiliser pour son bénéfice personnel et souvent exclusif. Alors la plate-forme doit être envisagée comme un hébergeur de données que l'usager lui a confiées (comme dans le cadre de la situation 2 relative à l'hébergement de renseignements du CV d'un professeur d'Université au Canada)[54]. Il pourra enfin également transmettre des renseignements personnels à autrui ou il pourra souhaiter accéder à des renseignements personnels relatifs à autrui (comme dans le cadre de la

---

53 *Supra*, Partie préliminaire, Chapitre 1, Section 1, 2A.

54 *Supra*, Partie préliminaire, Chapitre 1, Section 1, 2B.

situation 3 précitée et relative au site web 2.0 de promotion touristique)[55].

En somme, l'accomplissement d'un nombre grandissant de prestations en ligne (PEL) suppose que les usagers accèdent en ligne à des documents technologiques en leur donnant la possibilité de faire circuler (transmettre, héberger, accéder, communiquer, collecter, etc.) certains d'entre eux qui détiendraient des renseignements personnels et même, éventuellement, d'en disposer en, par exemple, les modifiant ou les effaçant. Cependant, et au regard des incidences juridiques susceptibles de découler de ces situations, il est donc important de les décrire adéquatement et de les qualifier en fonction de ce qu'elles sont vraiment[56]. Également, et là encore en conformité avec ce que nous verrons plus tard, la variation du contrôle de l'usager va assurément avoir une incidence sur celle-ci[57].

---

55 *Supra*, Partie préliminaire, Chapitre 1, Section 1, 2C.

56 *Infra*, Partie préliminaire, Chapitre 2, Section 1 sur la qualification juridique.

57 *Infra*, Partie 1, Chapitre 1, Section 1 sur « Les différentes intensités dans le contrôle de l'information ».

CHAPITRE 2
CHANGEMENTS JURIDIQUES RELATIFS À LA CIRCULATION DES RP : ILLUSTRATION D'UNE « ÉVOLUTION »

Face à la révolution de l'électronisation de la gestion documentaire, il est en revanche rassurant de constater que le droit dispose de son lot de stabilité, et ce, même si plusieurs considèrent que les technologies nous confrontent à des hypothèses de « vide juridique ». Que nenni ![58] Plus souvent qu'autrement, il est possible d'adapter le vieux droit aux faits nouveaux et cette adaptation est d'autant plus facile à faire dès lors qu'elle confronte des principes plurimillénaires qui permettent de distinguer (dans le sens utilisé en *common law*[59]), d'adapter les faits au droit. Or, justement, confronter le droit aux faits est de la nature même de l'opération juridique qui exige par conséquent de vérifier la qualification des personnes impliquées et des opérations qu'elles effectuent aux innovations technologiques (Section 1). Ensuite, et toujours dans cette quête d'identification des moyens offerts par le droit pour permettre davantage de souplesse, nous présenterons sommairement la latitude que l'on peut associer à chacune des sources juridiques qui peuvent être utilisées dans les circonstances (Section 2).

---

[58] André LUCAS, « La réception des nouvelles techniques dans la loi : l'exemple de la propriété intellectuelle », dans Ysolde GENDREAU (dir.), *Le lisible et l'illisible*, Montréal, Éditions Thémis, 2003, p. 125, à la page 134 : « Il y a un véritable fantasme, relayé par les médias et souvent par les responsables politiques, du vide juridique. La vérité est que les groupes de pression appellent vide juridique la règle existante qui ne leur convient pas. Prétendre légiférer à chaque nouvelle percée technique, c'est se condamner à une fuite en avant qui ne peut être que porteuse d'insécurité juridique. »

[59] Voir notamment la définition donnée dans Wikipedia à ce concept. <http://en.wikipedia.org/wiki/Distinguish>.

SECTION 1 – ÉVOLUTION DU DROIT : VERS UNE MEILLEURE QUALIFICATION JURIDIQUE DES ÉLÉMENTS EN CAUSE

La souplesse du droit va d'abord se matérialiser sur la capacité de qualifier deux aspects de la même médaille : en effet, face à des situations nouvelles, qui se développent en marge des lois et règlements appliqués à un domaine en particulier, il importe de qualifier tant les personnes concernées (1) que les opérations que celles-ci effectuent (2). Et assurément, la manière dont on interprète l'un ou l'autre de ces éléments va avoir une incidence certaine sur l'application des lois.

1 – Existence et qualification des intermédiaires

Dans les réseaux, il y a des entités qui contrôlent l'information, peuvent y accéder et les communiquer à d'autres tandis qu'il y a des entités qui assurent des fonctions d'intermédiaires, assurant le traitement des informations sans pour autant avoir le contrôle sur celles-ci.

La personne qui exerce le contrôle sur une information ou se comporte de manière à exercer un contrôle sur la diffusion de celle-ci en assume la responsabilité. Ainsi, mettre des informations en ligne, c'est assumer une fonction éditoriale. L'éditeur publie les informations. Publier signifie communiquer de l'information à des tiers en sachant que cette information sera lue, vue ou entendue. La publication s'effectuant de manière volontaire suppose une connaissance de la teneur de l'information transmise[60]. Dans le contexte d'Internet, la publication peut résulter de la transmission de fichiers, de discussions dans le cadre de conférences électroniques, de l'envoi d'un courriel à un nombre indéterminé de personnes ou encore par la mise à disposition

---

60 Pierre TRUDEL, « Responsibilities in the Context of the Global Information Infrastructure », (1997) 29 *International Information & Library Review*, 479-482 ; Loftus E. BECKER Jr., « The Liability of Computer Bulletin Board Operators for Defamation Posted by Others », (1989) 22 *Connecticut Law Review* 203-239, 217.

d'information dans des fichiers de documents pouvant être transférés via le réseau. Dans l'échange de personne à personne, la personne qui exerce un contrôle sur une information peut la communiquer ou accorder différentes permissions à l'égard de cette information.

L'exercice du contrôle à l'égard de la diffusion d'une information s'assimile à l'exercice de la fonction éditoriale. Celle-ci implique le pouvoir de choisir ce qui sera diffusé, de décider de le diffuser et de décider à qui ou auprès de qui l'information sera diffusée. Ainsi, un fournisseur d'accès Internet qui examinerait tous les messages avant de les retransmettre et se réserverait le droit de n'acheminer que les messages qu'il juge conformes à ses politiques, se comporterait comme un éditeur. Dans de pareilles situations, il est une constante : la décision de publier appartient à l'éditeur. Il s'agit pour lui d'une faculté : il n'a pas d'obligation de publier. Dans le monde de la presse et de l'édition, il est usuel de tenir que le directeur de publication est en mesure de contrôler les informations qui circulent du fait de son entreprise[61]. De ce pouvoir de contrôle découle la responsabilité pour la transmission d'informations.

Dans le contexte d'Internet, les intermédiaires sont des personnes, entreprises ou organismes qui interviennent dans l'accomplissement d'une tâche effectuée entre le point d'expédition d'une transmission de document et le point de réception final. Le trait commun à tous ces intervenants, c'est qu'ils n'exercent pas de droit de regard sur l'information qui transite dans leurs environnements technologiques. Ainsi, les intermédiaires peuvent être des services de conservation de documents technologiques[62], des hébergeurs, des services de référence à des documents tech-

---

61 Pierre TRUDEL, « Liability in Cyberspace », in Theresa FUENTES-CAMACHO, *The International Dimensions of Cyberspace Law*, Aldershot Ashgate Publishing, UNESCO, 2000, p. 189-211. David R. Johnson et Kevin A. Marks, « Mapping Electronic Data Communications onto Existing Legal Metaphors : Should We Let Our Conscience (and Our Contracts) be Our Guide ? », (1993) 38 *Vill. L. Rev.* 487, 492.

62 Selon l'article 3 de la *Loi concernant le cadre juridique des technologies de l'information*, L.R.Q., c. C-1.1, en ligne : <http://www.canlii.org///qc/legis/

nologiques, des moteurs de recherche, ou des fournisseurs de services sur un réseau de communication. Il peut également s'agir d'entreprises offrant des services de conservation ou de transmission de documents technologiques, de services de transmission de documents technologiques ou de services de conservation sur un réseau de communication de documents technologiques fournis par un client.

Le statut des intermédiaires varie à l'infini. Sur Internet, une entité peut accomplir une ou plusieurs des fonctions nécessaires à la communication ou à la transmission d'informations. Les désignations que se donnent les acteurs telles que « fournisseur d'accès à Internet », fournisseur de connectivité, simple transporteur ne recouvrent pas toujours les mêmes activités. Il faut donc, pour chaque situation, examiner soigneusement ce que fait l'intermédiaire visé et déterminer quel est le degré de friction qu'il a avec l'information qui « passe » en sa possession, afin de le qualifier adéquatement au plan de la responsabilité qu'il assume.

2 – Qualification des opérations

De la même manière que l'analyse qui vient d'être faite relativement au statut des personnes impliquées dans la circulation de documents contenant des renseignements personnels, il est nécessaire de s'interroger quant à la nature des opérations qui sont effectuées par ces dernières.

La circulation inhérente au fonctionnement des prestations en ligne s'inscrit dans un processus comportant diverses phases qui n'emportent pas toutes, loin de là, l'exercice d'un contrôle sur l'information transmise ou mise en dépôt. Par exemple, l'organisme qui administre les répertoires permettant aux chercheurs de déposer leur CV dans le CV commun canadien ne collecte pas, lui-même, de renseignements personnels du fait qu'il fournit une fonction de conservation de documents technologiques sur un

---

loi/c-1.1/20080818/tout.html>, les documents technologiques sont des documents dont le support fait appel aux technologies de l'information.

réseau[63]. Une telle entité exerce une fonction d'intermédiaire, celle visée à l'article 22 de la *Loi concernant le cadre juridique des technologies de l'information*[64]. D'autres entités peuvent exercer des fonctions correspondant à celles visées à l'article 22 susmentionné comme les prestataires qui agissent à titre d'intermédiaire pour offrir des services de référence à des documents technologiques, dont un index, des hyperliens, des répertoires ou des outils de recherche.

Ainsi, en fonction de ce niveau de contrôle, une même opération pourra être analysée différemment. Le droit aura donc à interpréter si transmission, communication, collecte, conservation, utilisation il y a au regard de cette capacité de maîtrise sur lesdits renseignements personnels.

SECTION 2 – ÉVOLUTION INHÉRENTE AU DROIT

Outre ce premier exercice de qualification, tel que nous l'avons décrit dans la précédente section, il est aussi un constat à considérer selon lequel le droit est un merveilleux outil d'adaptation face à la réalité mouvante qu'il recherche à encadrer. Cette évolution du droit en général, et dans le cas qui nous intéresse, du droit de la protection des renseignements personnels, s'effectuera harmonieusement dès lors, en premier lieu, que la matière sera analysée d'une manière globale et non seulement en fonction du seul prisme de la protection des individus. En effet, ce domaine dédié à un objectif clairement identifié dans les lois mêmes, la protection des individus, ne peut se comprendre que si l'on met cet objectif en perspective avec d'autres considérations (1). En second lieu, nous pourrons également constater que les outils habituellement disponibles en droit positif bénéficient d'une grande souplesse parfaitement utilisable dans l'encadrement des technologies de l'information (2).

---

63 *Supra*, Partie préliminaire, Chapitre 1, Section 1, 2B.

64 Article 22 de la *Loi concernant le cadre juridique des technologies de l'information*, L.R.Q., c. C-1.1, en ligne : <http://www.canlii.org///qc/legis/loi/c-1.1/20080818/tout.html>.

1 – Évolution du droit de la protection des RP

Mais en premier lieu, nous croyons important de rappeler que le droit de la protection des renseignements personnels doit être analysé d'une manière plus globale que le strict objectif de protection qui apparaît dans les titres même des lois en cause. Ainsi, si ce domaine doit être vu comme étant en concurrence avec d'autres domaines, également identifiés par d'autres lois (B), il faut aussi l'analyser en fonction d'un certain niveau de risques, qui sans être absent, ne doit pas être surévalué non plus (A).

A – Évolution en fonction de l'insécurité sublimée des RP

Le droit tente d'encadrer une « réalité vivante »[65] qui évolue par nature. Une évolution qui est d'autant plus sensible dès lors que l'on traite des technologies de l'information dont la rapidité d'évolution et l'obsolescence est sans précédent.

Cette rapidité est assurément la source d'une insécurité, souvent sublimée, selon laquelle la protection des renseignements personnels n'existe plus ou ne peut plus être maîtrisée. Il y a assurément ici une différence à faire entre le risque, qui semble à bien des égards exagéré, et la perception du risque qui elle est en effet largement présente dans l'esprit tant des internautes que des gestionnaires de renseignements personnels.

Une insécurité qu'il est difficile de déceler tant sa mesure est déficiente, et ce, que ce soit sur le plan objectif que subjectif[66]. Sur le plan objectif en premier lieu, il est difficile de trouver des études qui semblent évoquer une hausse notable de la criminalité

---

65 Expression de Jacques GHESTIN, « L'utile et le juste dans les contrats », (1981) 26 *Archives de philosophie du droit* 35, 57.

66 Cette double dimension est évoquée par l'ORGANISATION MONDIALE DE LA SANTÉ, *Sécurité et promotion de la sécurité : aspects conceptuels et opérationnels*, septembre 1998, p. 8 et 9, citée par COMMISSION DE L'ÉTHIQUE DE LA SCIENCE ET DE LA TECHNOLOGIE, *Viser un juste équilibre, un regard éthique sur les nouvelles technologies de surveillance et de contrôle à des fins de sécurité*, Gouvernement du Québec, 2008, p. 3.

informatique. Et si plusieurs recherches financées par des commerçants dédiés à la proposition de biens et services en sécurité semblent évoquer des données assez apocalyptiques[67], dont il est légitime de se méfier[68], d'autres, plus crédibles, semblent au contraire être plus mesurées[69]. Malheureusement, et cela nous permet de faire un lien avec le second plan, les études les plus « sensationnelles » sont davantage reprises dans les médias, donnant l'impression d'un niveau de risques sans précédent et que le risque est partout[70]. Mais par-dessus tout, il faut déplorer la carence d'analyse sur les moyens juridiques et normatifs d'assurer la sécurité véritable.

Bien évidemment, l'objet de la discussion ici n'est pas de dire que l'insécurité n'existe pas. Seulement, nous croyons qu'à cause d'études souvent utilisées en dépit de méthodologies peu convaincantes, il est parfois tendance à vouloir faire supporter auprès des gestionnaires de renseignements personnels un niveau de sécurité qui, a bien des égards, est bien supérieur à celui qui prévaut dans le monde papier. D'ailleurs, il est généralement prouvé que l'immense majorité du vol d'identité, pour ne prendre que cet exemple, provient d'une mauvaise gestion d'informations person-

---

67 On peut notamment au tout récent rapport délivré par McAfee en décembre 2008, plus d'information en ligne : <http://www.gautrais.com/Recent-rapport-McAfee-sur-la ?var_recherche=rapport%20mcafee>.

68 Benoit DUPONT et Vincent GAUTRAIS, « Crime 2.0 : le web dans tous ses états ! », à paraître.

69 Benoit DUPONT et Benoit GAGNON, « La sécurité précaire des données personnelles en Amérique du Nord : une analyse des statistiques disponibles », note de recherche no. 1, 2008 ; Javelin Strategy, « ID Theft/Fraud : Rising or Declining ? », en ligne : <http://www.javelinstrategy.com/2008/02/15/id-theft-fraud-rising-or-declining/> ; FTC, « Consumer Fraud and Identity Theft Complaint Data : January – December 2007 » (pdf – 92 pages), en ligne : <http://www.ftc.gov/opa/2008/02/fraud.shtm> ; BBB, « 2006 Identity Fraud Survey Report », en ligne : <http://www.javelinstrategy.com/products/99DEBA/27/delivery.pdf>.

70 COMMISSION DE L'ÉTHIQUE DE LA SCIENCE ET DE LA TECHNOLOGIE, *Viser un juste équilibre-un regard éthique sur les nouvelles technologies de surveillance et de contrôle à des fins de sécurité*, Gouvernement du Québec, 2008, p. 4 et 5.

nelles dans des documents sur support papier et non des renseignements personnels disponibles sur Internet[71].

Or, la conséquence de cette insécurité ressentie donne l'impression qu'il faille interpréter avec rigueur un droit qui demande plus de protection. Mais outre le fait que cette insécurité soit pour le moins difficile à évaluer, il n'y a aucune preuve selon laquelle plus de contrôle *a priori* s'effectue et plus de protection est ainsi assurée. Au contraire. Si l'on souhaite trop encadrer des situations où un tel contrôle ne s'impose pas selon nous, il est un risque de voir le droit systématiquement violé, bafoué, les gestionnaires le considérant comme inadapté aux situations factuelles qui sont les leurs[72]. Il est donc important que le droit soit en accord harmonieux avec les faits.

B – Évolution en fonction de la concurrence de certains droits

Par essence, le droit de la protection des renseignements personnels est un droit opposant des intérêts divergents.

En fait, et avant de traiter ce domaine en particulier, par essence, le droit est toujours en quête de cet équilibre entre des intérêts catégoriels distincts. Un bon exemple peut sans doute être le droit constitutionnel ou les libertés publiques où il s'agit pour les juges de dispenser une opinion mesurée et rationnelle, et donc prévisible, sur des intérêts contraires. Par exemple, lorsqu'il s'agit de déterminer le droit à l'image, comme dans l'affaire *Aubry c. Vice-Versa*[73], il faut confronter le droit à la vie privée et l'intérêt du public. C'est aussi le cas en droit d'auteur où les technologies invitent à repenser le partage des revenus entre les différents intervenants ; c'est également le cas dans l'affaire *Dell* traitée

---

71 Conformément à une étude produite en 2005 par *Javelin Strategy*.

72 Comme cela s'effectue actuellement dans le domaine du droit d'auteur en ce qui a trait à la gestion des réseaux P2P (pairs à pairs) dont l'illégalité est avérée dans de nombreux pays sans que l'on ne soit en mesure de ralentir le phénomène.

73 *Aubry c. Éditions Vice-Versa*, [1998] 1 R.C.S. 591, en ligne : <http://csc.lexum.umontreal.ca/fr/1998/1998rcs1-591/1998rcs1-591.html>.

récemment par la Cour suprême[74] où il s'agissait de tracer une ligne entre le droit de l'arbitrage – et le droit des entreprises à utiliser un système juridictionnel jugé efficace, notamment par elles –, et le droit de la protection des consommateurs – et notamment le droit de ces derniers à recourir aux services offerts à travers les recours collectifs. Utilisant une image non issue du registre légal, l'on pourrait prétendre que les domaines du droit, spécialisés de surcroît, peuvent être assimilés au phénomène que l'on aperçoit dans les « cloches à vide », à savoir, comme dans un environnement de vide, un ballon de baudruche qui va se dilater jusqu'aux limites de la paroi du récipient où l'expérience s'effectue. De la même manière, un domaine du droit, face à certains éléments de doutes, va souvent s'étendre, se développer, jusqu'au moment où les prérogatives accordées à une catégorie d'individus vont porter atteinte à celles d'une autre catégorie de personnes, protégées elles-mêmes par d'autres règles[75].

Le droit, en pareil cas, est donc fermement associé à l'image populaire de la balance qui est d'ailleurs fort appropriée. Et à cet égard, le domaine de la protection des renseignements personnels traduit bien ce partage qui doit être fait entre des intérêts ou des domaines de droit distincts.

En premier lieu, la protection de l'individu doit être analysée en tenant compte de la multiplicité des intérêts en cause. Par exemple, certains croient que la publication à grande échelle de décisions judiciaires dans des banques de données disponibles sur Internet est possiblement attentatoire à la protection des renseignements personnels ; mais d'autres de considérer que cet accès est un moyen de diffusion du droit sans précédent qui assure une transparence judiciaire sans précédent. Dans le même sens, le droit de la protection des renseignements personnels peut

---

74 *Dell Computer* c. *Union des Consommateurs*, 2007 CSC 34 (CanLII), en ligne : <http://www.canlii.ca/fr/ca/csc/doc/2007/2007csc34/2007csc34.html>.

75 Image développée relativement au projet de loi relatif aux amendements à la *Loi sur le droit d'auteur* (<http://www.gautrais.com/Bill-C-61-boules-et-billes>) et sur l'affaire *Dell* (<http://www.gautrais.com/Dell-et-les-audiences-en-Cour>).

être en opposition au droit d'auteur dès lors qu'il s'agit de dévoiler les noms correspondant aux adresses « IP » cachés derrière les fameux « pirates » qui téléchargent de la musique protégée par le droit d'auteur[76].

En second lieu, le droit protégeant les renseignements personnels doit également être mis en perspective non seulement avec des intérêts distincts mais aussi avec des droits différents. Par exemple, à bien des égards, nous ne pourrons faire l'économie d'une analyse des règles de responsabilité relatives aux intermédiaires de services, et notamment celles établies dans la *Loi concernant le cadre juridique des technologies de l'information*[77]. En effet, il serait pour le moins illogique de déterminer si une organisation a enfreint une loi sur la protection des renseignements personnels si l'on ignore et l'on omet de traiter, au préalable, le fait de savoir si elle bénéficie ou non d'un régime d'exonération de responsabilité[78]. Aussi, en dépit du fait que ce sont deux domaines de droit distincts, ils s'interpénètrent et exigent un traitement parallèle.

2 – Évolution propre aux différentes sources juridiques

Classiquement, parmi les sources juridiques pour encadrer les activités humaines, il y a toujours eu trois outils principaux qui disposent chacun de leur lot d'adaptation aux mondes changeants qui se sont succédé dans l'histoire de l'humanité. Ainsi, nous verrons successivement le contrat (A), la manière d'interpréter les lois (B) et la jurisprudence qui plus souvent qu'autrement recherche à favoriser l'intégration du neuf (C).

---

[76] Par exemple, voir la décision BMG : BMG Canada Inc. c. John Doe, 2004 CF 488 (CanLii), en ligne : <http://www.canlii.ca/fr/ca/cfpi/doc/2004/2004cf488/2004cf488.html>.

[77] *Loi concernant le cadre juridique des technologies de l'information*, L.R.Q., c. C-1.1, en ligne : <http://www.canlii.org///qc/legis/loi/c-1.1/20080818/tout.html>.

[78] *Infra*, Partie 1.

A – Contrat sous surveillance face aux technologies

Le contrat est l'outil de prédilection pour encadrer de nouvelles situations ; souvent considéré comme la « loi des parties », il est en effet d'une souplesse redoutable tant il est possible d'y inclure une grande diversité de stipulations. Néanmoins, la portée pluriséculaire a perdu de son autonomie, surtout depuis que le contrat d'adhésion est devenu la manière usuelle de contracter. Ainsi, le contrat est un outil juridique sous le contrôle étroit du juge qui est habilité à le disqualifier, à le réduire dès lors qu'il mettrait en place des stipulations par trop abusives[79] et, finalement, à vérifier de la qualité du consentement de l'adhérent. En effet, sur ce dernier point, et conformément à ce que nous dirons dans la partie 2, il est important de rappeler la signification de la portée du consentement dans le domaine de la protection des renseignements personnels ; une signification sans doute distincte de celle qui prévaut dans le Code civil du Québec au livre portant sur le droit des obligations[80].

Également, nous verrons qu'il a un certain « coût » en terme de gestion, tant pour l'entité qui gère les renseignements personnels que les usagers eux-mêmes. Il importe donc de ne pas abuser de la souplesse qui lui est propre. Aussi, des trois sources juridiques étudiées ici, c'est sans doute celle qu'il importe d'utiliser avec le plus de parcimonie.

B – Évolution générale de la loi face aux technologies

Outre le contrat, la Loi qui se doit, par définition, d'être large, souple et permanente, constitue un outil remarquable d'adaptation au changement. Que ce soit par sa lettre ou par le biais des règles d'interprétation qui s'appliquent à elle, afin de lui faire découvrir sa « substantielle moelle », il est clair qu'il est possible d'appliquer un vieux texte à une nouvelle situation. Paradoxalement, il est même souvent plus facile d'appliquer une vieille loi à

---

79 Article 1437 C.c.Q.

80 *Infra*, Partie 2, Chapitre 1, Section préliminaire, 2.

une situation neuve qu'une nouvelle loi à un nouveau contexte. En effet, le vieux bénéficie de davantage de souplesse interprétative et il est possible dans le premier cas d'appliquer des approches historiques ou téléologiques qui ne sont pas utilisables avec une nouvelle loi.

Mais plus que la quête d'une seule méthode d'interprétation, c'est bien davantage selon une vision globale, « moderne » selon le propos de Driedger[81], que les lois s'interprètent. A ce propos, la Cour suprême fait sienne la citation de l'auteur dans plusieurs de ses décisions selon laquelle :

> « Aujourd'hui il n'y a qu'un seul principe ou solution : il faut lire les termes d'une loi dans leur contexte global en suivant le sens ordinaire et grammatical qui s'harmonise avec l'esprit de la loi, l'objet de la loi et l'intention du législateur. »[82]

Un « non-critère » interprétatif est donc utilisable afin de laisser la latitude nécessaire aux juges pour interpréter les lois. Une latitude que l'on est également capable d'identifier derrière le concept de « rationalité » que l'on retrouve développé par certains auteurs.

Gregory Mandel par exemple identifie les difficultés jurisprudentielles à encadrer l'avènement du télégraphe en 1844, notamment en ce qui a trait à la responsabilité d'un message qui ne se rend pas en temps et lieu[83]. La question qui fut généralement traitée était de savoir si un tel service devait être assujetti au régime de responsabilité que la loi avait attribué au « Common Carrier ». La jurisprudence oscilla, sans raison apparente, vers le

---

81 Elmer A. DRIEDGER, *Construction of Statutes*, 2e éd., Toronto, Butterworths, 1983.

82 Elmer A. DRIEDGER, *Construction of Statutes*, 2e éd., Toronto, Butterworths, 1983, p. 87, cité dans *Stubart Investments Ltd.* c. *La Reine*, [1984] 1 R.C.S 536, p. 578.

83 Gregory N. MANDEL, « History Lessons for a General Theory of Law and Technology », (2007) 8 *Minn. J. L. Sci. & Tech*. 551, 553 et s., en ligne : <http://papers.ssrn.com/sol3/papers.cfm ?abstract_id=1012612>.

« oui »[84] puis le « non »[85], utilisant des formules vagues telles que « there is no difference in the general nature of the legal obligation of the contract »[86] ou au contraire qu'il s'agit d'une « new form of message delivery »[87].

Davantage qu'une réponse au fait de savoir si un télégraphe est assimilable au transport de marchandises, et donc que le premier puisse être considéré comme un bien, il s'agit de vérifier plutôt quelles sont les « rationalités » derrière une construction légale :

> « a decision-maker must consider the **rationale** for the existing legal categories in the first instance, and then determine whether that rationale applies to the new technology. Legal categories (such as common carrier) are only that – legal constructs. Such constructs may need to be revised in the face of technological change. »[88] (nos soulignements)

Dans le cas du transport de marchandises, la responsabilité des transporteurs pouvait être suggérée du fait de l'incapacité des usagers de s'assurer eux-mêmes. Avec le télégraphe, il était possible pour le client de faire un accusé de réception vérifiant ainsi, de manière efficace, rapide et peu dispendieuse, que tant l'existence que le contenu du message ont bien été transmis à l'expéditeur[89]. La gestion de risques était donc possiblement derrière cette responsabilité ; or, celle-ci était drastiquement remise en cause dans le cadre de la nouvelle technologie de l'époque. Une

---

84 *Parks* c. *Alta California Telegraph*, (1859) 13 Cal. 422.

85 *Breese* c. *U.S. Telegraph*, (1871) 48 N.Y. 132.

86 *Parks* c. *Alta California Telegraph*, précitée, 424.

87 Gregory N. MANDEL, « History Lessons for a General Theory of Law and Technology », (2007) 8 *Minn. J. L. Sci. & Tech*. 551, 553, 556 et s., en ligne : <http://papers.ssrn.com/sol3/papers.cfm ?abstract_id=1012612>.

88 Gregory N. MANDEL, « History Lessons for a General Theory of Law and Technology », (2007) 8 *Minn. J. L. Sci. & Tech*. 551, 556, en ligne : <http://papers.ssrn.com/sol3/papers.cfm ?abstract_id=1012612>.

89 Gregory N. MANDEL, « History Lessons for a General Theory of Law and Technology », (2007) 8 *Minn. J. L. Sci. & Tech*. 551, 557, en ligne : <http://papers.ssrn.com/sol3/papers.cfm ?abstract_id=1012612>.

vision qui n'est pas très différente de perception développée par Pierre-André Côté selon laquelle :

> « Dans chaque cas, il s'agit de savoir d'une part, si la finalité de la disposition en justifie l'application à la nouvelle invention et, d'autre part, si le texte est rédigé d'une manière suffisamment générale pour que l'interprète puisse y soumettre des cas d'espèce inconnus à l'époque de l'adoption. »[90]

Pour ce faire, il importe donc d'identifier si un concept juridique est assimilable à un médium en particulier. Dans le domaine qui est le nôtre, il importe de vérifier si le concept légal à interpréter est orienté vers le papier (pour calquer l'expression anglaise de « paper-oriented ») ou s'il fait preuve d'une relative indépendance technologique.

C'est d'ailleurs suivant cette approche globale, attachée aux finalités des lois, que nous effectuerons la suite de nos travaux. Notamment, il importera d'analyser comment s'interprètent des termes qui sont, soit associés à la gestion dans un environnement papier soit dont la nouveauté incite à considérer un niveau de protection qui n'existait pas pour les documents papier[91]. Une approche également utilisée en ce qui a trait à la rationalité du consentement dans le domaine de la protection des renseignements personnels[92].

C – Rôle facilitateur de la jurisprudence face aux technologies

Suite logique de cette souplesse interprétative, plus souvent qu'autrement, et contrairement à une croyance que l'on entend parfois (notamment pour justifier la mise en place d'une nouvelle loi), les juges sont plutôt enclins à interpréter les concepts juridiques de manière à favoriser le développement et l'utilisation des technologies. Ceci est d'autant plus vrai avec des textes anciens

---

90 Pierre-André CÔTÉ, *Interprétation des lois*, 3e éd., Montréal, Éditions Thémis, 1999, p. 333 et 334.

91 *Infra*, Partie 1, Chapitre 2.

92 *Infra*, Partie 2, Chapitre 1.

qui bénéficient d'une plus grande capacité interprétative par les juges.

À titre d'illustration, nous pouvons citer certains extraits de jugements qui traduisent bien cette permissivité des juges. Par exemple, la Cour suprême, dans le cadre d'un *obiter,* dans un arrêt de droit criminel, avait à interpréter si l'absence d'une signature dans la déclaration d'un policier, bien que requise par la loi, était suffisante pour refuser toute portée audit document. Conformément à la vision du Doyen Flour qui considéra que le législateur met les formes et le juge les défait[93], les juges, à l'unanimité, considérèrent avec souplesse l'interprétation à donner à la réception des technologies et affirmèrent que :

> « lorsque cette question se pose, il convient d'y répondre, d'une part, en tenant compte du contexte, et notamment de l'importance de l'attestation personnelle, et, d'autre part, **en faisant preuve de la souplesse nécessaire pour permettre le recours à la technologie en constante évolution**. »[94] (nos soulignements)

Dans la même veine, et relativement à l'interprétation à donner au terme « écrit », notamment sur le fait de savoir s'il pouvait être réalisé par un télex, la Cour d'appel d'Ontario répondit par l'affirmative, basant principalement son interprétation sur une perception globale selon laquelle :

> « where technological advances have been made which facilitate communications and expedite the transmission of documents we see no reason why they should not be utilized. Indeed, they should be encouraged and approved. »[95]

---

93 Jacques FLOUR, « Quelques remarques sur l'évolution du formalisme », dans *Le droit privé français au milieu du vingtième siècle – Études offertes à Georges Ripert*, t. 1, Paris, L.G.D.J., 1950, p. 93, à la page 114.

94 *R.* c. *McIvor*, 2008 CSC 11 ; voir sur le sujet, en ligne : <http://www.gautrais.com/Enseignements-de-R-c-McIvor-CSC>.

95 *Rolling* c. *Williann Investments*, (1989) 70 O.R. 2d 578. Voir sur le sujet, en ligne : <http://www.gautrais.com/Calme-toi-la-Loi>.

Sans rendre la liste d'autorités en ce sens trop longue, l'on peut simplement dire qu'à plusieurs reprises, les juges se sont montrés sympathiques à l'utilisation des technologies de l'information, notamment, en droit criminel, relativement à la finalité d'un meilleur accès à la justice (surtout quant à l'usage d'une technologie de l'information pour permettre l'audition d'un témoin[96] ou d'instruire plus efficacement un jury[97] ou la légalité d'un mandat[98] ou l'écoute d'un avocat[99]). Également, et toujours relativement à la quête de la rationalité derrière un texte plus ancien que l'on doit interpréter, des perspectives équivalentes ont

---

96 *Wright* c. *Wasilewski,* [2001] O.J. No. 248 ; 52 O.R. (3d) 410 ; 102 A.C.W.S. (3d) 1105 (ON. S. C.) (LN/QL). On peut y lire : « **Case management encourages litigants to embrace modern technology, particularly where it will serve to simplify procedures, reduce costs, prevent unnecessary delay or give access where access might otherwise be denied**. Videoconferencing will not replace live trials. However, it does allow a party to overcome obstacles such as those presented in this case, and allow a party to fully and completely present her case. » (nos soulignements)

97 *Robinson Estate* c. *Doolittle Estate*, [1988] A.J. No. 325 ; 58 Alta. L.R. (2d) 390 ; 90 A.R. 376 ; 9 A.C.W.S. (3d) 409 (ABCA) (LN/QL). On peut y lire : « We encourage initiative, including modern technology or any other technique that might work to make the case simpler for the jury. »

98 *R.* c. *Weir*, [1998] A.J. No. 155 ; 1998 ABQB 56 ; [1998] 8 W.W.R. 228 ; 59 Alta. L.R. (3d) 319 ; 213 A.R. 285 ; 37 W.C.B. (2d) 302 (LN/QL), confirmé par [2001] A.J. No. 869 ; 2001 ABCA 181 ; [2001] 11 W.W.R. 85 ; 95 Alta. L.R. (3d) 225 ; 281 A.R. 333 ; 156 C.C.C. (3d) 188 ; 85 C.R.R. (2d) 369 ; 50 W.C.B. (2d) 463 (LN/QL). On peut notamment lire : « [81] **While I agree with the defence that s.487**, before the addition of subsection 2.1 and 2.2, **uses old language** (old in the use of the word « **things** » in the context of technology), **I disagree that the use of the old language precludes search and seizure to facilitate an investigation of technologically sophisticated offences**. » (nos soulignements)

99 *C.S.* c. *A.J.*, [2004] A.J. No. 73 ; 2004 ABQB 73 ; 50 Alta. L.R. (4th) 91 ; 153 A.C.W.S. (3d) 848 (LN/QL) ; 2004 CarswellAlta 383, en ligne : <http://www.canlii.org/en/ab/abqb/doc/2004/2004abqb73/2004abqb73.html>. On peut y lire : « it should be noted that the court encourages the use of contemporary technology wherever possible and would certainly hear a special chambers application by telephone if counsel wished to make their submissions in that way. »

été décelées tant dans des matières touchant au droit fiscal[100] qu'à d'autres en droit civil[101].

---

[100] *British Columbia Telephone Co.* c. *Canada* (F.C.A.), [1992] F.C.J. No. 27 ; [1992] A.C.F. no 27 ; 139 N.R. 211 ; [1992] 1 C.T.C. 26 ; 92 D.T.C. 6129 ; 31 A.C.W.S. (3d) 326 (LN/QL). On peut y lire : « In general, Courts have found that new technology is embraced by old language : Taylor v. Goodwin (1879), 4 Q.B.D. 228 ("bicycle" within "carriage") ; *Attorney General v. The Edison Telephone Company of London Ltd.*, (1880), 6 Q.B.D. 244 ("telephone" within "telegraph") ; *Canadian Pacific Railway Co. v. McCabe Grain Co. Ltd.*, (1968), 69 D.L.R. (2d) 313 (B.C.C.A.) (LN/QL) ("rape-seed" within "grain") ; *Lumberland Inc. v. Nineteen Hundred Tower Limited*, [1977] 1 S.C.R. 581 (LN/QL) ("form work" within "construction") ; Case X35 (1990), 90 ATC 316 (A.A.T.) ("invertor" within "converter") ; *Deneault* c. *Monette* (1933), 55 B.R. 111 (Que.) ("truck" within "horse and carriage"). The absence in Class 3 (j) of specifically expansive words such as "or similar" or "or other", used in some other Classes of Schedule II, cannot be decisive. Such expansive terms are expressly open-textured, but many other words may be implicitly so. »

[101] *Entreprises Robert Mazeroll ltée c. Expertech – Bâtisseur de réseaux inc.* [2005] J.Q. no 61 ; J.E. 2005-496 (Cour du Québec) (LN/QL). On peut y lire : « Le Tribunal est d'avis que l'article 2874 permettrait d'utiliser en preuve, lors du procès, la déclaration faite par le biais de la vidéoconférence en présence d'un sténographe. Cet article réfère à la loi concernant le cadre juridique des technologies de l'information. Cette loi, adoptée en 2001, établit l'interchangeabilité et la liberté de choix des supports et des technologies. Afin d'atteindre les objectifs de cette nouvelle loi, il faut interpréter la volonté du législateur de manière à innover dans le choix des moyens à prendre pour se conformer à la règle de droit. (…)

Cette loi qui s'applique à toute la législation québécoise, montre bien l'intention du législateur de permettre le recours aux technologies de l'information dans la mesure où une technologie n'est pas strictement interdite par la loi. (…)

Dans le cas qui nous occupe, il est vrai que le Code de procédure civile ne prévoit pas la possibilité de recourir à la vidéoconférence pour un interrogatoire au préalable, mais rien ne l'interdit.

L'article 294 du Code de procédure civile, applicable aux interrogatoires au préalable par le biais de l'article 395, prévoit que sauf lorsque qu'il est autrement prescrit, dans toutes causes contestées, les témoins sont interrogés à l'audience, la partie adverse présente ou dûment appelée. Il est possible d'imaginer différentes façons technologiques d'être présent. Le Code de procédure civile ne définie pas ce qu'est l'audience et n'implique pas forcément que les parties soient en présence physique l'une de l'autre. Le Code

Dans les faits, l'exercice judiciaire est un outil d'une grande adaptabilité face aux changements. Et au-delà du constat subjectif quant à l'approche relativement favorable des juges face aux technologies, l'on peut même affirmer, qu'en général, les juges ont effectué leur tâche avec une certaine clairvoyance. Éric Caprioli, dans une conférence organisée à l'automne 2008 à la Faculté de droit de l'Université de Montréal a même affirmé :

> « les juges sont capables d'appliquer une règle à un cas d'espèce. (…). Jusqu'à maintenant, ils ont fait du bon boulot, faisons leur confiance ![102] »

de procédure civile n'interdit pas qu'une partie interrogée au préalable soit dans un endroit différent de celui où se trouve le procureur qui l'interroge dans la mesure où la technologie est fiable. Ce qui est le cas de la vidéoconférence doublée par la présence d'un sténographe. »

[102] Éric CAPRIOLI, « Neutralité technologique », conférence en ligne : <http://www.gautrais.com/Videos>.

Partie 1

Principales opérations du cycle de circulation des RP.

Comme nous l'avons vu dans la Partie préliminaire, les nouvelles façons de faire, ainsi que les modes de fonctionnement induits par les nouveaux réseaux, nécessitent de mieux identifier le sens à donner à certaines notions cruciales fondant le cadre juridique de la protection des renseignements personnels. La circulation des documents dans des environnements en réseaux nécessite de mieux **qualifier** les situations juridiques multiples qui peuvent exister lorsqu'un document passe d'un point à un autre dans le cadre des différents processus d'affaires qui caractérisent les services fournis en réseaux. Et c'est exactement ce que nous nous proposons de faire désormais.

Aussi, les lois en matière de protection des renseignements personnels utilisent des termes que nous nous devons de décortiquer, tels que notamment « communiquer », « collecter », « transmettre », « détenir », « conserver », « utiliser », termes qu'il importe de revisiter au regard des nouvelles circonstances entraînées par les tendances récentes d'utilisation des technologies de l'information. Aussi, cette reconsidération, cette qualification, et cette interprétation cherchant à appliquer le droit aux faits nouveaux, seront illustrées au regard des trois illustrations factuelles que nous avons préalablement identifiées (Chapitre 2). Mais avant cela, il nous apparaît important de signaler que ces termes qui ont un sens souvent lié au support papier, doivent être interprétés au regard d'une notion, certes formellement absente des lois, à savoir, la notion de **contrôle** (Chapitre 1). En préalable, ce concept de contrôle doit, selon nous, être étudié dans la mesure où nous croyons qu'il est implicitement relié à la protection des renseignements personnels en général. En effet, cette protection ne peut être envisagée que ce sur quoi nous avons une certaine maîtrise. Pas de contrôle équivaut à pas de protection. C'est ce que nous verrons maintenant.

CHAPITRE 1
CADRE THÉORIQUE : LA NOTION DE CONTRÔLE

En effet, pour être tenu à des obligations en matière de renseignements personnels, il importe d'être en position de contrôle à l'égard des documents qui contiennent de tels renseignements. Cela est évident dans le monde des dossiers consignés uniquement sur support papier. Il en va de même pour les documents technologiques, ceux qui sont sur des supports faisant appel aux technologies de l'information. Par contre, dans l'univers numérique, la gamme des situations qu'il faut qualifier au regard de l'intensité du contrôle paraît plus étendue. Dans un réseau, certains acteurs peuvent théoriquement avoir la possibilité de contrôler physiquement les documents alors qu'en fait, ils sont dans une situation qui leur interdit de le faire. Il est donc opportun de préciser comment se pose la question du contrôle des documents dans les univers numérisés. Aussi, dans l'espace des réseaux et notamment dans celui dans lequel s'effectuent plusieurs prestations impliquant l'Administration et un citoyen, il importe d'analyser davantage la nature et la portée, notamment jurisprudentielle, qu'il est possible de trouver à cette notion de contrôle qui, si elle n'est pas nommément identifiée dans les lois, demeure reprise par plusieurs décisions de justice (Section préliminaire). Ensuite, nous envisagerons la situation selon laquelle les différents organismes publics n'exercent pas tous le contrôle sur ces renseignements à des degrés égaux et les conséquences que cela peut avoir en termes de responsabilité (Section 1). Enfin, nous constaterons que cette variété aura une incidence sur la définition que nous pourrions apporter à cette notion centrale de contrôle (Section 2).

SECTION PRÉLIMINAIRE – NOTION DE CONTRÔLE : LE CRITÈRE IMPLICITE DE LA PROTECTION DES RP

Dans le cadre de ces propos préliminaires, nous voudrions montrer, par l'exemple, que si la qualité de « contrôle » n'est pas explicitement présente dans les lois sur la protection des renseignements personnels, elle n'en demeure pas moins implicitement

déterminante et dans son sens premier, « contrôler », c'est exercer un rôle de surveillance, de vérification. Contrôler, c'est maîtriser.

À cet égard, le premier exemple que nous pourrions fournir concerne la situation où il s'agissait de déterminer si des documents détenus par une Administration devaient être qualifiés comme étant sous le contrôle d'une autorité soumise à la législation relative au droit d'accès. Précisément, dans *Commissaire à la protection de la vie privée* c. *Conseil canadien des relations de travail*[103], la juge Alice Desjardins de la Cour d'appel fédérale a statué sur la question de savoir si des notes « relèvent » d'une institution fédérale et de ce fait, pouvaient donner lieu à un droit d'accès de la part d'un citoyen. La réponse négative de la juge fut sans équivoque et explique, au paragraphe 5 de la décision que :

> « [5] Il n'est pas nécessaire que nous nous prononcions sur la question de savoir si les notes que les membres du Conseil ont prises constituent ou non des « renseignements personnels », **car il nous apparaît évident que ces notes ne « relèvent » pas du Conseil** au sens de l'alinéa 12(1) b) de la *Loi sur la protection des renseignements personnels*. Ces notes sont prises dans le cadre d'une instance quasi judiciaire non pas par des employés du Conseil, mais par des représentants du gouverneur en conseil investis de fonctions juridictionnelles qu'ils doivent exercer, non pas en qualité de mandataires du Conseil, mais de façon indépendante par rapport aux autres membres de celui-ci, y compris le président dudit Conseil ou d'une institution fédérale. Les membres du Conseil ne sont nullement tenus de prendre des notes, bien qu'ils puissent le faire. **Les notes ne font pas partie des archives officielles du Conseil et ne sont versées dans aucun autre système de tenue de registres sur lequel celui-ci exercerait un contrôle.**
>
> [6] Le juge de première instance a formulé les remarques suivantes auxquelles nous souscrivons :

[103] 2000 CanLII 15487 (C.A.F.), en ligne : <http://www.canlii.org/fr/ca/caf/doc/2000/2000canlii15487/2000canlii15487.html>.

> ... Il est évident que ni le Code canadien du travail, ni la politique et les procédures du CCRT, ne renferment de règle relative à ces notes. Les notes sont considérées par leurs auteurs comme quelque chose leur appartenant. **Les membres du CCRT sont entièrement libres de prendre des notes**, là où ils estiment que c'est indiqué, et ils peuvent aussi bien choisir de ne pas en prendre. Les notes sont destinées à n'être lues que par leur auteur. Nulle autre personne n'est autorisée à voir, à lire ou à utiliser ces notes, et leur auteur s'attend manifestement à ce que personne d'autre ne les voie. **Les membres restent responsables de la conservation et de la sauvegarde de leurs notes et peuvent à tout moment les détruire**. **Les notes, enfin, ne font pas partie des archives officielles du CCRT, et ne sont versées dans aucun fichier sur lequel le CCRT exercerait un contrôle administratif**. »[104] (Nos soulignements)

Dans le même esprit, une deuxième illustration peut être trouvée dans *Dhont* c. *Minister of Education et al*[105], où le tribunal explique que :

> « In my opinion, there is a distinction between "custody" and "control" as those terms are used in s.12(1)(c) of the Act. I am influenced in this regard by the conclusions of the Alberta Information and Privacy Commissioner when analyzing the Alberta legislation, which contained a transfer provision in exactly the same language as the Northwest Territories statute, in Order 2000-021 ; Re Alberta Justice, [2000] A.I.P.C.D. No. 38. **The Alberta Commissioner held (in para. 30) that "custody" refers to the physical possession of the actual records, while "control" refers to the authority to manage the records, whether or not they are in the physical possession of the body claiming control**. That, in my opinion, is the

---

[104] *Commissaire à la protection de la vie privée* c. *Conseil canadien des relations de travail*, 2000 CanLII 15487 (C.A.F.), en ligne : <http://www.canlii.org/fr/ca/caf/doc/2000/2000canlii15487/2000canlii15487.html>, citant 1996 CanLII 4084 (F.C.), (1996), 118 F.T.R. 1, p. 52, par. 105.

[105] *Dhont* c. *Minister of Education et al*, 2008 NWTSC 40, en ligne : <http://www.canlii.org/en/nt/ntsc/doc/2008/2008nwtsc40/2008nwtsc40.html>.

> correct interpretation of s.12(1)(c) of the Act. It accords as well with the interpretation given to "control" in federal access to information legislation, where the term has been held to include documents under the managerial or administrative control of the public body in question or under the public body's ultimate control : see Canada (Privacy Commissioner) v. Canada (Labour Relations Board), 1996 CanLII 4084 (F.C.), [1996] 3 F.C. 609 (T.D.), aff'd [2000] F.C.J. No. 617 (C.A.). » (Nos soulignements)

Encore, relativement à ces demandes liées à des accès de certains documents, en troisième lieu, dans son Ordonnance M – 165 du 21 juillet 1993, *Regional Municipality of Halton Police Services Board*, le Commissaire à la vie privée de l'Ontario convient de l'impossibilité d'établir une définition précise de « contrôle ». Mais il met de l'avant un ensemble de dix facteurs à considérer qui permettent d'aider à déterminer si une entité exerce ou non un contrôle à l'égard d'un renseignement personnel. Ces facteurs sont les suivants :

> « 1. Was the record created by an officer or employee of the institution ?
>
> 2. What use did the creator intend to make of the record ?
>
> 3. Does the institution have possession of the record, either because it has been voluntarily provided by the creator or pursuant to a mandatory statutory or employment requirement ?
>
> 4. If the institution does not have possession of the record, is it being held by an officer or employee of the institution for the purposes of his or her duties as an officer or employee ?
>
> 5. Does the institution have a right to possession of the record ?
>
> 6. Does the content of the record relate to the institution's mandate and functions ?
>
> 7. Does the institution have the authority to regulate the record's use ?

8. To what extent has the record been relied upon by the institution ?
9. How closely is the record integrated with other records held by the institution ?
10. Does the institution have the authority to dispose of the record ? »[106]

Ces facteurs, sur lesquels nous reviendrons[107], peuvent aider à déterminer, lorsqu'une pluralité d'entités est impliquée à l'égard d'un dossier ou d'un renseignement personnel, laquelle ou lesquelles de celles-ci exercent effectivement un contrôle à l'égard dudit renseignement personnel.

Dernier exemple enfin. Il est, en droit de la protection des renseignements personnels, un principe fondateur qui apparaît à de nombreuses reprises, à savoir celui de **la personne responsable des renseignements personnels**. Or, et au regard de la Loi anglaise de 1998 relative à la protection des renseignements et appelée *Data Protection Act,* il est fait référence à la notion de « Data controller »[108], non loin de celle que l'on trouve en France dans la *Loi numéro 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés* qui réfère au concept du « responsable d'un traitement de données à caractère personnel »[109]. Cette notion n'est pas éloignée de celle de « responsable » que l'on trouve dans les articles 4.1, 4.1.3, 4.8.2 a), et 4.10.1 de l'Annexe n° 1 de la *Loi sur la protection des renseignements personnels et*

---

106 Ordonnance M – 165 du 21 juillet 1993, *Regional Municipality of Halton Police Services Board*.

107 *Infra*, Partie 1, Chapitre 1, Section 1, 2.

108 *Data Protection Act 1998* – surtout les *"schedule 1 part II, schedule 2, schedule 3* & *schedule 4"* en ligne : <http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_11>

109 Articles 3, 5, 22 et 39 de la **Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés** en ligne : <http://www.legifrance.gouv.fr/affichTexte.do ?cidTexte=LEGITEXT000006068624&dateTexte=20090823>.

les documents électroniques plus communément connue sous l'acronyme de PIPEDA[110].

En effet, l'appellation anglaise de « Data controller » illustre, ne serait ce qu'a un niveau purement linguistique – puisque les textes de lois canadiens, québécois et français en expriment tout autant le concept par la notion de « responsable » – l'étroite relation entre les renseignements personnels et celui qui les « contrôle ». Cette étroite relation relève tant de la nature du renseignement personnel, de son degré d'intimité ou de sensibilité, que de l'identité de la personne qui effectue ce contrôle et l'étendue du contrôle qu'il a le droit d'effectuer sur le renseignement personnel en question. C'est pourquoi, dans tout le processus de « circulation » des renseignements personnels, en commençant par la « possession fortuite » ou la « collecte intentionnelle » et jusqu'à la « destruction » du renseignement personnel, tout en passant par sa « transmission », sa « publication », etc…, la notion de « contrôle » est omniprésente et constitue la composante incontournable de chacune de ces opérations, même si elle se manifeste dans chacune d'elles à un degré différent.

D'ailleurs, pour déterminer les rôles, droits et devoirs des divers acteurs qui prennent part à la circulation d'une information dans un réseau, il faut examiner sa relation avec le support de même qu'avec le contenu du message transmis[111]. Ce critère de contrôle serait même un pré-requis à l'imputation de toute responsabilité, y compris celle qui découle du traitement de renseignements personnels. Henry H. Perritt explique en effet à cet égard que :

---

110 Voir les articles 4.1, 4.1.3, 4.8.2 a), et 4.10.1 de l'Annexe n° 1 de la *Loi sur la protection des renseignements personnels et les documents électroniques*, L.C. 2000, c. 5, plus communément connue sous l'acronyme de PIPEDA en ligne : <http://www.canlii.ca/fr/ca/legis/lois/lc-2000-c-5/derniere/lc-2000-c-5.html>.

111 Pierre TRUDEL, « Liability in Cyberspace » dans Theresa FUENTES-CAMACHO, *The International Dimensions of Cyberspace Law,* UNESCO Press / Ashgate Publishing, 2000, 189-211.

> « In all three categories of tort liability (defamation, copyright infringement and invasion of privacy), the requisite fault cannot be proven without showing either that the actor and potential tort feasor exercised **some actual control** over content or that it was feasible for it to control content and that it could foresee the possibility of harm **if it did not control content**. » [112] (Nos soulignements)

Ainsi, lorsque des renseignements personnels ont été consignés par un employé ou un autre préposé d'un organisme et que ces renseignements sont conservés dans un document à l'usage de ce même organisme, ce dernier a très probablement le contrôle du document. Il en est de même lorsque l'organisme détient un document parce qu'il lui a été volontairement remis par son auteur ou lui a été remis en application d'une disposition impérative de la Loi. Cette première catégorie de situations est assez simple et concerne des hypothèses classiques qui sont souvent celles que l'on retrouve relativement à des documents sur support papier.

Des situations intermédiaires peuvent aussi être identifiées : par exemple, un organisme peut ne pas avoir la possession physique d'un document comportant des renseignements personnels auxquels il a le droit d'accéder mais il est détenu par un autre organisme effectuant avec lui une prestation en ligne de manière partagée. Alors, en pareil cas, les deux organismes peuvent se trouver dans une situation selon laquelle ils partagent le contrôle relatif à ce renseignement personnel.

Par contraste, lorsqu'un document est placé dans un environnement relevant de l'organisme public de la seule et unique volonté d'une personne, sans que cela serve à assurer une prestation à l'égard de ce citoyen ou d'une autre personne, on sera généralement dans la situation ou ledit organisme n'exerce pas de contrôle à l'égard des renseignements contenus dans un document.

---

[112] Henry H. PERRITT JR., « Tort Liability, the First Amendment and Equal Access to Electronic Networks », (1992) 5 *Harvard J. of L. & Tech.* 65, 110-111.

En fin de compte, le prérequis à l'application des obligations relatives à la protection des renseignements personnels est que l'entité ait effectivement le contrôle du renseignement et du document dans lequel celui-ci est consigné. Lorsque le contrôle exercé sur un document est limité, l'organisme pourra n'être tenu qu'à des devoirs de garde d'un document[113]. Lorsque plus d'un organisme participe à l'accomplissement d'une prestation à l'égard d'un citoyen, l'un et l'autre de ces organismes pourront être en position de contrôle.

D'ailleurs, et pour compléter le tout, il nous est possible de citer la toute récente décision de la Cour suprême *R. c. Patrick*[114] relativement à la situation selon laquelle la Cour a considéré comme valide la fouille faite par la police dans les poubelles du dénommé Patrick[115]. Or, la réponse de la Cour suprême est claire, presque unanime, avec la dissidence de Madame la juge Abella : pas de protection de la vie privée sur les poubelles. Au-delà de l'analyse de l'équilibre qui doit être proposé entre des intérêts contradictoires, comme presque toujours en matière constitutionnelle, la construction argumentaire s'est forgée autour de la **notion de « contrôle »**.

---

113 Cette notion de garde est celle que l'on trouve à l'article 26 de la *Loi concernant le cadre juridique des technologies de l'information*, L.R.Q., c. C-1.1, en ligne : <http://www.canlii.org///qc/legis/loi/c-1.1/20080818/tout.html>.

114 *R.* c. *Patrick*, 2009 CSC 17, en ligne : <http://csc.lexum.umontreal.ca/fr/2009/2009csc17/2009csc17.html>.

115 *R.* c. *Patrick*, 2009 CSC 17, en ligne : <http://csc.lexum.umontreal.ca/fr/2009/2009csc17/2009csc17.html>. Voir notamment le paragraphe de résumé : « Les policiers soupçonnaient P d'exploiter un laboratoire d'ecstasy dans sa maison. À plusieurs reprises, ils ont pris des sacs d'ordures que P avait déposés, en vue de leur ramassage, à l'arrière de sa maison, qui est contiguë à une ruelle. Les policiers n'ont pas eu à pénétrer sur la propriété de P pour s'emparer des sacs, mais ils ont toutefois dû allonger les bras au-dessus des limites de sa propriété pour le faire. Les policiers ont utilisé des éléments de preuve d'activités criminelles trouvés dans le contenu des ordures de P pour obtenir un mandat les autorisant à perquisitionner dans la maison et le garage de ce dernier. Des éléments de preuve additionnels ont été saisis durant la perquisition. »

Le dénommé Patrick, en décidant de mettre ses poubelles à la rue, avait décidé de perdre le **contrôle** sur ses propres données. Ces données pouvaient donc être utilisées par autrui et notamment, en l'occurrence, les services de police. Voici les paragraphes pertinents, dans le résumé préliminaire d'abord.

> « Le caractère raisonnable de l'attente en matière de respect de la vie privée varie selon la nature de l'élément à l'égard duquel la protection est revendiquée, le lieu et les circonstances de l'intrusion de l'État, ainsi que l'objet de cette intrusion. En l'espèce, les ordures de P ont été déposées à l'endroit habituel à la limite de la propriété ou à proximité de celle-ci, en vue de leur ramassage, **et aucun signe n'indiquait le maintien du contrôle sur les ordures ou de l'affirmation d'un droit au respect de la vie privée à leur égard** ».[116] (Nos soulignements)

Plus loin, on peut également lire :

> « Objectivement parlant, P a renoncé à son droit au respect de sa vie privée à l'égard des renseignements en cause au moment où il a déposé les sacs d'ordures en vue de leur ramassage à l'arrière de sa propriété, à la limite du terrain. Il avait fait tout ce qu'il fallait pour confier ses ordures au système municipal de ramassage. Les sacs n'étaient pas protégés et ils se trouvaient à la portée de quiconque circulait dans la ruelle, notamment les sans-abri, les ramasseurs de bouteilles, les fouilleurs de poubelles, les voisins fouineurs et les galopins, sans oublier les chiens et autres animaux, ainsi que les éboueurs et les policiers. Toutefois, jusqu'au moment où les ordures sont placées à la limite du terrain ou à la portée de quelqu'un se trouvant à cette limite, **l'occupant conserve une part de contrôle sur la façon dont il en sera disposé**. On ne saurait dire qu'il les a abandonnées de façon certaine si elles se trouvent sur une galerie, dans un garage ou à proximité immédiate de la résidence. En l'espèce, l'abandon est fonction à la fois du lieu et de l'intention de P. » [117] (Nos soulignements)

---

[116] *R.* c. *Patrick*, 2009 CSC 17, en ligne : <http://csc.lexum.umontreal.ca/fr/2009/2009csc17/2009csc17.html>.

[117] *R.* c. *Patrick*, 2009 CSC 17, en ligne : <http://csc.lexum.umontreal.ca/fr/2009/2009csc17/2009csc17.html>.

Et dans le corps du texte, voici aussi trois paragraphes très intéressants :

> « [39] **Quatre éléments factuels** sont d'une importance primordiale dans le présent pourvoi : (i) les ordures ont été déposées par l'appelant à l'endroit habituel en vue de leur ramassage ; (ii) cet endroit se trouvait à la limite de la propriété, ou près de cette limite ; **(iii) aucun signe (tel un réceptacle verrouillé) n'indiquait le maintien du contrôle sur les ordures** ou de l'affirmation d'un droit au respect de la vie privée à leur égard ; (iv) les policiers ont pris les sacs afin d'y chercher des renseignements sur des activités ayant lieu dans la maison, dans le cadre d'une enquête criminelle en cours. »
>
> « [62] Néanmoins, jusqu'au moment où les ordures sont placées à la limite du terrain ou à la portée de quelqu'un se trouvant à cette limite, **l'occupant conserve une part de contrôle** sur la façon dont il en sera disposé et on ne saurait dire qu'il les a abandonnées de façon certaine, surtout si elles se trouvent sur une galerie, dans un garage ou à proximité immédiate de la résidence, où s'appliquent les principes énoncés dans les arrêts portant sur les « perquisitions périphériques », tels Kokesch, Grant et Wiley.
>
> [63] Dans les municipalités où les éboueurs viennent jusqu'au garage ou à la galerie pour y chercher les ordures et les apporter à la rue (s'il existe encore de telles municipalités), les éboueurs pénètrent sur la propriété en vertu d'une autorisation (au moins) implicite du propriétaire. Cette autorisation ne s'étend pas aux policiers. Toutefois, lorsque les ordures sont placées à la limite de la propriété pour la collecte, **j'estime que le propriétaire a suffisamment renoncé au droit et au contrôle qu'il avait à leur égard pour qu'il ne subsiste plus aucun droit objectivement raisonnable en matière de respect de sa vie privée**. » [118] (Nos soulignements)

---

[118] *R.* c. *Patrick*, 2009 CSC 17, en ligne : <http://csc.lexum.umontreal.ca/fr/2009/2009csc17/2009csc17.html>.

Ainsi, et comme dans les autres exemples préalablement soulevés, cette décision constitue une nouvelle illustration de la plus haute cour qui montre le caractère implicite de la notion de contrôle dans la gestion des documents contenant des renseignements personnels.

SECTION 1 – DIFFÉRENTES INTENSITÉS DANS LE CONTRÔLE DE L'INFORMATION

Le degré de contrôle de l'information se situe sur un *continuum*. Il est rare que l'on se trouve dans une situation de contrôle total ou d'absence complète de contrôle. Dans les processus de gestion caractéristiques des administrations en réseau, une entité peut partager le contrôle d'un document avec une autre, elle peut exercer un contrôle complet ou partiel sur un document. Les entités peuvent aussi se trouver en situation de non-contrôle à l'égard d'un renseignement personnel ce qui signifie alors qu'elles pourront avoir des obligations conséquentes à l'égard du document et des renseignements qu'il comporte.

1 – Notion d'échelle de contrôle

Pour rendre compte du régime juridique applicable à la protection des renseignements personnels dans un réseau et calibrer de façon adéquate les droits et les obligations de ceux qui interviennent dans les diverses opérations de traitement de ces documents technologiques, il est nécessaire de caractériser plus précisément les types de maîtrise et de contrôle qui sont exercés sur les documents.

L'objet et la portée des droits et responsabilités des différents acteurs qui interviennent dans la communication électronique tiennent au degré de contrôle et de maîtrise qu'ils exercent – ou qu'ils sont réputés exercer – sur l'information se trouvant entre leurs mains et les communications qui se déroulent dans les réseaux. L'imputation de la responsabilité à une entité requiert d'identifier les acteurs qui ont la maîtrise de l'information dans

les divers lieux de cet environnement virtuel.[119] Dès 1993, Eric Schlachter écrivait à cet égard que :

> « There is a **sliding scale of control** in relation to forced access. At one end of the scale are primary publishers, who have virtually unrestrained discretion over what they print or to whom they give access to disseminate information. Also on this end are owners of private property, who are similarly protected from mandatory or forced access. (...) At the other end of the sliding scale from primary publishers are common carriers who by definition must be available to all comers and cannot refuse to provide service in a discriminatory fashion ».[120] (Nos soulignements)

Cette « échelle mobile » concerne aussi bien les droits d'accès aux informations que l'ensemble des autres relations qui peuvent exister entre un acteur donné et l'information qui transite dans un réseau. C'est à partir de ce constat que la doctrine et les tribunaux ont développé les principes relatifs à la responsabilité des acteurs dans un réseau. C'est à ces principes qu'il faut se référer lorsque vient le temps de départager la nature et l'intensité des obligations à l'égard des renseignements personnels. Schlachter relève à cet égard que

> « Those entities with more **editorial control** generally also have greater exposure to tort liability for the statements or actions of others. »[121] (Nos soulignements)

Le « contrôle » auquel Schlachter fait référence doit être entendu en son sens générique : celui du contrôle sur l'informa-

---

119 Voir Pierre TRUDEL, « La protection des droits et des valeurs dans la gestion des réseaux ouverts », dans CRDP, *Les autoroutes électroniques : usages, droit et promesses*, Montréal, Éditions Yvon Blais, 1995, p. 324 et 325.

120 Eric SCHLACHTER, « Cyberspace, the Free Market and the Free Marketplace of Ideas : Recognizing Legal Differences in Computer Board Functions », (1993) 16 Hastings Comm/Ent L.J. 113 et suiv.

121 Eric SCHLACHTER, « Cyberspace, the Free Market and the Free Marketplace of Ideas : Recognizing Legal Differences in Computer Board Functions », (1993) 16 Hastings Comm/Ent L.J. 113 et suiv.

tion, c'est à dire l'exercice à l'égard de celle-ci des divers pouvoirs qui sont possibles. Par exemple, lorsque je donne un renseignement me concernant, j'exerce une fonction de contrôle à l'égard de cette information. Ainsi, il est donc possible de caractériser l'intensité de la responsabilité à partir de l'intensité du contrôle qu'une personne exerce effectivement sur l'information dans une situation déterminée.

C'est d'ailleurs en tenant compte de l'intensité du contrôle exercé sur un document que fut développé le cadre juridique présidant à la détermination des droits et des responsabilités relatives aux informations circulant dans les réseaux. Plus on a le contrôle sur un document, plus on en répond.

Dans un réseau, tout comme dans le monde physique, l'information voyage entre les mains d'une pluralité d'acteurs qui, tout en contribuant à déplacer l'information, n'acquièrent sur celle-ci qu'un contrôle strictement physique : le postier qui livre une lettre à certes le contrôle physique sur celle-ci pendant le déroulement des différentes étapes de sa livraison, mais il ne dispose d'aucun contrôle qui lui permettrait de prendre connaissance des renseignements qu'elle contient. Inversement, lorsqu'une personne se fait communiquer un document, elle peut, selon sa situation juridique se voir conférer des droits de contrôle étendus sur celui-ci.

2 – Critères d'identification de l'intensité du contrôle

Au Québec, un changement législatif significatif a dû être considéré avec l'introduction en 2001 de la *Loi concernant le cadre juridique des technologies de l'information*. Dans ce texte ambitieux, il s'agissait notamment de distinguer les deux éléments que sont le support et l'information[122]. Il est donc important que

[122] *Loi concernant le cadre juridique des technologies de l'information*, L.R.Q., c. C-1.1, en ligne : <http://www.canlii.org///qc/legis/loi/c-1.1/20080818/tout.html>. On peut notamment référer sur ce point à l'article 3 qui dispose que « Un document est constitué d'information portée par un support. » « Information » et « support » : deux composantes essentielles d'un document.

l'évaluation de l'intensité du contrôle soit distincte du support physique dans lequel est structurée l'information.

Aussi, cette loi énonce les principes qui permettent de mieux qualifier les différents participants à des activités de communication en ligne. Nous croyons que cette loi nous aide à déterminer – soit explicitement soit implicitement – des critères précisant la nature et l'intensité du contrôle exercé par les acteurs en cause.

Par ailleurs, il nous semble utile de constater que le contrôle s'exerce aussi en vertu de la *Loi sur la protection des renseignements personnels et des documents électroniques*[123], qui est une loi fédérale canadienne, applicable à la fois aux secteurs public et privé. C'est d'ailleurs à ce titre que, le 16 Juillet 2009, le Commissariat à la protection de la vie privée du Canada a rendu public son rapport de conclusions de l'enquête menée suite à la plainte déposée par la *Clinique d'Intérêt Public et de Politique d'Internet du Canada* (CIPPIC) contre *Facebook*[124], déclarant *Facebook* en contravention aux droits à la vie privée des canadiens à raison de huit sujets sur douze sur lesquels portait la plainte[125]. A plusieurs reprises en effet, le rapport évoque l'importance de la notion de contrôle en tant que fondement de la loi elle-même :

> « 7. À une époque où tout le monde semble laisser l'empreinte numérique de ses points de vue, photos, croyances et parfois même de ses aléas amoureux, **notre notion du contrôle de ses propres renseignements personnels — qui constitue le fondement de la Loi sur la protection des renseignements**

---

123 *Loi sur la protection des renseignements personnels et les documents électroniques* (PIPEDA) en ligne : <http://www.canlii.ca/fr/ca/legis/lois/lc-2000-c-5/derniere/lc-2000-c-5.html>.

124 Rapport du Commissariat à la protection de la vie privée du Canada dans l'enquête menée suite à la plainte de la *Clinique d'Intérêt Public et de Politique d'Internet du Canada* (CIPPIC) contre *Facebook* en ligne : <http://www.priv.gc.ca/cf-dc/2009/2009-008-0716-f.pdf>.

125 Rapport du Commissariat à la protection de la vie privée du Canada dans l'enquête menée suite à la plainte de la *Clinique d'Intérêt Public et de Politique d'Internet du Canada* (CIPPIC) contre *Facebook* en ligne : <http://www.priv.gc.ca/cf-dc/2009/2009-008-0716-f.pdf>.

> **personnels et les documents électroniques — se trouve sérieusement ébranlée.** » (…)
>
> « 13. **Le contrôle qu'exerce une personne sur ses propres renseignements personnels est l'une des principales notions qui sous-tend la Loi**. » (…)
>
> « 19. Nous sommes reconnaissants envers Facebook de leur coopération pendant toute la durée de l'enquête et nous apprécions son engagement manifeste à permettre aux utilisateurs d'exercer un **contrôle** sur leurs renseignements personnels tout en leur offrant la possibilité d'entrer en contact avec d'autres. » (…)
>
> « 87. Il est digne de mention que Facebook fournit aux utilisateurs des paramètres de confidentialité très complets. Je considère que ces paramètres donnent suite aux principes de la **Loi en permettant aux utilisateurs de contrôler l'échange de leurs renseignements**. Toutefois, tel que mentionné ci-dessus, Facebook pourrait améliorer certains de ces paramètres. » (nos soulignements)[126]

Ce point de vue à d'ailleurs été confirmé par le second rapport sur le même sujet par la Commissaire adjointe à la vue privée Elizabeth Denham[127].

---

[126] Rapport du Commissariat à la protection de la vie privée du Canada dans l'enquête menée suite à la plainte de la *Clinique d'Intérêt Public et de Politique d'Internet du Canada* (CIPPIC) contre *Facebook* en ligne : <http://www.priv.gc.ca/cf-dc/2009/2009-008-0716-f.pdf>.

[127] Mot d'ouverture lors d'une conférence de presse sur Facebook, en ligne : <http://www.priv.gc.ca/speech/2009/sp-d_20090827_ed_f.cfm> « Je tiens à mettre l'accent ici. Plusieurs des changements que nous abordons avec Facebook visent à *donner le contrôle* aux utilisateurs. Il va sans dire que nous encourageons les personnes à prendre connaissance et à tirer avantage des nouveaux renseignements et mécanismes que Facebook est en voie d'introduire. » (les soulignements proviennent de l'auteure)

A – Critère de l'activité de l'utilisateur

Le prestataire visé à l'article 22 de la *Loi concernant le cadre juridique des technologies de l'information* , celui qui agit à titre d'intermédiaire pour offrir des services de conservation de documents technologiques sur un réseau de communication, n'est pas directement responsable des activités accomplies par l'utilisateur du service au « moyen des documents remisés par ce dernier ou à la demande de celui-ci ».

Ce principe a un caractère général : il marque la distinction entre le prestataire qui exerce le contrôle sur un document et celui qui, bien que pouvant se trouver en possession du document n'a pas de contrôle sur celui-ci. Le second alinéa de l'article 22 explicite le processus par lequel le prestataire peut engager sa responsabilité. L'article 22 pose en effet qu'

> « il peut engager sa responsabilité, notamment s'il a de fait connaissance que les documents conservés servent à la réalisation d'une activité à caractère illicite ou s'il a connaissance de circonstances qui la rendent apparente et qu'il n'agit pas promptement pour rendre l'accès aux documents impossible ou pour autrement empêcher la poursuite de cette activité. » [128]

Ce principe aide à déterminer à quel moment naît une obligation de se comporter à l'égard d'un document comme si on en avait acquis le contrôle.

L'article 22 en question vise les prestataires qui « agissent » à titre d'intermédiaires. Le régime qui module leur responsabilité énoncée à l'article 22 trouve application lorsqu'ils « agissent » à titre d'intermédiaire. Selon les situations, un même acteur peut agir à différents titres : par exemple, un maître de blogue peut publier des documents dont il est l'auteur et laisser diffuser sur son blogue des documents en provenance d'autrui. Ce qui caractérise l'intermédiaire visé à l'article 22 est le fait qu'il n'accomplit

---

[128] *Loi concernant le cadre juridique des technologies de l'information*, L.R.Q., c. C-1.1, en ligne : http ://www.canlii.org///qc/legis/loi/c-1.1/20080818/tout.html.

pas lui-même les activités qui se réalisent au moyen des services qu'il fournit.

Pour que joue la règle énoncée à l'article 22, il faut que le prestataire agisse à titre d'intermédiaire pour offrir des services de conservation de documents technologiques sur un réseau de communication. Le principe de non-responsabilité du prestataire de « services de conservation » vise les

> « activités accomplies par l'utilisateur du service au moyen des documents remisés par ce dernier ou à la demande de celui-ci. »[129]

Pour déterminer si le prestataire de service est régi par le régime de non-responsabilité, il faut déterminer si les activités sont accomplies par l'utilisateur du service au moyen des documents. Le critère est celui de l'accomplissement d'une activité par l'utilisateur. Le principe de non-responsabilité de l'intermédiaire joue dès lors que l'on se trouve en présence d'une activité accomplie par l'utilisateur du service au moyen de documents remisés par ce dernier.

Lorsque l'activité menée dans un environnement est « accomplie » par l'utilisateur du service, le principe de non responsabilité du prestataire entre en ligne de compte. Par exemple, dans le CV commun des professeurs d'université au Canada que nous avons vu dans ce que nous avons appelé « l'illustration 2 » relative à « PEL et garde de RP »[130], c'est l'utilisateur qui introduit les documents et qui décide des commandes afin de rendre disponible l'information à tel ou tel organisme.

Il en est de même dans un site où l'utilisateur dépose des documents afin qu'ils y soient diffusés ou rendus disponibles au public en général, comme dans « l'illustration 3 » relative à « PEL et publication de RP »[131].

---

[129] Article 22 al. 1, *Loi concernant le cadre juridique des technologies de l'information*, L.R.Q., c. C-1.1, en ligne : <http://www.canlii.org///qc/legis/loi/c-1.1/20080818/tout.html>.

[130] *Supra*, Chapitre 1, Section 1, 2, B.

[131] *Supra*, Chapitre 1, Section 1, 2, C.

La règle s'applique aussi lorsqu'un utilisateur, dans un site où l'accès lui est exclusif, dépose des documents et détermine à qui ceux-ci seront transmis ou communiqués.

Ainsi, le critère de départage est l'accomplissement d'activités par l'utilisateur. Dès lors que celui-ci accomplit des activités, celles-ci relèvent nécessairement de sa responsabilité. Le rôle actif de l'utilisateur est ici crucial.

Il est donc possible d'identifier une échelle d'intensité dans le contrôle des documents. Lorsque ces documents résultent de la seule activité de l'utilisateur, le principe de non-responsabilité du prestataire joue pleinement. À l'inverse, lorsque le document est utilisé seulement par le prestataire, on ne se trouve pas dans la situation visée à l'article 22 établissant un régime d'exonération de responsabilité. Au contraire, il s'agira plutôt d'appliquer le régime de responsabilité attaché par les lois sur la protection des renseignements personnels.

Notons enfin que l'importance du rôle de l'utilisateur a également été expressément mis de l'avant dans l'affaire *Facebook* traitée par le Commissariat fédéral de protection de la vie privée[132], et ce, même si cet élément n'est pas à proprement parler

---

132 Voir notamment la lettre de la Commissaire adjointe Madame Denham, en ligne : <http://www.priv.gc.ca/speech/2009/sp-d_20090827_ed_f.cfm>, qui sous le paragraphe explicite « Responsabilité des utilisateurs » se lit ainsi : « Comme entreprise, Facebook a certaines obligations en vertu de la loi canadienne sur la protection des renseignements personnels. Notre rôle est de s'assurer que Facebook respecte la loi.

Les utilisateurs aussi ont un rôle important à jouer.

Je tiens à mettre l'accent ici. Plusieurs des changements que nous abordons avec Facebook visent à *donner le contrôle* aux utilisateurs. Il va sans dire que nous encourageons les personnes à prendre connaissance et à tirer avantage des nouveaux renseignements et mécanismes que Facebook est en voie d'introduire.

Les utilisateurs de Facebook — et de tout autre site de réseautage social, d'ailleurs — ont leur part de responsabilité. Ils doivent s'informer de la manière dont leurs renseignements personnels seront utilisés et partagés. Prenez le temps de lire les politiques de confidentialité ! Et servez-vous des paramètres de confidentialité offerts sur les sites ! »

dans la lettre même de la loi fédérale sur la protection des renseignements personnels[133].

B – Critère de l'activité de la PEL

Il en est donc différemment dès lors que le prestataire effectue des vérifications sur les documents remisés par les utilisateurs. Par exemple, afin de s'assurer que les documents déposés respectent le thème, on ne peut soutenir qu'il « utilise » le document ou qu'il acquiert un contrôle sur celui-ci. Le fait d'effectuer ce type de vérifications ne constitue pas une « utilisation » du document. C'est une opération comparable à celle que ferait le dépositaire de livres et de revues afin de classer les publications qu'il offre en vente dans les espaces appropriées.

Dans de telles situations, le prestataire ne reçoit pas communication du document : il s'en tient à effectuer sur celui-ci des vérifications purement matérielles afin de déterminer si le document est correctement classé ou qu'il correspond effectivement au thème assigné à l'espace d'hébergement.

Comme l'explique le rapport des députés français Dionis du Séjour et Erthel :

> (…) un fournisseur d'hébergement est nécessairement conduit à structurer l'information qu'il stocke sur son ou ses serveurs. Il doit en effet au moins allouer à l'hébergé un espace déterminé de son serveur et, pour que l'internaute puisse consulter cet espace, rendre visible cette structure au sein de la page même sur laquelle figurent les informations hébergées.
>
> La structure donnée au service d'hébergement participe donc de l'essence même de ce service.
>
> La loi ne fait d'ailleurs pas dépendre la qualité d'hébergeur de la manière dont le service d'hébergement est organisé.

---

133 *Loi sur la protection des renseignements personnels et les documents électroniques* (PIPEDA) en ligne : <http://www.canlii.ca/fr/ca/legis/lois/lc-2000-c-5/derniere/lc-2000-c-5.html>.

> En tout état de cause, un hébergeur qui définit une typologie des blogs sur son site, et qui ventile ces blogs, au sein du classement qu'il a établi, en fonction de leur nature annoncée a une action **beaucoup plus proche de celle d'une chaîne de kiosques à journaux**, qui regroupe sur ses présentoirs les magazines en fonction de leurs centres d'intérêt, que celle d'un éditeur.[134] (Nos soulignements)

Ces distinctions au sujet des fonctions de l'hébergeur et la qualification qui en résulte au regard de sa relation avec les documents et l'information permettent de mettre en lumière les différents degrés dans la relation entre un document et les entités qui le détiennent.

L'entité qui contrôle un document est celle qui le crée et l'utilise. D'ailleurs, la plupart des dix critères mis de l'avant par le commissaire ontarien[135] ont rapport à l'utilisation du document. Plus l'organisme utilise ou est en position d'utiliser le document, plus l'on tend à déduire qu'il exerce le contrôle à l'égard de celui-ci.

C'est ainsi que dans cette décision précitée, un premier critère a trait à la création du document (1. Was the record created by an officer or employee of the institution ?). Créer un document correspond à en déterminer l'existence et le sens ; aussi, il est difficile d'imaginer un acte de création sans l'exercice d'un contrôle manifeste sur le document.

Les autres critères sont relatifs à l'utilisation des documents. Le droit à la possession d'un document doit forcément être qualifié en regard du contrôle. (5. Does the institution have a right to possession of the record ?). C'est à cette dimension que renvoient les critères relatifs à l'utilisation ou au droit d'utiliser un docu-

---

134 Jean DIONIS DU SÉJOUR et Corinne ERTHEL, *Rapport d'information no. 627 déposé en application de l'article 86, alinéa 8, du Règlement sur la mise en application de la loi no. 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique*, Assemblée nationale, 23 janvier 2008, p. 21. <http://www.assemblee-nationale.fr/13/rap-info/i0627.asp >.

135 Ordonnance M – 165 du 21 juillet 1993, *Regional Municipality of Halton Police Services Board*.

ment. Lorsque l'entité utilise le document, elle dispose forcément d'un certain contrôle sur celui-ci, ce qui renvoie au second critère (2. What use did the creator intend to make of the record ?)

Le motif de la possession du document est aussi à prendre en considération : le troisième critère invite à s'interroger sur le caractère volontaire de la possession d'un document par l'organisme (3. Does the institution have possession of the record, either because it has been voluntarily provided by the creator or pursuant to a mandatory statutory or employment requirement ?)

La même approche vaut pour le huitième critère (8. To what extent has the record been relied upon by the institution ?) . Si une entité se fie à l'information d'un document, elle doit forcément avoir à l'égard de celui-ci un certain contrôle ou au minimum, une connaissance de celui-ci.

Lorsque le document est intégré à un ensemble documentaire contrôlé par une entité pour ses propres fins, il en découle habituellement une situation dans laquelle l'organisme exerce un contrôle sur le document, ce qui correspond à la situation du neuvième critère (9. How closely is the record integrated with other records held by the institution ?)

Même sans avoir la possession physique d'un document, une personne peut l'avoir et exercer un contrôle plus ou moins intense sur le document ce qu'évoque le quatrième critère (4. If the institution does not have possession of the record, is it being held by an officer or employee of the institution for the purposes of his or her duties as an officer or employee ?)

C – Critère du pouvoir d'action sur le document

Également, d'autres critères ne sont pas en eux-mêmes déterminants au regard du contrôle mais évoquent néanmoins un potentiel à cet égard. Ainsi, la teneur d'un document peut relever du mandat d'un organisme, et ce, même si cela ne signifie pas que ce dernier soit en toutes circonstances en position de contrôle à l'égard d'un document spécifique. Le critère évoqué dans cette même décision

« (6. Does the content of the record relate to the institution's mandate and functions ? »[136].

Il en va de même pour les documents à l'égard desquels l'entité possède un pouvoir de réglementation, ce qui renvoie au septième critère

« (7. Does the institution have the authority to regulate the record's use ?). »[137]

Le même raisonnement s'applique à l'égard du pouvoir de détruire le document identifié dans le principe 10 selon lequel

« 10. Does the institution have the authority to dispose of the record ?). »[138]

Ainsi, si l'on situe les différentes situations révélant l'intensité du contrôle exercé à l'égard d'un document l'on obtient la gradation suivante : à une extrémité de *continuum*, il y a la situation du contrôle complet pouvant notamment impliquer, à titre d'illustration, création du document en le rédigeant ou en décidant de son contenu et de son sens ; utilisation dans le cadre de processus décisionnel ; capacité de modifier le document ou capacité de régir l'utilisation du document, ou de façon générale, ce qui peut en être fait.

Dans d'autres hypothèses, il est des situations dans lesquelles on n'a pas le contrôle du document et comme par exemple celles qui découlent de circonstances où une entité n'effectue pas d'utilisation du document. Il en va ainsi de la possession du document à titre précaire, pour le compte d'un autre. Dans cette situation, l'entité peut effectuer des actions à caractère mécanique sur le document comme les vérifications purement formelles (type de fichiers, type d'informations, présence ou absence de certains

---

136 Ordonnance M – 165 du 21 juillet 1993, *Regional Municipality of Halton Police Services Board*.

137 Ordonnance M – 165 du 21 juillet 1993, *Regional Municipality of Halton Police Services Board*.

138 Ordonnance M – 165 du 21 juillet 1993, *Regional Municipality of Halton Police Services Board*.

mots ou de certaines catégories de données) ou de conformité formelle à certains critères.

Dans cet ensemble d'opérations, il existe un point de bascule entre la possession purement physique du document et la connaissance de l'information[139]. Il peut en effet arriver que le prestataire intermédiaire effectuant certaines opérations à caractère mécanique ou routinier pourrait acquérir la connaissance de certaines informations. Alors, sans en avoir eu le contrôle initialement, il pourrait se trouver en situation de connaître certaines informations dans un document. Cette situation emporte alors un changement dans les responsabilités qui lui incombent, les renforçant et les soumettant à plus de contraintes que sa situation initiale ne le permet.

D – Critère de la connaissance du PEL

En effet, pour le prestataire intermédiaire visé à l'article 22, la connaissance est la condition nécessaire afin que naissent pour lui des obligations à l'égard de l'information qu'il conserve. Par exemple, toujours aux termes de l'article 22 de la *Loi concernant le cadre juridique des technologies de l'information,* et comme nous l'avons vu précédemment, le prestataire qui agit à titre d'intermédiaire pour offrir des services de conservation de documents technologiques sur un réseau n'est pas responsable des « activités accomplies par l'utilisateur du service au moyen des documents remisés par ce dernier »[140]. Ainsi, lorsque le « prestataire-intermédiaire » propose une plateforme dans laquelle il est loisible aux usagers de déposer des informations afin que celles-ci soient rendues disponibles à des tiers, le prestataire qui offre de tels services de conservation n'en acquiert pas pour autant le contrôle sur les documents ainsi traités. Ces documents ne lui sont pas communiqués : ils sont rendus publics par l'usager qui choisit de le

---

139 Infra, Chapitre 1, Section 2, 2

140 Article 22 al.1 de la *Loi concernant le cadre juridique des technologies de l'information*, L.R.Q., c. C-1.1, en ligne : <http://www.canlii.org///qc/legis/loi/c-1.1/20080818/tout.html>.

faire *via* la plateforme. C'est davantage l'usager qui contrôle les documents et décide de les transmettre à un tiers.

Plusieurs cas de figure sont susceptibles d'être envisagés relativement à de pareilles situations. Premier exemple, un usager peut utiliser une plateforme de conservation de documents technologiques pour communiquer avec un prestataire afin que celui-ci lui fournisse des renseignements. Ainsi, l'usager peut exercer son droit d'accéder à ses propres renseignements personnels à partir d'un prestataire en ligne. Il appelle donc à lui ses renseignements qu'il conserve dans le répertoire offert par le prestataire de services de conservation. Là encore ce prestataire n'a pas eu communication des documents.

Une autre illustration que nous pouvons apporter ici tient au fait que certaines prestations en ligne peuvent servir à la réalisation d'une opération préalable à la réalisation d'une transaction. Par exemple, afin de s'identifier auprès d'un prestataire de services gouvernementaux, un usager pourra choisir d'accéder à ses renseignements personnels détenus par un organisme public à partir de la plateforme d'un prestataire de services de conservation. Ayant reçu ses renseignements, l'usager pourra décider de les acheminer à un autre organisme public. Dans un tel schéma, l'intermédiaire exploitant la plateforme de conservation n'a pas reçu communication des renseignements personnels traités par l'usager. C'est plutôt l'usager qui a reçu communication des renseignements. Par la suite, l'usager a décidé de communiquer ces renseignements à un autre organisme. La communication a été faite uniquement à l'organisme auquel l'usager a transmis ses renseignements personnels.

Le principe d'exonération énoncé à l'article 22 de la *Loi concernant le cadre juridique des technologies de l'information* ne pourra s'appliquer que dans des situations où le « prestataire-intermédiaire » n'a aucunement connaissance de ces informations ou bien il n'a pas vocation à avoir connaissance de ces documents ni en fait ni en droit. Certes, il est techniquement possible pour ce prestataire de prendre connaissance du document et s'il le fait, il pourra devoir en être responsable. Mais comment peut-on le rendre responsable tant qu'il ne prend pas connaissance du document ?

Il importe donc de distinguer entre le droit et la possibilité technique de prendre connaissance d'un document. Imposer un ensemble d'obligations à une entité sur la seule base que celle-ci a la capacité technique d'en prendre connaissance est une approche tout à fait disproportionnée[141]. Il est dans pareilles situations amplement suffisant de s'assurer d'appliquer les sanctions si des accès non autorisés devaient être constatés.

La situation est la même à l'égard de la responsabilité de l'intermédiaire passif qui transporte les documents technologiques tel que l'intermédiaire visé à l'article 36 de la *Loi concernant le cadre juridique des technologies de l'information*[142], celui-ci n'agissant que comme transmetteur. Cet intermédiaire n'est pas, en principe, responsable des actions accomplies par autrui au moyen des documents qu'il transmet ou qu'il conserve durant le cours normal de la transmission et pendant le temps nécessaire pour en assurer l'efficacité. Mais il peut engager sa responsabilité dans les situations mentionnées à l'article 36.

Lorsque le prestataire a un contrôle accru sur le document, sa responsabilité à l'égard du document augmente. Ainsi, le prestataire qui est à l'origine de la transmission du document est en quelque sorte considéré avoir lui-même décidé de le transmettre. Alors, il n'est plus vraiment un intermédiaire passif. Il joue un rôle actif dans la décision de transmettre, ce qui est de la nature de l'exercice d'un certain contrôle sur le document.

Le prestataire qui sélectionne ou modifie l'information du document est donc plus susceptible d'exercer une fonction éditoriale. Il devient la personne qui prend la décision de formuler ou de faire circuler un document. Il est alors considéré avoir parti-

---

141 C'est aussi une approche qui peut se révéler dangereuse en ce qu'elle porte l'entité à s'enquérir de la teneur des documents pour lesquels elle a une responsabilité. On aura alors une plus grande diffusion de renseignements personnels qu celle qui auraient lieu en respectant le rôle de l'intermédiaire.

142 Article 36 de la *Loi concernant le cadre juridique des technologies de l'information,* L.R.Q., c. C-1.1, en ligne : <http://www.canlii.org///qc/legis/loi/c-1.1/20080818/tout.html>.

cipé à la décision de produire le document dans l'état où il est et donc exercer un contrôle sur sa teneur. Du coup, il est plus susceptible d'en répondre.

Le prestataire qui sélectionne la personne qui transmet le document, qui le reçoit ou qui y a accès fait plus que simplement le transmettre. Il décide des personnes qui transmettent, reçoivent ou peuvent accéder à un document. Le prestataire qui sélectionne la personne qui transmet décide lui-même de la transmission : il n'en est plus un agent passif. Il en va de même s'il sélectionne le récipiendaire ou celle qui peut y accéder.

Le prestataire qui conserve le document plus longtemps que nécessaire pour sa transmission se trouve à être en possession du document et exerce sur celui-ci un contrôle accru qui dépasse ce qui est nécessaire afin d'assurer la transmission. Ce peut être par exemple le cas s'il intercepte le document ; le contrôle physique effectif est alors exercé par une personne qui, sachant qu'elle contribue à la diffusion d'un document, a la possibilité de retirer le message en question et de mettre un terme à sa circulation en s'arrogeant un contrôle sans autorisation.

Par contraste, lorsque toutes ces décisions sont prises par l'usager, c'est celui-ci qui effectue la communication au sein d'un environnement d'information en ligne ou hors ligne, non le prestataire de services qui procure à l'usager une plateforme afin de lui permettre d'effectuer la communication de renseignements personnels ou de tout autre document technologique.

Ces principes étant rappelés et contextualisés dans le cadre étendu de la communication en ligne, ils permettent d'éclairer le sens et la portée de notions cruciales dans le processus de circulation de documents, y compris ceux qui comportent des renseignements personnels. Ces principes mettent également en lumière le fait que des degrés différenciés de contrôle et de maîtrise peuvent être exercés à l'égard de l'information circulant dans les environnements en réseaux. C'est dire l'importance de situer avec plus de précision la manière dont s'exerce effectivement le contrôle de l'information dans un réseau.

SECTION 2 – Obligations consécutives de cet état de contrôle de l'information

Contrôler l'information, c'est exercer à son égard, les prérogatives qui autorisent l'exercice des attributs qu'elle comporte. Par exemple, celui qui, dans un environnement en ligne reçoit une vidéo qu'il télécharge, lui donnant la capacité d'en prendre connaissance en utilisant un logiciel approprié, dispose d'un certain contrôle sur l'information.

C'est dans le cadre de ces catégories qu'il est utile d'aborder la signification des notions du droit de la protection des renseignements personnels dans le contexte des réseaux. Cela permettra de mieux situer le sens des opérations de « communication », « collecte », « transmission », « conservation » et autres éléments du cycle de circulation des renseignements personnels et de distinguer les situations où les entités en cause sont en contrôle de l'information (1) de celles où, au contrôle, elle ne l'on pas, ou en ont un de différent ordre (2).

1 – Obligations des entités en état de contrôle des RP

Contrôler une information, c'est pouvoir en prendre connaissance. C'est pouvoir l'utiliser pour des fins déterminées ou pour des fins indéterminées, le tout en conformité avec les lois. Par exemple, la propriété intellectuelle peut limiter le droit de reproduire certaines œuvres ou la capacité de communiquer certains documents au public. Dans le contexte de secret, c'est avoir l'obligation d'en assurer la confidentialité et en dehors du secret, c'est pouvoir transmettre l'information à d'autres.

Le contrôle de l'information peut être un contrôle *de facto :* une personne obtient par exemple un fichier, le reproduit et le diffuse à d'autres personnes sans détenir les autorisations aux termes des lois sur le droit d'auteur ou sur la protection des renseignements personnels.

Mais le contrôle de l'information peut être également *de jure* comme celui par exemple permettant qu'une personne dispose d'un droit exclusif d'interdire la diffusion d'un fichier.

Lorsqu'un renseignement personnel est en cause, les prérogatives associées au contrôle de cette information sont balisées. Ainsi, l'article 59 de la *Loi sur l'accès* et l'article 7(3) de la *Loi sur la protection des renseignements personnels et les documents électroniques* (PIPEDA)[143] dispose qu'un organisme public ne peut communiquer un renseignement personnel sans le consentement de la personne concernée. Mais aux termes de l'article 62 de la *Loi sur l'accès*,

> « Un renseignement personnel est accessible, sans le consentement de la personne concernée, à toute personne qui a qualité pour le recevoir au sein d'un organisme public lorsque ce renseignement est nécessaire à l'exercice de ses fonctions. »[144]

Ainsi, le contrôle sur les renseignements personnels est conditionnel à ce que celui-ci soit nécessaire à l'exercice de fonctions spécifiques au sein d'un organisme public. La personne qui a droit d'accès à un tel renseignement se trouve à acquérir sur celui-ci un contrôle qui est limité à ce qui est nécessaire à l'accomplissement de fonctions spécifiques. En dehors de l'exercice de telles fonctions, le document comportant des renseignements personnels n'est pas accessible.

L'article 63.1 de la *Loi sur l'accès* précise les obligations des entités **qui sont en contrôle** de documents comportant des renseignements personnels. Il prévoit qu'

> « un organisme public doit prendre les mesures de sécurité propres à assurer la protection des renseignements personnels collectés, utilisés, communiqués, conservés ou détruits et qui sont raisonnables compte tenu, notamment, de leur

---

143 Art. 59 de la *Loi sur l'Accès aux documents des organismes publics et sur la protection des renseignements personnels*, L.R.Q., c. A-2.1, 2006, c. 22. en ligne : <http://canlii.org/fr/qc/legis/lois/lrq-c-a-2.1/derniere/lrq-c-a-2.1.html> et Art. 7(3) de la *Loi sur la protection des renseignements personnels et les documents électroniques* (PIPEDA) en ligne : <http://www.canlii.ca/fr/ca/legis/lois/lc-2000-c-5/derniere/lc-2000-c-5.html>.

144 Art. 62 de la *Loi sur l'Accès aux documents des organismes publics et sur la protection des renseignements personnels*, L.R.Q., c. A-2.1, 2006, c. 22. en ligne : <http://canlii.org/fr/qc/legis/lois/lrq-c-a-2.1/derniere/lrq-c-a-2.1.html>.

sensibilité, de la finalité de leur utilisation, de leur quantité, de leur répartition et de leur support. »[145]

Plus spécifiquement, et toujours du fait ce de contrôle, l'article 63.2 de la même loi indique que les organismes publics, à l'exception du Lieutenant-gouverneur, de l'Assemblée nationale et d'une personne qu'elle désigne pour exercer une fonction en relevant, doivent protéger les renseignements personnels en mettant en oeuvre les mesures édictées à cette fin par règlement du gouvernement[146].

Cette notion de protection des articles 63.1 et 63.2 de la *Loi sur l'accès*[147] est d'ailleurs reprise aux articles 4.7 à 4.7.5 de l'annexe 1 de la *Loi sur la protection des renseignements personnels et les documents électroniques* (PIPEDA) qui disposent :

« **4.7 Septième principe — Mesures de sécurité**

Les renseignements personnels doivent être protégés au moyen de mesures de sécurité correspondant à leur degré de sensibilité.

4.7.1 Les mesures de sécurité doivent protéger les renseignements personnels contre la perte ou le vol ainsi que contre la consultation, la communication, la copie, l'utilisation ou la modification non autorisées. Les organisations doivent protéger les renseignements personnels quelle que soit la forme sous laquelle ils sont conservés.

4.7.2 La nature des mesures de sécurité variera en fonction du degré de sensibilité des renseignements personnels recueillis,

---

145 Art. 63.1 de la *Loi sur l'Accès aux documents des organismes publics et sur la protection des renseignements personnels*, L.R.Q., c. A-2.1, 2006, c. 22. en ligne : <http://canlii.org/fr/qc/legis/lois/lrq-c-a-2.1/derniere/lrq-c-a-2.1.html>.

146 Art. 63.2 de la *Loi sur l'Accès aux documents des organismes publics et sur la protection des renseignements personnels*, L.R.Q., c. A-2.1, 2006, c. 22. en ligne : <http://canlii.org/fr/qc/legis/lois/lrq-c-a-2.1/derniere/lrq-c-a-2.1.html>.

147 Art. 63.1 et 63.2 de la *Loi sur l'Accès aux documents des organismes publics et sur la protection des renseignements personnels*, L.R.Q., c. A-2.1, 2006, c. 22. en ligne : <http://canlii.org/fr/qc/legis/lois/lrq-c-a-2.1/derniere/lrq-c-a-2.1.html>.

de la quantité, de la répartition et du format des renseignements personnels ainsi que des méthodes de conservation. Les renseignements plus sensibles devraient être mieux protégés. La notion de sensibilité est présentée à l'article 4.3.4.

4.7.3 Les méthodes de protection devraient comprendre :

a) des moyens matériels, par exemple le verrouillage des classeurs et la restriction de l'accès aux bureaux ;
b) des mesures administratives, par exemple des autorisations sécuritaires et un accès sélectif ; et
c) des mesures techniques, par exemple l'usage de mots de passe et du chiffrement.

4.7.4 Les organisations doivent sensibiliser leur personnel à l'importance de protéger le caractère confidentiel des renseignements personnels.

4.7.5 Au moment du retrait ou de la destruction des renseignements personnels, on doit veiller à empêcher les personnes non autorisées d'y avoir accès (article 4.5.3) ».[148].

En conclusion, il est évident que tant la *Loi sur l'accès* au niveau provincial que la *Loi sur la protection des renseignements personnels et les documents électroniques* (PIPEDA) au niveau fédéral sont conscients de la nécessité de distinguer le contrôle qu'on pourrait avoir sur le document en tant que simple support, du contrôle effectif qu'on pourrait avoir sur le contenu du document en question à savoir le renseignement personnel en soi. C'est à ce titre d'ailleurs que les deux lois en question imposent l'adoption de mesures de sécurité importantes pour la protection des renseignements personnels indépendamment de ce qui pourrait être exigé pour la protection du document de support, comme nous le démontrerons ci-après.

---

[148] Art. 4.7 à 4.7.5 de l'annexe 1 de la *Loi sur la protection des renseignements personnels et les documents électroniques* (PIPEDA) en ligne : <http://www.canlii.ca/fr/ca/legis/lois/lc-2000-c-5/derniere/lc-2000-c-5.html>.

2 – Obligations des entités en état de non contrôle des RP

Les entités qui n'ont pas le contrôle effectif de l'information peuvent néanmoins avoir certains devoirs. Ainsi, l'article 25 de la *Loi concernant le cadre juridique des technologies de l'information*[149] dispose que :

> « **25.** La personne responsable de l'accès à un document technologique qui porte un renseignement confidentiel doit prendre les mesures de sécurité propres à en assurer la confidentialité, notamment par un contrôle d'accès effectué au moyen d'un procédé de visibilité réduite ou d'un procédé qui empêche une personne non autorisée de prendre connaissance du renseignement ou, selon le cas, d'avoir accès autrement au document ou aux composantes qui permettent d'y accéder. »

Des obligations incombent donc aux prestataires qui n'ont pas comme tel le contrôle de l'information qui est entre leurs mains ; toutefois, ces obligations ne sont pas les mêmes que celles auxquelles sont tenus les entités qui ont effectivement le contrôle sur des documents technologiques. Ainsi, les entités qui ne font que conserver physiquement des documents n'ont pas nécessairement le droit d'en prendre connaissance à moins que les documents comportent des informations qui sont publiques par nature. L'article 26 de la *Loi concernant le cadre juridique des technologies de l'information* fait obligation à quiconque qui confie le document à un prestataire de services pour en assurer la **garde** d'informer ce dernier de la protection que requiert le document :

> « 26. Quiconque confie un document technologique à un prestataire de services pour qu'il en assure la **garde** est, au préalable, tenu d'informer le prestataire quant à la protection que requiert le document en ce qui a trait à la confidentialité de

[149] Article 25 de la *Loi concernant le cadre juridique des technologies de l'information,* L.R.Q., c. C-1.1, en ligne : <http://www.canlii.org///qc/legis/loi/c-1.1/20080818/tout.html>.

l'information et quant aux personnes qui sont habilitées à en prendre connaissance. » [150]

Il lui faut donner des informations adéquates sur les mesures de protection de la confidentialité que le document nécessite. Il faut pareillement indiquer quelles sont les personnes habilitées à en prendre connaissance. De son côté, le prestataire de services doit faire en sorte que les moyens technologiques convenus d'un commun accord avec la personne qui lui a confié le document soient mis en place durant toute la période pendant laquelle il en la garde.

Le prestataire qui a la garde d'un document est tenu, durant la période où il en a la garde, de voir à ce que les moyens technologiques soient mis en place pour en assurer la sécurité en préserver l'intégrité et le cas échéant, en protéger la confidentialité et en interdire l'accès à toute personne qui n'est pas habilitée à en prendre connaissance. Au surplus, le prestataire a l'obligation de respecter toute autre obligation prévue dans une loi relativement à la conservation d'un document.

Le contenu des articles 25 et 26 de la *Loi concernant le cadre juridique des technologies de l'information* rejoint d'ailleurs les dispositions des articles 63.1 et 63.2 de la *Loi sur l'accès* ainsi que les dispositions des articles 4.7 à 4.7.5 de l'annexe 1 de la *Loi sur la protection des renseignements personnels et les documents électroniques* (PIPEDA)[151], ce qui dénote d'une certaine volonté commune des législateurs Canadien et Québécois d'assurer la « protection » des renseignements personnels et de définir les prérogatives des personnes ou entités ayant un certain « contrôle » sur les renseignements personnels en question depuis leur « possession » ou « collecte » jusqu' à leur « destruction ».

---

[150] Article 26 de la *Loi concernant le cadre juridique des technologies de l'information,* L.R.Q., c. C-1.1, en ligne : <http://www.canlii.org///qc/legis/loi/c-1.1/20080818/tout.html>.

[151] Art. 4.7 à 4.7.5 de l'annexe 1 de la *Loi sur la protection des renseignements personnels et les documents électroniques* (PIPEDA) en ligne : <http://www.canlii.ca/fr/ca/legis/lois/lc-2000-c-5/derniere/lc-2000-c-5.html>.

Cependant, aux termes de l'article 27 de la *Loi concernant le cadre juridique des technologies de l'information*[152], l'intermédiaire qui fournit des services sur un réseau de communication ou qui y conserve ou y transporte des documents technologiques n'est pas tenu d'en surveiller l'information. Par contre :

> « il ne doit prendre aucun moyen pour empêcher la personne responsable de l'accès aux documents d'exercer ses fonctions, notamment en ce qui a trait à la confidentialité, ou pour empêcher les autorités responsables d'exercer leurs fonctions, conformément à la loi, relativement à la sécurité publique ou à la prévention, à la détection, à la preuve ou à la poursuite d'infractions. »[153]

Ces dispositions qui explicitent les obligations incombant aux intermédiaires sur un réseau montrent bien que ceux-ci ne sont pas dans une position où ils exercent un « contrôle » véritable sur les documents technologiques qui viennent en leur possession physique. Il ne viendrait pas à l'esprit de considérer que le facteur ou l'entreposeur de courrier dans le monde du support papier dispose du contrôle sur l'information contenue dans les lettres entreposées : la situation des intermédiaires est fonctionnellement analogue.

---

[152] Article 27 de la *Loi concernant le cadre juridique des technologies de l'information,* L.R.Q., c. C-1.1, en ligne : <http://www.canlii.org///qc/legis/loi/c-1.1/20080818/tout.html>.

[153] Article 27 de la *Loi concernant le cadre juridique des technologies de l'information,* L.R.Q., c. C-1.1, en ligne : <http://www.canlii.org///qc/legis/loi/c-1.1/20080818/tout.html>.

CHAPITRE 2
CADRE APPLICATIF : L'INFLUENCE DE LA NOTION DE CONTRÔLE SUR LES OPÉRATIONS DÉFINIES DANS LES LOIS SUR LA PROTECTION DES RP

Sur un plan plus conceptuel, il nous apparaît fondamental de dire que la notion de contrôle que nous venons d'examiner est déterminante dans le cadre du traitement de la gestion des renseignements personnels et plus généralement dans la gestion documentaire en général. Et ceci est vrai même si elle n'a jamais été adoubée spécifiquement par les lois qui s'appliquent en la matière. De manière plus concrète, il importe maintenant d'appliquer cette notion aux diverses étapes du cycle de traitement d'un document au sein d'un réseau. À cet égard, il nous importe de faire ressortir l'intérêt de distinguer entre le droit d'accès à un document et les possibilités techniques d'accéder à ce même document. L'analogie avec le monde physique vient ici éclairer les enjeux : nous l'avons déjà vu avec l'illustration du postier, lorsqu'il livre une lettre, il n'a pas pour autant le droit d'accès au contenu de celle-ci. Il dispose toutefois de la possibilité technique d'y accéder. C'est une interdiction provenant d'une règle de droit qui l'empêche de faire usage des possibilités techniques qui sont à sa disposition pour accéder au contenu informationnel du document.

En effet, le droit d'accès à un document découle de la loi. Lorsque la possibilité d'accéder à un document existe, il faut des mécanismes (notamment techniques, administratifs et juridiques) de sécurité afin de réserver aux seules personnes y ayant le droit, l'accès au document. Le droit doit également organiser le régime de sanction pour des accès non autorisés par ceux qui en ont les possibilités techniques.

On a également pu reconnaître, précédemment, l'existence d'intensités différenciées dans le contrôle d'un document. Ces différences se reflètent également dans l'intensité et la portée que l'on se doit de donner aux différentes opérations qui jalonnent le cycle de vie d'un document ; des opérations auxquelles tant les

lois relatives à la protection des renseignements personnels au niveau québécois (*Lois sur l'accès*[154]*, Loi sur la protection des renseignements personnels dans le secteur privé*[155]), qu'au niveau fédéral (*Loi sur la protection des renseignements personnels et les documents électroniques*[156]) que les lois sur la gestion documentaire (*Loi concernant le cadre juridique des technologies de l'information*[157]) non seulement réfèrent mais associent des conséquences juridiques. Parmi lesdites opérations en cause qu'il nous apparaît important de traiter désormais, il y a notamment celles de « communication », « collecte », « transmission », « détention », « conservation », « utilisation » et de « destruction » auxquelles le droit apporte un encadrement et des conséquences juridiques.

Il est à signaler que si les opérations de « communication », « collecte », « transmission », « détention », « conservation », « utilisation » et de « destruction » ont leurs origines dans les deux domaines du droit précités, à savoir le droit de la protection des renseignements personnels et le droit de la gestion documentaire, les définitions des termes sus indiqués utilisés dans le cadre d'un des deux droits en question ne s'accordent parfaitement avec ceux du second. Il nous apparaît donc important de tenter de les concilier ; de scruter les chevauchements, de les distinguer et de les analyser dans le contexte qui les a vu apparaître. Aussi, de ces différentes opérations précitées, il nous semble que trois grandes catégories peuvent être dessinées. En premier lieu, un « ménage définitionnel » doit être fait au regard des termes généralement liés à la circulation *stricto sensu* d'informations et surtout de ren-

---

154 *Loi sur l'Accès aux documents des organismes publics et sur la protection des renseignements personnels*, L.R.Q., c. A-2.1, 2006, c. 22. en ligne : <http://canlii.org/fr/qc/legis/lois/lrq-c-a-2.1/derniere/lrq-c-a-2.1.html>.

155 *Loi sur la protection des renseignements personnels dans le secteur privé*, L.R.Q., c. P-39.1, en ligne : <http://www.canlii.org/fr/qc/legis/lois/lrq-c-p-39.1/derniere/lrq-c-p-39.1.html>.

156 *Loi sur la protection des renseignements personnels et les documents électroniques* (PIPEDA) en ligne : <http://www.canlii.ca/fr/ca/legis/lois/lc-2000-c-5/derniere/lc-2000-c-5.html>.

157 *Loi concernant le cadre juridique des technologies de l'information,* L.R.Q., c. C-1.1, en ligne : <http://www.canlii.org///qc/legis/loi/c-1.1/20080818/tout.html>.

seignements personnels. Il faut entendre par là qu'il faudra, en premier lieu, considérer les opérations de **communication** et de **transmission** des données personnelles référant généralement à une notion de mouvement entre différents intervenants, et auxquelles les lois apportent des conséquences juridiques (Section 1) ; alors qu'en deuxième lieu, et toujours dans le cycle de vie des différentes opérations de gestion documentaire, il faudra considérer qu'il en est d'autres qui davantage sont reliées à une certaine immobilisation des renseignements personnels. Entendons par là les termes de **conservation**, **détention** et **collecte** qui méritent aussi d'être éclaircis (Section 2). Enfin, en troisième lieu, il importera de revenir sur la notion d'**utilisation**, très proche de celle de traitement que l'on trouve plutôt en Europe, et qui devra également être circonscrite davantage (Section 3).

Aussi, nous nous limiterons aux six termes suivants (communication – transmission – conservation – détention – collecte – utilisation) qui donnent lieu à des conséquences juridiques dans les lois sur la protection des renseignements personnels. Mais il est d'autres terminologies que l'on retrouve dans d'autres lois et que nous ne traiterons qu'incidemment. C'est notamment le cas des termes de garde – hébergement – etc.

SECTION 1 – Opérations de communication et de transmission de documents comportant des RP

1 – Distinction entre communication et transmission

A – Opération de communication

La notion de communication est à la base de la protection des renseignements personnels et il est clairement établi qu'il est interdit qu'un renseignement personnel adressé à une organisation soit communiqué à une autre. En effet, l'article 59 de la *Loi sur l'accès* dispose :

> « Un organisme public ne peut communiquer un renseignement personnel sans le consentement de la personne concernée. »

De même, l'article 7(3) de la *Loi sur la protection des renseignements personnels et les documents électroniques* (PIPEDA) dispose de son côté :

> « **7. (3)** Pour l'application de l'article 4.3 de l'annexe 1 et malgré la note afférente, l'organisation ne peut communiquer de renseignement personnel à l'insu de l'intéressé et sans son consentement (…) »[158]

Aussi, l'article 4.3 de l'annexe 1 de ladite loi dispose :

> « **4.3** Toute personne doit être informée de toute collecte, utilisation ou communication de renseignements personnels qui la concernent et y consentir, à moins qu'il ne soit pas approprié de le faire.
>
> Note : Dans certaines circonstances, il est possible de recueillir, d'utiliser et de communiquer des renseignements à l'insu de la personne concernée et sans son consentement.(…) »[159].

Et outre certaines exceptions que l'on traitera plus loin[160], aucune définition n'est proposée ni dans la *Loi sur l'accès* ni dans la *Loi sur la protection des renseignements personnels et les documents électroniques* sur ce à quoi correspond ce verbe.

La définition même du mot communication suppose que l'information est portée à la connaissance d'une personne. Dans son vocabulaire juridique, Gérard Cornu définit ainsi le mot « communication » :

---

158 Art. 7(3) de la *Loi sur la protection des renseignements personnels et les documents électroniques* (PIPEDA) en ligne : <http://www.canlii.ca/fr/ca/legis/lois/lc-2000-c-5/derniere/lc-2000-c-5.html>.

159 Art. 4.3 de l'annexe 1 de la *Loi sur la protection des renseignements personnels et les documents électroniques* (PIPEDA) en ligne : <http://www.canlii.ca/fr/ca/legis/lois/lc-2000-c-5/derniere/lc-2000-c-5.html>.

160 *Infra*, Partie 2, Chapitre 2.

> « Fait de porter un événement ou un élément d'information à la **connaissance** d'une personne déterminée d'un groupe d'intéressés ou du public. »[161] (Nos soulignements)

De façon identique, dans le *Dictionnaire de droit québécois et canadien*[162], le mot communication est défini comme étant une

> « action de porter un fait ou un élément d'information à la **connaissance** de quelqu'un ». (Nos soulignements)

En *common law*, la notion de « connaissance » est également associée à la communication. C'est notamment vrai dans une version ancienne du dictionnaire Black's[163] où l'on peut lire la définition suivante :

> « Information given ; the sharing of knowledge by one with another ; conference ; consultation or bargaining preparatory to making a contract. Also intercourse ; connection. »

La définition est reprise dans l'édition de 2004 :

> « Communication » 1. The expression or exchange of information by speech, writing, gestures, or conduct ; the process of bringing an idea to another's perception. 2. The information so expressed or exchanged[164].

La jurisprudence confirme d'ailleurs encore plus explicitement le sens donné au mot communication en l'associant clairement à une certaine maîtrise du contenu informationnel. Dans *Goldman c. R.*[165], le juge Mcintyre écrit aux pages 994 et 995 que :

---

161 Gérard CORNU, *Vocabulaire juridique*, Paris, Presses universitaires de France, 2007.

162 Hubert REID, *Dictionnaire de droit québécois et canadien*, 3e éd., Montréal, Wilson Lafleur, 2004.

163 Henry Campbell BLACK, *A dictionary of law*, New York (NY), Lawbook Exchange, 1891.

164 Bryan A. GARNER (dir.), *Black's law dictionary*, 8e éd., St. Paul (Minn.), Thomson/West, 2004.

165 *Goldman* c. *R.*, [1980] 1 S.C.R. 976.

> Il est élémentaire de dire que les cours doivent dégager l'intention du législateur et l'appliquer quand elles interprètent les lois. C'est en examinant les mots employés dans la loi que l'on doit dégager l'intention, car c'est à l'intention exprimée par le législateur qu'il faut donner effet. C'est pour cela qu'il faut examiner le sens des termes de la loi et faire parfois de subtiles distinctions. A mon avis, la différence entre le mot conversation et le mot communication est importante dans le contexte de cette disposition. Une **communication comprend la transmission de pensées, d'idées, de mots ou de renseignements d'une personne à une autre**. Le terme conversation est plus large et inclurait, comme toutes les conversations, l'échange d'une série de communications distinctes. (Nos soulignements)

Communiquer un document implique de conférer un contrôle sur celui-ci. Cela suppose de permettre à l'entité à qui l'on communique – le destinataire – de prendre connaissance du document.

D'ailleurs cette perspective est comparable à celle qui est suivie dans la *Loi sur le droit d'auteur* où à la différence des autres termes, l'on dispose d'une définition de la notion dans le cadre de l'analyse de la « communication au public » :

> « 2.4(1)*b*) : **n'effectue pas une communication au public** la personne qui ne fait que **fournir à un tiers les moyens de télécommunication nécessaires** pour que celui-ci l'effectue »[166] (Nos soulignements)

Au sujet de cet article, la jurisprudence a eut l'occasion de préciser le sens à donner à la notion et en dépit de sa longueur il importe de reporter les propos de la Cour suprême dans *SOCAN* c. *Association canadienne des fournisseurs Internet*[167] sur le sujet :

---

[166] *Loi sur le droit d'auteur*, L.R.C 1985, c. C-42, en ligne : <http://www.canlii.org/ca/loi/c-42/tout.html>.

[167] *Société canadienne des auteurs, compositeurs et éditeurs de musique c. Association canadienne des fournisseurs Internet*, [2004] 2 R.C.S. 427, en ligne : <http://www.canlii.org/fr/ca/csc/doc/2004/2004csc45/2004csc45.html>.

> « ¶89 L'alinéa 2.4(1) *b*) n'est pas une échappatoire, mais **un élément important de l'équilibre** établi par le régime législatif en cause. Il tire peut-être son **origine du moyen de défense fondé sur la diffusion de bonne foi** dont peuvent parfois se prévaloir **librairies**, **bibliothèques**, **marchands de journaux** et commerçants apparentés qui, de façon générale, n'ont **aucune connaissance de la diffamation alléguée,** n'ont **aucune raison de supposer son existence** et n'ont **pas fait preuve de négligence en ne la découvrant pas**. » (Nos soulignements)

À ce propos, la Cour suprême évoque d'ailleurs que cet article de la *Loi sur le droit d'auteur*, exonérant les intermédiaires, est le fruit d'une réflexion véritable notamment initiée par des recommandations d'un sous-comité multipartite sur la révision du droit d'auteur du Comité permanent des communications et de la culture de la Chambre des communes. D'ailleurs, dès 1985, dans le cadre d'une *charte des droits des créateurs et créatrices*[168], il fut entendu que l'on devait interpréter le terme « communication » dans un sens large pour y inclure toutes les hypothèses ne touchant pas directement au contenu informationnel.

> « ¶90 […] Parallèlement, le sous-comité a recommandé (à la p. 88) que celui qui participe à une **retransmission « qui n'est destinée qu'à relayer le signal entre la source d'émission et un retransmetteur dont les services sont offerts au grand public » ne soit pas injustement visé** par la définition élargie. L'objectif manifeste, selon le sous-comité, était **d'éviter la superposition inutile d'obligations** relatives au droit d'auteur qui se produirait si l'on ciblait la retransmission « en gros » (p. 88)
>
> [¶91 : Il faut interpréter les termes employés à l'al. 2.4(1)*b*) dans leur sens ordinaire et grammatical, selon le contexte. La signification du mot « nécessaire » (« *necessary* », en anglais) varie en quelque sorte en fonction du contexte. (…). Dans le

---

168 CANADA, Chambre des communes – Sous-comité du Comité permanent des communications et de la culture sur la révision du droit d'auteur. *Une charte des droits des créateurs et créatrices*. Ottawa : Chambre des communes, 1985.

contexte considéré, un moyen est « nécessaire » au sens de l'al. 2.4(1)*b*) s'il est raisonnablement utile et approprié pour l'obtention des avantages que sont une économie et une efficacité accrues.

¶92 : […] L'intermédiaire Internet **qui ne se livre pas à une activité touchant au contenu** de la communication, dont la **participation n'a aucune incidence sur celui-ci** et qui **se contente d'être « un agent » permettant à autrui de communiquer** bénéficie de l'application de l'al. 2.4(1)*b*). (Nos soulignements)

Citant une nouvelle fois ladite Commission, la Cour suprême fait sien les propos suivants :

¶94 « Toute communication d'une œuvre a lieu parce qu'une personne a accompli toutes les démarches nécessaires pour la rendre disponible pour communication. Le fait que cela se réalise à la demande du destinataire ou par l'intermédiaire d'un tiers ne change rien au fait que **le fournisseur de contenu est l'auteur de la communication**. » [souligné dans le texte]

Et la Cour suprême de continuer dans cette même veine :

¶96 : « En **1891**, appelée à statuer sur un litige contractuel opposant des compagnies de téléphone, notre Cour a adopté un point de vue comparable relativement à une infrastructure technologique : « [traduction] **On ne peut dire des propriétaires des fils téléphoniques, qui ignorent tout de la nature du message devant être transmis, qu'ils transmettent, au sens de la convention, un message dont ils ignorent la teneur**. » (Electric Despatch Co. of Toronto c. Bell Telephone Co. of Canada 1891 CanLII 11 (S.C.C.), (1891), 20 R.C.S. 83, p. 91, le juge Gwynne) » »[169] (Nos soulignements)

[169] *Société canadienne des auteurs, compositeurs et éditeurs de musique c. Association canadienne des fournisseurs Internet*, [2004] 2 R.C.S. 427, en ligne : <http://www.canlii.org/fr/ca/csc/doc/2004/2004csc45/2004csc45.html>.

Cette compréhension des choses n'est d'ailleurs pas isolée. Et cette décision cite la *Directive sur le commerce électronique* européenne qui possède un considérant allant exactement dans le même sens en établissant ceci :

> « l'intermédiaire Internet ne peut être tenu responsable lorsque son **activité est limitée « au processus technique d'exploitation et de fourniture d'un accès à un réseau de communication** sur lequel les informations fournies par des tiers sont transmises ou stockées temporairement, dans le seul but d'améliorer l'efficacité de la transmission. **Cette activité revêt un caractère purement technique**, **automatique** et **passif**, qui implique que **[l'intermédiaire Internet] n'a pas la connaissance ni le contrôle** des informations transmises ou stockées. »[170]. (Nos soulignements)

Cette distinction permet de rendre compte du fait qu'on ne songe pas à rendre responsable une entité qui ne fait que déplacer un document d'un point d'expédition à un autre point dans la mesure où elle n'acquiert pas le contrôle sur ce document. **La seule circulation des renseignements personnels n'est donc pas systématiquement synonyme de communication, du fait de cette absence de connaissance.** Et toujours sur l'exemple du facteur qui livre une lettre, celui-ci a beau être en pleine possession de celle-ci, il n'a pas le contrôle du document puisqu'il n'a pas le droit d'en prendre connaissance. Et ceci vaut tant pour la lettre que pour la carte postale où l'information est différemment disponible. Ainsi, lorsqu'une personne en possession physique d'un document comportant des renseignements personnels n'a pas le droit de les utiliser, ceux-ci ne lui sont pas communiqués.

D'ailleurs, cette équation entre connaissance de l'information et conséquences juridiques se vérifie dans d'autres hypothèses. Par exemple, aux termes de l'article 22 de la *Loi concernant le*

---

[170] Considérant. 42 du préambule de la Directive sur le commerce électronique européenne, cité dans *Société canadienne des auteurs, compositeurs et éditeurs de musique* c. *Association canadienne des fournisseurs Internet*, [2004] 2 R.C.S. 427, en ligne : <http://www.canlii.org/fr/ca/csc/doc/2004/2004csc45/2004csc45.html>, par. 98.

cadre juridique des technologies de l'information[171], le prestataire qui agit à titre d'intermédiaire pour offrir des services de conservation de documents technologiques sur un réseau, n'est pas responsable des activités accomplies par l'utilisateur du service au moyen des documents remisés par ce dernier. Ainsi, lorsque le « prestataire-intermédiaire » propose une plateforme dans laquelle il est loisible aux usagers de commander des informations, par exemple en actionnant un lien pour ensuite les acheminer à un tiers, le prestataire qui offre de tels services de conservation n'acquiert pas le contrôle sur les documents ainsi traités. Faute de contrôle, ces documents ne lui sont pas communiqués. C'est bien davantage l'usager qui se fait communiquer des documents et décide de les transmettre à un tiers.

La communication se distingue donc de la **transmission** qui consiste à rendre disponible un document pour une communication. Tant que le document n'est que transmis, il n'est pas effectivement communiqué. Par contre, la transmission se présente habituellement comme une situation ayant vocation à mener à la communication du document.

B – Opération de transmission

Transmettre n'est pas « communiquer ». Alors que la seconde, nous l'avons vu, réfère à la connaissance de l'information concernée, la transmission semble impliquer bien davantage le caractère « mécanique » de la connexion entre un point « A » à un point « B ». D'ailleurs, la notion de transmission est généralement utilisée dans la *Loi sur l'accès* et autres lois sur la protection des renseignements personnels dans une perspective qui n'est pas celle de la communication. Plus exactement, les vingt cinq occurrences dans la *Loi sur l'accès* référant au terme de transmission,

---

[171] Article 22 de la *Loi concernant le cadre juridique des technologies de l'information,* L.R.Q., c. C-1.1, en ligne : <http://www.canlii.org///qc/legis/loi/c-1.1/20080818/tout.html>.

ou à une de ses variantes, concernent généralement l'envoi de documents d'une personne à une autre[172].

Ainsi, l'opération de transmission ne dispose pas d'un encadrement rigoureux en termes de protection des renseignements personnels. En revanche, la *Loi concernant le cadre juridique des technologies de l'information*[173] réfère à cette notion de manière beaucoup plus explicite.

L'article 28 de cette loi précise en effet qu'

> « un document peut être transmis, envoyé ou expédié par tout mode de transmission approprié à son support, à moins que la loi n'exige l'emploi exclusif d'un mode spécifique de transmission »[174].

Transmettre un document, c'est donc l'expédier d'un point d'expédition à un point de réception. C'est le faire passer d'un point à l'autre. La transmission s'analyse donc comme une opération technique pouvant éventuellement emporter communication.

Le caractère confidentiel d'un document emporte évidemment des obligations lors de la transmission, l'article 34 de la *Loi concernant le cadre juridique des technologies de l'information* dispose que

> « [l]orsque la loi déclare confidentiels des renseignements que comporte un document, la confidentialité de ces derniers doit être protégée par un moyen approprié au mode de transmis-

---

172 On peut nommer par exemple l'envoi d'avis à la *Commission d'accès à l'information* (articles 8, 64, 68.1), de l'envoi d'un document par un organisme public suite à une demande d'accès (article 11, 43), etc.

173 Article 28 de la *Loi concernant le cadre juridique des technologies de l'information,* L.R.Q., c. C-1.1, en ligne : <http://www.canlii.org///qc/legis/loi/c-1.1/20080818/tout.html>. 2, en ligne avec annotations à <http://www.msg.gouv.qc.ca/gel/cadre_juridique_intro.html> (site visité le 15 octobre 2008) ; Pierre TRUDEL, « Notions nouvelles pour encadrer l'information à l'ère du numérique : l'approche de la *Loi concernant le cadre juridique des technologies de l'information* », [2004] 106 *Revue du notariat* 287-339.

174 Article 28 de la *Loi concernant le cadre juridique des technologies de l'information,* L.R.Q., c. C-1.1, en ligne : <http://www.canlii.org///qc/legis/loi/c-1.1/20080818/tout.html>.

sion et cela y compris sur les réseaux de communication. »
[175]

Il est par ailleurs important de signaler que la position de cette loi québécoise relative à la gestion documentaire, quant aux obligations relatives à la protection des renseignements personnels confidentiels est confirmée par les articles Art. 4.7 à 4.7.5 de l'annexe 1 de la *Loi sur la protection des renseignements personnels et les documents électroniques* (PIPEDA)[176].

La transmission doit donc s'effectuer de manière à protéger la confidentialité des renseignements. Le choix des moyens quant à la façon d'assurer la protection des renseignements confidentiels lors de la transmission d'un document est laissé à ceux qui en ont la responsabilité. Ceux-ci doivent cependant être en mesure de fournir, au besoin, la documentation expliquant comment les moyens pris permettent d'assurer la protection de la confidentialité. Cette documentation pourra établir, si requis, que la confidentialité a été maintenue lors de la transmission.

Par conséquent, la transmission n'est pas en soi une situation emportant la communication d'un document. Seul le destinataire, celui à qui est destiné le document, a communication de celui-ci. Les autres prestataires impliqués dans le processus de transmission ont pour leur part une obligation de mettre en œuvre les moyens conséquents au mode de transmission afin de garantir la confidentialité de l'information transmise.

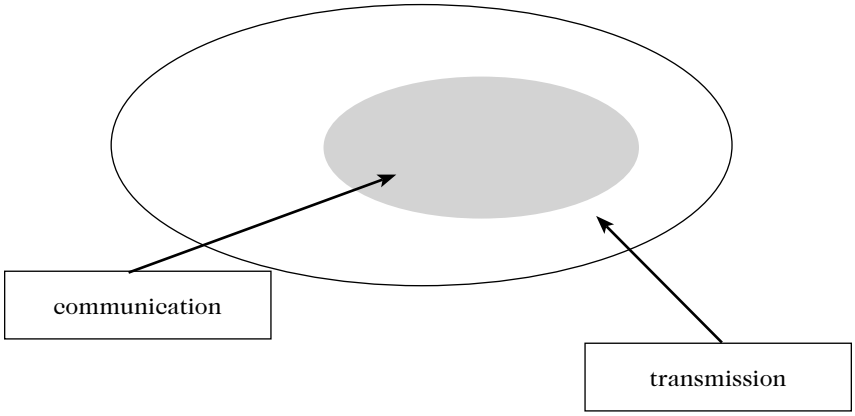
En résumé, et pour reprendre une dichotomie particulièrement présente dans la *Loi concernant le cadre juridique des technologies de l'information*, alors que la communication s'attache à l'information, au renseignement, et dans le cas qui nous intéresse au renseignement personnel, la transmission concerne

---

[175] *Loi concernant le cadre des technologies de l'information*, L.R.Q., c. C-1.1, en ligne : <http://www.canlii.org///qc/legis/loi/c-1.1/20080818/tout.html>.

[176] *Loi sur la protection des renseignements personnels et les documents électroniques* (PIPEDA) en ligne : <http://www.canlii.ca/fr/ca/legis/lois/lc-2000-c-5/derniere/lc-2000-c-5.html>.

davantage le support qui « porte » ladite information[177]. Il nous semble donc clair que la communication est un sous-ensemble de la transmission, la première requérant la connaissance qui s'additionne à une transmission.



2 – Définitions et illustrations

A – Définitions

i) Définition de communication

Communiquer un renseignement ou un document implique de conférer un droit de prendre connaissance de la teneur du document ou du renseignement. Si le document est mis en possession physique ou juridique d'une entité, cela ne signifie pas pour autant que celle-ci ait obtenu communication du document ou du renseignement.

Dans un environnement en réseau, l'information circule d'un point à l'autre. Mais la circulation de l'information n'emporte pas

[177] Article 3 de la *Loi concernant le cadre juridique des technologies de l'information,* L.R.Q., c. C-1.1, en ligne : <http://www.canlii.org///qc/legis/loi/c-1.1/20080818/tout.html>. Cet article dispose que « Un document est constitué d'information portée par un support. » Voir aussi, *Supra*, Partie 1, Chapitre 1, Section 1.

sa communication à chacun des points dans lesquels elle est relayée. Personne n'irait prétendre qu'un postier en possession physique pendant quelques temps d'une lettre comportant des renseignements personnels s'est vu communiquer ces renseignements… Il y a en effet dans le cycle de traitement du renseignement personnel, et particulièrement, dans le traitement des documents technologiques pouvant comporter de tels renseignements, des situations qui ne constituent pas une « communication ». Opérations qui pourraient être en bien des cas, comme nous le verrons, des simples « **transmissions** »[178].

Par exemple, lorsque l'usager effectue une opération sur un site, il demande de l'information à un organisme, il prend connaissance de l'information puis l'achemine à un autre organisme, cette opération n'emporte pas que le site acquiert le contrôle sur l'information ainsi transitée.

Le site tient alors un rôle d'intermédiaire technique. Selon la Cour de cassation belge, citée par le professeur Montero, l'intermédiaire est

> « celui dont l'activité revêt un caractère purement technique, automatique et passif, ce qui implique qu'il ne connaît pas et n'exerce pas de **contrôle** sur l'information qui est transmise et stockée. »[179] (Nos soulignements)

ii) Définition de transmission

Transmettre un document, c'est l'expédier d'un point d'expédition à un point de réception. C'est le faire passer techniquement d'un point à l'autre. En d'autres mots, et pour reprendre une image préalablement évoquée, la transmission est au « support » ce que la communication est à l'« information ». « Support » et « information » : les deux composantes essentielles du document

---

178 *Infra*, Partie 1, Chapitre 2, Section 1, 2, A, ii).

179 Étienne MONTERO, « Les responsabilités liées au Web 2.0 », [2008] *R.D.T.I.,* 363 p. 367.

que l'on retrouve clairement identifiées dans la *Loi concernant le cadre juridique des technologies de l'information*[180].

B – Illustrations

i) Illustrations de communication

Illustration 1 :

Dans la première situation relative à la méthode d'authentification d'identité du citoyen aux fins de permettre l'accès à un service déterminé, et comme nous l'avons présenté dans la Partie préliminaire, plusieurs communications pourraient être susceptibles d'être envisagées. Au regard de nos précédents propos, nous croyons davantage qu'aucune communication ne doit être juridiquement considérée en pareil cas.

En guise de résumé, l'usager, citoyen, qui souhaite accéder à un service offert par un organisme 1, contacte un organisme 2 qui vérifie l'identité de l'usager auprès de l'organisme 3. Pour un seul service, à l'initiative de l'usager lui-même, il y a eu plusieurs « communications » techniques pour effectuer des vérifications tout aussi techniques. Pourtant, et au regard de nos propos précédents, l'on ne peut qualifier juridiquement une communication technique dès lors que les organismes en cause ne disposent d'aucun contrôle sur les renseignements personnels techniquement communiqués. Un contrôle qui est au contraire entre les mains du citoyen qui peut toujours mettre fin à sa propre requête et qui est aussi en mesure de vérifier si les informations transmises sont bien les siennes.

Bien sûr, les organismes sont tentés d'introduire des consentements à chacune des étapes de la « communication » technique ; et qui s'appelle plus correctement une « transmission ». Mais attention, et comme nous le verrons ci-après[181], ces consentements perdent

---

[180] *Loi concernant le cadre juridique des technologies de l'information,* L.R.Q., c. C-1.1, en ligne : <http://www.canlii.org///qc/legis/loi/c-1.1/20080818/tout.html>, art. 3.

[181] *Infra*, Partie 2, Chapitre 1.

leur pertinence et leur finalité, ne servant en bout de ligne qu'à rassurer les organismes de leur conformité au droit. Le citoyen quant à lui, bien au contraire, risque fortement de trouver que cette obligation est un irritant à son processus d'utilisation d'un service électronique offert par un organisme public. **De plus, et toujours relativement à cette exception qu'est le consentement, il nous apparaît possible de justifier que le seul fait pour l'usager de recourir à ce service pourrait être analysé comme un consentement implicite à ladite communication**[182]**.**

Bien sûr aussi, et toujours conformément à des développements ultérieurs[183], il est possible pour les organismes de demander une habilitation ou une entente, et ce notamment au regard de l'article 68 al. 2 de la *Loi sur l'accès*. Néanmoins, et malgré le fait que cet amendement de 2006 à la *Loi sur l'accès* semble avoir été introduit exactement pour remplir cette finalité, la cohérence avec nos développements antérieurs nous oblige d'affirmer que ce processus ne nous apparaît pas nécessaire dès lors qu'il est possible de croire que les organismes en cause ne disposent pas d'un contrôle nécessaire à une prise de connaissance véritable des renseignements personnels.

Illustrations 2 et 3 :

Quant aux exemples 2 et 3 relatifs respectivement à l'hébergement de renseignements du CV d'un professeur d'Université au Canada et au site web 2.0 de promotion touristique, et portant tous les deux sur le dépôt d'information par un usager, l'opération de communication ne nous y paraît pas devoir être sujet à une difficulté d'interprétation.

C'est d'ailleurs ce qui est mentionné clairement dans le contrat d'adhésion au CV Commun Canadien[184] :

> « Les renseignements contenus dans ce système vous appartiennent et ils ne seront pas partagés sans votre connaissance

---

182 *Infra*, Partie 2, Chapitre 1, Section 3.

183 *Infra*, Partie 2, Chapitre 2.

184 Le CV Commun Canadien est en ligne : <http://www.commoncv.net/index_f.html>.

> ou votre consentement. **Seuls les renseignements que vous avez saisis seront sauvegardés.** Aucun autre renseignement personnel ne sera ajouté à votre compte sans votre connaissance. **Vous avez le contrôle des mises à jour de vos données, et ultimement, de la suppression de votre compte au système CVC** (…) »
>
> « **Le système CVC sauvegarde** vos renseignements personnels sur des ordinateurs placés dans un environnement sécure et avec accès contrôlé pour protéger contre l'accès, l'utilisation ou la révélation non autorisée (…) »

La communication est effectuée au moment ou l'usager décide d'effectuer les démarches requises pour permettre aux entités de prendre connaissance et donc « communication » des renseignements. Tant que cette décision et ces démarches de l'usager ne sont pas enclenchées, il n'y a pas de communication.

ii) Illustrations de transmission

La transmission, du fait de son aspect strictement mécanique, est présente dans la grande majorité des prestations en ligne. Pour traiter, pour rendre les services électroniques disponibles, il faut plus souvent qu'autrement, juste transmettre. Une transmission qui se traduit dans la notion de « circulation » que nous avons définie dans la Partie préliminaire[185].

Illustration 1

Dans l'illustration 1 relative à la méthode d'authentification d'identité du citoyen aux fins de permettre l'accès à un service déterminé, une circulation accrue est requise pour que le service soit rendu. Elle se traduit en une série d'envoi de documents entre les quatre intervenants en cause, respectivement l'usager, le prestataire en ligne d'identification, l'organisme public utilisé pour la vérification, l'organisme public proposant le service à l'usager[186] ;

---

185 *Supra*, Partie préliminaire, Chapitre 1, Section 1, 1, B.
186 *Supra*, Partie préliminaire, Chapitre 1, Section 1, 2.

quatre envois que nous devrions plus justement nommer des transmissions. En revanche, et comme nous venons de le voir dans la Section 1, ces échanges – ces transmissions – ne peuvent être considérés comme des communications dans la mesure où ils n'impliquent pas un contrôle suffisant sur l'information, de sorte à permettre d'avoir connaissance de son contenu.

Illustration 2 et 3

Pour les illustrations 2 et 3 relatives respectivement à l'hébergement de renseignements du CV d'un professeur d'Université au Canada et au site web 2.0 de promotion touristique, deux situations qui semblent devoir être considérées identiquement, les prestations en ligne impliquent toutes deux des transmissions, notamment celles impliquant l'envoi par l'usager de documents qu'il va déposer sur le site du prestataire en ligne.

Ceci est particulièrement clair dans le cas du site du CV Commun Canadien[187] où il est clairement stipulé que :

> « Ce système vous permet **d'entrer,** de sauvegarder, et de mettre à jour votre CV et aussi de l'imprimer en utilisant le format exigé par un organisme membre (…)
>
> « Les renseignements contenus dans ce système vous appartiennent et ils ne seront pas partagés sans votre connaissance ou votre consentement. Seuls **les renseignements que vous avez saisis** seront sauvegardés (…)
>
> « Lorsque vous le **soumettez électroniquement**, le système vous montrera une version PDF (que vous pouvez imprimer) de l'information que vous partagez avec l'organisme (…)
>
> « Toute **l'information que vous entrez** dans ce système sera protégée selon les lois et politiques provinciales et fédérales applicables (…)
>
> « Le système CVC utilise un logiciel qui surveille la **transmission** des données sur le réseau pour déceler toute tentative

[187] Le CV Commun Canadien en ligne : <http://www.commoncv.net/index_f.html>.

non autorisée de télécharger ou de modifier des renseignements ou de causer d'autres dommages (...) » (nos soulignements)

Conformément au régime juridique applicable tel que déterminé dans la *Loi concernant le cadre juridique des technologies de l'information*[188], notamment à l'article 22, le prestataire en ligne n'est pas responsable du contenu transmis, sous réserve de sa connaissance d'une transmission d'un document dont le contenu irait à l'encontre du droit.

Le site du CV Commun Canadien est une illustration de cette politique qui veut que la responsabilité et le contrôle du contenu des documents transmis soient à la charge du seul déposant des renseignements personnels en ligne :

« **Vous avez le contrôle** des mises à jour de vos données, et ultimement, de la suppression de votre compte au système CVC (...)

Le RCVC révélera votre information personnelle sans communication préalable, seulement si c'est demandé par la loi ou si nous croyons de bonne foi qu'une telle action est nécessaire pour : (a) **se conformer aux édits de la loi** ou se conformer au processus légal requis par le RCVC ou le site CVC (b) protéger et défendre les droits ou la propriété du RCVC et du site Web CVC et, (c) agir selon une urgence pour protéger la sûreté personnelle des utilisateurs du système CVC ou le public. (…)

Les organismes qui sont membres possèdent les droits d'auteurs des formulaires de CV spécifiques à eux. » (nos soulignements)

---

188 *Loi concernant le cadre juridique des technologies de l'information,* L.R.Q., c. C-1.1, en ligne : <http://www.canlii.org///qc/legis/loi/c-1.1/20080818/tout.html>, art. 22.

SECTION 2 – Opérations de collecte, conservation et détention de RP

Après les opérations de « mouvement » que représentent la communication et la transmission, il en est d'autres, plus stables, qu'il importe de traiter ensemble du fait que plusieurs d'entre elles sont susceptibles d'être confondues.

En effet, en l'absence de définitions tout à fait claires, plus exactement de définitions qui en bien des cas l'étaient dès lors qu'elles s'interprétaient uniquement dans un environnement lié au support papier, il importe de s'attarder successivement sur les opérations de collecte (1), conservation (2) et détention (3). Trois opérations qui ne sont d'ailleurs pas, comme nous le verrons, les seuls termes auxquels les lois associent des conséquences juridiques.

1 – Opération de collecte

A – Mise en contexte

Plusieurs prestations en ligne correspondent à des situations où il n'est pas tout à fait clair si une collecte est véritablement effectuée. C'est pourquoi il importe de revenir aux sources et de définir exactement ce à quoi correspond cette opération qui engendre un ensemble d'obligations, assez lourdes, pour l'organisation qui l'effectue.

La notion de collecte, qui apparaît à quelques reprises dans la *Loi sur l'accès*, est plus souvent retrouvée sous l'expression de « cueillir » ou de « recueillir » (de même étymologie que le verbe collecter), voire même à cette notion de « première collecte ». Le terme de « première collecte » qui apparaît d'ailleurs dans la lettre même de l'article 65 de la *Loi sur l'accès*, où on envisage expressément l'hypothèse de la cueillette initiale[189]. Par conséquent, il

[189] Art. 65 de la *Loi sur l'Accès aux documents des organismes publics et sur la protection des renseignements personnels*, L.R.Q., c. A-2.1, 2006, c. 22. en ligne : <http://canlii.org/fr/qc/legis/lois/lrq-c-a-2.1/derniere/lrq-c-a-2.1.html> : « Quiconque, au nom d'un organisme public, recueille verbalement un rensei-

ne peut y avoir collecte sur une information que l'on possède déjà. Il importe de le rappeler ici dans la mesure où il est des situations où la question se pose[190].

La collecte est une opération qui bénéficie dans les lois sur la protection des renseignements personnels d'un encadrement particulier. Mais avant cet encadrement, il s'agit en effet d'une opération qui donne lieu à un contrôle de pertinence, notamment au regard de l'article 64 de la *Loi sur l'accès,* et qui a comme corollaire les articles 4.2.5 et 4.2.6 de l'Annexe 1 de de la *Loi sur la protection des renseignements personnels et les documents électroniques* (PIPEDA)[191]. En effet, l'article 64 de la *Loi sur l'accès* dispose :

> « **64. Nul ne peut**, au nom d'un organisme public, **recueillir un renseignement personnel si cela n'est pas nécessaire à l'exercice des attributions de cet organisme** ou à la mise en œuvre d'un programme dont il a la gestion.
>
> Un organisme public peut **toutefois recueillir** un renseignement personnel si cela est **nécessaire à l'exercice des attributions** ou à la mise en ouvre d'un programme de l'organisme public avec lequel il collabore pour la prestation de services ou pour la réalisation d'une mission commune. »[192] (Nos soulignements)

De même, les articles 4.2.5 et 4.2.6 de l'Annexe 1 de la *Loi sur la protection des renseignements personnels et les documents électroniques* (PIPEDA) disposent de leur côté :

---

gnement personnel auprès de la personne concernée doit se nommer et, lors de la première collecte de renseignements et par la suite sur demande, l'informer : (…) ».

190 *Infra*, voir l'illustration 1.

191 Art. 4.2.5 et 4.2.6 de l'annexe 1 de la *Loi sur la protection des renseignements personnels et les documents électroniques* (PIPEDA) en ligne : <http://www.canlii.ca/fr/ca/legis/lois/lc-2000-c-5/derniere/lc-2000-c-5.html>.

192 Art. 64 de la *Loi sur l'Accès aux documents des organismes publics et sur la protection des renseignements personnels*, L.R.Q., c. A-2.1, 2006, c. 22. en ligne : <http://canlii.org/fr/qc/legis/lois/lrq-c-a-2.1/derniere/lrq-c-a-2.1.html>.

> **4.2.5** Les personnes qui **recueillent** des renseignements personnels devraient être en mesure d'expliquer à la personne concernée **à quelles fins sont destinés ces renseignements**.
>
> **4.2.6** Ce principe est étroitement lié au **principe de la limitation de la collecte (article 4.4)** et à celui de **la limitation de l'utilisation, de la communication et de la conservation** (article 4.5). (nos soulignements)

Sinon, plusieurs mesures de protection sont introduites dans les lois sur la protection des renseignements personnels relativement à la collecte, que ce soit notamment sur le respect des règles de sécurité[193], de l'information de l'individu[194] ou de sa destruction[195].

Mais la *Loi sur l'accès*, pas plus que la *Loi sur la protection des renseignements personnels dans le secteur privé*, ne définissent ce qu'il faut entendre par collecte de renseignements personnels. Encore une fois, il n'y a rien d'étonnant à cela car il n'est nul besoin de le faire pour ce qui se conçoit bien. En effet, collecter ne pose pas vraiment de problèmes lorsque cela s'entend dans un contexte du support papier où les renseignements personnels sont à un seul endroit et donc généralement détenus par une seule personne. La loi dispose donc des exigences à satisfaire lorsqu'un organisme recueille des renseignements personnels mais elle ne précise pas les situations ou l'on doit prendre pour acquis qu'une collecte est effectuée. Le Rapport Paré[196], qui a conduit à l'adoption de la *Loi d'accès* est également muet sur la définition de collecte.

---

193 Dans la *Loi sur l'Accès aux documents des organismes publics et sur la protection des renseignements personnels*, L.R.Q., c. A-2.1, 2006, c. 22, on peut notamment référer aux articles 63.1, 64, 65. Dans la *Loi sur le Ministère du Revenu*, on peut identifier l'article 69.

194 Art. 65 de la *Loi sur l'Accès aux documents des organismes publics et sur la protection des renseignements personnels*, L.R.Q., c. A-2.1, 2006, c. 22. en ligne : <http://canlii.org/fr/qc/legis/lois/lrq-c-a-2.1/derniere/lrq-c-a-2.1.html>.

195 Art. 73 de la *Loi sur l'Accès aux documents des organismes publics et sur la protection des renseignements personnels*, L.R.Q., c. A-2.1, 2006, c. 22. en ligne : <http://canlii.org/fr/qc/legis/lois/lrq-c-a-2.1/derniere/lrq-c-a-2.1.html>.

196 *Rapport de la Commission d'étude sur l'accès du citoyen à l'information gouvernementale et sur la protection des renseignements personnels*, Québec, 1981, p. 65.

Or, la collecte dans un environnement électronique est sujette à beaucoup plus de complexité, et la personne qui va être en charge de collecter, à proprement parler, les renseignements personnels, soit de l'individu, soit d'un tiers autorisé[197], plus souvent qu'autrement, va opérer la gestion desdits renseignements par le biais d'un système d'impartition. Le rapport de collection n'implique pas que les seuls « collecté » et « collecteur ». Davantage, il est tout à fait possible d'imaginer que cette opération s'effectue en externalisant tout ou partie du processus. Quelle que soit l'expression utilisée, tel que « outsourcing » ou sous-traitance par exemple, il est donc désormais possible pour des raisons notamment d'efficacité et de gestion des coûts, d'avoir une multitude d'acteurs en cause dans le cadre d'une opération somme toute assez simple[198]. Une dichotomie s'impose donc : il importe de dissocier la **collecte juridique** qui est une opération juridique effectuée délibérément par l'organisme qui est responsable de la collecte et ayant des conséquences juridiques, et la **collecte technique**, qui est une opération strictement mécanique, et qui peut être effectuée par une autre organisation que la première.

Si l'on s'en remet aux définitions courantes, collecter de l'information, c'est non seulement acquérir une nouvelle information mais de surcroît disposer sur celle-ci d'un contrôle effectif. Ainsi, le Grand dictionnaire terminologique définit collecte comme étant l'« action de rassembler des données de différentes provenances en vue d'un traitement informatique » ou l'« action de rassembler les données variables destinées à un traitement ». En somme, il n'y a pas de collecte de renseignement si une personne n'acquiert pas, du fait de l'opération, un contrôle sur le renseignement.

Comme elle suppose l'acquisition du contrôle à l'égard de l'information concernée, la collecte implique soit d'avoir connais-

---

197 Voir notamment l'art. 65 de la *Loi sur l'Accès aux documents des organismes publics et sur la protection des renseignements personnels*, L.R.Q., c. A-2.1, 2006, c. 22. en ligne : <http://canlii.org/fr/qc/legis/lois/lrq-c-a-2.1/derniere/lrq-c-a-2.1.html>.

198 Sur la notion d'impartition, voir notamment la page dédiée à ce concept sur Wikipedia, en ligne : <http://fr.wikipedia.org/wiki/Outsourcing>.

sance des renseignements personnels en cause, soit de disposer du droit d'en prendre connaissance ou encore, lorsque la collecte est effectuée au nom d'autrui, du droit de transmettre à l'entité qui a le droit de prendre connaissance du renseignement.

Le fait d'être en possession physique d'un support comportant une information ne constitue pas forcément une collecte. Par exemple, le livreur qui est chargé de transporter une caisse de documents comportant des renseignements personnels ne collecte pas de renseignements personnels. Il n'a à l'égard de ces informations, aucun droit d'en prendre connaissance mais par contre, il a une obligation de traiter ces documents de façon conséquente selon les directives ou indications que lui a données l'entité qui lui en a confié la garde[199]. Également, le fait qu'il ait la capacité physique de le faire n'implique pas forcément une qualification différente de l'opération. Simplement, des règles de responsabilités sont envisageables s'il devait contourner ses obligations.

Pour être tenu à des obligations associées à une collecte de renseignements personnels, il faut nécessairement que l'on ait acquis le contrôle des renseignements personnels, qu'on ait à la fois le droit et la possibilité technique d'en prendre connaissance. Ainsi, lorsque les lois encadrent la notion de collecte, ou le fait de recueillir des renseignements personnels, elles concernent les organisations qui cumulent donc ce que nous avons appelé plus tôt la « collecte juridique » et la « collecte technique ». Le seul « collecteur » mécanique n'est pas assujetti à cet encadrement. Il sera notamment davantage vu sous la notion de **conservation** ou de **garde** que nous verrons plus tard.

D'ailleurs, l'une des meilleures illustrations de ces différentes notions de « collecte » est l'Affaire *Note2be* en France[200]

---

[199] Art 26 de la *Loi concernant le cadre juridique des technologies de l'information*, L.R.Q., c. C-1.1, en ligne : <http://www.canlii.org///qc/legis/loi/c-1.1/20080818/tout.html>.

[200] Ces quelques lignes sont directement inspirées d'un article Vincent GAUTRAIS, « Give me Five ? Traitement jurisprudentiel du commerce électronique », (2009) 21-2 *Cahiers de la propriété intellectuelle* 389, 401.

« Dans une perspective très « web 2.0 », nous voudrions désormais faire état d'une décision française, plus exactement d'une série de décisions, relativement à un site de notation de professeurs, www.note2be.com. Conformément à une mode qui se propage comme une traînée de poudre, il est désormais en effet possible de noter sur Internet, son professeur bien sûr, mais aussi son maire, son médecin, son policier, son notaire, son voisin, et bien d'autres. En janvier 2008, un entrepreneur français qui décide de lancer ce type de « services » comme cela se fait partout sans aucune contestation légale (États-Unis, Australie, Allemagne, etc., et bien sûr Canada), se voit dans l'obligation d'affronter une réaction pour le moins vive de nombreux enseignants, de leurs syndicats, de parents d'élèves, le tout avec le support et l'assentiment du Ministre français de l'éducation. Et le litige va bon train : en moins de 4 mois, un jugement du *Tribunal de grande instance de Paris* (03 mars 2008)[201], un avis de la *CNIL* (Commission nationale Informatique et liberté) (06 mars 2008)[202] et finalement un arrêt de la *Cour d'appel de Paris* (25 juin 2008)[203] sont rendus pour, unanimement et malgré la variété des arguments utilisés, condamner le site pour atteinte à la protection des données personnelles. En contrepoint de cette pléthore jurisprudentielle, l'on peut également évoquer une couverture médiatique considérable, sans oublier une réaction doctrinale particulièrement féconde[204].

---

201 TGI Paris, réf., 3 mars 2008, *SNES FSU et a.* c. *Sté Note2be.com*, n° 08/51650, aussi disponible en ligne : <www.foruminternet.org>.

202 CNIL, le site note2be.com est illégitime au regard de la loi informatique et libertés, 06 mars 2008, en ligne : <http://www.cnil.fr/index.php ?id=2405&news[uid]=528&cHash=7c1cd2d002>.

203 Cour d'appel de Paris 14ème chambre, section A Arrêt du 25 juin 2008, *Note2be.com* c. *SNES FSU et autres*.

204 Sans prétendre à l'exhaustivité, l'on peut néanmoins citer Emmanuel DERRIEUX, « Internet et protection des données personnelles », (Mai 2008) 36 Revue *Lamy Droit de l'immatériel* n°1211 ; Jean FRAYSSINET, « Note2be.com : la notation ou pas des enseignants, telle est la question… », (Mai 2008) 36 *Revue Lamy Droit de l'immatériel* 30-36 ; Petr MUZNY, « La notation des enseignants sur Internet : être, ou plutôt ne pas être » (2008) 16 *Dalloz*

Disons-le tout de suite, ces trois décisions n'ont pas objet de révolutionner le droit et ne font qu'interpréter, de manière assez prosaïque, l'état de la question. Point de réflexion en profondeur, ce qui se comprend mieux dans le cas des jugements et moindrement dans l'hypothèse de l'avis de la CNIL[205]. Pourtant, il nous apparaît qu'un débat a été totalement occulté relativement à deux éléments fondamentaux derrière la protection des renseignements personnels.

En premier lieu, il nous semble pertinent de s'interroger sur le fait de savoir si le nom, le prénom, l'établissement d'enseignement et éventuellement une notation qui pourrait y être associée, constituent des renseignements personnels. De par leur caractère public, de par leur faible sensibilité, la question nous semble devoir être posée. C'est d'ailleurs pour cela que la *Loi fédérale sur la protection des renseignements personnels et les documents électroniques*[206] a pris le soin d'exclure de la définition même de renseignements personnels, à l'article 2, ces données pour le moins banales. D'une manière quelque peu similaire, et comme le fait remarquer le professeur

1124 -1127 ; Agathe LEPAGE, « Les professeurs notés sur Internet » (Avril 2008) 4 *Communication Commerce électronique* comm. 58 ; Maxim JAILLET, « La publication d'informations à l'épreuve de la protection des données personnelles » (Mai 2008) 36 Revue *Lamy Droit de l'immatériel* n°1169 ; Agathe LEPAGE, « Les liens entre nom et vie privée » (Juillet 2008) 7 *Communication Commerce électronique* comm. 9 ; Anne-Laure BLOUET-PATIN, « Illégitimité d'un site de notation de professeur au regard de la loi « informatique et liberté » » *Lexbase Hebdo* ; Marc D'HAULTFOEUILLE, « Bulletin d'actualités Clifford Chance – Département Communication Média & Technologies – Mars 2008 » *Lexbase*.

[205] Jean FRAYSSINET, « Note2be.com : la notation ou pas des enseignants, telle est la question… », (Mai 2008) 36 *Revue Lamy Droit de l'immatériel* 30-36.

[206] Jean FRAYSSINET, « Note2be.com : la notation ou pas des enseignants, telle est la question… », (Mai 2008) 36 *Revue Lamy Droit de l'immatériel* 30-36 : « *On ne peut que regretter la grande superficialité et faiblesse de l'argumentation de la CNIL qui a* manqué l'occasion de construire un début de doctrine à partir du cas d'espèce. »

Frayssinet, l'article 10 alinéa 2 de la Loi modifiée de 1978 n'a nullement été invoqué[207].

En second lieu, et de manière plus substantielle, il nous apparaît difficile de soutenir que le fait pour les internautes de déposer des « renseignements personnels » – à supposer qu'ils en soient – sur le site de www.note2be.com puisse constituer une collecte pour ce dernier. Car telle est bien la prétention des plaignants qui dans leur requête, conformément à ce que l'on peut lire dans l'arrêt de Cour d'appel, prétendent que l'activité est en violation de la loi de 1978

« puisque : les données ne sont pas **collectées** de manière loyale (1°), les données sont **collectées** pour des finalités illégitimes (2°), (…), elles sont **collectées** sans limitation de durée (5°) »[208].

La notion clé de collecte, bien que nullement définie, correspond généralement à une situation sensiblement différente de celle à laquelle nous sommes confrontés avec cette affaire. Et comme nous avons pu le faire valoir dans le présent ouvrage, la présente notion doit être envisagée au regard de l'intensité de contrôle que le site dispose sur les renseignements personnels. Dans la situation présente, une partie du contrôle est exercée par les usagers eux-mêmes, le site ne semblant avoir ici qu'une capacité de réaction *a posteriori*. À cet égard, il est surprenant que nulle part dans aucune de ces décisions l'on ne réfère au régime juridique des intermédiaires tel que cela été prévu dans la *Loi sur la confiance dans l'économie numérique*[209]. Car ces lois voulaient au départ introduire un régime

---

207 « Aucune autre décision produisant des effets juridiques à l'égard d'une personne ne peut être prise sur le seul fondement d'un traitement automatisé de données destiné à définir le profil de l'intéressé ou à évaluer certains aspects de sa personnalité. »

208 Loi n° 78-17 du 6 Janvier 1978 relative à l'informatique, aux fichiers et aux libertés, en ligne : http ://www.legifrance.gouv.fr/affichTexte.do ?cidTexte=LEGITEXT000006068624&dateTexte=20091221.

209 Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, en ligne : http ://www.legifrance.gouv.fr/affichTexte.do ?cidTexte=JORFTEXT000000801164.

d'exonération *a priori* et seulement permettre un contrôle *a posteriori*. L'idée derrière cela était que l'on ne voulait pas handicaper trop lourdement des vocations commerciales afin d'éviter la situation qui avait court dans les années 90 où tout le monde intentait une action comme les intermédiaires. Ainsi, tant celui qui se plaignait d'une information publiée que celui qui avait vu cette information retirée se retournaient contre l'entité qui se trouvait au milieu. Aussi la solution médiane adoptée fut de retenir l'irresponsabilité de cet intermédiaire pour autant qu'il agisse promptement lorsqu'on lui notifie une infraction.

À cet égard, et en conclusion, cette affaire retentissante ne nous apparaît pas véritablement dangereuse et ressemble un peu aux moulins à vent de *Don Guichotte*. Le mal n'est pas là, notamment parce que les activités sont visibles et les excès peuvent être réparés en faisant une démarche auprès des prestataires de service. Si l'électronisation à outrance des renseignements personnels est susceptible, dans le futur, d'être attentatoire aux intérêts des individus, c'est bien davantage dans l'opacité des arrière-boutiques que dans de pareilles vitrines ouvertes au monde. »[210]

B – Définition et illustrations

i) Définition

La collecte de renseignements personnels s'entend donc comme une opération par laquelle des renseignements sont placés sous le contrôle d'une entité qui du fait de cette opération acquiert, à l'égard des documents ou renseignements, un droit d'en prendre connaissance. Pour qu'il y ait « collecte » de renseignements ou de documents, il faut que ces documents ou rensei-

[210] Vincent GAUTRAIS, « Give me Five ? Traitement jurisprudentiel du commerce électronique », (2009) 21-2 *Cahiers de la propriété intellectuelle* 389, 401.

gnements aient été communiqués à une entité, à une personne qui a le droit d'en prendre connaissance.

ii) Illustrations

Illustration 1 :

Les trois illustrations vues plus tôt sont toutes susceptibles de donner lieu à interpréter le terme « collecter ». Dans l'hypothèse 1, concernant l'identification des usagers, où ne serait pas considéré comme étant une collecte la situation par laquelle une administration reçoit des renseignements personnels d'un usager, renseignements que ce dernier serait uniquement porté à donner afin que le prestataire en ligne puisse reconnaître l'identité de la personne. L'administration ne collecte dans ce cas que les renseignements qu'elle n'a pas.

On ne saurait non plus considérer qu'il y a collecte lorsque le prestataire en ligne ne fait qu'utiliser des renseignements personnels qui seraient sous le contrôle d'autres organismes. On ne pourrait non plus considérer qu'il y a collecte lorsque des documents contenant des renseignements personnels ne sont pas dans une version intelligible.

Illustration 2 :

De manière plus évidente que l'illustration 1, la situation 2 en est une qui présente une hypothèse s'apparentant à une telle action. En effet, il s'agit ici d'évaluer la situation où un usager, un professeur d'université au Canada par exemple, décide, sans aucune demande de la part de l'administration, de déposer un contenu pouvant comporter des renseignements personnels. L'information est sans aucun doute gardée techniquement par l'organisme public qui propose l'application du CV commun. D'ailleurs le contrat d'adhésion du site en question le confirme en ces mots :

> **Les renseignements** contenus dans ce système **vous appartiennent** et **ils ne seront pas partagés sans votre connaissance ou votre consentement**. Seuls **les renseignements que vous avez saisis seront sauvegardés** (...)

> **Vos renseignements personnels sont à l'abri de l'accès, de l'utilisation ou de la révélation non autorisée**. **Le système CVC sauvegarde vos renseignements personnels** sur des ordinateurs placés dans un environnement sécure et **avec accès contrôlé pour protéger contre l'accès, l'utilisation ou la révélation non autorisée.** Toutes **les données circulant entre le CVC et le matériel informatique des utilisateurs finaux**, ou entre le CVC et le matériel informatique des organismes membres, **sont encodées avec des technologies d'encryptage de 128 bits et sont transmises à l'aide du protocole SSL (Secure Socket Layer)** (…) (nos soulignements)[211]

De même, la politique de confidentialité du site du Fonds québécois de la recherche sur la nature et les technologies (FQRNT) mentionne que :

> « Le Fonds a instauré des mesures de sécurité à la fine pointe de la technologie **afin de vous protéger contre la perte ou l'utilisation non autorisée des informations vous concernant qui seront sous son contrôle**. De plus, les serveurs du Fonds sont protégés par une technologie de type coupe-feu[212].(nos soulignements)

Mais sur le plan juridique, il en est différemment dans la mesure où l'information n'est pas sous son contrôle, l'usager pouvant à tout moment l'effacer, la modifier, l'altérer. D'autre part, le prestataire en ligne est tenu à des obligations quant à la **garde** de ces informations, et même s'il pourrait être en mesure de prendre connaissance des informations en cause, il n'a normalement pas le droit de le faire.

---

[211] Le CV Commun Canadien est en ligne : <http://www.commoncv.net/index_f.html>.

[212] La politique de confidentialité du site du Fonds québécois de la recherche sur la nature et les technologies (FQRNT) en ligne : <http://www.fqrnt.gouv.qc.ca/>.

Illustration 3 :

La collecte est également envisageable dans la situation 3[213]. Pourtant, selon nous, il n'en est rien. En effet, l'usager est à l'initiative du dépôt effectué[214]. Le droit encadre les activités de **conservation** de l'administration et l'on peut facilement imaginer que celui qui a déposé le contenu, pour fins de diffusion, dispose de la capacité de le retirer à sa convenance. Du fait de ce contrôle de la part de l'usager, et du contrôle limité de la part de l'organisme de promotion du tourisme, il est impossible de qualifier cette action de diffusion comme étant une collecte.

Mais il y a plus. En effet, dans la mesure où il y a une diffusion de l'information au public, l'administration peut légitimement retirer des documents qui ne correspondraient pas aux exigences thématiques ou disciplinaires auxquelles le site est assujetti. On peut même dire qu'elle est obligée de le faire selon la *Loi concernant le cadre juridique des technologies de l'information*[215] qui encadre les activités d'hébergement (article 22) et de garde (article 26). Ainsi, tout comme *Facebook* qui a récemment retiré des images liées à la promotion de l'allaitement maternel, une administration faisant la promotion d'une région, d'une ville, d'une province ou d'un pays, pourrait retirer une vidéo qu'il considérerait comme inappropriée et sans but aucun avec la raison d'être du site. Généralement, tant la capacité d'enlever lesdits documents que la détermination des domaines appropriés, sont établis par contrat. Comme cela a été préalablement mentionné dans un rapport français, ce n'est pas parce qu'un « hébergeur » opère un certain ordonnancement des fichiers déposés par autrui, qu'il

---

213 La plupart des projets correspondants à cette situation établissent dans leur contrat d'adhésion un consentement à une collecte. Un consentement pour le moins fictif et contestable. *Infra*.

214 *Supra*, voir le premier critère évoqué préalablement à *Partie 1, Chapitre 1, Section 1, 2, A*, s'intitulant « Critère de l'activité de l'utilisateur ».

215 Art 22 et 26 de la *Loi concernant le cadre juridique des technologies de l'information*, L.R.Q., c. C-1.1, en ligne : <http://www.canlii.org///qc/legis/loi/c-1.1/20080818/tout.html>.

perdra de ce fait l'exonération de responsabilité que la loi apporte à son statut[216].

Ainsi, il faut éviter de se méprendre sur la nature d'un pareil « contrôle » qui peut être effectué par le responsable dudit site ; un contrôle qui peut s'effectuer soit *a priori* soit *a posteriori*. Dans le premier cas, l'organisme effectue ce que nous appellerons un « filtrage » pour le distinguer d'une activité de contrôle éditorial. Dans le second, il s'agit d'une réaction qui est clairement exigée à l'article 22 de la *Loi concernant le cadre juridique des technologies de l'information*.

Si cette seconde situation renforce la qualification de conservation de l'opération – et non de collecte –, il importe de préciser la première. Le « filtrage » aurait pour objet de s'intéresser aux dépôts des utilisateurs que l'organisme jugerait déviants ou attentatoires à leurs objectifs de promotion, mais n'implique pas nécessairement que celui-ci se livre à un travail d'édition. Simplement, l'administration exerce par ce biais un tri selon certains critères de documents qui ne seraient en aucun cas compatibles avec la finalité recherchée du site. Par exemple, si un site public contrôle des documents, éventuellement automatiquement afin de contrôler des images inappropriées ou du contenu haineux, elle ne pourrait être tenue responsable d'une image qui irait par exemple à l'encontre de la protection des renseignements personnels. En fait, il ne peut nous être imputable que ce que l'on contrôle.

Bien entendu, ce « filtrage » – terme que nous nous permettons d'utiliser ici au lieu de « contrôle » pour le distinguer du contrôle éditorial – est donc un moyen de contrôler, un peu, l'usage dont il est fait d'un tel site. Mais ce « filtrage » n'étant qu'un contrôle d'une intensité réduite[217] (par exemple le caractère inapproprié par rap-

---

[216] Jean DIONIS DU SÉJOUR et Corinne ERTHEL, *Rapport d'information no. 627 déposé en application de l'article 86, alinéa 8, du Règlement sur la mise en application de la loi no. 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique*, Assemblée nationale, 23 janvier 2008, p. 21. <http://www.assemblee-nationale.fr/13/rap-info/i0627.asp>. Voir notamment la citation de ces auteurs en ligne : la note 110.

[217] *Supra*, voir la *Partie 2, Chapitre 1, Section 3, 1, C*, s'intitulant « Illustration 3 : consentement et publication par les usagers ».

port à la finalité du site des renseignements qui y sont déposés), il ne pourra être imputable au prestataire qui opère ce filtrage que de ce qu'il contrôle vraiment. Ainsi, il serait responsable de la publication, si contrôle *a priori*, ou du non retrait, si contrôle *a posteriori*, d'une image inappropriée, car c'est ce qu'il contrôle, mais pas de la publication d'un renseignement personnel, si ce n'est pas ce qu'il entend baliser. Ce filtrage pourrait d'ailleurs très bien s'opérer de manière mécanique, notamment par l'intermédiaire d'un logiciel, chose qui semble plus difficile pour la seconde hypothèse de contrôle des renseignements personnels. Or, un tel contrôle par une « machine », par exemple un logiciel qui serait programmé à détecter les seuls documents jugés déviants au regard de critères prédéterminés, renforcerait aussi l'absence de connaissance *a priori*, par le prestataire en ligne, d'une violation aux lois sur la protection des renseignements personnels[218].

2 – Opération de conservation

A – Mise en contexte

La conservation est une opération qui est explicitement encadrée dans les lois sur la protection des renseignements personnels, et apparaît tout particulièrement dès l'article 1 de la *Loi sur l'Accès aux documents des organismes publics et sur la protection des renseignements personnels*, sous le titre « application de la loi » où il est prévu la disposition suivante :

> « 1. La présente loi s'applique aux documents détenus par un organisme public dans l'exercice de ses fonctions, que leur **conservation** soit assurée par l'organisme public ou par un tiers. »[219]

---

[218] Relativement au critère de la « connaissance », voir *Supra*, voir le quatrième critère évoqué préalablement à *Partie 1, Chapitre 1, Section 1, 2, D*, s'intitulant « Critère de la connaissance du PEL ».

[219] Article 1 de la *Loi sur l'Accès aux documents des organismes publics et sur la protection des renseignements personnels*, L.R.Q., c. A-2.1, 2006, c. 22. en ligne : <http://canlii.org/fr/qc/legis/lois/lrq-c-a-2.1/derniere/lrq-c-a-2.1.html>.

Outre cet article qui donne une portée très générale à l'opération, il est possible de citer l'article 63.1 de la même Loi qui est la référence en matière de sécurité en disposant qu'

> « Un organisme public **doit prendre les mesures de sécurité** propres à assurer la protection des renseignements personnels collectés, utilisés, communiqués, **conservés** ou détruits et qui sont raisonnables compte tenu, notamment, de leur sensibilité, de la finalité de leur utilisation, de leur quantité, de leur répartition et de leur support. »[220]

Par ailleurs, les articles 4.7.1 et 4.7.2 de l'Annexe 1 de la *Loi sur la protection des renseignements personnels et les documents électroniques* (PIPEDA) sont le pendant fédéral du contenu des articles 1 et 63.1 de la *Loi sur l'accès* puisqu'ils disposent :

> « **4.7.1** Les mesures de sécurité doivent protéger les renseignements personnels contre la perte ou le vol ainsi que contre la consultation, la communication, la copie, l'utilisation ou la modification non autorisées. Les organisations doivent protéger les renseignements personnels quelle que soit la forme sous laquelle ils sont conservés. »
>
> « **4.7.2** La nature des mesures de sécurité variera en fonction du degré de sensibilité des renseignements personnels recueillis, de la quantité, de la répartition et du format des renseignements personnels ainsi que des méthodes de **conservation**. Les renseignements plus sensibles devraient être mieux protégés. La notion de sensibilité est présentée à l'article 4.3.4. »[221] (nos soulignements)

Éventuellement, l'on pourrait citer également l'article 72 de la *Loi sur l'accès* qui oblige

---

[220] Article 63.1 de la *Loi sur l'Accès aux documents des organismes publics et sur la protection des renseignements personnels*, L.R.Q., c. A-2.1, 2006, c. 22. en ligne : <http://canlii.org/fr/qc/legis/lois/lrq-c-a-2.1/derniere/lrq-c-a-2.1.html>.

[221] Art. 4.7.1 et 4.7.2 de l'annexe 1 de la *Loi sur la protection des renseignements personnels et les documents électroniques* (PIPEDA) en ligne : <http://www.canlii.ca/fr/ca/legis/lois/lc-2000-c-5/derniere/lc-2000-c-5.html>.

> « [u]n organisme public (…) à ce que les renseignements personnels qu'il **conserve** soient à jour, exacts et complets pour servir aux fins pour lesquelles ils sont recueillis ou utilisés. »[222] (nos soulignements)

Cela dit, aucune définition véritable de la « conservation » n'est présente dans la *Loi sur l'accès*, alors qu'elle l'est passablement mais de manière imprécise dans la *Loi concernant le cadre des technologies de l'information*, où la conservation semble être envisagée comme l'action de maintenir intact, dans le même état.

Ainsi, et selon l'article 19 de la *Loi concernant le cadre des technologies de l'information,* dès lors qu'une personne est tenue de conserver un document, elle a le devoir d'en

> « assurer le maintien de son intégrité et voir à la disponibilité du matériel permettant de le rendre accessible et de l'utiliser aux fins auxquelles il est destiné »[223].

Mais en dépit de cet éclaircissement, des risques de chevauchement persistent.

*i) Conservation **versus** hébergement*

La **conservation** peut d'abord être envisagée, et distinguée, en fonction de la finalité associée à cette opération. Et si comme nous venons de voir, le devoir de conserver est généralement associé à une obligation de préservation de l'intégrité d'un document, il est possible de la comparer à une activité **d'hébergement**. Bien sûr, ce terme, au Québec du moins, n'est pas juridiquement

---

222 Article 72 de la *Loi sur l'Accès aux documents des organismes publics et sur la protection des renseignements personnels*, L.R.Q., c. A-2.1, 2006, c. 22. en ligne : <http://canlii.org/fr/qc/legis/lois/lrq-c-a-2.1/derniere/lrq-c-a-2.1.html>.

223 Article 19, *Loi concernant le cadre juridique des technologies de l'information*, L.R.Q., c. C-1.1, en ligne : <http://www.canlii.org///qc/legis/loi/c-1.1/20080818/tout.html>, dispose ceci : « Toute personne doit, pendant la période où elle est tenue de conserver un document, assurer le maintien de son intégrité et voir à la disponibilité du matériel qui permet de le rendre accessible et intelligible et de l'utiliser aux fins auxquelles il est destiné. ».

pertinent. En effet, cette opération ne donne lieu ni à une définition ni même à une utilisation du terme dans la *Loi concernant le cadre juridique des technologies de l'information*. Néanmoins, elle correspond à une réalité où un prestataire en ligne offre un service à un usager permettant à ce dernier de publier un document, quel qu'il soit (texte, audio, photo, vidéo, etc.). Une situation qui peut d'ailleurs être rapprochée du cas de l'illustration 3 où une entité publique fait la promotion du tourisme de sa région en revêtant le statut de prestataire en ligne qui est prévue à l'article 22 de la *Loi concernant le cadre juridique des technologies de l'information*[224]. Ce terme d'hébergement semble donc correspondre à la réalisation de conservation par un tiers. L'hébergement est donc bien une activité de conservation mais qui correspond à une réalité assez précise à savoir celle pour un prestataire « de mettre à disposition des internautes des sites web conçus et gérés par des tiers.[225] ».

*ii) Conservation **versus** garde*

Dans d'autres hypothèses, il est également possible de croire que la conservation puisse être rapprochée de la finalité de **garde** qui ne semble pas substantiellement différente de la première. La notion de garde est développée sous l'article 26 de la *Loi concernant le cadre juridique des technologies de l'information* et se lit comme suit :

> « **Garde** d'un document technologique.
>
> **26.** Quiconque confie un document technologique à un prestataire de services pour qu'il en assure la **garde** est, au préalable, tenu d'informer le prestataire quant à la protection que requiert le document en ce qui a trait à la confidentialité de

[224] *Loi concernant le cadre juridique des technologies de l'information,* L.R.Q., c. C-1.1, en ligne : <http://www.canlii.org///qc/legis/loi/c-1.1/20080818/tout.html>, article 22.

[225] Voir la définition d'hébergeur Internet sur le site Wikipedia à <http://fr.wikipedia.org/wiki/Hébergement_Internet>.

l'information et quant aux personnes qui sont habilitées à en prendre connaissance »[226]

La distinction entre conservation et garde est difficile à faire, d'abord parce que les deux termes peuvent assez facilement être inter-changés dans le langage courant ; ensuite, parce que l'article 26 sur la garde se situe dans la *Loi concernant le cadre juridique des technologies de l'information* sous le paragraphe de « la consultation » ce qui ne nous semble pas logique. Encore, il n'est pas possible de croire que la garde correspondrait à l'opération effectuée par un tiers de conserver des documents pour le compte d'autrui – ce que l'on appelle parfois un tiers-archiveur –, alors que la conservation serait davantage le fait de garder pour son propre compte. En effet, l'article 22 de la *Loi concernant le cadre des technologies de l'information* prévoit spécifiquement l'hypothèse du « prestataire de services qui agit à titre d'intermédiaire pour offrir des services de conservation »[227], tout comme l'article 26 de la même loi relativement à la garde. Une organisation peut donc garder pour autrui, sous réserve de respecter les obligations identifiées dans ledit article, tout comme elle peut conserver des documents, là encore avec un certain nombre de conditions. Or, c'est sur ces dernières que la distinction devrait se manifester. Et s'il est une spécificité qui semble découler de ces conditions relatives à la garde, c'est apparemment la prise en considération de la donne sécuritaire.

Aux termes de l'article 26 de la *Loi concernant le cadre juridique des technologies de l'information*[228] la personne qui confie le document à un prestataire de services pour en assurer la garde a envers le prestataire de services les trois obligations suivantes :

---

[226] *Loi concernant le cadre juridique des technologies de l'information,* L.R.Q., c. C-1.1, en ligne : <http://www.canlii.org///qc/legis/loi/c-1.1/20080818/tout.html>, article 26.

[227] *Loi concernant le cadre juridique des technologies de l'information,* L.R.Q., c. C-1.1, en ligne : <http://www.canlii.org///qc/legis/loi/c-1.1/20080818/tout.html>, article 22.

[228] *Loi concernant le cadre juridique des technologies de l'information,* L.R.Q., c. C-1.1, en ligne : <http://www.canlii.org///qc/legis/loi/c-1.1/20080818/tout.html>.

1) informer ce dernier de la protection que requiert le document lors de la remise du document ; 2) lui donner des informations adéquates au prestataire sur les mesures de protection de la confidentialité que le document nécessite, et 3) lui indiquer quelles sont les personnes habilitées à en prendre connaissance.

De son côté, et toujours en transposant l'article 26 sus mentionné, le prestataire de services doit faire en sorte que les moyens technologiques convenus d'un commun accord avec la personne qui lui a confié le document soient 4) mis en place durant toute la période pendant laquelle il en la garde. Ainsi, il est tenu, durant la période où il en a la garde, de veiller 5) à ce que les moyens technologiques soient mis en place pour en assurer la sécurité, en préserver l'intégrité et, le cas échéant, en protéger la confidentialité et en interdire l'accès à toute personne qui n'est pas habilitée à en prendre connaissance. Au surplus, le prestataire a l'obligation 6) de respecter toute autre obligation prévue dans une loi relativement à la conservation d'un document.

La garde telle que décrite à l'article 26 de la *Loi concernant le cadre juridique des technologies de l'information* dispose donc de mesures de sécurité passablement plus rigoureuses que la seule obligation du respect de l'intégrité que l'on retrouve à l'article 22 de la même loi. L'opération de garde constitue donc une hypothèse de conservation à laquelle on associe une obligation sécuritaire de la part du prestataire suite à l'information en ce sens faite par l'intéressé. La garde est donc une sous-catégorie de la conservation.

D'ailleurs, le contrat d'adhésion du site du CV Commun Canadien confirme cette idée de garde en ces mots :

> « Vos renseignements personnels sont à l'abri de l'accès, de l'utilisation ou de la révélation non autorisée. Le système CVC sauvegarde vos renseignements personnels sur des ordinateurs placés dans un environnement sécure et avec accès contrôlé pour protéger contre l'accès, l'utilisation ou la révélation non autorisée. Toutes les données circulant entre le CVC et le matériel informatique des utilisateurs finaux, ou entre le CVC et le matériel informatique des organismes membres, sont encodées avec des technologies d'encryptage de

> 128 bits et sont transmises à l'aide du protocole SSL (Secure Socket Layer)(...) [229]

*iii) Conservation **versus** donner accès*

La notion de conservation peut également être comparée à la situation selon laquelle un document doit être disponible pendant un certain temps. Dans la notion de conservation, il y a en effet cette notion d'accessibilité, qui en est la raison d'être ; la disponibilité étant une des composantes de la conservation. Également, et relativement aux documents technologiques portant un renseignement confidentiel, un certain contrôle d'accès doit être opéré par un prestataire, assurant que certains puissent y accéder et que d'autres ne le puissent pas. Cette situation donne d'ailleurs lieu à un encadrement passablement strict, aux termes de l'article 25 de la *Loi concernant le cadre juridique des technologies de l'information* selon lequel :

> « [l]a personne responsable de l'accès à un document technologique qui porte un renseignement confidentiel doit prendre les mesures de sécurité propres à en assurer la confidentialité, notamment par un contrôle d'accès effectué au moyen d'un procédé de visibilité réduite ou d'un procédé qui empêche une personne non autorisée de prendre connaissance du renseignement ou, selon le cas, d'avoir accès autrement au document ou aux composantes qui permettent d'y accéder. » [230]

Un article en bien des points similaire à la portée de l'article 63.1 précité de la *Loi sur l'accès*[231] et de l'article 4.7.3 de l'Annexe 1 de la Loi sur la protection des *renseignements personnels et les documents électroniques* (PIPEDA) qui dispose :

---

229 Le CV Commun Canadien est en ligne : <http://www.commoncv.net/index_f.html>.

230 *Loi concernant le cadre des technologies de l'information*, L.R.Q., c. C-1.1, en ligne : <http://www.canlii.org///qc/legis/loi/c-1.1/20080818/tout.html>.

231 Article 63.1 de la *Loi sur l'Accès aux documents des organismes publics et sur la protection des renseignements personnels*, L.R.Q., c. A-2.1, 2006, c. 22. en ligne : <http://canlii.org/fr/qc/legis/lois/lrq-c-a-2.1/derniere/lrq-c-a-2.1.html>.

« 4.7.3 Les méthodes de protection devraient comprendre :
a) des moyens matériels, par exemple le verrouillage des classeurs et la restriction de l'accès aux bureaux ;
b) des mesures administratives, par exemple des autorisations sécuritaires et un **accès** sélectif ; et
c) des mesures techniques, par exemple l'usage de mots de passe et du chiffrement. »[232] (nos soulignements)

Encore une fois, le contrat d'adhésion du site du CV Commun Canadien confirme cette idée de donner accès en ces mots :

> Les organismes membres n'auront pas l'accès en ligne à vos données sans votre consentement. **Seuls les organismes auxquels vous donnez le consentement y auront accès**. Vous pouvez donner et mettre à jour votre consentement à tout moment à partir de la page « Accueil – Mon CV »(...)
>
> Le système CVC utilise un logiciel qui surveille la transmission des données sur le réseau **pour déceler toute tentative non autorisée de télécharger ou de modifier des renseignements** ou de causer d'autres dommages (...)
>
> Ceux qui **accèdent au système sans autorisation**, ou qui **abusent de leur autorité pour accéder** à des renseignements personnels sans raison valable, sont exposés à une poursuite légale.
>
> **Vos renseignements personnels sont à l'abri de l'accès**, de l'utilisation ou de la révélation **non autorisée**. Le système CVC sauvegarde vos renseignements personnels sur des ordinateurs placés dans un **environnement sécure et avec accès contrôlé pour protéger contre l'accès, l'utilisation ou la révélation non autorisée**. [233]

---

[232] Art. 4.7.3 de l'annexe 1 de la *Loi sur la protection des renseignements personnels et les documents électroniques* (PIPEDA), en ligne : <http://www.canlii.ca/fr/ca/legis/lois/lc-2000-c-5/derniere/lc-2000-c-5.html>.

[233] Le CV Commun Canadien est en ligne : <http://www.commoncv.net/index_f.html>.

Ainsi, l'accès à des renseignements personnels est assujetti à des limites et il importe de se dissocier de la croyance correspondant à un certain « sens commun » selon laquelle dès lors qu'on est en « possession » physique d'un document, on a le droit d'en prendre connaissance.

D'ailleurs, l'article 25 précité réaffirme au contraire que l'obligation de contrôler doit être effectuée par la personne responsable, personne qui n'est pas forcément celle qui gère « physiquement » le document en cause. La Loi lui impose plutôt l'obligation de voir à ce que les moyens technologiques convenus soient mis en place pour en assurer la sécurité, en préserver l'intégrité et, le cas échéant, en protéger la confidentialité.

iv) Conservation ***versus*** *communication*

La conservation d'un document est aussi une opération distincte de la **communication** et ce n'est pas parce qu'une entité conserve un document, qu'elle a le droit d'y accéder ou de le communiquer. Si un document confidentiel tel un document comportant des renseignements personnels est confié à une entité, celle-ci a l'obligation de s'assurer que la consultation du document soit réservée aux seules personnes qui ont le droit de se voir communiquer le document.

Le seul fait de confier un document à une entité pour qu'elle le conserve n'emporte pas le droit de le communiquer s'il comporte des renseignements confidentiels ou des renseignements auxquels une personne n'a pas le droit d'accéder.

v) Conservation ***versus*** *archivage*

La conservation peut en certains cas être également distinguée de la notion d'**archivage** dans la mesure où il est parfois entendu que cette dernière opération succède à la conservation, dès lors que le document en cause ne devient plus actif[234]. La

[234] Michel ROBERGE, *La gestion de l'information administrative – Application globale, systémique et systématique*, Documentor, Québec, 1992, p. 261 :

conservation semble donc s'appliquer durant toute la vie « active » du document, l'archivage correspondant à la période temporelle postérieure à la conservation.

Pourtant, cette vision ne semble pas compatible avec la *Loi sur les archives* qui entend s'occuper dans le cadre son application des documents « actifs », « semi-actifs » mais aussi « inactifs », conformément à ce qui est défini à son article 2[235]. Là encore, il n'est pas toujours aisé de distinguer ce terme de celui de conservation, mais l'on sait seulement qu'une distinction semble avoir été introduite dans la *Loi concernant le cadre juridique des technologies de l'information*[236], notamment à l'article 6 alinéa 2, l'archivage étant assurément une sous-catégorie de la conservation.

Une autre distinction qui est également envisageable est que l'archivage s'intéresse au **contenu intellectuel** d'un document alors que la conservation est davantage attachée au support en tant que tel et à l'ensemble de son processus de gestion. Également, alors que l'archivage est souvent associé à une finalité ayant soit un caractère historique soit un caractère de permanence, la conservation est généralement liée au respect de délais légaux imposés pour des fins de preuve ou notamment d'obligations comptables ou administratives. C'est notamment cette opposition qui semble de mise dans les définitions offertes par la *Bibliothèque nationale du Canada* qui prévoit ceci :

> « **Archivage** : Les documents sont versés sur un serveur institutionnel dans le but de préserver leur **contenu intellectuel** de façon **permanente**. L'archivage s'entend dans son sens le plus

---

« Archives (d'une organisation) : ensemble de document dont la valeur administrative en général ou la valeur financière ou légale en particulier est éteinte, qui ont une valeur de recherche ou de témoignage et qui doivent être conservés en permanence. »

235 *Loi sur les archives*, L.R.Q., c. A-21.1, article 2.

236 *Loi concernant le cadre des technologies de l'information*, L.R.Q., c. C-1.1, en ligne : <http://www.canlii.org///qc/legis/loi/c-1.1/20080818/tout.html>, art. 6 al.2 qui dispose : « L'intégrité du document doit être maintenue au cours de son cycle de vie, soit depuis sa création, en passant par son transfert, sa consultation et sa transmission, jusqu'à sa **conservation**, y compris son **archivage** ou sa destruction »

> large, et couvre les concepts de compilation, de conservation et de mise en disponibilité à long terme. »
>
> « **Conservation** : Activité […], qui garantit la longévité des **collections**. Les activités de préservation comprennent la conservation des collections, la création de substituts, le contrôle des conditions ambiantes et l'établissement des conditions d'utilisation. (Politique de conservation de la BNC, 1989). En ce qui concerne les publications électroniques, les activités de conservation englobent l'organisation, la description, la mise à jour et la migration de l'information électronique afin d'assurer l'accessibilité à long terme des publications. »[237] (Nos soulignements)

Ces définitions qui nous semblent celles avec lesquelles nous sommes le plus à l'aise montrent aussi que

> « [c]es définitions étant posées, il est évident que, dans un monde numérique, la nuance est subtile entre archivage et conservation. » [238]

*vi) Conservation **versus** détention*

Autre élément de distinction, la conservation doit être distinguée de la notion, passablement floue, de **détention**. Ce dernier concept est extérieur à la gestion documentaire et ne trouve un développement que dans le cadre du droit d'accès prévu dans la

---

[237] BIBLIOTHÈQUE NATIONALE DU CANADA, Groupe de coordination des collections électroniques. *Politiques et directives relatives aux publications électroniques diffusées en réseau*, octobre 1998. Référence citée par Guylaine BEAUDRY et Gérard BOISMENU, Conception d'un portail de production, de diffusion et de gestion de publications électroniques – Étude de faisabilité, Chapitre 5, 2000, en ligne : <http://www.erudit.org/documentation/etude/accueil.html>.

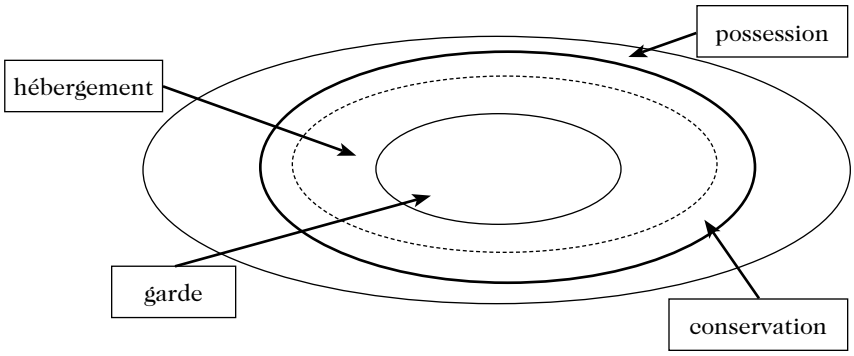
[238] Guylaine BEAUDRY et Gérard BOISMENU, Conception d'un portail de production, de diffusion et de gestion de publications électroniques – Étude de faisabilité, Chapitre 5, 2000, en ligne : <http://www.erudit.org/documentation/etude/accueil.html>.

Loi sur l'accès. C'est ce que nous verrons dans le paragraphe 3 sous la présente section.

*vii) Conservation **versus** possession*

Le terme de **possession** est un terme uniquement générique qui ne bénéficie d'aucune utilisation à proprement parler dans les lois et qui ne correspond non plus à aucune signification particulière sur le plan technique. De ce fait, l'on devrait sans doute éviter de l'utiliser. Il semblerait néanmoins avoir une signification très globale.

En guise de résumé, il est possible de dire que plusieurs termes ont été précisés dans la *Loi concernant le cadre juridique des technologies de l'information* relativement à des opérations « techniques » susceptibles de survenir durant le cycle de vie des documents, et notamment de ceux contenant des renseignements personnels. Ces termes pourraient d'ailleurs être illustrés selon la façon suivante : la notion centrale est celle de la **conservation**, notion qui inclut celle de **garde** (qui semble être une opération de conservation à laquelle on a ajouté des exigences sécuritaires supplémentaires). À côté de ces deux termes particulièrement encadrés, l'on peut greffer ceux d'hébergement, qui correspond à un type particulier de conservation de données sur Internet, pouvant donner lieu à une communication, et ce, même si cette opération n'est pas spécifiquement prévue par le droit québécois. Enfin, et en marge de ces termes, il est possible de situer le terme « possession », même s'il est conseillé de l'éviter du fait de sa généralité.



En revanche, il est plus difficile de mettre en perspective les notions précitées avec d'autres opérations telles que celles de « collection » et de « détention » qui sont à l'origine des lois sur la protection des renseignements personnels et qui semblent référer davantage à des obligations de nature juridique pour des organismes qui ont un contrôle véritable sur les documents contenant des renseignements personnels.

B – Définition et illustrations

i) Définition

La **conservation** est l'action de maintenir l'intégrité d'un document, que celui-ci contienne – ou non – des renseignements personnels, et ce, durant toute la durée active du document afin que ce dernier demeure accessible.

ii) Illustrations

Illustration 1

Dans la première hypothèse relative à la méthode d'authentification d'identité du citoyen aux fins de permettre l'accès à un service déterminé, la conservation ne semble pas poser de difficultés d'interprétation. En effet, le prestataire en ligne doit conserver les renseignements personnels des usagers avec toutes les obligations attachées à cette opération. Notons que ceci ne requiert aucune autorisation préalable, aucun consentement. Simplement, il ne doit accorder un accès, permettre une utilisation, ou plus globalement, une circulation des renseignements personnels que lorsque cela est autorisé. Concrètement, et en resituant le questionnement à notre hypothèse impliquant les quatre intervenants à savoir le citoyen (1), le ministère ou organisme (MO) qui rend le service (2), le « prestataire en ligne » (PEL) (3) et le ministère ou organisme (MO) qui est responsable de la banque de données avec laquelle on va vérifier la véracité desdits renseignements personnels (4)[239], il appert que le prestataire en

[239] *Supra*, voir le schéma 1 dans Partie préliminaire, Chapitre 1, Section 1, 2, A, i).

ligne (3), par ailleurs mandaté par autrui à savoir l'organisme qui rend le service (2), joue le rôle d'« interface ». Ce rôle pourrait en certains cas impliquer une conservation lorsque des renseignements personnels sont gardés par le prestataire en ligne. Cette conservation serait assujettie à l'article 26 de la *Loi concernant le cadre juridique des technologies de l'information* qui organise les responsabilités dans cette situation d'impartition de documents. Dans d'autres cas, il est même possible de croire qu'aucune conservation n'aurait lieu, notamment dans l'hypothèse où les renseignements personnels ne seraient utilisés que pour les fins d'identification et ensuite détruits ou chiffrés par le prestataire en ligne. En d'autres mots, toutes les entités qui se trouvent en possession d'une version intelligible des documents échangés peuvent se trouver dans une position où ils ont des obligations de conservation.

Illustration 2

Relativement à l'illustration 2, concernant l'hébergement de renseignements du CV d'un professeur d'Université au Canada, le CV Commun Canadien en question correspondrait à une situation de garde conformément à l'article 26 de la *Loi concernant le cadre juridique des technologies de l'information*, et ce, tant que l'usager – le professeur – ne consente pas à une autre finalité que celle pour laquelle l'information a été déposée auprès du prestataire en ligne (en l'occurrence le dépôt d'un CV pour évaluer une demande de subvention où seules les personnes autorisées auront un droit d'accès aux renseignements personnels que le dossier contient). Le prestataire en ligne a l'obligation d'assurer la garde des documents déposés par les chercheurs. Là encore, la garde concerne en bien des cas des renseignements personnels et les obligations habituelles y relatives, telle que la sécurité de ces derniers et le fameux consentement, vont s'appliquer, pour remettre en cause le caractère secret de ces informations. Néanmoins, et c'est une différence d'avec la première illustration, il est toujours possible pour l'usager d'accéder, corriger voire détruire la plupart des données en cause. Dans la mesure où nous considérons que la conservation est associée à une obligation de garder intacts les informations et notamment les renseignements personnels, cette obligation ne serait bien évidemment pas maintenue ou remise en cause par la destruction de l'usager.

En revanche, il est selon nous imaginable que ce statut de garde puisse être modifié si la finalité de la conservation change elle aussi. Par exemple, si, ce qui est fort possible, l'usager décide de rendre public l'ensemble de ses renseignements personnels inclus dans son CV, une qualification plus proche de celle de l'hébergeur au sens de l'article 22 de la *Loi concernant le cadre juridique des technologies de l'information* semblerait s'appliquer à l'administration autorisant une telle mise en ligne de ces renseignements.

Illustration 3

Enfin, dans la troisième hypothèse, soit le cas de sites visant à promouvoir le tourisme, ces prestataires en ligne proposent des fonctionnalités permettant aux internautes de publier en ligne leurs commentaires, leurs photos ou leurs vidéos. Cette L'entité qui gère ce type d'environnement le fait à titre d'intermédiaire, d'hébergeur, « pour offrir des services de conservation de documents technologiques sur un réseau de communication » au sens de l'article 22 de la *Loi concernant le cadre juridique des technologies de l'information*. Aussi, ladite entité n'est pas obligée de surveiller activement les documents ainsi publiés. Et comme les documents sont par définition publiés, la question du droit d'y accéder ne se pose pas. L'entité a le devoir de conserver les documents en conformité avec les conditions de fonctionnement du site.

Ainsi, nous croyons que les obligations de conservation risquent d'être passablement différentes dans la mesure où, par exemple, l'obligation de sécurité ou de garder secret des renseignements personnels va forcément devoir être revue dans la mesure où lesdits renseignements personnels sont publics. En effet, il faut savoir que la notion de conservation va être difficile à appliquer dès lors que, d'une part, les renseignements sont déposés par autrui et, d'autre part, ils sont accessibles à tous. D'ailleurs, l'article 2 de la *Loi sur l'accès* prend le soin de spécifier que les renseignements personnels dans les « documents conservés dans les bureaux de la publicité des droits à des fins de publicité » ne sont pas assujettis à la Loi. La rationalité derrière tout cela consisterait à déterminer comment protéger des données qui ne sont pas privées.

3 – Opération de détention

A – Mise en contexte

L'article 1 al.1 de la *Loi sur l'accès*[240] dispose que celle-ci

> « s'applique aux documents **détenus** par un organisme public dans l'exercice de ses fonctions, que leur conservation soit assurée par l'organisme public ou par un tiers. »

Le terme « détention » est difficile à définir. À la différence des autres termes identifiés ici (du moins ceux de transmission, communication, conservation, garde, hébergement), il semble en dehors du cycle de vie tel que défini dans la *Loi concernant le cadre juridique des technologies de l'information*[241] et la détention semble davantage référer à une notion de détention juridique que de détention « technique ».

Cette difficulté d'interprétation est également consacrée pour au moins **trois raisons** différentes. En premier lieu, le terme est général, **générique**, nul part défini et il est généralement compris dans le sens courant qui signifie « garder », « tenir en sa possession »[242]. Les auteurs Doray et Charrette relèvent d'ailleurs que la notion de détention est très large et recouvre à la fois la conservation des documents par l'organisme, mais aussi toute forme de possession ou de garde au sens courant du terme.

En deuxième lieu, cette notion englobe non seulement la détention « technique » des documents par l'organisme lui-même mais également la **détention juridique**, soit leur conservation, possession ou garde, par des tiers, à la demande ou pour le compte

---

240 Article 1 al.1 de la *Loi sur l'Accès aux documents des organismes publics et sur la protection des renseignements personnels*, L.R.Q., c. A-2.1, 2006, c. 22. en ligne : <http://canlii.org/fr/qc/legis/lois/lrq-c-a-2.1/derniere/lrq-c-a-2.1.html>.

241 *Loi concernant le cadre juridique des technologies de l'information*, L.R.Q., c. C-1.1, en ligne : <http://www.canlii.org///qc/legis/loi/c-1.1/20080818/tout.html>, art. 6 al.2.

242 *Duchesneau* c. *Dunham (Ville de)*, (1984-86) 1 CAI 5.

de l'organisme[243]. Si la détention juridique découle généralement d'un mandat ou d'un contrat de service confié à un tiers, consultant ou professionnel[244], la détention « technique » correspond davantage à des termes que nous avons vus précédemment, notamment dans le cadre des hébergeurs et prestataires en ligne qui relèvent plutôt du cadre juridique dessiné par l'article 22 de la *Loi concernant le cadre des technologies de l'information*[245].

Le détenteur est la personne qui est en possession d'une chose. La possession est un fait : celui d'être en contrôle d'un bien. Strictement, la détention s'applique au support sur lequel est consignée l'information. L'information est connaissance. Lorsqu'on détient de l'information, c'est qu'on a connaissance de celle-ci, c'est donc que l'information nous a été communiquée. Par contre, dans le déroulement des différentes phases de la circulation de l'information, il peut arriver qu'un acteur en particulier soit simplement détenteur d'un support comportant de l'information.

D'ailleurs, cette vision des choses est également considérée en **droit criminel** où il semble être unanimement reconnu que la simple consultation de documents de matériel pédopornographique sur Internet ne constitue pas une infraction de possession ou de détention – les deux termes étant généralement utilisés uniformément –, et ce, même si des traces ont été conservées sur l'ordinateur de la personne en cause. On peut notamment lire dans une décision à cet effet que :

---

243 Raymond DORAY et François CHARETTE, *Accès à l'information, Loi annotée, Jurisprudence Analyse et commentaires*, volume 1, mis à jour au 10 décembre 2008, Cowansville, Éditions Yvon Blais, 2001, p. III/83-5. *Montminy c. Commission d'accès à l'information*, [1985] C.S. 140, confirmée en appel : [1986] C.A.I. 217.

244 Raymond DORAY et François CHARETTE, *Accès à l'information, Loi annotée, Jurisprudence Analyse et commentaires*, volume 1, mis à jour au 10 décembre 2008, Cowansville, Éditions Yvon Blais, 2001, p. I/1-6.

245 *Loi concernant le cadre juridique des technologies de l'information*, L.R.Q., c. C-1.1, en ligne : <http://www.canlii.org///qc/legis/loi/c-1.1/20080818/tout.html>, art. 22.

> « le seul fait d'ouvrir un fichier obtenu par courrier électronique ou par un support informatique et de procéder à le supprimer ne constitue pas un élément de possession. De même, la manipulation de fichiers en bloc pour libérer de l'espace sur un support informatique et transférer en bloc ces fichiers sur un autre support informatique ne constitue pas nécessairement une possession. Il est toujours nécessaire d'évaluer, de façon concomitante, la connaissance de l'accusé à l'égard du matériel pour lequel il y a manipulation »[246].

La même position a été suivie dans plusieurs décisions françaises[247]. Pour que l'action de détention soit consacrée, il importe donc qu'une personne fasse preuve d'une volonté de conserver des fichiers incriminants et

> « [l]a création de fichiers temporaires ne rentre donc pas dans le champ d'application de l'incrimination étant donné que l'élément intentionnel fait défaut. En effet, ces fichiers s'enregistrent de manière automatique sur l'ordinateur sans aucun acte volontaire de la part de la personne. De ce fait, les éléments constitutifs de l'infraction de détention ou de possession ne peuvent être remplis ».[248]

Enfin, en troisième lieu, la jurisprudence relative à la détention résulte de décisions relatives à des **demandes d'accès** à des documents. Ces décisions ont été rendues dans un contexte où il n'y avait pas lieu d'apporter les nuances reflétant la complexité des environnements en réseaux.

---

246 *R.* c. *Tremblay*, 2003 CanLII 30621 (QC C.Q.), référence citée par Caroline VALLET, protection des mineurs sur le réseau Internet face à la pédopornographie, thèse de Doctorat, à paraître.

247 Voir notamment les exemples jurisprudentiels dans Caroline VALLET, protection des mineurs sur le réseau Internet face à la pédopornographie, Thèse de Doctorat, à paraître. Voir notamment Étienne WÉRY, « La cour de cassation a tranché : consulter une image pédophile n'est pas la détenir », (2005) droit et technologies en ligne : <http://www.droit-technologie.org/actuality-867/la-cour-de-cassation-a-tranche-consulter-une-image-pedophile-n-est-p.html>.

248 Caroline VALLET, protection des mineurs sur le réseau Internet face à la pédopornographie, Thèse de Doctorat, à paraître.

Dans ces situations, la *Commission d'accès à l'information* (CAI) a appliqué une conception large de la notion de détention. Pour que la loi s'applique, l'organisme doit être détenteur du document dans l'exercice de ses fonctions. De la jurisprudence de la CAI, résumée par Doray et Charette, il ressort les principes suivants :

- Pour être un détenteur du document au sens de la *Loi sur l'accès*, un organisme n'a pas à être l'auteur ou le commanditaire du document. Mais s'il n'est pas l'auteur ou s'il a préparé un document pour le compte d'un autre organisme, l'article 48 peut s'appliquer et l'organisme doit référer le demandeur à un autre organisme qui est plus à même de répondre à la demande.[249]
- La propriété du document n'a pas de pertinence pour l'application de la *Loi sur l'accès*. Les documents d'un tiers effectivement détenus par un organisme public tombent sous l'application de la loi même s'ils n'appartiennent pas à l'organisme.[250]
- De même, le fait qu'un document ne soit pas officiel ou approuvé n'a pas de pertinence pour l'application de la loi.[251]
- Le fait que le document est détenu temporairement n'est pas pertinent si le document est entre les mains de l'organisme ou conservé pour lui par un tiers[252].
- « Dès que l'organisme, dans ses bureaux, dans ses classeurs, dans ses ordinateurs, dans ses archives ou par le biais de ses

---

249 Raymond DORAY et François CHARETTE, *Accès à l'information, Loi annotée, Jurisprudence Analyse et commentaires*, volume 1, mis à jour au 10 décembre 2008, Cowansville, Éditions Yvon Blais, 2001, p. I/1-4.

250 Raymond DORAY et François CHARETTE, *Accès à l'information, Loi annotée, Jurisprudence Analyse et commentaires*, volume 1, mis à jour au 10 décembre 2008, Cowansville, Éditions Yvon Blais, 2001, p. I/1-4 et I/1-17.

251 Raymond DORAY et François CHARETTE, *Accès à l'information, Loi annotée, Jurisprudence Analyse et commentaires*, volume 1, mis à jour au 10 décembre 2008, Cowansville, Éditions Yvon Blais, 2001, p. I/1-4.

252 Raymond DORAY et François CHARETTE, *Accès à l'information, Loi annotée, Jurisprudence Analyse et commentaires*, volume 1, mis à jour au 10 décembre 2008, Cowansville, Éditions Yvon Blais, 2001, p. I/1-4.

employés détient un document dans l'exercice de ses fonctions, la Loi sur l'accès s'applique à ce document. Il a même été décidé que des documents colligés ou rédigés par un employé dans le cadre de ses fonctions et que celui-ci conservait à son domicile étaient détenus par l'organisme public au sens de l'article 1. »[253]

- La détention du document doit être dans l'exercice des fonctions de l'organisme. Les fonctions englobent toutes les tâches de l'organisme, même celles qui découlent accessoirement de ses fonctions principales. (ex : documents découlant de soumission pour la location de bureaux, régie interne, administration, gestion de personnel)[254] ou celles qu'il accepte volontairement[255] mais pas les documents personnels reçus ou rédigés par les employés[256].

Compte tenu de la conception large qui est donnée à la notion de détention, il appert que dès lors qu'un document est en la possession « physique » d'un organisme public dans le cadre de l'exercice de ses fonctions, la *Loi sur l'accès* s'y applique, et ce, quelle que soit la manière dont s'organise cette possession (conservation, hébergement, garde, etc.). Lorsqu'un tel document comporte des renseignements personnels, l'organisme détenteur doit se conformer aux exigences relatives aux droits d'accès et de rectification dont dispose la personne concernée par le document.

Mais lorsqu'un organisme est simplement « possesseur » d'un document qui est sous le contrôle d'une autre entité, est-ce qu'il

---

253 Raymond DORAY et François CHARETTE, *Accès à l'information, Loi annotée, Jurisprudence Analyse et commentaires*, volume 1, mis à jour au 10 décembre 2008, Cowansville, Éditions Yvon Blais, 2001, p. I/1-4.*; Centre hospitalier régional de Lanaudière* c. *Mireault*, [1993] C.A.I. 332.

254 Raymond DORAY et François CHARETTE, *Accès à l'information, Loi annotée, Jurisprudence Analyse et commentaires*, volume 1, mis à jour au 10 décembre 2008, Cowansville, Éditions Yvon Blais, 2001, p. I/6-1.

255 *Demers c. St-Laurent (Ville de),* C.A.I. no 93 08 71, 31 mars 1994.

256 Raymond DORAY et François CHARETTE, *Accès à l'information, Loi annotée, Jurisprudence Analyse et commentaires*, volume 1, mis à jour au 10 décembre 2008, Cowansville, Éditions Yvon Blais, 2001, p. I/1-7. *Malenfant* c. *Commission de la santé et de la sécurité au travail*, [1984-86] 1 C.A.I. 177 ; *Robillard* c. *Hôpital Ste-Justine*, [1989] C.A.I. 296.

est toujours possible de considérer que l'organisme détient le document dans l'exercice de ses fonctions ? Les précédents propos établis relativement aux articles 22 et 26 de la *Loi concernant le cadre juridique des technologies de l'information*[257] nous apparaissent difficilement compatibles avec une réponse affirmative sur ce point.

Selon nous, lorsqu'un document est « détenu » – dans le sens générique du terme – par un organisme qui agit à titre d'intermédiaire pour offrir des services de conservation de documents technologiques sur un réseau de communication, l'organisme en question n'est pas responsable dudit réseau. Dans le contexte de la *Loi sur l'accès*, l'opération de détention devrait uniquement référer à une situation où un organisme en cause dispose d'un certain contrôle sur le document. Mais par contre, s'il s'avère que le document est détenu sans droit de la part de l'entité qui en a le contrôle, le second alinéa de l'article 22 de la *Loi sur le cadre juridique des technologies de l'information*[258] devient applicable. Par conséquent, l'organisme pourrait engager sa responsabilité, notamment s'il a de fait connaissance que les documents conservés ou gardés servent à la réalisation d'une activité à caractère illicite ou s'il a connaissance de circonstances qui la rendent apparente et qu'il n'agit pas promptement pour rendre l'accès aux documents en question impossible ou pour autrement empêcher la poursuite d'une telle activité.

En somme, la détention d'un document comportant des renseignements personnels est une opération issue de la *Loi sur l'accès*, ayant une consonance plutôt juridique que technique, qui doit nécessairement être qualifiée « techniquement ». Est-ce que la détention est le reflet de l'exercice effectif d'une fonction de contrôle par l'organisme détenteur à l'égard du document ou est-

---

[257] *Loi concernant le cadre juridique des technologies de l'information*, L.R.Q., c. C-1.1, en ligne : <http://www.canlii.org///qc/legis/loi/c-1.1/20080818/tout.html>, art. 22 et 26.

[258] *Loi concernant le cadre juridique des technologies de l'information*, L.R.Q., c. C-1.1, en ligne : <http://www.canlii.org///qc/legis/loi/c-1.1/20080818/tout.html>, art. 22.

ce que la détention n'est qu'à titre d'intermédiaire pour le compte d'une entité qui exerce le contrôle à l'égard du document ?

Cela dit, et comme mentionné précédemment, il est important d'avoir à l'esprit que cette conception large de la notion de détention, fruit de la jurisprudence, est à l'origine d'un cadre très particulier lié au fait qu'elle ne s'interprète que dans le cadre des demandes d'accès. Aussi, cette largesse associée à une rationalité protectrice – qui est de s'assurer, pour des fins de transparence, que les citoyens aient le plus possible accès aux documents publics – ne sera pas forcément présente dans l'hypothèse d'une finalité, par exemple, sécuritaire ou de protection des renseignements personnels. D'ailleurs, la notion de détention ne peut être isolée de celle de conservation que nous avons vu précédemment ; une notion qui, de son côté, a été passablement mieux précisée et encadrée par la *Loi concernant le cadre juridique des technologies de l'information*[259].

À titre d'illustration, nous pouvons reprendre l'exemple de l'affaire traitée par le Commissariat à la vie privée de l'Ontario, Ordonnance M – 165 du 21 juillet 1993, *Regional Municipality of Halton Police Services Board*[260], où il s'agissait de déterminer si l'accès pouvait être opéré à des notes manuscrites faites pas un fonctionnaire. La réponse fut négative de la part du commissaire qui considéra qu'il n'y avait pas un contrôle suffisant sur lesdites notes. Sur la base de ce critère, dans une pareille affaire, il serait possible de croire qu'il n'y a pas de détention sur un tel type de documents.

Aussi, et en dépit d'une analyse doctrinale et jurisprudentielle vierge, nous croyons que la détention semble devoir être analysée avec précaution dès lors que l'on tente de la considérer dans le cadre d'une interprétation documentaire et de protection des renseignements personnels.

---

[259] *Infra*, Partie 1, Chapitre 2, Section 5.

[260] Ordonnance M – 165 du 21 juillet 1993, *Regional Municipality of Halton Police Services Board*.

B – Définition et illustrations

i) Définition

La détention est un terme qui a son origine non pas dans le domaine de la gestion documentaire mais dans la *Loi sur l'accès*. Elle correspond à la situation selon laquelle un organisme est **responsable juridiquement** du support sur lequel sont consignés un ou des renseignements personnels. Le terme de détention, dans une perspective de gestion documentaire – et non de mise en application du devoir de transparence en fonction des dispositions de la *Loi sur l'accès* – doit être distingué de la possession physique que ne signifie plus grand chose dans une perspective de gestion électronique.

ii) Illustrations

Le terme « détention » est dans le cadre de nos trois illustrations ci-dessous d'une utilité pratique très limitée, dans la mesure où elle s'interprète principalement en ce qui a trait au droit d'accès prévu dans la *Loi sur l'accès*. Or, il est difficile de prévoir un accès dans le cadre de l'illustration 1, les renseignements personnels n'étant pas accessibles, sauf à l'individu intéressé. Dans l'illustration 2, même chose ; il ne peut y avoir d'accès à une personne autre que l'individu, sauf consentement de sa part. Enfin, dans le cadre de la promotion du tourisme, il ne peut y avoir d'accès relativement à des informations déjà publiques.

Illustration 1

Dans le cas du système de vérification de l'identité, nous avons pu observer que pour une simple opération de vérification d'identité, quatre intervenants sont requis : le citoyen ; le ministère qui rend le service, le « prestataire en ligne » et le ministère qui est responsable de la banque de données avec laquelle on va vérifier la véracité desdits renseignements personnels. Chacune des entités qui se trouvent en possession d'une version intelligible des documents échangés peut être considérée comme détenteur.

Illustration 2

La situation du CV Commun Canadien correspond à une situation d'hébergement. L'organisme mis en place par un consortium d'organismes de soutien à la recherche propose une infrastructure qui a pour mission de permettre aux chercheurs de placer dans un environnement les éléments de CV dont ils pourront avoir besoin pour les transmettre, lorsqu'ils le décideront à un organisme subventionnaire. Dans ce cas, l'organisme hébergeur des CV des professeurs en question ne peut être qualifié de détenteur de renseignements personnels puisqu'il n'a aucun contrôle et encore moins connaissance des renseignements hébergés.

Illustration 3

Dans le cas de sites visant à promouvoir le tourisme et qui proposent des configurations permettant aux internautes de publier en ligne leurs commentaires, leurs photos ou leurs vidéos, l'entité qui gère ce type d'environnement ne détient les renseignements qui sont ainsi hébergés qu'à titre d'intermédiaire « pour offrir des services de conservation de documents technologiques sur un réseau de communication » au sens de l'article 22 de la *Loi concernant le cadre juridique des technologies de l'information*. L'entité en question exerce la détention physique des documents mais elle n'est pas obligée de surveiller activement les documents ainsi publiés. Et comme les documents sont par définition publiés, la question du droit d'y accéder ne se pose pas.

SECTION 3 – UTILISATION DE RP

1 – Mise en contexte

Le terme « utilisation » d'un renseignement personnel ou d'un document pose problème pour plusieurs raisons. En premier lieu, il s'agit d'une opération qui est évoquée à de nombreuses reprises dans les lois sur la protection des renseignements personnels[261],

[261] Voir notamment les articles 41.2, 55, 59, 63.1, 65.1 (qui est le plus général), 67.2, 67.3, 70.1, 72, 73, 80, 125, 127, 166 de la *Loi sur l'Accès aux docu-*

sans que l'on ne sache vraiment à quoi elle correspond. En effet, en deuxième lieu, le terme est vague et susceptible d'être utilisé très largement, et dans plusieurs sens. Aussi, la moindre « utilisation » pourrait impliquer l'application de l'ensemble des dispositions de la loi. Ce terme est à cet égard comparable à celui de « traitement » que l'on retrouve dans la *Directive européenne* qui, lui aussi, se veut très inclusif[262].

Dans la *Loi sur l'accès*, le mot utilisation est employé au regard des finalités. Ainsi, l'article 65.1 de la *Loi sur l'accès* dispose que :

---

ments des organismes publics et sur la protection des renseignements personnels, L.R.Q., c. A-2.1, 2006, c. 22. en ligne : <http://canlii.org/fr/qc/legis/lois/lrq-c-a-2.1/derniere/lrq-c-a-2.1.html>, et les articles 9, 19, 35, 44, 45, 46, 48, 52, 57, et 64 de la *Loi concernant le cadre des technologies de l'information*, L.R.Q., c. C-1.1, en ligne : <http://www.canlii.org///qc/legis/loi/c-1.1/20080818/tout.html>, et les articles 1, 8, 10, 11, 12, 13, 14, 17, 18, 21, 21.1, 22, 23, 25, 26, 81, 83, 91 et 97 de la *Loi sur la Protection des renseignements personnels dans le secteur privé,* L.R.Q., c. P-39.1, en ligne : <http://www.canlii.org/fr/qc/legis/lois/lrq-c-p-39.1/derniere/lrq-c-p-39.1.html> et en ce qui concerne, au niveau fédéral, de la *Loi sur la protection des renseignements personnels et les documents électroniques* (PIPEDA), en ligne : <http://www.canlii.ca/fr/ca/legis/lois/lc-2000-c-5/derniere/lc-2000-c-5.html>, le préambule de la Loi, et les articles 3, 4, 5, 7, 23, 25, 26, 30, 50 de la loi proprement dit et les articles 4.2.4, 4.2.6, 4.3, 4.3.1, 4.3.2, 4.3.3, 4.3.7, 4.5, 4.6.1, 4.7.1, 4.9.2 de l'Annexe 1 de la même loi.

262 Directive, 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, J.O. 23 nov. 1995, en ligne : : <http://www.internet-observatory.be/internet_observatory/pdf/legislation/dir_1995-10-24_fr.pdf>, et qui prévoit à l'article 2 b) : « « traitement de données à caractère personnel » (traitement) : toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, **l'utilisation**, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction ; » (nos soulignements)

« **65.1**. Un renseignement personnel ne peut être utilisé au sein d'un organisme public **qu'aux fins pour lesquelles il a été recueilli.**

L'organisme public peut toutefois utiliser un tel renseignement à une autre fin avec le consentement de la personne concernée ou, sans son consentement, 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.

Pour qu'une fin soit compatible au sens du paragraphe 1° du deuxième alinéa, il doit y avoir un **lien pertinent et direct avec les fins pour lesquelles le renseignement a été recueilli.**

Lorsqu'un renseignement est utilisé dans l'un des cas visés aux paragraphes 1° à 3° du deuxième alinéa, le responsable de la protection des renseignements personnels au sein de l'organisme doit inscrire l'utilisation dans le registre prévu à l'article 67.3. [263] » (Nos soulignements)

Il y va de même en ce qui concerne les articles 5(3), et 7(4) de la *Loi sur la protection des renseignements personnels et les documents électroniques* (PIPEDA), et les articles 4.2.4 et 4.5 de son Annexe 1 qui disposent :

« **5.(3)** (de PIPEDA) : L'organisation ne peut recueillir, **utiliser** ou communiquer des renseignements personnels **qu'à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances**. »

« **7.(4)** (de PIPEDA) : Malgré l'article 4.5 de l'annexe 1, l'organisation peut, dans les cas visés au paragraphe (2), **utiliser** un

[263] Art. 65.1 de la *Loi sur l'Accès aux documents des organismes publics et sur la protection des renseignements personnels*, L.R.Q., c. A-2.1, 2006, c. 22, en ligne : <http://canlii.org/fr/qc/legis/lois/lrq-c-a-2.1/derniere/lrq-c-a-2.1.html>.

renseignement personnel **à des fins autres que celles auxquelles il a été recueilli.** [264] »

« **4.2.4** (de l'Annexe 1 de PIPEDA) : Avant de se servir de renseignements personnels à des fins non précisées antérieurement, **les nouvelles fins doivent être précisées avant l'utilisation**. À moins que les nouvelles fins auxquelles les renseignements sont destinés ne soient prévues par une loi, il faut obtenir le consentement de la personne concernée avant **d'utiliser les renseignements à cette nouvelle fin**. Pour obtenir plus de précisions sur le consentement, se reporter au principe du consentement (article 4.3). »

« **4.5** (de l'Annexe 1 de PIPEDA) : Les renseignements personnels ne doivent pas être **utilisés** ou communiqués **à des fins autres que celles auxquelles ils ont été recueillis** à moins que la personne concernée n'y consente ou que la loi ne l'exige. On ne doit conserver les renseignements personnels qu'aussi longtemps que nécessaire pour la réalisation des fins déterminées[265]. (Nos soulignements)

L'utilisation est liée aux finalités de la collecte, donc à des « fins compatibles » comme dirait le texte de l'article 65.1. de la *Loi sur l'accès*[266] Il s'agit d'un critère objectif. Selon Doray et Charrette, il faut que les renseignements personnels soient utilisés à des fins compatibles avec celles pour lesquelles ils ont été recueillis, et il faut être en mesure de démontrer un lien pertinent et direct avec les fins pour lesquelles les renseignements ont été recueillis :

---

[264] Art. 5.(3) et 7.(4) de la *Loi sur la protection des renseignements personnels et les documents électroniques* (PIPEDA), en ligne : <http://www.canlii.ca/fr/ca/legis/lois/lc-2000-c-5/derniere/lc-2000-c-5.html>.

[265] Art. 4.2.4 et 4.5 de l'annexe 1 de la *Loi sur la protection des renseignements personnels et les documents électroniques* (PIPEDA), en ligne : <http://www.canlii.ca/fr/ca/legis/lois/lc-2000-c-5/derniere/lc-2000-c-5.html>.

[266] Art. 65.1 de la *Loi sur l'Accès aux documents des organismes publics et sur la protection des renseignements personnels*, L.R.Q., c. A-2.1, 2006, c. 22, en ligne : <http://canlii.org/fr/qc/legis/lois/lrq-c-a-2.1/derniere/lrq-c-a-2.1.html>.

> « est-ce qu'une personne raisonnable jugerait qu'il y a un lien pertinent logique et prévisible (lien direct) entre l'usage primaire et l'usage secondaire ».[267]

L'article 55 2e alinéa de la *Loi sur l'accès*[268] traite également de l'hypothèse de l'utilisation « illégitime » de renseignements personnels à caractère public. Il énonce que :

> « Un renseignement personnel qui a un caractère public en vertu de la loi n'est pas soumis aux règles de protection des renseignements personnels prévues par le présent chapitre. Cependant, un organisme public qui détient un fichier de tels renseignements peut en refuser l'accès, en tout ou en partie, ou n'en permettre que la consultation sur place si le responsable a des motifs raisonnables de croire que les renseignements seront **utilisés à des fins illégitimes**. » (Nos soulignements)

De son côté, l'article 11 de la Loi sur la protection des renseignements dans le secteur privé (LPRPSP)[269] prévoit que :

> « Toute personne qui exploite une entreprise doit veiller à ce que les dossiers qu'elle détient sur autrui soient à jour et exacts au moment où elle les utilise pour prendre une décision relative à la personne concernée. »

Le même principe est énoncé à l'article 72 de la *Loi sur l'accès*[270] :

> « Un organisme public doit veiller à ce que les renseignements personnels qu'il conserve soient à jour, exacts et complets pour servir aux fins pour lesquelles ils sont recueillis ou **utilisés**. »

---

267 Raymond DORAY et François CHARRETTE, *Accès à l'information*, vol. 1, Cowansville, Éditions Yvon Blais, 2008.

268 Art. 55 al.2 de la *Loi sur l'Accès aux documents des organismes publics et sur la protection des renseignements personnels*, L.R.Q., c. A-2.1, 2006, c. 22, en ligne : <http://canlii.org/fr/qc/legis/lois/lrq-c-a-2.1/derniere/lrq-c-a-2.1.html>.

269 Art. 11 de la *Loi sur la Protection des renseignements personnels dans le secteur privé*, L.R.Q., c. P-39.1, en ligne : <http://canlii.ca/fr/qc/legis/lois/lrq-c-p-39.1/derniere/lrq-c-p-39.1.html>.

270 Art. 72 de la *Loi sur l'Accès aux documents des organismes publics et sur la protection des renseignements personnels*, L.R.Q., c. A-2.1, 2006, c. 22, en ligne : <http://canlii.org/fr/qc/legis/lois/lrq-c-a-2.1/derniere/lrq-c-a-2.1.html>.

Il y va de même aussi dans les articles 4.6 à 4.6.3 de l'Annexe 1 de la *Loi sur la protection des renseignements personnels et les documents électroniques* (PIPEDA) qui disposent :

> « **4.6 Sixième principe — Exactitude**
>
> Les renseignements personnels doivent être aussi exacts, complets et à jour que l'exigent les fins auxquelles ils sont destinés. » (Nos soulignements)
>
> « **4.6.1** Le degré d'exactitude et de mise à jour ainsi que le caractère complet des renseignements personnels dépendront de l'usage auquel ils sont destinés, compte tenu des intérêts de la personne. Les renseignements doivent être suffisamment exacts, complets et à jour pour réduire au minimum la possibilité que des renseignements inappropriés soient **utilisés** pour prendre une décision à son sujet. » (Nos soulignements)
>
> « **4.6.2** Une organisation ne doit pas systématiquement mettre à jour les renseignements personnels à moins que cela ne soit nécessaire pour atteindre les fins auxquelles ils ont été recueillis. » (Nos soulignements)
>
> « **4.6.3** Les renseignements personnels qui servent en permanence, y compris les renseignements qui sont communiqués à des tiers, devraient normalement être exacts et à jour à moins que des limites se rapportant à l'exactitude de ces renseignements ne soient clairement établies. »[271] (Nos soulignements)

Cette obligation de mise à jour ne s'applique que lorsque l'organisme est appelé à **utiliser** les renseignements et si un renseignement est devenu semi-actif ou inactif, l'organisme n'aura pas l'obligation d'en assurer la mise à jour ni à veiller à ce qu'il soit exact et complet en tout temps[272], à moins que cela ne soit nécessaire aux fins pour lesquelles le renseignement a été collecté,

---

[271] Art. 4.6 à 4.6.3 de l'annexe 1 de la *Loi sur la protection des renseignements personnels et les documents électroniques* (PIPEDA), en ligne : <http://www.canlii.ca/fr/ca/legis/lois/lc-2000-c-5/derniere/lc-2000-c-5.html>.

[272] Raymond DORAY et François CHARRETTE, *Accès à l'information*, vol. 1, Cowansville, Éditions Yvon Blais, 2008, III/72-1.

comme le confirme l'article 4.6.2 de l'Annexe 1 de la *Loi sur la protection des renseignements personnels et les documents électroniques* (PIPEDA)[273].

En dépit de la généralité du terme, il n'y a pas de raison de l'interpréter de manière différente de la façon utilisée pour les précédents termes. Ainsi, pour utiliser des renseignements personnels, il faudra généralement en avoir connaissance. Il faut donc que ceux-ci nous aient été communiqués en tout ou en partie. L'on fait usage d'information afin de décider. Soit que l'on doit disposer d'un certain degré de certitude ou que l'on a besoin d'établir des faits qui donnent ouverture à une décision.

Il y a forcément un rapport entre l'utilisation et la finalité. La plupart des dispositions législatives et des décisions qui se prononcent à l'égard de l'utilisation de renseignements personnels visent à déterminer si l'utilisation est pour une finalité conforme ou compatible avec celles en vertu desquelles le renseignement a été recueilli.

2 – Définition et illustrations

A – Définition

Utiliser des renseignements personnels implique d'en avoir connaissance et de décider d'agir ou non à la lumière de la connaissance que ces renseignements confèrent.

B – Illustrations

Illustration 1

En ce qui a trait au système de vérification de l'identité, seule l'entité à laquelle il est fait recours afin de vérifier les renseignements soumis avec ceux qu'ils possèdent déjà, utilise les renseignements.

---

[273] Art. 4.6.2 de l'annexe 1 de la *Loi sur la protection des renseignements personnels et les documents électroniques* (PIPEDA), en ligne : <http://www.canlii.ca/fr/ca/legis/lois/lc-2000-c-5/derniere/lc-2000-c-5.html>.

Illustration 2

Dans le CV Commun Canadien[274], l'utilisation des documents déposés par les chercheurs qui se prévalent de ce service fait nécessairement suite à une décision de chaque personne ayant consigné des renseignements dans le système de CV Commun Canadien. Il s'agit d'une situation d'hébergement. L'entité qui administre le CV Commun Canadien n'utilise pas les documents ou renseignements consignés.

Illustration 3

L'entité qui gère les sites visant à promouvoir le tourisme et qui proposent des configurations permettant aux internautes de publier en ligne leurs commentaires, leurs photos ou leurs vidéos, est le type d'environnement qui a le devoir de conserver les documents en conformité avec les conditions de fonctionnement du site. Cependant, elle n'utilise pas les documents et renseignements. Ceux-ci sont placés par les usagers dans le site pour le bénéfice des autres usagers et du public en général. Plus exactement, il pourrait y avoir éventuellement une utilisation à la suite, par exemple, d'une plainte, ce qui ferait en sorte que le prestataire aurait une connaissance effective d'un document en cause et par le fait même en obtiendrait le contrôle. Mais dans le cours normal d'un document déposé par autrui, ce ne serait pas le cas. De la même manière, on pourrait imaginer une utilisation dans l'hypothèse non pas d'un simple « filtrage » mais dans celle d'un véritable contrôle éditorial quant au contenu même des documents mis en ligne.

CONCLUSION

L'analyse des diverses étapes du cycle de traitement d'un document au sein d'un réseau fait ressortir l'intérêt de distinguer entre les différentes opérations susceptibles de survenir lors du cycle de vie des documents technologiques. L'analogie avec le

---

274 Le CV Commun Canadien est disponbible en ligne : <http://www.commoncv.net/index_f.html>.

monde physique vient ici éclairer les enjeux : lorsqu'un postier livre une lettre, il n'a pas le droit d'accès au contenu de celle-ci. Il dispose toutefois de la possibilité technique d'y accéder. C'est une interdiction provenant d'une règle de droit qui l'empêche de faire usage des possibilités techniques qui sont à sa disposition pour accéder au document.

Comme le droit d'accès à un document découle de la loi, lorsque la possibilité technique d'accès à un document existe, il faut des mécanismes techniques de sécurité afin de réserver aux seules personnes y ayant le droit, l'accès au document. Le droit doit également organiser le régime de sanction pour des accès non autorisés par ceux qui en ont les possibilités techniques.

Or, et au-delà de ces analogies qui militent vers une interprétation teintée de « bon sens », il importe d'analyser derrière les simples critères qui ont été identifiés dans les lois sur la protection des renseignements personnels, à une autre époque, sous un autre support, la « substantielle moelle » qui a construit ce droit, somme toute assez neuf. C'est dans cette optique que nous avons mis de l'avant la notion de contrôle comme élément fondateur derrière ce domaine du droit protecteur. Une notion qui transcende les lois en matière de protection des renseignements personnels tout en étant parfaitement cohérente avec les lois applicables en matière de gestion documentaire. La notion de contrôle permet de faire la paix entre deux domaines du droit qui n'ont pas exactement la même finalité.

D'ailleurs, c'est précisément l'exercice effectué par la Cour suprême dans la toute récente affaire *R.* c. *Patrick*[275], en déclarant que les poubelles ne sont pas assujetties à une protection sur la base des lois sur la vie privée[276]. Pour arriver à cette solution, les juges, à l'unanimité moins une voix, ont tous mis de l'avant, à plusieurs reprises dans l'arrêt, que l'absence de la protection est directement tributaire de l'absence de **contrôle** de la part de l'in-

---

275 *R.* c. *Patrick*, 2009 CSC 1, en ligne : <http://csc.lexum.umontreal.ca/fr/2009/2009csc17/2009csc17.html>.

276 *Supra*, Partie 1, Chapitre 1, Section préliminaire s'intitulant « Notion de contrôle : le caractère implicite de la protection des RP ».

téressé. Ainsi, en dépit de l'absence du terme en tant que tel, ni dans la *Loi sur l'accès*[277], ni dans *Loi sur la Protection des renseignements personnels dans le secteur privé*[278], ni dans la *Loi sur la protection des renseignements personnels et les documents électroniques* (PIPEDA)[279] (hormis le contrôle de l'application du droit qui est différent du contrôle qui nous intéresse et qui est celui qu'on a sur un renseignement ou un document) ni dans la *Loi concernant le cadre juridique des technologies de l'information,*[280] il nous apparaît clair que ce concept phare, comme dans la situation nouvelle traitée par la Cour suprême, sera d'une utilité incontournable dès lors que les lois sur la protection des renseignements personnels doivent être interprétées dans un contexte électronique nouveau, comme celui du web 2.0.

---

277 *Loi sur l'Accès aux documents des organismes publics et sur la protection des renseignements personnels*, L.R.Q., c. A-2.1, 2006, c. 22, en ligne : <http://canlii.org/fr/qc/legis/lois/lrq-c-a-2.1/derniere/lrq-c-a-2.1.html>.

278 *Loi sur la Protection des renseignements personnels dans le secteur privé*, L.R.Q., c. P-39.1, en ligne : <http://canlii.ca/fr/qc/legis/lois/lrq-c-p-39.1/derniere/lrq-c-p-39.1.html>.

279 *Loi sur la protection des renseignements personnels et les documents électroniques* (PIPEDA), en ligne : <http://www.canlii.ca/fr/ca/legis/lois/lc-2000-c-5/derniere/lc-2000-c-5.html>.

280 *Loi concernant le cadre juridique des technologies de l'information*. L.R.Q., c. C-1.1, en ligne : <http://www.canlii.org///qc/legis/loi/c-1.1/20080818/tout.html, À l'exception de l'article 25>.

Partie 2

Souplesse des lois sur la protection des RP face à leur circulation

Face aux accroissements considérables de la possibilité de circulation de renseignements personnels aux fins d'offrir des prestations en ligne aux citoyens, le cadre législatif de la gestion des renseignements personnels comporte divers mécanismes permettant d'assouplir et de mieux adapter les protections là ou cela compte vraiment. Une série de dispositions, d'autorisations – que certains appellent exceptions[281] – à la circulation ont été introduites, soit initialement soit tout récemment[282], pour s'assurer que les ministères et organismes puissent « user » (terme volontairement large et distinct de ceux déjà utilisés et définis plus tôt dans la Partie 1) des renseignements en tout respect du droit. Et au-delà du principe « quasi-biblique » du « tu ne circuleras point ! »[283], les lois offrent une grande diversité de mesures afin de s'adapter à la réalité parfois capricieuse de la mise en application des projets concrets de prestations en ligne.

Cela dit, et en dépit de la grande diversité de ces dispositions, cela ne veut pas dire qu'elles constituent la solution idéale à la situation des prestations en ligne. Bien au contraire. En bien des cas, les solutions offertes présentent plus de difficultés que d'avantages, et nous opèrerons ici une analyse sur les dangers présentés par chacune d'elles. Aussi, en premier lieu, nous envisagerons la mesure maîtresse qu'est le consentement dont la flexibilité fait oublier qu'il constitue à la fois un irritant dans les processus de navigation des internautes, d'autant qu'il est en bien de situations, utilisé à tort et à travers (Chapitre 1). Ensuite, nous énumérerons d'autres autorisations plus ponctuelles qui

---

281 Nous avons décidé de ne pas évoquer le terme « exception » mais plutôt « autorisation » à la circulation, et ce, pour deux raisons. D'une part, ces « exceptions » ne sont pas exceptionnelles, bien au contraire, mais plutôt nombreuses et de différentes formes. D'autre part, et en conformité avec le terme de circulation défini dans la Partie préliminaire, la protection des renseignements personnels a toujours intégré cette circulation de l'information. Le mouvement de l'information n'est donc pas antinomique avec la protection.

282 Et notamment les changements qui sont apparus dans l'amendement de la *Loi sur l'accès* en 2006.

283 *Supra*, Partie préliminaire.

sont également susceptibles de s'appliquer à la situation des prestations en ligne (Chapitre 2).

CHAPITRE 1
CONSENTEMENT COMME SÉSAME UTILISABLE À LA CIRCULATION DES RP

Le consentement constitue le sésame, le laissez-passer, que les gestionnaires de renseignements personnels peuvent utiliser pour faire en toute légalité ce qui serait autrement interdit. Un outil d'une grande souplesse dont les lois sur la protection des renseignements personnels usent et abusent systématiquement tant elles considèrent que c'est le moyen idéal pour permettre la circulation des données (Section préliminaire). Pourtant, la réalité est moins rose dès lors qu'on applique cette technique juridique aux environnements électroniques et nous croyons qu'en certains cas elle peut être jugée soit inutile (Section 2) et malheureusement, en d'autres, carrément nuisible (Section 1) au regard de son objectif initial, à savoir, la protection du citoyen.

SECTION PRÉLIMINAIRE – Autorisation de circulation par le consentement

Ce consentement, qu'en est-il ? Avant d'étudier la particularité électronique quant à l'utilisation du consentement, il nous apparaît important d'abord de faire le constat selon lequel tout est mis en place dans les lois pour que cette façon de faire soit adoubée par le droit et dans les faits très souvent utilisée par les gestionnaires (1). Aussi, il nous apparaît également crucial de remettre l'accent sur les raisons fondamentales qui sont derrière cette autorisation, et ce, notamment, afin de vérifier si elles sont satisfaites (2).

1 – Usage facilité du consentement

Dans les lois relatives à la protection des renseignements personnels, le consentement est un principe fondamental bénéficiant d'une certaine flexibilité (A) et dont les hypothèses d'application (B) sont passablement nombreuses.

A – Flexibilité du consentement

Dans l'immense majorité des lois visant à assurer la protection des renseignements personnels, le consentement est partout. Une fréquence d'ailleurs qui ne semblait pas forcément de mise dans les tous premiers textes internationaux évoquant la protection des renseignements personnels[284]. Ainsi, il est clairement établi qu'aucune « circulation » ne peut être faite – que ce soit sous l'appellation de « communication », « collecte », « utilisation », etc. – sans que l'individu concerné n'ait consenti à cette opération[285].

Pourtant, il existe, comme dans tout consentement, des limites qui portent tant sur certains éléments de forme que de fond.

Relativement, en premier lieu, à la forme, il est déjà un constat qui nous apparaît important de signaler, selon lequel les différentes lois sur la protection des renseignements personnels n'établissent pas les mêmes exigences sur ce point. Ainsi, notons d'abord que l'article 59 de la *Loi sur l'Accès aux documents des organismes publics et sur la protection des renseignements personnels*[286], dispose d'une manière générale qu'

> « Un organisme public ne peut communiquer un renseignement personnel sans le consentement de la personne concernée. »

Ce principe de droit québécois est repris au fédéral par l'article 7(3) de l'Annexe 1 de la Loi sur la protection des *renseignements personnels et les documents électroniques* (PIPEDA) qui dispose :

---

284 Voir par exemple CONSEIL DE L'EUROPE, *Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel*, Strasbourg, 28 janvier 1981, où la notion de consentement semble absente.

285 *Infra*, par. B.

286 Art. 59 de la *Loi sur l'Accès aux documents des organismes publics et sur la protection des renseignements personnels*, L.R.Q., c. A-2.1, 2006, c. 22, en ligne : <http://canlii.org/fr/qc/legis/lois/lrq-c-a-2.1/derniere/lrq-c-a-2.1.html>.

> **7. (3)** Pour l'application de l'article 4.3 de l'annexe 1 et malgré la note afférente, l'organisation ne peut communiquer de renseignement personnel à l'insu de l'intéressé et sans son consentement que dans les cas suivants : (…)[287]

Un principe d'autant plus important qu'il ne bénéficie pas dans cette loi, comme d'ailleurs dans la *Loi sur le Ministère du revenu*[288], de la précision et de la force que la *Loi sur la Protection des renseignements personnels dans le secteur privé*[289] lui donne dans son article 14 :

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

Ainsi, cette obligation de bien s'assurer que le consentement soit clairement exprimé semble plus appuyée pour les institutions assujetties à la loi applicable dans le secteur privé que pour les ministères et organismes. C'est aussi vrai quant à sa manifestation, à ses conséquences que quant à sa durée. Néanmoins, relativement à cette exigence de forme, nous devons constater que des limites doivent être ajoutées à ce premier constat. En effet, la jurisprudence semble interpréter, en dépit de cette distinction de

---

287 Art. 7.(3) de la *Loi sur la protection des renseignements personnels et les documents électroniques* (PIPEDA), en ligne : <http://www.canlii.ca/fr/ca/legis/lois/lc-2000-c-5/derniere/lc-2000-c-5.html>.

288 Article 69 alinéa 1 de la *Loi sur le Ministère du revenu*, L.R.Q., c. M-31, en ligne : <http://www.canlii.ca/qc/legis/loi/m-31/20080818/tout.html> : « Le dossier fiscal d'une personne est confidentiel et tout renseignement qu'il contient ne peut être utilisé ou communiqué à moins que cette personne **n'y consente** ou que cette utilisation ou communication ne soit effectuée conformément à la présente loi. » (nos soulignements)

289 Art. 14 de *Loi sur la Protection des renseignements personnels dans le secteur privé*, L.R.Q., c. P-39.1, en ligne : <http://canlii.ca/fr/qc/legis/lois/lrq-c-p-39.1/derniere/lrq-c-p-39.1.html>.

la lettre de la loi, les trois articles à savoir l'article 59 *de la Loi sur l'Accès*[290] et l'article 7(3) de la PIPEDA[291] d'une part et l'article 14 de la *Loi sur la Protection des renseignements personnels dans le secteur privé*[292], de la même manière[293], et ce de façon équivalente à ce qui semble se faire en Europe[294]. La *Commission d'accès à l'information* l'a d'ailleurs précisé dans sa politique intitulée *Le consentement des personnes à la communication de renseignements nominatifs les concernant*, adoptée le 6 mars 1985[295].

---

[290] Art. 59 de la *Loi sur l'Accès aux documents des organismes publics et sur la protection des renseignements personnels*, L.R.Q., c. A-2.1, 2006, c. 22, en ligne : <http://canlii.org/fr/qc/legis/lois/lrq-c-a-2.1/derniere/lrq-c-a-2.1.html>.

[291] Art. 7.(3) de la *Loi sur la protection des renseignements personnels et les documents électroniques* (PIPEDA), en ligne : <http://www.canlii.ca/fr/ca/legis/lois/lc-2000-c-5/derniere/lc-2000-c-5.html>.

[292] Art. 14 de *Loi sur la Protection des renseignements personnels dans le secteur privé*, L.R.Q., c. P-39.1, en ligne : <http://canlii.ca/fr/qc/legis/lois/lrq-c-p-39.1/derniere/lrq-c-p-39.1.html>.

[293] Raymond DORAY et François CHARETTE, *Accès à l'information*, vol. 1, Cowansville, Éditions Yvon Blais, p. III/53-5 : « Il faut noter à ce sujet que contrairement à l'article 14 de la Loi sur la protection des renseignements personnels dans le secteur privé, L.R.Q., c. P-39.1, qui précise que le consentement à la communication de renseignements personnels doit être « manifeste, éclairé et donné à des fins spécifiques » et que ce consentement « ne vaut que pour la durée nécessaire à la réalisation des fins pour lesquelles il a été demandé », La Loi sur l'accès ne contient pas de telles exigences. Néanmoins, on constate que la jurisprudence de la Commission, postérieure à 1994, applique maintenant ces règles tant dans le secteur privé que dans le secteur public. »

[294] En conformité avec l'article 2h) de la Directive, 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, J.O. 23 nov. 1995, et qui prévoit : « h) « consentement de la personne concernée » : toute manifestation de volonté, libre, spécifique et informée par laquelle la personne concernée accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement. »

[295] Dans cette politique datant de 1985, la C.A.I. excluait la notion de consentement présumé ou tacite. Ces types de consentement supposent un arbitraire, soit l'interprétation d'une personne sur le comportement d'une autre personne, ne permettant pas la consultation directe de la personne concernée. Elle jugeait acceptable le consentement implicite, étant donné qu'il est « virtuellement contenu sans être personnellement exprimé » (Dictionnaire Robert).

C'est ainsi, qu'exigeant d'abord un consentement par écrit ou en personne, la *Commission d'accès à l'information* est devenue par la suite plus souple en reconnaissant un consentement verbal, tacite ou implicite et même indirect selon les circonstances[296].

Sur le plan du fond ensuite, nous devons ajouter que ce consentement ne peut être utilisable en toutes circonstances et qu'il y a des éléments qui ne peuvent être consentis[297]. Cela fut par exemple jugé tout récemment en France où une politique de vie privée d'un site commercial fut jugée trop vague quant à la finalité du traitement des renseignements personnels et donc la clause contractuelle en cause fut par ce fait même jugée comme inapplicable au consommateur[298]. Bien que s'appliquant à un organisme privé, un même argument pourrait être utilisé contre un organisme du secteur public.

Cela dit, et en dépit de ces limitations d'utilisation, le consentement constitue un moyen de contournement simple et facile d'emploi pour les ministères et organismes qui cherchent à l'appliquer dans un grand nombre de situations.

B – Nombreuses hypothèses d'utilisation du consentement

Face à cette simplicité d'utilisation, il n'est pas étonnant de constater que les hypothèses où son emploi est expressément autorisé dans les lois visant à la protection des renseignements personnels sont pour le moins nombreuses.

---

296 Raymond DORAY et François CHARETTE, *Accès à l'information*, vol. 1, Cowansville, Éditions Yvon Blais Inc., p. III/53-4.

297 Voir tout le débat relatif à la capacité pour un ministère et organisme d'écarter un autre principe dès lors qu'un consentement est octroyé par l'individu concerné. À cet égard, relativement à la LPRPSP, voir *Ville de Laval* c. *X.*, [2003] IIJCAN 44085 (CQ), en ligne : http ://www.canlii.org/fr/qc/qccq/doc/2003/2003canlii44085/2003canlii44085.html.

298 Tribunal de grande instance de Paris 1ère chambre, section sociale Jugement du 28 octobre 2008, en ligne : <http://www.legalis.net/jurisprudence-decision.php3 ?id_article=2473>.

Ainsi, et relativement aux hypothèses qui nous intéressent[299], il est possible de vérifier que le consentement est utilisable dans quatre grandes catégories principales de situations.

En premier lieu, le consentement peut être donné par l'intéressé afin qu'une communication entre deux organisations puisse être faite, et ce, que ce soit dans des articles évoquant cette autorisation de façon générale[300] ou d'autres traitant davantage de situations particulières[301]. Les limites apportées à cette opération

---

299 Il est en effet des hypothèses où le consentement peut être utilisé pour des fins spécifiques (comme par exemple la recherche, etc.), ce qui nous intéresse moindrement ici.

300 Art. 59 de la *Loi sur l'Accès aux documents des organismes publics et sur la protection des renseignements personnels*, L.R.Q., c. A-2.1, 2006, c. 22, en ligne : <http://canlii.org/fr/qc/legis/lois/lrq-c-a-2.1/derniere/lrq-c-a-2.1.html> ; art. 13 et 15 de la *Loi sur la Protection des renseignements personnels dans le secteur privé,* L.R.Q., c. P-39.1, en ligne : <http://www.canlii.org/fr/qc/legis/lois/lrq-c-p-39.1/derniere/lrq-c-p-39.1.html> ; et au niveau fédéral, art. 7(3) de la *Loi sur la protection des renseignements personnels et les documents électroniques* (PIPEDA), en ligne : <http://www.canlii.ca/fr/ca/legis/lois/lc-2000-c-5/derniere/lc-2000-c-5.html>.

301 Comme par exemple les articles 23 (sur les secrets industriels), 24 (sur l'entrave potentielle à la négociation en vue de la conclusion d'un contrat), 59.1 (sur la prévention d'actes de violence), 61 (entre corps de police), 62 (aux personnes qui ont qualité pour recevoir lesdits renseignements personnels), 66 (d'un renseignement personnel que l'organisme possède déjà), 67 (pour l'application des lois), 67.1 (pour l'application d'une convention collective), 67.2 (pour l'application d'un mandat – voir *infra*, Partie 2, Chapitre 2, Section 2), 68 (en vertu de l'application d'une entente et notamment lorsque la communication donne lieu à la mise en place d'un service manifestement au bénéfice de l'intéressé), 68.1 (dans l'hypothèse d'un couplage de données) de la *Loi sur l'Accès aux documents des organismes publics et sur la protection des renseignements personnels*, L.R.Q.,, c. A-2.1, 2006, c. 22, en ligne : <http://canlii.org/fr/qc/legis/lois/lrq-c-a-2.1/derniere/lrq-c-a-2.1.html>. Les mêmes types d'autorisation existent dans la *Loi sur la Protection des renseignements personnels dans le secteur privé,* L.R.Q., c. P-39.1, en ligne : <http://www.canlii.org/fr/qc/legis/lois/lrq-c-p-39.1/derniere/lrq-c-p-39.1.html> et notamment les articles 18 (qui dispose sur une série d'autorisation précises telles qu'une communication à son procureur, dans une situation d'urgence, nécessaire à l'obtention d'une créance, à la prévention d'un crime, etc.), 18.1 (pour la prévention d'actes de violence), 18.2 (pour des fins d'archives), 21 (pour des fins de recherche), 21.1

sont sans aucun doute celles qui requièrent le plus d'encadrement législatif, et ce, que le consentement soit considéré comme un acte nécessaire à la circulation des renseignements personnels ou au contraire, comme un acte que la loi dispense d'être produit dans la gestion de ces derniers. En tout état de cause, le consentement y est assurément vu comme la pierre angulaire de la protection des renseignements personnels.

En deuxième lieu, il en va de même pour leur utilisation pour une autre finalité que pour laquelle la collecte fut faite. Ainsi, les détenteurs de renseignements personnels vont devoir demander à l'individu en cause son consentement si les données requises pour une fin doivent être utilisées pour une autre[302].

En troisième lieu, et conformément à ce que nous avons vu précédemment, le consentement peut aussi être envisagé pour disqualifier la nature même du renseignement personnel ou plus précisément, son caractère confidentiel[303].

(relative à la communication d'informations relatives aux activités professionnelles de certains ordres), 22 (pour des fins de prospection commerciale ou philanthropique), 40 (interdiction de divulguer sauf exception des renseignements personnels), etc. et au niveau fédéral, les art. 7(2), 7(3) et 7(4) de la *Loi sur la protection des renseignements personnels et les documents électroniques* (PIPEDA) et les art. 4.1.3 et 4.5 de son Annexe 1, en ligne : <http://www.canlii.ca/fr/ca/legis/lois/lc-2000-c-5/derniere/lc-2000-c-5.html>. Plusieurs de ces exceptions à l'exigence du consentement doivent s'exécuter avec l'accord de la *Commission d'accès à l'information*.

302 Art. 65.1 de la *Loi sur l'Accès aux documents des organismes publics et sur la protection des renseignements personnels*, L.R.Q., c. A-2.1, 2006, c. 22, en ligne : <http://canlii.org/fr/qc/legis/lois/lrq-c-a-2.1/derniere/lrq-c-a-2.1.html> ; art. 12 et 13 de la *Loi sur la Protection des renseignements personnels dans le secteur privé,* L.R.Q., c. P-39.1, en ligne : <http://www.canlii.org/fr/qc/legis/lois/lrq-c-p-39.1/derniere/lrq-c-p-39.1.html> et au niveau fédéral, l'art. 7(3) de la *Loi sur la protection des renseignements personnels et les documents électroniques* (PIPEDA) et l'art. 4.5 de son Annexe 1 en ligne : <http://www.canlii.ca/fr/ca/legis/lois/lc-2000-c-5/derniere/lc-2000-c-5.html>.

303 Art. 53 de la *Loi sur l'Accès aux documents des organismes publics et sur la protection des renseignements personnels*, L.R.Q., c. A-2.1, 2006, c. 22, en ligne : <http://canlii.org/fr/qc/legis/lois/lrq-c-a-2.1/derniere/lrq-c-a-2.1.html>, et au niveau fédéral, l'art. 4.7.4 de l'Annexe 1 de la *Loi sur la protection des renseignements personnels et les documents électroniques* (PIPEDA) et en

Enfin, et dans le cadre d'une rubrique quelque peu « fourre-tout », il nous semble important de citer aussi des hypothèses plus ponctuelles selon lesquelles le consentement est requis – ou au contraire pas nécessaire – afin que la circulation des renseignements personnels se fasse. Ainsi, citons par exemple la situation selon laquelle il est possible de limiter les demandes d'accès d'un individu dès lors que ladite requête aurait pour effet de dévoiler des informations d'une tierce personne[304]. Toujours sur la demande d'accès, mais cette fois du côté d'une entreprise, celle-ci se voit dans l'obligation de gérer – et de limiter – les accès de ses employés à seulement ceux qui en ont besoin pour effectuer leur travail[305]. Dernière disposition que nous pourrions citer ici, le consentement doit de manière générale être demandé auprès de la personne concernée pour qu'une collecte par une entreprise se fasse auprès de tiers[306].

Le consentement est donc un principe central[307] autour duquel toute la gestion des renseignements personnels tourne, même si une série de limitations à son usage a par la suite été introduite dans les lois. Ainsi, si ce consentement est un principe que l'on ne retrouve pas forcément dans les premiers textes initiaux – souvent internationaux – dont les lois nationales se sont

---

ligne : <http://www.canlii.ca/fr/ca/legis/lois/lc-2000-c-5/derniere/lc-2000-c-5.html>.

304 Art. 88 de la *Loi sur l'Accès aux documents des organismes publics et sur la protection des renseignements personnels*, L.R.Q., c. A-2.1, 2006, c. 22, en ligne : <http://canlii.org/fr/qc/legis/lois/lrq-c-a-2.1/derniere/lrq-c-a-2.1.html>.

305 Art. 20 de la *Loi sur la Protection des renseignements personnels dans le secteur privé,* L.R.Q., c. P-39.1, en ligne : <http://www.canlii.org/fr/qc/legis/lois/lrq-c-p-39.1/derniere/lrq-c-p-39.1.html>.

306 Art. 6 de la *Loi sur la Protection des renseignements personnels dans le secteur privé,* L.R.Q., c. P-39.1 en ligne : <http://www.canlii.org/fr/qc/legis/lois/lrq-c-p-39.1/derniere/lrq-c-p-39.1.html>.

307 Jennifer STODDART, « An overview of Canada's new private sector privacy law : The *Personal Information Protection and Electronic Documents Act* », (1er avril 2004), en ligne : Office of the Privacy Commissioner of Canada, <http://www.privcom.gc.ca/speech/2004/vs/vs_sp-d_040331_e.asp>, cite par Ian R. KERR, Jennifer BARRIGAR, Jacquelyn BURKELL et Katie BLACK, « Soft Surveillance, Hard Consent », (2006) 6 *Personally Yours* 1-14, dans la note 33, en ligne : <http://papers.ssrn.com/sol3/papers.cfm ?abstract_id=915407>.

inspirées[308], le consentement constitue une sorte de « lubrifiant » pour que la « machine » fonctionne, soit en exigeant le consentement des individus soit au contraire en considérant qu'il n'est pas requis. Dans le cadre de la gestion des renseignements personnels, le législateur a donc introduit une gestion des consentements, requis ou exonéré, au cas par cas, sans qu'une vision globale ne semble avoir été pensée. Afin que celui-ci ne soit donc pas regardé comme une porte ouverte béante vers une circulation qui serait possiblement attentatoires aux intérêts de l'individu[309], il importe à cette étape de considérer les rationalités derrière ce principe fondamental du droit de la protection des renseignements personnels. Une porte béante, et possiblement attentatoire aux intérêts des citoyens, qui est d'autant plus problématique que rares sont les hypothèses où les tribunaux interprètent ces contrats qui apparaissent sur les sites Internet, tant publics que privés d'ailleurs[310]. Et au-delà de la souplesse nécessaire à la gestion des renseignements personnels, le consentement, a quoi sert-il donc ?

2 – Rationalité protectrice du consentement

Et au-delà de la souplesse du procédé, érigé en « principe suprême », ce qui satisfait bien évidemment le gestionnaire, il faut s'interroger de la finalité derrière ce principe suprême qu'est le consentement. Malheureusement, nous craignions que derrière la compréhension initiale du consentement, et afin de s'assurer que

---

308 Voir notamment tant les règles de l'OCDE de 1980 (et leur mise à jour) que la Convention 109 de 1990.

309 Ian R. KERR, « If Left to Their Own Devices ... How DRM and Anti-Circumvention Laws Can be Used to Hack Privacy », dans Michael GEIST, (dir.), *In the Public Interest : The Future of Canadian Copyright Law, Irwin Law, 2005* , p. 198 et 199. L'auteur cite notamment, sur le même sujet Daniel J. SOLOVE, *The Digital Person : Technology and Privacy in the Information Age* (New York : NYU Press, 2005) p. 82–85.

310 En effet, rares sont les citoyens, consommateurs, internautes, qui trouvent un intérêt pécuniaire ou moral suffisant pour envisager d'intenter une poursuite pour une « politique » de vie privée (qui est toujours un contrat rempli de consentement autorisant la circulation de ses renseignements personnels).

l'individu ait un **contrôle** sur les informations le concernant, il y ait dans la pratique actuelle un glissement vers une acceptation de l'individu à ce que le gestionnaire de renseignements personnels puisse utiliser comme il le souhaite, ou presque, lesdites informations.

Au départ, le consentement est basé sur la prémisse selon laquelle l'usager est en mesure de « contrôler » les informations le concernant ; cette « fameuse » notion de contrôle qui fut déjà le concept clé dans notre analyse sur la qualification des opérations vue dans la partie 1[311]. Au regard du sacro-saint principe d'autonomie de la volonté, conformément à son étymologie grecque (« auto » pour « soi-même » et « nomos » pour la « loi »), c'est donc par le consentement que l'individu autorise la circulation des renseignements personnels. Ainsi, l'on considère implicitement que la protection passe par l'immobilisation, mais que la circulation des informations peut néanmoins être faite dès lors que la personne y consent ; comme si ce dernier acceptait d'être moins bien protégé, ce qui n'apparaît pas tout à fait logique.

Mais avant d'envisager cette notion de « contrôle » quant à la circulation des renseignements personnels, nous voudrions d'abord faire un constat selon lequel il y a lieu, en certains cas, de faire une distinction entre le consentement vu selon une vision généraliste, inspirée du droit des obligations traditionnel, et l'acceptation du même concept en ce qui a trait au droit de la protection des renseignements personnels, sous-catégorie du droit de la personnalité. En effet, les rationalités ne semblent pas les mêmes et nous croyons que dans cette dernière situation il y a

> « a need for a much higher original threshold of consent in privacy law than in contract law »[312].

En premier lieu, la protection des renseignements personnels évoque la gestion d'informations qui correspondent à un certain

---

311 *Infra*.

312 Ian R. KERR, Jennifer BARRIGAR, Jacquelyn BURKELL et Katie BLACK, « Soft Surveillance, Hard Consent », (2006) 6 *Personally Yours* 1-14, en ligne : <http://papers.ssrn.com/sol3/papers.cfm ?abstract_id=915407>.

niveau de sensibilité de par ce lien avec les droits de la personne[313]. Une sensibilité qui impose donc une retenue tant dans l'utilisation que dans la forme assortie au consentement. En second lieu, le consentement semble être un consentement rétractable et qui dispose d'un rapport au temps différent que dans le cadre d'un contrat de vente par exemple[314]. Même si cela n'apparaît pas expressément dans les définitions mêmes de ce qu'est un consentement[315], il peut être sous-entendu, tant de l'esprit des lois sur la protection des renseignements personnels, que des dispositions et de leur interprétation, que ce consentement doit être renforcé. À cet égard, les auteurs d'une étude évoquant la situation, guère différente et assurément pas moins protectrice de la loi fédérale qu'est la *Loi sur la protection des renseignements personnels et les documents électroniques* (PIPEDA)[316], mettent l'accent sur la nature intemporelle du consentement :

> « *PIPEDA*'s consent model is best understood as providing ***an ongoing act of agency*** to the information subject and is a much more robust than the usual model for consent in private law which treats consent as an isolated moment of contractual agreement during an information exchange. (…) Organizations wishing to use personal information must obtain the ***ongoing consent*** of the information subject for **continued**

---

313 Art. 35 du Code civil du Québec, situé dans le Chapitre 3 (Du respect de la réputation et de la vie privée) du Titre 2 (De certains droits de la personnalité) du Livre premier (Des personnes) dudit Code.

314 Néanmoins, et contrairement à la pratique de certains organismes, il a été déjà jugé qu'un consentement n'a pas besoin d'être récent et tant qu'il n'est pas révoqué, il est toujours valide. *X* c. *Québec (Société de l'assurance automobile)* décision non rapportée, C.A.I., no PP 98 09 09, 9 décembre 1999) Doray, III/59-19.

315 À la différence de la *Loi fédérale sur la protection des renseignements personnels et les documents électroniques*, article 4.3.8. de l'annexe 1 : « ne personne peut retirer son consentement en tout temps, sous réserve de restrictions prévues par une loi ou un contrat et d'un préavis raisonnable. L'organisation doit informer la personne des conséquences d'un tel retrait. »

316 *Loi sur la protection des renseignements personnels et les documents électroniques* (PIPEDA), en ligne : <http://www.canlii.ca/fr/ca/legis/lois/lc-2000-c-5/derniere/lc-2000-c-5.html>.

> **use**. In other words, the ***continued use*** of personal information must be understood as a necessary consequence of the information subject's ***continuing consent*** to its use and not merely as a consequence of the initial consent to collect the information.[317] » (Nos soulignements)

Cette perception du consentement permet de revisiter l'idée première derrière cette technique législative qu'est le consentement. Et au-delà de sa portée assouplissante pour le gestionnaire des renseignements personnels, elle sous-entend que l'individu est en droit de disposer d'un certain « contrôle » sur ses propres données.

> « *PIPEDA* generally allows the information subject to withdraw consent at any time. *PIPEDA* is predicated on the notion that individuals **have a *right* to control personal information** about them. This ongoing right of control is reinforced in law by the corollary requirement of ongoing consent codified in Principle 4.3.8 of *PIPEDA*. Consequently, unless they surrender it, individuals retain ultimate control over their personal information and can withdraw consent at any time.[318] » (Nos soulignements)

À bien des égards, plusieurs principes fondateurs de la protection des renseignements personnels militent pour une même analyse : ainsi, l'accès aux renseignements et la capacité de les corriger voire de les effacer illustre cette capacité de contrôle[319] ;

---

317 Ian R. KERR, Jennifer BARRIGAR, Jacquelyn BURKELL et Katie BLACK, « Soft Surveillance, Hard Consent », (2006) 6 *Personally Yours* 1-14, p. 5, en ligne : <http://papers.ssrn.com/sol3/papers.cfm ?abstract_id=915407>.

318 Ian R. KERR, Jennifer BARRIGAR, Jacquelyn BURKELL et Katie BLACK, « Soft Surveillance, Hard Consent », (2006) 6 *Personally Yours* 1-14, p. 5, en ligne : <http://papers.ssrn.com/sol3/papers.cfm ?abstract_id=915407>. (Les notes de bas de pages ont été enlevés).

319 Nous pouvons citer par exemple l'article 76 de la de la *Loi sur l'Accès aux documents des organismes publics et sur la protection des renseignements personnels*, L.R.Q., c. A-2.1, 2006, c. 22. en ligne : <http://canlii.org/fr/qc/legis/lois/lrq-c-a-2.1/derniere/lrq-c-a-2.1.html>, et au niveau fédéral, les art. 4.5.3 et 4.7.5 de l'Annexe 1 de la *Loi sur la protection des rensei-*

même perspective en ce qui a trait à l'obligation de destruction des renseignements personnels dès lors que la finalité pour laquelle ils ont été collectés est remplie[320] ; les définitions qui traitent parfois le consentement d'une façon telle qu'on « ne trouve guère de parallèle dans les Codes civils usuels »[321]. À cet égard, l'analogie proposée par les auteurs Kerr et suivants avec le contrat de « licence » est fort à propos[322] : le consentement visant à déterminer la circulation des renseignements personnels est l'équivalent de ce contrat *sui generis* qui ne constitue qu'un droit d'usage et non une cession de la propriété de l'œuvre. Une notion de contrôle qui est d'ailleurs explicitement reprise par la Commission d'accès à l'information elle-même lorsqu'elle affirme ceci :

> « Le droit à la vie privée sous-entend qu'une personne dispose d'un certain **contrôle** sur la circulation des renseignements la concernant. Vous devez donc vous assurer qu'une information personnelle ne pourra circuler sans l'autorisation préalable de la personne concernée, en évaluant notamment les moyens par lesquels vous obtenez ce consentement, les limi-

---

gnements personnels et les documents électroniques (PIPEDA), en ligne : <http://www.canlii.ca/fr/ca/legis/lois/lc-2000-c-5/derniere/lc-2000-c-5.html>.

320 Nous pouvons citer dans cette hypothèse l'exemple de l'article 73 de la de la *Loi sur l'Accès aux documents des organismes publics et sur la protection des renseignements personnels*, L.R.Q., c. A-2.1, 2006, c. 22, en ligne : <http://canlii.org/fr/qc/legis/lois/lrq-c-a-2.1/derniere/lrq-c-a-2.1.html>, et au niveau fédéral, l'art. 4.5.3 de l'Annexe 1 de la *Loi sur la protection des renseignements personnels et les documents électroniques* (PIPEDA), en ligne : <http://www.canlii.ca/fr/ca/legis/lois/lc-2000-c-5/derniere/lc-2000-c-5.html>.

321 François RIGAUX, <http://www.asmp.fr/travaux/gpw/internetvieprivee/rapport2/chapitr8.pdf>.

322 Ian R. KERR, Jennifer BARRIGAR, Jacquelyn BURKELL et Katie BLACK, « Soft Surveillance, Hard Consent », (2006) 6 *Personally Yours* 1-14, p. 6, en ligne : <http://papers.ssrn.com/sol3/papers.cfm ?abstract_id=915407>. Les auteurs affirment notamment : « Taken altogether, the consent provisions in *PIPEDA* strongly suggest that consent acts like a "license" that permits some *limited* collection, use, or disclosure. Thus, the consent given to an organization to use an individual's personal information is necessarily restricted and *does not* give the organization ultimate control over personal information in perpetuity. »

tes que vous lui attribuez et l'usage que vous en faites. »[323]. (Nos soulignements)

En guise de conclusion sur ce point, revenons sur un point précédemment envisagé, selon lequel nous croyons que le consentement dans le cas de la protection des droits de la personnalité doit être reconsidéré, et ce, en opérant une certaine distance de ses assises traditionnelles : car au-delà de ce concept fondateur du droit en général, il est des hypothèses où derrière ce « consent-fetichism »[324], la mise en place même du consentement implique un renoncement à la finalité même du droit de la protection des renseignements personnels. La finalité de ce champ du droit est d'assurer un certain contrôle de la part de l'intéressé sur les informations qui le caractérisent. Mais le consentement est trop souvent considéré comme un outil mécanique qui autorise le gestionnaire à user – voire abuser – des renseignements.

Du consentement « protection » *via* le contrôle de l'intéressé sur ses données, dans ce droit ayant une portée « rémédiatrice visant à favoriser l'exercice des droits »[325], on ne doit pas faire de liens trop hâtivement dressés avec le droit général qui considère plutôt le consentement comme un « commutateur » « donnant passage à un courant dont la source est ailleurs »[326]. Pour repren-

---

323 CAI, *Guide en matière de protection des renseignements personnels dans le développement des systèmes d'information à l'intention des ministères et organismes ,publics*, décembre 2002, en ligne : <http://www.cai.gouv.qc.ca/06_documentation/01_pdf/guide.pdf>, p. 9.

324 Roger BROWNSWORD, « The Cult of Consent : Fixation and Fallacy » (2004) 15 *King's College Law Journal* 223 et 224.

325 *Conseil de Presse du Québec* c. *Lamoureux-Gaboury*, 2003 IIJCAN 33002 (QC C.Q.)

326 Henri MAZEAUD, *Leçons de droit civil,* t. 2, Paris, Montchrestien, 1956, n° 116. Dans le même sens, utilisant également la métaphore électrique, Xavier MARTIN, « Nature humaine et Code Napoléon », (1985) 2 *Droits* 120 : « le contact des volontés formant le contrat ne créé pas plus d'énergie juridique que le doigt actionnant le commutateur ne créé d'énergie électrique : dans les deux cas, l'énergie vient d'ailleurs, et suppose tout un appareil, un réseau sans commune mesure avec le pan relativement très faible d'initiative et de pouvoir qui revient à l'individu. » Voir aussi, par exemple, ,Wallace K. LIGHTSEY, « A Critique of the Promise Model of Contract », (1984-85) 26

dre une opposition souvent faite relativement au consentement justement, celui-ci oscille, selon les circonstances, entre, dans certains cas, une approche visant à satisfaire une fonction « utilitaire » plus grande alors qu'en d'autres cas, il est plutôt en quête de davantage de « justice » ; ce « juste et utile » si souvent utilisé en ce qui a trait à l'analyse du consentement[327], et dont la balance entre les deux concepts risque de varier dans l'un et l'autre cas.

Également, il est possible de s'interroger sur cette pratique qui veut que, *via* le consentement, on ne s'intéresse plus à la protection des renseignements personnels mais à la capacité dont dispose l'individu de refuser, mais plus souvent, d'admettre un certain usage de son espace personnel[328]. Du consentement « protection » s'est donc opéré en pratique un glissement vers le consentement « permission ». Un glissement qui parait aller à l'encontre de la raison d'être du consentement ; une sorte de ce que les *common lawyers* appellent en droit des contrats la notion de « fundamental breach »[329]. Un glissement qui semble en violation des principes fondateurs derrière la notion de consentement en matière de protection des renseignements personnels voulant que l'individu dispose d'un certain contrôle, d'une certaine maîtrise[330], de ce qui le caractérise et de ce qui l'identifie.

William and Mary Law Review 45, selon qui la volonté joue « a vital role in triggering obligation but a trivial role in shapping it (...). The relationship itself may also be a source of contractual obligation ».

327 Par exemple Jacques GHESTIN, « L'utile et le juste dans les contrats », (1981) 26 *Archives de philosophie du droit* 35.

328 Steven L. WILLBORN, « Consenting Employees : Workplace Privacy and the Role of Consent », (2006) 66 *Louisiana Law Review* 975, 979.

329 G.H.L. FRIDMAN, *The Law of Contract in Canada*, 3e éd., Barrie (Ont.), Carswell, 1996, p. 561 et suiv.

330 François RIGAUX, p. 3, à la note 8, évoque qu'en droit allemand cette maîtrise qu'il qualifie de « droit à la maîtrise des données personnelles » (Recht *auf « informationelle ‚Selbstbestimmung »)* a été tenu pour un droit constitutionnellement garanti (BV*erf*G, 15 décembre 1983, *BVerfGE,* 65, 1, 43).

SECTION 1 – UTILISATION NOCIVE DU CONSENTEMENT

La pratique contractuelle est bien loin de la réalité de cette théorie protectrice. Dans les faits, les contrats, souvent longs[331], constituent davantage un moyen de s'assurer du respect du droit par le gestionnaire des renseignements personnels. Un droit qui se génère lui-même et dont la finalité protectrice semble éloigner de l'ordonnancement contractuel. Nous voilà face à une situation ubuesque où le gestionnaire de renseignements personnels met en place des règles de nature contractuelle afin de se protéger lui-même. Par le biais d'un consentement trop présent, « sur-valorisation » (over-valuation)[332], l'outil juridique qu'est ce dernier vise à protéger le gestionnaire afin de s'assurer qu'il est en droit de faire circuler les renseignements personnels. Comme le relève un auteur à l'égard du cas spécifique du consentement dans le cadre très précis de la protection du patient en droit médical :

> « But instead of focusing on the goals that the requirement of obtaining informed consent sought to promote—patient self determination, informed decision-making, and protection from harm chief among them—lawyers instead focused on documenting whether information had been disclosed, even if in fact it had not been. Thus the centerpiece of informed consent became the consent form rather than the process of disclosure—and the opportunity it provided for discussion between physician and patient.[333] »

Dans la continuité des propos précédents, il apparaît important d'avoir un point de vue critique sur cette pratique du consentement, et ce, tant à cause du fait de la « distraction » qu'il est susceptible d'apporter à la relation entre l'individu et l'organisation détentrice des renseignements personnels (1) que de la « pol-

---

331 *Infra*.

332 Roger BROWNSWORD, « The Cult of Consent : Fixation and Fallacy », (2004) 15 *King's College Law Journal* 223 et 224.

333 Alan MEISEL, « From Tragedy to Catastrophe : Lawyers and the Bureaucratization of Informed Consent », (2006) 6 *Yale Journal of Health Policy, Law, and Ethics* 479.

lution » que, de la même manière, il peut entraîner en faisant que l'intéressé perd l'essentiel quant à la relation contractuelle entre les deux protagonistes (2). Une distraction quant au « fond » du droit et une pollution davantage quant à la forme que peuvent prendre ces consentements.

1 – Consentement « distraction »

Comme mentionné plus tôt, la précédente section nous a permis d'envisager le consentement comme une manière de faire dont l'objet est d'assurer la protection de l'usager. Or, les pratiques contractuelles dédiées à la gestion des renseignements personnels vont justement dans le sens contraire. Les consentements sont en effet sur-utilisés et ont pour effet de « distraire » l'usager non spécialiste en droit avec une multitude de stipulations qui ont pour effet soit de l'effrayer soit de l'empêcher de lire ce qui est important.

Le consentement dispose donc d'effets secondaires qui militent pour un emploi plus mesuré ; alors que la réalité du consentement doit être assurée quant à la circulation de certains renseignements, et ce, de la façon la plus effective possible dans l'esprit de l'usager, il pourrait être judicieux d'éviter certains consentements qui s'imposent peut-être moins du fait de raisons variées telles qu'une moindre sensibilité des renseignements en cause, une situation de risque moins élevée, son inutilité notamment à cause du caractère implicite qu'il est susceptible d'avoir[334]. Ainsi, le consentement, en matière de protection de renseignements personnels peut-être plus que dans d'autres domaines, traduit ici le paradoxe d'un trop plein d'information :

> « However, providing the user with a lot of information regarding the processing of personal data **may paradoxically be a burden for the user because it encourages or requires the user to stop and reflect on the relevance of the information**. Consequently, there seems to be a more general tension between the goal of providing a seamless user experience and

[334] *Infra*.

> information requirements to ensure the principle of self-determination. If seamlessness leads to a non-transparent service, where the user does not know who can process his information and for what purposes, then it is questionable whether total seamlessness is at all desirable. From the perspective of data protection, a seamless integration of services should still ensure that the user can make informed decisions about how and by whom he or she wants personal data to be processed.[335] »
> (Nos soulignements)

Et la pratique quant à la manière de consentir est à cet égard déplorable. Car dans la mesure où le gestionnaire cherche à se protéger lui-même, sans considérer ni l'usager ni la finalité protectrice des lois vis-à-vis de ce dernier, il est différents travers quant au fond des consentements qui peuvent être trouvés.

En premier lieu, de par les juridismes, de par la matière évoquée, les consentements sont d'une complexité remarquable qui rend la compréhension difficile au non spécialiste qu'est presque systématiquement l'usager. Une complexité découlant soit de la syntaxe[336], du choix des termes, tels que des adverbes imprécis[337], et d'autres choix linguistiques aussi[338]. Ainsi, le résultat fait sou-

---

335 Tholas OLSEN et Tobias MAHLER, « Identity Management and Data Protection Law : Risk, Responsibility and Compliance in "Circles of Trust" » (2007), p.26 et 27.

336 Irène POLLACH, A Typology of Communicative Strategies in Online Privacy « Policies : Ethics, Power and Informed Consent » (2005) 62 *Journal of Business Ethics* 221, 228 : « One cannot safely say whether these statements are just poorly constructed or intended to obscure unethical data handling practices, but they do not give users a straightforward answer as to whether or not a certain practice is carried out, thus preventing informed consent. »

337 Irène POLLACH, A Typology of Communicative Strategies in Online Privacy « Policies : Ethics, Power and Informed Consent » (2005) 62 *Journal of Business Ethics* 221, 230 : « the use of adverbs of frequency does not tell users exactly when and how their data are made available to third parties, which prevents informed consent and mitigates unethical data handling practices. »

338 Irène POLLACH, A Typology of Communicative Strategies in Online Privacy « Policies : Ethics, Power and Informed Consent » (2005) 62 *Journal of*

vent que la lecture, qui est rendue fastidieuse, est en définitive inaccessible au commun des internautes.

En deuxième lieu, cette inaccessibilité est sans aucun doute favorisée par des consentements qui, en bien des cas, n'apparaissent pas à première vue, comme des consentements remettant en cause certaines prérogatives de la part de l'adhérant. C'est notamment dû au fait que plus souvent qu'autrement, les gestionnaires de renseignements personnels souhaitent diluer l'occurrence du consentement sous des titres trompeurs de « politique de renseignements personnels », « Avis », « Notice légale », « Avertissement », « Conditions d'utilisation », à savoir des intitulés plus neutres et moins « épeurants » mais qui traduisent mal ledit consentement ; une traduction qui illustre aussi malheureusement que trop bien la perte de la finalité protectrice de l'usager[339].

Enfin, en troisième lieu, notons que trop souvent, à cause de l'imprécision déjà signalée, ou à cause de l'ampleur des renonciations faites par l'usager, il est des hypothèses où les clauses qui donnent lieu au consentement pourraient être considérées comme abusives ou autrement illégales[340].

Business Ethics 221, 231 : « The use of the passive voice is another linguistic strategy found in privacy statements. It removes the agent from the subject position and foregrounds the object of the sentence instead. Also, the agent is sometimes removed altogether, which obscures responsibility for an action, as no one in particular appears to be responsible for it. »

339 Vincent GAUTRAIS, « Les contrats de cyberconsommation sont presque tous illégaux ! » (2005)

340 1437 C.c.Q. Voir à titre d'illustration TGI France, *précitée*, note 134. Vincent GAUTRAIS, « Les contrats de cyberconsommation sont presque tous illégaux ! » (2005) *Revue du Notariat* 617.

2 – Consentement « pollution »

« Encore des mots toujours des mots, les mêmes mots
Rien que des mots
Des mots faciles des mots fragiles
C'était trop beau »
(DALIDA ET ALAIN DELON)[341]

Dans la même veine que le précédent paragraphe, plusieurs études montrent que cette « hyper-oxygénation »[342] contractuelle est néfaste en rendant irréaliste l'appropriation par le lecteur-usager des consentements relatifs à la protection des renseignements personnels, et ce, au-delà des problèmes de forme que ce document peut prendre. Ainsi, il est plusieurs pathologies rédactionnelles qui peuvent être envisagées.

En premier lieu, les consentements sont souvent longs, beaucoup trop longs, tant ils égrènent des clauses souvent inutiles qui empêchent en fin de compte une appropriation du contenu. Par exemple, souvent, des pages et des pages de contrats s'évertuent à reproduire le droit existant et à recopier la substance de lois ou autres sources juridiques. Une problématique d'autant plus grande dans un contexte électronique où il n'y a pas de limites physique à l'insertion de texte[343]. Une problématique d'autant plus grande

---

341 DALIDA et Alain DELON, *Paroles, paroles* ; texte L. CHIOSSO, traduction MICHAËLE, musique G. FERRIO (1973), cité dans Vincent GAUTRAIS et Adriane PORCIN « Les 7 pêchés de la LPC : actions et omissions applicables au commerce électronique », (2009) *Thémis* (à paraître).

342 Vincent GAUTRAIS, « Les contrats de cyberconsommation sont presque tous illégaux ! » (2005) *Revue du Notariat* 617.

343 Vincent GAUTRAIS, « Les contrats de cyberconsommation sont presque tous illégaux ! » (2005) : « Sur un support électronique, la mise à la disposition du document est sans limite physique voire financière. Or, l'influence de la longueur est directe sur la compréhension du lecteur. La longueur est d'autant plus problématique que le destinataire du contrat électronique a des attentes de vitesse et qu'il procède ainsi souvent pour gagner du temps. Aussi, nous croyons devoir dénoncer cette tendance malheureuse des contrats « au kilo » qui n'est que peu sanctionnée par les juges. » Voir aussi Robert A. HILLMAN et Jeffrey J. RACHKLINSKI, « Standard-Form Contracting in the Electronic Age », (2002) 77 *New York University Law Review* 429, p. 451 et 452.

que la lisibilité d'un document – notamment un contrat de consentement, est à bien des égards, moins bonne sur un écran que sur une feuille de papier[344].

En deuxième lieu, et là encore il s'agit d'une spécificité du support électronique, le consentement contient souvent une clause autorisant le gestionnaire des renseignements personnels de le modifier sans obligation précise de notification, à charge pour l'adhérant d'aller vérifier si le contenu a évolué[345]. Une clause qui est d'ailleurs reconnue par certains droits comme étant illégale[346] et un projet dans le même sens semblait devoir être adopté au Québec dans le cas précis du droit de la consommation[347].

Encore, en troisième lieu, il est possible de citer les liens hypertextes qui ont pour effet de modifier la manière de lire un document, passant, dans le monde papier, à une lecture linéaire, du haut vers le bas, et de gauche à droite, à une forme nouvelle, différente, hypertextuelle cette fois[348]. Non que cette manière de faire soit forcément attentatoire à la capacité de « l'individu – lecteur » de prendre connaissance du contenu auquel il s'engage[349], simplement nous croyons qu'au regard d'études en communica-

---

344 Vincent GAUTRAIS, « Les contrats de cyberconsommation sont presque tous illégaux ! » (2005) *Revue du Notariat* 617.

345 Irène POLLACH, A Typology of Communicative Strategies in Online Privacy « Policies : Ethics, Power and Informed Consent » (2005) 62 *Journal of Business Ethics* 221, 231.

346 Code la consommation, article R. 132-2, Décret 97-298 du 27 mars 1997 – art. 1 (V) JORF 3 avril 1997, qui considère que « Dans les contrats conclus entre professionnels et non-professionnels ou consommateurs, est interdite la clause ayant pour objet ou pour effet de réserver au professionnel le droit de modifier unilatéralement les caractéristiques du bien à livrer ou du service à rendre. »

347 Vincent GAUTRAIS et Adriane PORCIN, « Les 7 pêchés de la LPC : actions et omissions applicables au commerce électronique », (2009) *Thémis* (à paraître).

348 Vincent GAUTRAIS, « Les contrats de cyberconsommation sont presque tous illégaux ! », (2005) *Revue du Notariat* 617 ; David MIALL, « Hypertextual reading : what's the difference », (1998) en ligne : <http://www.ualberta.ca/~dmiall/reading/hypdiff.htm>.

349 Comme l'a d'ailleurs établi la Cour suprême dans l'affaire *Dell Computer* c. *Union des Consommateurs*, 2007 CSC 34 (CanLII), en ligne : <http://www.canlii.ca/fr/ca/csc/doc/2007/2007csc34/2007csc34.html>.

tion, il semble important de rappeler qu'une certaine réserve s'impose quant à l'utilisation de tels procédés[350].

Enfin, et pour ne pas rendre la liste des pathologies possibles trop longue, nous finirons notre énumération en établissant que souvent les consentements électroniques utilisent des procédés pour manifester leur consentement qui peuvent porter à caution. Aussi, dans la lignée d'une acceptation majoritaire des contrats de type « shrinkwrap »[351] (aussi appelé les contrats étiquettes où l'on consent en déchirant le papier cellophane couvrant une boîte de type de celle qu'on utilise généralement pour les logiciels), une tendance équivalente a été initiée par les tribunaux pour les contrats « clickwrap »[352]. Davantage de doutes en revanche sont associés aux contrats de type « browsewrap », et ce, même si une décision canadienne a déjà mentionné le contraire[353].

Fort de ces écueils, le constat pratique est souvent implacable : l'usager non spécialiste qui entre dans une relation d' « usager / gestionnaire de renseignements personnels » ne dispose pas du contrôle précité quant à l'usage de l'information l'identifiant en tant qu'individu. Il ne contrôle pas car dans les faits, il ne lit pas[354] ; il ne contrôle pas car dans les faits il ne peut pas lire[355].

---

350 Vincent GAUTRAIS, « Le vouloir électronique selon l'affaire Dell Computer : dommage ! », (2008) *Revue Générale de droit, également* en ligne : <http://www.gautrais.com/IMG/pdf/200702GautraisEpreuve1.pdf>.

351 Pour une différence entre ces trois modèles de contrats, voir Vincent GAUTRAIS, « La couleur du consentement électronique », (2003) 16-1 *Cahiers de la propriété intellectuelle* 61-130, également en ligne : <http://www.gautrais.com/IMG/pdf/consentement2003CPI.pdf>.

352 *Dell Computer* c. *Union des Consommateurs*, 2007 CSC 34 (CanLII), en ligne : <http://www.canlii.ca/fr/ca/csc/doc/2007/2007csc34/2007csc34.html>.

353 Arrêt *Kanitz* c. *Rogers*, (2002) 58 O. R. 3rd 299 (Cour supérieure de l'Ontario).

354 Robert A. HILLMAN, « Online Boilerplate : Would Mandatory Web Site Disclosure of e-Standard Terms Backfire ? », dans Omri BEN-SHAHAR (dir.), *Boilerplate The Foundation of Market Contracts*, New-York, Cambridge University Press, 2007, p.83, à la page 94.

355 Aleecia M. MCDONALD and Lorrie Faith CRANOR (Carnegie Mellon University) s'intitulant « The Cost of Reading Privacy Policies », en ligne : <http://tprcweb.com/files/CostOfReadingPrivacyPolicies.pdf> et expliquant qu'un

Nous le verrons davantage plus tard avec une analyse concrète des choses[356].

SECTION 2 – UTILISATION INUTILE DU CONSENTEMENT

Pour reprendre une dichotomie présentée par Roger Brownsword[357], deux menaces peuvent être identifiées relativement au consentement, à savoir, soit sa « sur-valorisation » – ce que nous venons de voir dans la précédente section – soit au contraire une certaine « sous-valorisation »[358]. À l'égard de ce dernier point, l'auteur évoque notamment l'état de présomption ou de consentement implicite où l'on peut déduire une volonté de la part de l'intéressé. Pourtant, à bien des égards, et notamment dans les hypothèses où le gestionnaire veut bien faire, nous croyons davantage qu'il existe un certain nombre de situations où l'on exige des consentements pour rien. Il existe donc des hypothèses de trop plein de droit qui ont pour effet de rendre le service rendu source de confusion pour l'usager. Cette situation se pose d'une part dans l'hypothèse où nul consentement ne nous apparaît devoir être présenté (1) ou bien celle où le consentement peut être déduit implicitement des faits (2).

---

usager moyen d'Internet devrait utilise une vingtaine d'heures par mois pour être en mesure de lire les politiques de vie privée qu'il consent de suivre pour utiliser les sites disponibles.

356 *Infra*, Section 3.

357 Roger BROWNSWORD, « The Cult of Consent : Fixation and Fallacy » (2004) 15 *King's College Law Journal* 223.

358 Roger BROWNSWORD, « The Cult of Consent : Fixation and Fallacy » (2004) 15 *King's College Law Journal* 223 et 224 : « If individuals are to be taken seriously, if we are to respect one another as equals, then the development of a culture of consent surely must be welcomed. However, the integrity of such a culture needs to be defended against **two distinct kind of threat** -on the one hand, the threat of **under-valuation** and, on the other, that of **over-valuation**. » (Nos soulignements)

1 – Consentement pas nécessaire

Relativement à ce risque de « sous-valorisation » que le consentement est susceptible d'avoir et qui se définit de la manière suivante par l'auteur précité :

> « The threat of *under-valuation* is a familiar one. As a matter of doctrinal principle, it is commonly found where consent is read as "presumed", or "deemed" or "implied", or the like. On closer inspection, such consents will often prove to be pure fiction. »[359]

Certes. Ce genre de situations existe. Néanmoins, les hypothèses que nous apercevons très souvent, notamment à travers des excès de zèle chargés d'une volonté réelle de bien faire, sont celle où, au contraire, l'on requiert des consentements alors qu'ils ne sont pas nécessaires.

La raison première derrière cette situation de fait est, dans la plupart des cas, et en conformité avec ce que nous avons déjà vu dans la Partie 1, un problème de qualification d'une opération de circulation (collecte – communication – transmission – utilisation – etc.) qui n'en est pas vraiment une. Nous ne voulons pas reprendre la problématique ici.

Dans tous les cas, ce consentement inutile a un coût pour l'usager. D'abord, en terme d'informations, dans la mesure où il dilue ce qu'il est important de savoir, puisqu'il mêle les « vrais » consentements qui sont opérés par-ci par-là dans le cadre prestations en ligne avec de « faux » consentements non nécessaires. Par la multiplication de tels consentements, l'individu risque donc de ne plus faire la distinction entre le bon grain de l'ivraie informationnelle. Ensuite, il ralentit le processus du service commun et plus souvent qu'autrement, constitue des irritants qui, en bout de ligne, sont autant d'arguments pour que l'usager ne lise rien et clique de manière compulsive sur l'icône « j'accepte ».

---

[359] Roger BROWNSWORD, « The Cult of Consent : Fixation and Fallacy » (2004) 15 *King's College Law Journal* 223 et 224.

2 – Consentement implicite

Une autre hypothèse de consentement inutile est celle où les faits sont tellement évidents qu'à eux seuls il est possible de déduire que le consentement des individus est sans aucun doute clair et précis. Il peut s'agir par exemple, du patient qui décide de se rendre chez son médecin pour se faire soigner. Relativement aux prestations en ligne, il s'agit plutôt de l'hypothèse où un citoyen se connecte à un site gouvernemental afin d'accéder à un service donné.

Pourtant, certains auteurs, se basant sur la lettre des lois québécoises sur la protection des renseignements personnels, se posent la question sur le fait de savoir si ce type de consentement peut être autorisé[360]. En interprétant l'article 14 LPRPSP, ils considèrent, en effet, que le caractère exprès du consentement semble interdire davantage de souplesse. Pourtant, nous ne croyons pas qu'il peut en être ainsi. D'ailleurs, le consentement implicite existe relativement à des données dont la confidentialité est pour le moins sensible, à savoir, le domaine de la santé[361] (B). Ensuite, ces auteurs rapportent qu'une telle approche serait infaisable[362].

---

360 Voir notamment Karl DELWAIDE et Antoine AYLWIN, *Leçons tirées de dix ans d'expérience : la Loi sur la protection des renseignements personnels dans le secteur privé du Québec*, (2005), en ligne : <http://www.privcom.gc.ca/information/pub/dec_050816_f.asp>, se posent la question de la manière suivante : « Les exigences énoncées à l'article 14 de la Loi sur le secteur privé du Québec concernant un consentement valide nous enseignent que, contrairement à la LPRPDE, la Loi sur le secteur privé du Québec ne prévoit pas de consentement implicite. Seuls les consentements exprès sont valides. »

361 Par exemple *Bédard* c. *Robert*, 2003 CanLII 33179 (QC C.S.), en ligne : <http://www.canlii.org/fr/qc/qccs/doc/2003/2003canlii33179/2003canlii33179.html>.

362 Karl DELWAIDE et Antoine AYLWIN, « Toutefois, même la Loi sur le secteur privé du Québec ne règle pas la question de savoir si un consentement peut être considéré inhérent ou intrinsèque à un certain acte ou à une situation particulière qui prévaut. Par exemple, il est généralement reconnu qu'une personne qui réclame des dommages-intérêts ou une prestation d'invalidité auprès d'une société d'assurance consent à ce que soient communiqués les dossiers médicaux pertinents. On pourrait dire que dans un tel contexte le consentement est intrinsèque à la situation évoquée, parce que partie intégrante ou étant inhérent aux relations et aux interactions nécessaires entre

Il importe donc avant de voir cette situation particulière, d'envisager la question dans une perspective plus générale au regard des faits qui nous intéresse, à savoir la situation des prestations en ligne (A).

A – Consentement implicite dans l'hypothèse de PEL

Il est au départ une précision terminologique à faire, car « tacite » n'est pas « implicite » et conformément à ce qui est dit par Adrian Popovici :

> « Ce qui est tacite est non exprimé, sous entendu. Ce qui est implicite est une conséquence nécessaire, c'est ce qui, sans être formellement exprimé, peut-être tiré par déduction ou induction, peut-on apprendre. »[363]

En d'autres mots, le tacite découlerait du non-dit ; l'implicite d'une action qui sous-entendrait une acceptation[364]. Or, il est dans le domaine qui nous intéresse une grande variété de situations où des consentements découlent, selon nous, assurément du comportement même des internautes usagers des prestations en ligne offertes par le gouvernement. Ainsi, par exemple, lorsqu'une prestation en ligne est proposée aux usagers pour que ceci puissent déposer des renseignements personnels (comme éventuellement

---

les parties concernées. Pour que le consentement soit manifeste et exprès, fallait-il que l'intention définie soit expressément inscrite ou était-il suffisant qu'il soit logiquement ou naturellement inclus dans l'intention initiale ?

Comme il en ressort des causes mentionnées ci-après, la démonstration d'un consentement valide demeure une tâche qui requiert un degré de précision et de doigté pour refléter les objets précis devant être couverts et les renseignements nécessaires à recueillir, à utiliser ou à divulguer. Un consentement ne doit pas être trop étendu, sinon il sera alors sans effet. Il ne doit pas non plus être trop restrictif, parce que l'entreprise pourrait se voir interdire de recueillir, utiliser ou divulguer des renseignements personnels pour un objet qui n'est pas précisément visé par le consentement. »

363 Adrian POPOVICI, *La couleur du mandat*, Montréal, Éditions Thémis, 1995, p. 38.

364 Didier LLUELLES et Benoît MOORE, *Droit des obligations*, Montréal, Éditions Thémis, 2006, p. 166.

des photos, des informations, etc.), il serait facile de déduire de leur action une acceptation « implicite » (et non tacite) de cette communication d'information. Ainsi, au-delà de la question de savoir s'il s'agit d'une collecte[365] – ce que nous ne pensons pas –, s'il s'agit d'un renseignement personnel[366], il est possible d'affirmer que le contrôle plein et entier de l'usager sur ce qu'il décide, en connaissance de cause, de publier ou de ne pas publier, est une situation comportementale incluant nécessairement un consentement implicite.

Sur le registre du tacite cette fois, et ce, même si les hypothèses de prestations en ligne sont peut être moins nombreuses, on pourrait tout autant considérer ce que l'usager « veut », non seulement en agissant, mais également en utilisant ou accédant à un service qui est à son avantage. Ainsi, et comme l'est mentionné à l'article 1394 C.c.Q., un consentement tacite, peut donc découler du pur et simple silence dès lors que, notamment, des « circonstances particulières » peuvent être identifiées dans les faits en cause[367]. Aussi, à titre d'illustration, la doctrine tant française[368] que québécoise[369] cite à cet égard une ancienne décision de la Cour de cassation française[370] selon laquelle une offre qui serait à l'avantage exclusif de son destinataire pourrait être considérée comme étant acceptée par le silence de ce dernier.

Quoi qu'il en soit, et au-delà de cette différence, la jurisprudence est assez nourrie sur la question. Ainsi, et à titre d'exemple, la participation à une activité de groupe a été considérée comme un consentement implicite ou tacite à ce que les autres partici-

---

365 *Supra*, Partie 1, Chapitre 2, Section 2.

366 Bien que l'on puisse douter, en certains cas, du caractère personnel du renseignement dès lors qu'il devient accessible au public.

367 1394 « Le silence ne vaut pas acceptation, à moins qu'il n'en résulte autrement de la volonté des parties, de la loi ou de **circonstances particulières**, tels les usages ou les relations d'affaires antérieures. » (Nos soulignements)

368 Jacques GHESTIN, Traité de droit civil, Les obligations,- Le contrat : formation, 2e éd., Paris, L.G.D.J., 1988, p. 312.

369 Didier LLUELLES et Benoît MOORE, *Droit des obligations*, Montréal, Éditions Thémis, 2006, p. 168.

370 Cass. Civ., chambre des requêtes, 29 mars 1938, Dalloz. 1939. 1.5, note Voirin.

pants aient accès aux renseignements relatifs aux faits et gestes posés à cette occasion[371]. Pareillement, la diffusion, connue des signataires d'une pétition, peut comporter une renonciation à la confidentialité ou un consentement à la divulgation. Le contexte social ou politique dans lequel s'est déroulée la cueillette des signatures, caractère public ou officiel du texte d'une pétition, peut être utilisé pour l'analyse du contexte du consentement[372]. Dernière illustration, parmi d'autres sur lesquelles nous n'élaborerons pas ici[373], il a été jugé qu'une personne de nationalité anglaise qui se serait volontairement identifiée au demandeur dans une salle d'attente, dont ledit demandeur aurait oublié le nom, et qui veut la liste des patients de nationalité anglaise afin d'obtenir leurs témoignages lors d'un procès, aurait implicitement renoncé au privilège de refuser de fournir un renseignement personnel[374].

Bien sûr, l'on peut également trouver de la jurisprudence pour une perception plus restrictive du caractère implicite du consentement. Par exemple, et assez logiquement, le geste d'un tiers ne peut être interprété comme le consentement d'une personne[375]. Également, l'envoi d'une lettre à un journal ne constitue pas un consentement implicite à la communication de son adresse[376]. De la même manière, le consentement devant refléter une intention

---

371 *J.-U.P.* c. *Ministère de la sécurité publique* [2003] C.A.I. 268.

372 *Niocan*. c. *Oka (Municipalité d')*, [2001] C.A.I. 31.

373 *Legaré* c. *Municipalité du Bic*, [2007] C.A.I. 430 ; *Commission scolaire de la Jeune-Lorette*, [1997] C.A.I. 450 ; *Girard* c. *Service des achats du gouvernement*, [1986] C.A.I. 349.

374 *Thorsteinson* c. *Station Mont-Tremblay*, J.E. 2004-1123. Cité par Yvon DUPLESSIS, Jean HÉTU, sous la direction de Richard E. LANGELIER, *L'accès à l'information et la protection des renseignements personnels-Santé et services sociaux*, Brossard, Publications CCH Ltée, mise à jour septembre 2008, chapitre 4.157, 418.

375 *Chicoine* c. *Ministère de la sécurité publique*, [1989] C.A.I. 251, citée dans Yvon DUPLESSIS, Jean HÉTU, sous la direction de Richard E. LANGELIER, *L'accès à l'information et la protection des renseignements personnels-Santé et services sociaux*, Brossard, Publications CCH Ltée, mise à jour septembre 2008, chapitre 4.157, 610.

376 Woo c. Ville de Québec [1990] C.A.I. 324, citée par Yvon DUPLESSIS, Jean HÉTU, sous la direction de Richard E. LANGELIER, *L'accès à l'information et la protection des renseignements personnels-Santé et services sociaux*,

« positive », il a été considéré que le fait de subir un test polygraphique n'implique pas de consentir implicitement ou tacitement à la divulgation des résultats. Ne pas exprimer son désaccord à la transmission des résultats ne peut être interprété comme un consentement[377].

B – Analogie du consentement implicite dans le cas particulier du droit de la santé

En dépit de la différence de situation, nous croyons que, par analogie, la comparaison avec le domaine de la santé peut être utilisée de façon convaincante. Car si ce type de consentement est recevable dans un domaine aussi sensible que celui concernant la « vie », *a fortiori*, il le sera aussi dans celui concernant celui de la « vie privée ». Deux domaines où le consentement reçoit d'ailleurs un traitement équivalent dans le C.c.Q.

Aussi, le consentement implicite peut assurément être identifié dans certaines circonstances où le comportement du patient ne porte pas à caution. Ainsi :

> « [l]'exemple le plus fréquent est celui du patient qui se présente pour consultation ou pour examen de laboratoire. Du seul fait qu'il se présente, il est présumé consentir à l'examen : sa signature n'est pas requise. »[378]

Bien qu'il y soit mentionné qu'il ne faille trop librement interpréter la notion[379], le parallèle nous semble pouvoir être utilisé ici.

Dans le même sens, une certaine vision basée sur le pourtant autrement contestable « gros bon sens », a déjà permis à la juris-

---

Brossard, Publications CCH Ltée, mise à jour septembre 2008, chapitre 4., p. 157, 611.

377 *Dextraze* c. *Monty*, JE 2005-1314 (C.Q.) Doray, III/59-20.

378 Robert P. KOURI, Suzanne PHILIPS-NOOTENS et Pauline LESAGE-JARJOURA, *Éléments de responsabilité civile médicale – Le droit dans le quotidien de la médecine*, 3e éd., 2007.

379 G. SHARPE, *supra* , p. 31-34 cité dans Robert P. KOURI, Suzanne PHILIPS-NOOTENS et Pauline LESAGE-JARJOURA, *Éléments de responsabilité civile médicale – Le droit dans le quotidien de la médecine*, 3e éd., 2007.

prudence de considérer que la personne qui intente une action en justice sur la base de son état de santé ou celle qui exige le paiement d'un contrat d'assurance autorise par le fait même que ces renseignements personnels puissent être utilisés par la partie poursuivie ou débitrice[380].

SECTION 3 – UTILISATION CONCRÈTE DU CONSENTEMENT

Les propos tenus dans les trois précédentes sections montrent les imperfections tant dans la manière de concevoir, de penser que de réaliser les consentements attachés à la circulation des renseignements personnels. D'une manière plus pratique, il est tout autant possible de vérifier ces travers, et ce, relativement aux trois illustrations utilisées précédemment (1). Ce constat pratique est d'autant plus critiquable qu'il existe des solutions simples et efficaces pour améliorer la lisibilité et l'accessibilité des documents contractuels, qu'ils soient des contrats d'utilisation des sites ou des contrats quant à la gestion de la protection des renseignements personnels (2).

1 – Utilisation maladroite du consentement

Trop souvent, il est possible de constater que les consentements à la circulation des renseignements personnels son organisés de manière malhabile et s'éloignent de leur fonction initiale

---

380 Voir les décisions citées par Christiane LEPAGE, « La protection de l'information confidentielle dans le contexte de la « réingénierie », *Après le projet de loi 83: un nouveau réseau de la santé (2006), Service de la formation continue du Barreau du Québec*, 2006 et notamment *Laprise* c. *Bonneau* , [1985] C.A. 9 ; *Pilorgné . Desgens* , [1987] R.D.J. 341, EYB 1987-62473 ; *Goulet* c. *Lussier* , C.A.M., n ° 500-09-000398-891, 4 juillet 1989, EYB 1989-63376 ; *Robitaille* c. *Cie d'assurance C.N.A.* , [1979] A.J.Q. 1977 (C.S.) ; *Rousseau (Succession de)* c. *Groupe Desjardins (Le), assurances générales* , [1989] R.J.Q. 785, EYB 1989-63256 ; *Impériale (L'), cie d'assurance-vie* c. *Roy (Succession de)* , [1990] R.J.Q. 2468 (C.A.), EYB 1990-56812 ; *Favreau* , c. *La Solidarité, compagnie d'assurances sur la vie*, [1991] A.J.D.Q. 2111 (C.S.), EYB 1991-79499 ; *Dessurault* c. *Métropolitaine (La), cie d'assurance-vie*, [1996] A.J.D.Q. 2648 (C.S.).

qui est d'informer. De pareils constats peuvent être trouvés dans les trois exemples de prestations en ligne envisagées tout au long de notre analyse.

A – Illustration 1 : consentement et prestation d'identification

Si l'on ne peut, dans ce premier cas relatif à l'identification de l'usager d'un service public, et à la différence des deux autres illustrations, se baser sur des exemples existants, il est néanmoins possible d'identifier des risques associés au consentement à la circulation de renseignements personnels.

Lorsque l'on met en place une prestation d'identification, il est forcément nécessaire de faire en sorte que différentes pages se succèdent explicitant les différents processus pour ce faire. Ces processus peuvent ne pas être totalement faciles à appréhender pour le commun des internautes. Aussi, il est important de bien rappeler que chaque consentement qui sera introduit dans l'interface risque de complexifier la donne et, en bout de ligne, insérer des étapes dont l'usager aimerait pouvoir se passer.

D'ailleurs, par exemple, certains gestionnaires de telles prestations d'identification vont devoir gérer des « communications » entre différents organismes en introduisant des consentements les autorisant. Outre le fait que nous croyons, comme vu dans la Partie 1[381], que ces communications sont effectivement des communications sur les plans technologique et technique, mais n'en sont pas sur le plan de la qualification juridique que l'on doit en faire, il faut noter que l'introduction des consentements risque d'être parfois difficile à faire comprendre pour l'usager. En effet, la perception qu'il est facile de lui imputer est de ne pas comprendre que deux organismes faisant partie du même gouvernement, entité qu'il perçoit comme unique et unifié, aient besoin de son consentement pour communiquer une information le concernant. Plus qu'une mesure de protection, ce consentement risque bien plus d'être vu comme un irritant. Ceci sera encore plus vrai

[381] *Supra*, Partie 1, Chapitre 2, Section 1.

si le consentement en question est long et difficile à apprécier, comme cela apparaît un peu dans l'illustration 2 (B) relative au CV Commun Canadien[382] mais surtout dans l'illustration 3 (C) relative au site de promotion touristique[383]. Mais même dans l'hypothèse où un effort sera effectué à cet égard, cette étape nous apparaît difficilement en phase avec l'objectif de protection et de contrôle que le consentement est sensé avoir.

B – Illustration 2 : consentement et prestation de garde d'information

La présente analyse du consentement que nous voulons désormais faire concerne celui associé à la prestation en ligne d'un service de garde de documents technologiques pour le bénéfice d'un usager, et ce, comme dans l'hypothèse de ceux offerts aux universitaires par le FQRSC (concernant le Québec) ou le CRSH (concernant le Canada).

Là encore, un ou des consentements sont introduits dans le processus d'accès à la prestation en ligne, et ce, même si leur pertinence ne nous apparaît pas toujours très évidente. Par exemple, le consentement du FQRSC, certes très court, est une suite d'attestation sur l'état des chercheurs et sur leur obligation de garder leur mot de passe avec diligence[384]. En revanche, aucune mention n'est expressément faite sur l'éventuelle « collecte » ou « commu-

---

382 Le CV Commun Canadien est en ligne : http ://www.commoncv.net/index_f.html.

383 Communiqué du Ministère du Tourisme du 17 novembre 2008, « Concours Destination Québec-Le ministère du Tourisme lance un audacieux concours sur le Web 2.0 », en ligne : <http://www.bonjourquebec.com/mto/medias/communiques_pub/communique.asp ?no_comm=781&langue=francais&tri=date_comm&page=0>.

384 « Je déclare et atteste que :

1. Je suis un demandeur, ou un directeur d'études, ou un évaluateur ou un expert auprès du Fonds Nature et Technologies, du Fonds Société et Culture ou du Fonds de la recherche en santé du Québec.
2. J'atteste que tous les renseignements que je fournirai seront exacts et complets et je m'engage à dénoncer sans délai tout changement à un renseignement déjà donné.

nication » à des tiers autorisés. Un peu plus, ces éléments apparaissent dans la « Politique de confidentialité » accessible sur le site[385] qui, en dehors d'un consentement, explique uniquement que « nous n'utiliserons que l'information requise pour permettre au personnel du Fonds de répondre à votre message ou de donner suite à votre demande ». Le site n'envisage pas expressément la « collecte » qui pourrait être faite par le dépôt volontaire de l'usager de certains de ses renseignements personnels ; et c'est très bien.

La situation est passablement identique sur le site canadien du CRSH[386].

C – Illustration 3 : consentement et publication par les usagers

Nous l'avons vu, il existe une assez grande variété de sites faisant la promotion touristique[387]. Or, dans la quasi-totalité des exemples trouvés, il est frappant de voir l'ineffectivité des consentements des usagers en termes de protection de l'usager ; les consentements ont en revanche, conformément à nos propos antérieurs[388], davantage comme fonction de protéger le gestionnaire des sites afin de s'assurer qu'ils respectent le droit.

---

3. Je conviens d'observer la plus stricte confidentialité à l'égard de mon mot de passe personnel et aucune autre personne que le soussigné n'en fera usage. Je n'utiliserai dans la composition de mon mot de passe aucune combinaison de chiffres ou de lettres associées à mon numéro d'assurance sociale, ma date de naissance, mon numéro d'adresse civique ou autres données similaires qu'un tiers peut associer au soussigné.
4. Dans le cadre de toute demande ou communication électronique, je reconnais et conviens que le présent engagement s'applique intégralement au document que j'ai traité électroniquement, lorsque j'appuie sur la fonction J'accepte après le message d'attestation et d'engagement.
5. Je conviens que le présent engagement soit régi et interprété en vertu des lois applicables dans la province de Québec »

385 En ligne : <http://www.fqrsc.gouv.qc.ca/upload/accueil/politique-confidentialite.pdf>.

386 Voir sur le site <www.crsh.ca>.

387 *Supra*, Partie préliminaire, Chapitre 1, Section 1, 2, C.

388 *Supra*, Partie 2, Chapitre 1, Section préliminaire.

Ainsi, dans le cas du site www.holland.com, un contrat s'intitulant « terms of use » – et non contrat – ne fait pourtant aucun doute sur la nature contractuelle du document. En effet, on peut y lire au début :

> « All users of holland.com (« the site », « We », « Us ») are bound by the following terms of use. **If you do not agree to accept the terms herein, then please discontinue access to the site immediately**. Terms and conditions may be changed at the discretion of the Netherlands Board of Tourism & Conventions »[389] (Nos soulignements)

Aussi, en environ 4-5 pages d'équivalent d'un fichier « word », le site exige que l'usager accepte un certain nombre de comportements, dont plusieurs sont complètement inutiles. Par exemple, pourquoi, à l'article 6 dudit contrat, l'on suggère de ne pas violer le droit d'auteur ou, à l'article 9, on considère que les contributions des usagers « does not infringe any law ». De telles clauses sont inutiles, dans un contrat du moins, dans la mesure où la loi n'a pas besoin d'être indiquée par contrat pour exister. Elles sont également une source évidente de « pollution » dans la mesure où elle empêche de signaler aux citoyens ce qui est vraiment important. Toujours en prenant ce même exemple, il est frappant de constater comment les gestionnaires du site rédigent de vrais contrats mais sans donner l'impression que cela en est véritablement, utilisant les expressions « Terms and conditions » et « privacy policy ». Enfin, et ce sera la dernière pathologie contractuelle que nous signalerons dans ce cas, il importe de signaler que le contrat en question n'est aucunement un passage obligé et se présente sous la forme d'un « browsewrap »[390], forme de manifestation de consentement dont la légalité est loin d'être évidente.

Outre cette illustration européenne, le même constat peut être fait avec le site de Colombie-Britannique, www.helloBC.com[391]. Et

---

389 Voir le contrat en ligne : <http://us.holland.com/e/13854/>.

390 *Infra*, Partie 2, Chapitre 1, Section 3, 2, B.

391 Voir le contrat s'intitulant « Legal and privacy policy » en ligne : <http://www.hellobc.com/en-CA/AboutBC/CorporateInformation/Children/British-Columbia_LegalandPrivacyPolicy.htm>.

outre, les mêmes « erreurs » en termes de longueur (environ 7-8 pages), de manifestation de consentement[392], signalons également la clause suivante qui nous semble particulièrement problématique en affirmant relativement à la collecte :

> « You hereby authorize Tourism British Columbia to collect and retain all relevant information relating to your use of this site. You further authorize any third party to provide Tourism British Columbia with such information. »[393]

Le site préfère donc utiliser ce consentement, assez mal ficelé croyons-nous, plutôt que de considérer qu'aucune collecte n'est faite. En effet, et en conformité avec ce que nous avons déjà dit dans la Partie 1 en ce qui a trait à la collecte, elle n'est selon nous pas présente ici et donc ne requière donc pas un tel consentement. Néanmoins, pour se sécuriser soi-même, le site préfère l'intégrer, comme bien d'autres d'ailleurs[394].

---

392 Voir le contrat s'intitulant « Legal and privacy policy » en ligne : <http://www.hellobc.com/en-CA/AboutBC/CorporateInformation/Children/BritishColumbia_LegalandPrivacyPolicy.htm> et notamment la clause qui stipule ceci : « Please read these terms and conditions of website use carefully before using the HelloBC site. By continuing to use the HelloBC site, you agree to comply with and be bound by all of the terms and conditions set out below. We reserve the right, at our sole discretion, to modify these terms and conditions at any time, and such modifications shall be effective immediately upon posting of the modified terms and conditions. You agree to review the terms and conditions periodically to be aware of such modifications and your continued use of the HelloBC site shall be deemed your conclusive acceptance of the terms and conditions as modified from time to time. »

393 Voir le contrat s'intitulant « Legal and privacy policy » en ligne : <http://www.hellobc.com/en-CA/AboutBC/CorporateInformation/Children/BritishColumbia_LegalandPrivacyPolicy.htm>.

394 Le site de promotion de la ville de Montréal (<http://www.tourisme-montreal.org/Accueil/>) opte pour une solution identique. On peut notamment lire la clause suivante dans la politique de protection des renseignements personnels en ligne : <http://www.tourisme-montreal.org/Politique-de-confidentialite> : « LORSQUE VOUS FOURNISSEZ DES RENSEIGNEMENTS PERSONNELS IDENTIFIABLES A TOURISME MONTREAL POUR L'UTILISATION DES SERVICES OFFERTS SUR CE SITE WEB, **VOUS CONSENTEZ** (I) A LA **CUEILLETTE** DE CETTE INFORMATION PAR TOURISME MONTREAL, (II) A LA **DIVULGATION** DE CETTE INFORMATION AUX

2 – Solutions pratiques pour organiser des consentements

Outre le constat selon lequel les consentements disponibles sont souvent inutiles et dommageables pour la compréhension des usagers, nous devons ajouter que leur forme laisse à désirer. Une forme qui n'est pourtant pas si difficile à organiser, tant le respect de solutions pratiques pour rendre les documents contractuels permettrait en bien des cas de régler certains travers. Des solutions qui pourraient être appliquées tant pour la mise à la disposition de l'information à l'usager (A) que pour la manière pour ce dernier de manifester son consentement (B).

A – Solutions pratiques relatives à la mise à la disposition de l'information

En premier lieu, rappelons que pour développer la confiance des usagers, il importe d'expliciter et, contrairement à une croyance trop souvent véhiculée, de prendre son temps. Trop souvent, les gestionnaires de sites croient que plus le processus va vite et plus l'usager sera content. Au regard de spécialistes en communication et en marketing électronique, c'est tout le contraire qui prévaut[395]. Or, trop souvent, les consentements exigent d'être explicités aux usagers afin de leur faire comprendre que les renseignements personnels transmis entre deux ministères ou organismes par exemple, ne peuvent l'être sans leur consentement. Quoi qu'il en soit, tout gestionnaire doit avoir conscience,

FOURNISSEURS, PRESTATAIRES DE SERVICES ET PARTENAIRES D'AFFAIRES DE TOURISME MONTREAL POUR LES FINS ENONCEES CI-DESSUS, ET (III) A LA **CONSERVATION** DE CETTE INFORMATION PAR TOURISME MONTREAL POUR **UTILISATION** LORS DE DEMANDES SUBSEQUENTES. » (Nos soulignements).

395 Jacques NANTEL et Abdelouahab MEKKI-BERRADA, « L'efficacité et la navigabilité d'un site Web : rien ne sert de courir, encore faut-il aller dans la bonne direction », (2004) 29-4 Revue Gestion, en ligne : <http://www.hec.ca/chairerbc/indexf.htm> : « la performance d'un site, en matière de navigabilité, ne réside pas dans sa capacité de générer rapidement l'information désirée mais plutôt dans sa capacité de la générer avec le moins de frustration et de culs-de-sac pour le consommateur. »

que dans le monde « virtuel », électronique, plus que le monde réel, l'internaute étant souvent seul chez lui, sans autre mode d'interaction que son écran. Cette « distance » inhérence à ce type de communication doit donc être compensée par un suivi appliqué au médium.

En second lieu, et toujours selon une vision pluridisciplinaire, il est primordial de faire des textes contractuels qui soient courts et faciles à lire. Jakob Nielsen, spécialiste de communication électronique, et aucunement en droit, a mis en évidence les différences de capacité de lecture de l'usager devant un écran par comparaison avec celui qui consulte un document papier[396]. Le document écran est source de beaucoup plus d'imprécisions, d'éventuels quiproquos, d'une mémorisation moindre, etc. trop souvent, l'usager ne se donne pas la peine de lire et ne fait que « scroller » (*scrolling*), c'est-à-dire défiler le texte, sans capacité véritable d'absorber son contenu, pour finir par « cliquer » sans forcément avoir pleinement conscience de ce à quoi il s'engage.

Aussi, sur le plan concret, l'auteur propose des solutions toutes simples :

- un texte plus court, ne nécessitant pas ou nécessitant peu de défilement ;
- une utilisation de phrases simples ;
- l'utilisation d'un plan ;
- l'utilisation de puces pour bien distinguer les éléments importants ;
- l'utilisation de caractère gras, voire de majuscule ou des couleurs, pour mettre en exergue les points saillants ;
- l'utilisation modérée et contrôlée des liens hypertextes ;
- le bannissement de pratiques qui pourraient occasionner des doutes ou de l'inconfort auprès de l'adhérent comme le « *framing* » ou les sites qui bloquent le retour en arrière, etc.

---

396 Jakob NIELSEN, « Writing for the Web », <http://www.sun.com/980713/webwriting>.

Enfin, et sans volonté d'être exhaustifs, il serait pour le moins important pour les gestionnaires de site d'utiliser d'autres termes, plus évocateurs, que ceux que l'on a habituellement sur les sites des ministères et organismes, et ce, afin de bien montrer qu'il y a bien un consentement. En effet, parce que plus neutres, les sites préfèrent arborer des termes tels que « confidentialité », « avis », « vie privée », etc., alors qu'il s'agit d'abord et avant tout de contrat, de consentement[397].

B – Solutions pratiques relatives à la manifestation du consentement

Une même approche protectrice devra également être préconisée en ce qui a trait au consentement *stricto sensu*. De la même manière, il est essentiel que le consentement soit libre et entier, ce que certaines façons de faire, telles que celle notamment vues relativement à l'illustration 3[398], ne nous semblent pas satisfaire.

En effet, il est deux principales voies pour signifier un consentement de la part d'un adhérant. La première est celle du fameux « clic »[399] d'un icône par l'usager, qui exige généralement un comportement actif de ce dernier ; la seconde est celle que l'on qualifie sous l'appellation de « browsewrap » (lien hypertexte généralement en bas d'une page)[400] qui présentent tous les deux un certain nombre de différences[401].

---

397 *Supra*, Partie 2, Chapitre 1, Section 1, 1.

398 *Supra*, Partie 2, Chapitre 1, Section 3, 1.

399 Cette manière de faire est souvent appelée « clickwrap » par les auteurs. Afin de traduire cet anglicisme, l'office de la langue française a introduit la notion de « contrat d'achat au clic ». Eu égard, à l'incompréhension soulevée par ce néologisme, fort peu suivi, nous nous limiterons à l'expression originale.

400 Que plusieurs auteurs appellent aussi « webwrap ». Il n'existe pas à notre connaissance de terme équivalent en français.

401 Sur la difference entre « clickwrap » et « browsewrap », voir Kaustuv M. DAS, « Forum-Selection Clauses in Consumer Clickwrap and Browsewrap Agreements and the Reasonably Communicated Test », (2002) 77 *Washington Law Review* 481, p. 499-500 : « There are three important differences between clickwrap and browsewrap agreements. **First**, in the case of clickwrap agreements, users have constructive notice of the terms of the agree-

Sans aller dans le détail sur les manières de faire, il, apparaît que la jurisprudence, et notamment la fameuse décision *Dell Computer* c. *Union des consommateurs*[402], semble donner un avis positif sur ce mode de signification d'une acceptation. Cela dit, et outre les doutes associés à cette décision[403], l'on peut simplement dire que plus le consentement sera manifeste, et plus le gestionnaire pourra se protéger contre une éventuelle contestation de l'usager. Ainsi, il est possible d'identifier quelques risques juridiques quant à la validité de consentement dont l'usager n'a pas à présenter un comportement actif. Ce peut notamment être le cas lorsque, par exemple, des « boîtes » sont pré-cochées par le gestionnaire du site, à charge pour les usagers de les « décocher » s'ils ne souhaitent pas donner leur consentement à l'utilisation de leurs renseignements personnels.

De la même manière, il est possible d'avoir quelques doutes sur les consentements donnés en utilisant ce que l'on appelle communément les « browsewrap », à savoir, les manières de faire telle que présentées dans la plupart des situations de l'illustration 3.

---

ments because they are presented with all the terms of the agreements prior to entering into the agreement. However, with browsewrap agreements the terms of the agreement are displayed to users only if they click on the hyperlink that brings up the « terms and conditions » page. **Second**, in order to carry out their primary purpose (e.g., downloading software or purchasing tickets online), users must acknowledge the presence of both the clickwrap agreement and the displayed terms by clicking on a button. With a browsewrap agreement, users can carry out their primary purpose without ever clicking on the hyperlink that links to the « terms and conditions » and without ever seeing the agreement or its terms. **Finally**, with a browsewrap agreement users may not even realize that a contract is being formed. It is precisely because of these differences that courts have treated enforcement of these agreements differently. » (Nos soulignements).

402 *Dell Computer* c. *Union des Consommateurs*, 2007 CSC 34 (CanLII), en ligne : <http://www.canlii.ca/fr/ca/csc/doc/2007/2007csc34/2007csc34.html>.

403 Vincent GAUTRAIS, « Le vouloir électronique selon l'affaire Dell Computer : dommage ! », (2008) *Revue Générale de droit, également* en ligne : <http://www.gautrais.com/IMG/pdf/200702GautraisEpreuve1.pdf>.

CHAPITRE 2
AUTRES MÉCANISMES AUTORISANT LA CIRCULATION DES RP

Les législations relatives à la protection des renseignements personnels détenus par les autorités gouvernementales consacrent le principe selon lequel chacun des organismes publics sont des entités autonomes et responsables de la protection des renseignements personnels qu'ils ont en leur possession[404]. À la lumière de l'expérience de l'application des lois sur la protection des renseignements personnels, il s'est avéré que des dispositions prévoyant la possibilité pour un organisme de partager certaines informations personnelles moyennant le respect des conditions énoncées étaient nécessaires au fonctionnement adéquat des services publics. Ce besoin est particulièrement ressenti lorsqu'il s'agit d'assurer en ligne la prestation de services personnalisés à un citoyen.

Trois mécanismes sont prévus dans la *Loi sur l'accès* pour encadrer la circulation de renseignements personnels entre les entités gouvernementales. Tel que vu précédemment, le premier mécanisme consisterait en ce que la circulation soit autorisée avec le consentement de la personne concernée. Mais il y a, le second mécanisme qui consiste en des habilitations prévues expressément par les lois en vertu desquelles des renseignements personnels peuvent être communiqués à d'autres Administrations à des conditions qui y sont précisées. Le troisième mécanisme se matérialise par la conclusion d'ententes entre les entités gouvernementales pour le partage de renseignements personnels. Un ensemble de règles encadrent lesdites ententes de partage de renseignements personnels entre les entités gouvernementales.

Ces mécanismes autorisant la circulation des renseignements personnels (consentement, habilitations et ententes) de la législa-

---

404 Raymond DORAY et François CHARETTE, *Accès à l'information, Loi annotée, Jurisprudence Analyse et commentaires*, volume 1, mis à jour au 10 décembre 2008, Cowansville, Éditions Yvon Blais, 2001, p. III/59-2.

tion générale sur la protection des renseignements personnels sont généralement présents dans les régimes plus stricts de protection des renseignements personnels prévus spécifiquement à la *Loi sur le ministère du revenu*, en ce qui concerne le dossier fiscal[405], et à la *loi sur les services de santé et des services sociaux* (LSSSS) en ce qui concerne le dossier de l'usager[406].

---

405 Le projet de loi n° 14 (L.Q. 2002, c. 5, *Loi modifiant la Loi sur le ministère du Revenu et d'autres dispositions législatives relativement à la protection des renseignements confidentiels*) sanctionné le 15 mai 2002, a modifié la *Loi sur le ministère du Revenu* pour réviser complètement le régime applicable aux renseignements fiscaux. Il introduit la notion de dossier fiscal d'une personne qui est constitué des renseignements que le ministre détient à son sujet pour l'application ou l'exécution d'une loi fiscale. Ce dossier qui peut viser une personne physique ou une personne morale est confidentiel. Les renseignements contenus dans le dossier fiscal d'une personne ne peuvent être utilisés ou communiqués à moins que la personne concernée n'y consente ou que cette utilisation ou communication ne soit effectuée conformément à la *Loi sur le ministère du Revenu*. Ce régime particulier et plus sévère de protection du secret fiscal prévu à la *Loi sur le ministère du Revenu* n'est pas restreint par la *Loi sur l'accès* et a prépondérance sur elle (art. 171 par. 2.1 *Loi sur l'accès*). Ainsi, les exceptions à la confidentialité des renseignements personnels de la *Loi sur l'accès* ne s'appliquent pas au dossier fiscal d'une personne et les utilisations prescrites par la *Loi sur le ministère du revenu* sont les seules qui s'appliquent au dossier fiscal d'une personne. La protection accordée aux renseignements fiscaux par les article 69 à 71.6 de la *Loi sur le ministère du Revenu* a préséance lorsque cette protection est supérieure à celle accordée par la *Loi sur l'accès*. *La loi sur l'accès* continue de s'appliquer aux renseignements fiscaux à titre supplétif, dans la mesure où il n'existe aucune disposition législative dans la *Loi sur le ministère du Revenu* qui s'applique à la situation.

406 Les articles 17 à 27.3 de la *Loi sur les services de santé et les services sociaux* instaurent un régime de protection des renseignements contenus au dossier de l'usager. Ils prévoient les droits et les obligations de l'usager et de l'établissement du réseau en ce qui concerne la collecte, l'accès, la communication, la divulgation ou le transfert de renseignements de nature médicale ou psychosociale ou de tout autre information contenue au dossier de l'usager. En vertu de l'article 28 de la LSSSS, ces dispositions ont prépondérance sur la *Loi sur l'accès*, excluant ainsi l'application de cette dernière au dossier de l'usager des établissements du réseau de la santé et des services sociaux. La *loi sur l'accès* est cependant applicable à d'autres aspects de la gestion du dossier de l'usager, comme le droit de rectification.

SECTION 1 – HABILITATIONS À PARTAGER DES RP

1 – Habilitations à l'utilisation de RP

Les organismes publics ne peuvent utiliser les renseignements personnels qu'aux fins pour lesquelles ils ont été recueillis (art. 65 et 65.1 *de Loi sur l'accès et* art. 5(3) *de* la *Loi sur la protection des renseignements personnels et les documents électroniques* (PIPEDA))[407]. Ce principe de l'utilisation restreinte aux finalités lors de la collecte, et ce au sein de l'organisme, a été introduit à la *Loi sur l'accès* en 2006 et s'ajoute aux autres règles fondamentales de protection des renseignements personnels[408].

---

[407] L'organisme doit informer la personne auprès de laquelle des renseignements personnels sont recueillis des fins pour lesquelles ces renseignements sont recueillis (art. 65 par. 2 de la *Loi sur l'Accès aux documents des organismes publics et sur la protection des renseignements personnels*, L.R.Q., c. A-2.1, 2006, c. 22. en ligne : <http://canlii.org/fr/qc/legis/lois/lrq-c-a-2.1/derniere/lrq-c-a-2.1.html>) et « Un renseignement personnel ne peut être utilisé au sein d'un organisme public qu'aux fins pour lesquelles il a été recueilli » (art. 65.1 de la *Loi sur l'Accès aux documents des organismes publics et sur la protection des renseignements personnels*, L.R.Q., c. A-2.1, 2006, c. 22, en ligne : <http://canlii.org/fr/qc/legis/lois/lrq-c-a-2.1/derniere/lrq-c-a-2.1.html>) et au niveau fédéral, l'art. 5(3) de la *Loi sur la protection des renseignements personnels et les documents électroniques* (PIPEDA), en ligne : <http://www.canlii.ca/fr/ca/legis/lois/lc-2000-c-5/derniere/lc-2000-c-5.html>.

[408] Quant aux utilisations au sein du ministère du Revenu de renseignements contenus dans un dossier fiscal, elles sont limitées aux fins prévues à l'art. 69.0.0.7 de la *Loi sur le ministère du Revenu.* Elles sont généralement circonscrites, par exemple, à l'application ou l'exécution d'une loi fiscale ou de lois ou de programmes relevant du ministre, la réalisation d'une étude ou la production de statistiques, ou la réalisation de sondages ayant pour objet de connaître les attentes des personnes ou leur satisfaction à l'égard des lois et programme relevant de l'administration du ministre. L'utilisation de renseignements contenus dans un dossier fiscal aux fins de réaliser un sondage est entourée de conditions (art. 70.1).

En ce qui concerne la LSSSS, le projet de loi 83 est venu encadrer l'utilisation de certains renseignements contenus au dossier de l'usager à des fins de sollicitation ou à l'occasion de la réalisation de sondages. Il est permis à un établissement d'utiliser les nom, prénom et adresse d'un usager afin de l'inviter à verser un don au bénéfice de l'établissement ou d'une fondation

Trois assouplissements dans la loi permettent cependant l'**utilisation de renseignements personnels à une fin secondaire**. Avec ou sans le consentement, l'organisme public peut utiliser un renseignement personnel à d'autres fins si cette utilisation est compatible avec celles pour lesquelles il a été recueilli[409], ou si cette utilisation est manifestement au bénéfice de la personne[410], ou encore si cette utilisation est nécessaire à l'application d'une loi, que cette utilisation soit ou non prévue expressément par la loi (article 65.1 de la *Loi sur l'accès*[411] et articles 7(4) et 7(5) de PIPEDA [412]et les articles 4.2 à 4.2.6 et 4.5 à 4.5.4 de l'Annexe 1 de PIPEDA[413]).

Plusieurs objectifs sont ici recherchés par ces exceptions : on veut éviter à la personne concernée de fournir à nouveau des ren-

---

de cet établissement à moins que l'usager ne s'y oppose (opting out) (art. 27.3 L.S.S.S.S.). Un établissement peut aussi utiliser les nom, prénom, adresse et numéro de téléphone d'un usager pour la réalisation de sondages ayant pour objet de connaître les attentes des usagers et leur satisfaction à l'égard de la qualité des services offerts par l'établissement (art. 107 L.S.S.S.S.). Dans ces deux situations, des règles d'éthique doivent être respectées.

409 i.e. un lien pertinent et direct avec les fins initiales pour lesquelles les renseignements ont été recueillis (fins incompatibles à l'article 37 du Code civil). Selon Doray et Charette, c'est un critère objectif qui invite à se demander si une personne raisonnable considérerait que l'usage secondaire des renseignements personnels que veut entreprendre l'organisme public a un rapport (lien pertinent) logique et prévisible (lien direct) avec l'objet ou la finalité pour laquelle les renseignements ont été obtenus à l'origine.

410 Il ne doit pas y avoir de doute, la personne concernée ne saurait subir un préjudice de cet usage secondaire mais elle devrait en tirer un avantage

411 Art. 65.1 de la *Loi sur l'Accès aux documents des organismes publics et sur la protection des renseignements personnels*, L.R.Q., c. A-2.1, 2006, c. 22, en ligne : <http://canlii.org/fr/qc/legis/lois/lrq-c-a-2.1/derniere/lrq-c-a-2.1.html>.

412 Art. 7.(4) et 7.(5) de *Loi sur la protection des renseignements personnels et les documents électroniques* (PIPEDA), en ligne : <http://www.canlii.ca/fr/ca/legis/lois/lc-2000-c-5/derniere/lc-2000-c-5.html>.

413 Art. 4.2 à 4.2.6 et 4.5 à 4.5.4 de l'Annexe 1 de *Loi sur la protection des renseignements personnels et les documents électroniques* (PIPEDA), en ligne : <http://www.canlii.ca/fr/ca/legis/lois/lc-2000-c-5/derniere/lc-2000-c-5.html>.

seignements qu'elle a transmis à l'organisme, et ainsi accroître la rapidité du service et réduire la possibilité d'erreur[414].

Le responsable doit inscrire cette utilisation à d'autres fins que celles pour lesquelles les renseignements ont été recueillis dans le registre prévu à 67.3 de la *Loi sur l'accès* [415]. Ce registre est accessible en consultant le site de l'organisme public (art. 4 par. 6 *Règlement sur la diffusion de l'information et sur la protection des renseignements personnels*).

2 – Habilitations à la communication de RP

Au regard de la *Loi sur l'accès*[416], les organismes publics sont habilités par les lois à partager des renseignements personnels, entre autres, dans les cas où les renseignements sont nécessaires pour lutter contre le crime ou dans des situations d'urgence mettant la sécurité ou la vie de la personne concernée en danger ou à des fins d'étude ou de recherche. Par exemple, dans cette *Loi sur l'accès*, la communication d'un renseignement personnel, sans le

---

414 Yves D. DUSSAULT, *Modifications au régime de protection des renseignements personnels*, Texte présenté lors du Colloque du Barreau du Québec intitulé "Vie privée et protection des renseignements personnels", le 23 novembre 2006, p. 12. Selon cet auteur, ces motifs d'utilisation des RP à des fins secondaires respectent le droit du citoyen à une certaine expectative raisonnable de vie privée en ce qu'il ne se fait pas prendre par surprise par de tels motifs d'utilisation, voir *Journal des débats*, 37e législature, 2e session, 30 mai 2006, en ligne : < http ://www.assnat.qc.ca/fra/37Legislature2/DEBATS/journal/cc/060530.htm >.

415 Dans le cas d'utilisation d'un renseignement personnel à une autre fin que celle pour laquelle il a été recueilli, le registre comprend :

1° la mention du paragraphe du deuxième alinéa de l'article 65.1 permettant l'utilisation ;

2° dans le cas visé au paragraphe 3 du deuxième alinéa de l'article 65.1, la disposition de la loi qui rend nécessaire l'utilisation du renseignement ;

3° la catégorie de personnes qui a accès au renseignement aux fins de l'utilisation indiquée.

416 *Loi sur l'Accès aux documents des organismes publics et sur la protection des renseignements personnels*, L.R.Q., c. A-2.1, 2006, c. 22. en ligne : <http://canlii.org/fr/qc/legis/lois/lrq-c-a-2.1/derniere/lrq-c-a-2.1.html>.

consentement de la personne concernée, est autorisée entre autres dans les cas suivants[417] :

- Art. 59 al. 2 par. 1 (communication au procureur de l'organisme d'un renseignement personnel nécessaire aux fins d'une poursuite en cas d'infraction à une loi que cet organisme est chargé d'appliquer ou au directeur des poursuites criminelles et pénales si le renseignement est nécessaire aux fins d'une poursuite pour une infraction à une loi applicable au Québec)

---

[417] La *loi sur le ministère du Revenu* contient également des habilitations à communiquer des renseignements contenus au dossier fiscal, qui sont entourées de conditions strictes. Malgré les articles 53, 59 et 59.1 de la *Loi sur l'accès*, un renseignement contenu au dossier fiscal ne peut être communiqué sans le consentement de la personne que dans les cas prévus à la *loi sur le ministère du Revenu* (art. 69.0.0.10). Par exemple, la communication d'un renseignement contenu au dossier fiscal en vue de prévenir un acte de violence, dont un suicide (art. 69.0.0.11) ; la communication d'un renseignement à un corps de police avec l'autorisation d'un juge de la Cour du Québec dans le cadre de la lutte contre le crime organisé (art. 69.0.0.12) ; la communication d'un renseignement pour l'application d'une loi fiscale ou lors d'une infraction criminelle ou pénale (art. 69.0.0.16).

Quant à la LSSSS, l'article 19, renouvelé par le projet de loi 83 en 2006, a maintenu le principe de l'obtention d'un consentement pour autoriser la communication de renseignements contenus au dossier de l'usager. « Cependant, au nom de la protection de la santé publique et de la nécessité d'offrir des soins de santé et des services sociaux de qualité, continus, cohérents, adéquats et efficaces, le législateur donne aussi le feu vert à la circulation élargie de l'information confidentielle sans le consentement de la personne concernée » (Christiane LEPAGE, « La protection de l'information confidentielle dans le contexte de la « réingénierie » » dans Après le projet de loi 83 : un nouveau réseau de la santé, Cowansville, Éditions Yvon Blais, volume 260, Service de la formation continue du Barreau du Québec, 2006, p. 217). Malgré la nouvelle présentation de l'article 19, la plupart des exceptions demeurent les mêmes, quoiqu'elles sont plus explicites quant aux moments et aux circonstances où cette circulation est possible. Des communications de renseignements contenus au dossier de l'usager sont également prévues dans d'autres dispositions de la LSSSS, dans les règlements d'application de la LSSSS ou dans d'autres lois. Sur ces différentes exceptions à la confidentialité du dossier de l'usager, voir : Yvon DUPLESSIS, Jean HÉTU, sous la direction de Richard E. LANGELIER, L'accès à l'information et la protection des renseignements personnels-Santé et services sociaux, Brossard, Publications CCH Ltée, mise à jour septembre 2008, chapitre 4.

- Art. 59 al. 2 par. 2 (communication au procureur de l'organisme ou au Procureur général lorsqu'il agit comme procureur de cet organisme d'un renseignement personnel nécessaire aux fins d'une procédure autre que pénale ou criminelle)
- Art. 59 al. 2 par. 3 (communication à un organisme qui, en vertu de la loi, est chargé de prévenir, détecter ou réprimer le crime ou les infractions aux lois, si le renseignement est nécessaire aux fins d'une poursuite pour infraction à une loi applicable au Québec)
- Art. 59 al. 2 par. 4 (communication dans les situations d'urgence qui mettent en danger la vie, la santé ou la sécurité de la personne concernée)
- Art. 59 al. 2 par. 5 (communication à une personne autorisée par la Commission d'accès à l'information à utiliser ce renseignement à des fins d'étude, de recherche ou de statistique)
- Art. 59 al. 2 par. 8 (communication à une personne ou à un organisme, conformément aux articles 61, 66, 67, 67.1, 67.2, 68 et 68.1. Ce sont des situations de communication de renseignements personnels "qui sont assujettis à une procédure plus formelle, vraisemblablement en raison des plus grands risques qu'ils font peser sur la vie privée des citoyens"[418].)
- Art. 59 al. 2 par. 9 (communication de certains renseignements à une personne impliquée dans un événement ayant fait l'objet d'un rapport par un corps policier)
- Art. 59.1 (communication en vue de prévenir un acte de violence, dont un suicide)
- Art. 61 (communication entre corps de police)

---

[418] Raymond DORAY et François CHARETTE, *Accès à l'information, Loi annotée, Jurisprudence Analyse et commentaires*, volume 1, mis à jour au 10 décembre 2008, Cowansville, Éditions Yvon Blais, 2001, p. III/59-10.

- Art. 66 (communication d'un renseignement sur l'identité d'une personne afin de recueillir des renseignements personnels déjà colligés par une personne ou un organisme privé)[419]

Il est important de signaler que la plupart des principes ci-dessus sont repris au niveau fédéral par les articles 7(3) à 7(3)i) de la *Loi sur la protection des renseignements personnels et les documents électroniques* (PIPEDA)[420], et ce, de manière comparable à l'article 59 de la *Loi sur l'accès.*

Des dispositions de la *Loi sur l'accès* prévoient aussi qu'un organisme public peut communiquer, à toute personne ou à un autre organisme public, un renseignement personnel, sans l'accord de la personne concernée, si cette **divulgation est nécessaire pour l'application d'une loi**. Cette disposition est ainsi formulée :

> **67.** Un organisme public peut, sans le consentement de la personne concernée, communiquer un renseignement personnel à toute personne ou organisme si cette communication est nécessaire à l'application d'une loi au Québec, que cette communication soit ou non prévue expressément par la loi.

Encore une fois, le contenu de ce texte se retrouve, au niveau fédéral, à l'article 4.5 al. 1 de l'Annexe 1 de PIPEDA[421], et aux articles 7 (2) en tous ses alinéas et 7(3) c1) et d) de PIPEDA[422].

Il nous semble important de signaler qu'au lendemain de la mise en vigueur de la *Loi sur l'accès*, la Commission d'accès a eu

---

419 Art. 59, 59.1, 61 et 66 de la *Loi sur l'Accès aux documents des organismes publics et sur la protection des renseignements personnels*, L.R.Q., c. A-2.1, 2006, c. 22. en ligne : <http://canlii.org/fr/qc/legis/lois/lrq-c-a-2.1/derniere/lrq-c-a-2.1.html>.

420 Art. 7.(3) et 7.(3)i) de *Loi sur la protection des renseignements personnels et les documents électroniques* (PIPEDA), en ligne : <http://www.canlii.ca/fr/ca/legis/lois/lc-2000-c-5/derniere/lc-2000-c-5.html>.

421 Art. 4.5 al.1 de l'annexe 1 de *Loi sur la protection des renseignements personnels et les documents électroniques* (PIPEDA), en ligne : <http://www.canlii.ca/fr/ca/legis/lois/lc-2000-c-5/derniere/lc-2000-c-5.html>.

422 Art. 7.(2) et 7.(3) c1) et d) de *Loi sur la protection des renseignements personnels et les documents électroniques* (PIPEDA), en ligne : <http://www.canlii.ca/fr/ca/legis/lois/lc-2000-c-5/derniere/lc-2000-c-5.html>.

tendance à retenir une interprétation restrictive de la notion de nécessité pour l'application d'une loi. Tant et si bien qu'il fallait démontrer que la communication de ces renseignements est « indispensable, essentielle et primordiale ». Doray et Charrette rappellent que selon cette interprétation stricte :

> « […] il était essentiel qu'une loi mentionne expressément qu'un organisme public doit communiquer des renseignements nominatifs à une personne ou à un organisme public ou privé pour que l'article 67 puisse s'appliquer »[423].

Les amendements insérés en 2006 à la *Loi sur l'accès*[424] ont mis fin à cette tendance en introduisant la précision selon laquelle il n'est pas nécessaire que la communication soit prévue expressément par la loi. Dussault souligne « qu'il suffira, par exemple, que la loi ait prévu une collaboration ou une entente entre deux organismes concernant un programme relatif aux ressources humaines pour que l'on puisse comprendre une autorisation législative de communiquer des renseignements personnels »[425].

L'article 68.1 *de la Loi sur l'accès*[426] dont le contenu n'existe dans la *Loi sur la protection des renseignements personnels et les documents électroniques* (PIPEDA) que de manière implicite[427], permet à un organisme public de communiquer, sans consente-

---

423 Raymond DORAY et François CHARETTE, *Accès à l'information, Loi annotée, Jurisprudence Analyse et commentaires*, volume 1, mis à jour au 10 décembre 2008, Cowansville, Éditions Yvon Blais, 2001, p. III/67-2.

424 *Loi sur l'Accès aux documents des organismes publics et sur la protection des renseignements personnels*, L.R.Q., c. A-2.1, 2006, c. 22. en ligne : <http://canlii.org/fr/qc/legis/lois/lrq-c-a-2.1/derniere/lrq-c-a-2.1.html>.

425 Yves D. DUSSAULT, *Modifications au régime de protection des renseignements personnels*, Texte présenté lors du Colloque du Barreau du Québec intitulé "Vie privée et protection des renseignements personnels", le 23 novembre 2006, p. 16.

426 Art. 68.1 de la *Loi sur l'Accès aux documents des organismes publics et sur la protection des renseignements personnels*, L.R.Q., c. A-2.1, 2006, c. 22. en ligne : <http://canlii.org/fr/qc/legis/lois/lrq-c-a-2.1/derniere/lrq-c-a-2.1.html>.

427 *Loi sur la protection des renseignements personnels et les documents électroniques* (PIPEDA), en ligne : <http://www.canlii.ca/fr/ca/legis/lois/lc-2000-c-5/derniere/lc-2000-c-5.html>.

ment de la personne concernée, un fichier de renseignements personnels si cette communication est nécessaire à l'application d'une loi au Québec, **que cette communication soit ou non prévue expressément par la loi**.

Parmi les exceptions prévues au caractère confidentiel des renseignements personnels, il y a les dispositions autorisant la communication de renseignements personnels, non seulement à un autre organisme public, mais aussi à un organisme d'un autre gouvernement. L'article 68 par. (1°) de la *Loi sur l'accès*[428] qui est une loi québécoise indique qu'un organisme public peut communiquer un renseignement personnel

> « à un organisme public ou à un organisme d'un autre gouvernement lorsque cette communication est nécessaire à l'exercice des attributions de l'organisme receveur ou à la mise en œuvre d'un programme dont cet organisme a la gestion ».

L'alinéa 68 (1.1°) prévoit qu'un organisme public peut communiquer un renseignement personnel « à un organisme public ou à un organisme d'un autre gouvernement lorsque la communication est manifestement au bénéfice de la personne concernée »[429]. De même, l'alinéa 68 par. (3°) autorise la communication d'un renseignement personnel :

> « à une personne ou à un organisme si cette communication est nécessaire dans le cadre de la prestation d'un service à rendre à la personne concernée par un organisme public, notamment aux fins de l'identification de cette personne. »[430]

---

[428] Art. 68 (1) de la *Loi sur l'Accès aux documents des organismes publics et sur la protection des renseignements personnels*, L.R.Q., c. A-2.1, 2006, c. 22, en ligne : <http://canlii.org/fr/qc/legis/lois/lrq-c-a-2.1/derniere/lrq-c-a-2.1.html>.

[429] Art. 68 (1.1) de la *Loi sur l'Accès aux documents des organismes publics et sur la protection des renseignements personnels*, L.R.Q., c. A-2.1, 2006, c. 22, en ligne : <http://canlii.org/fr/qc/legis/lois/lrq-c-a-2.1/derniere/lrq-c-a-2.1.html>.

[430] Art. 68 (3) de la *Loi sur l'Accès aux documents des organismes publics et sur la protection des renseignements personnels*, L.R.Q., c. A-2.1, 2006, c. 22, en ligne : <http://canlii.org/fr/qc/legis/lois/lrq-c-a-2.1/derniere/lrq-c-a-2.1.html>.

Cette nouvelle exception, ajoutée en 2006 à la *Loi sur l'accès*, « ne peut être utilisée qu'au bénéfice de la personne concernée, plus particulièrement pour lui dispenser un service »[431] et peut aider à la mise en œuvre de projets liés au gouvernement en ligne, comme le partage d'un fichier d'adresses ou d'un système d'authentification.

Pour ce qui a trait aux communications à l'extérieur du Québec, « l'organisme public doit s'assurer qu'ils bénéficieront d'une protection équivalant à celle prévue à la présente loi »[432]. Si l'organisme public estime que les renseignements « ne bénéficieront pas d'une protection équivalant à celle prévue à la présente loi, il doit refuser de les communiquer ou refuser de confier à une personne ou à un organisme à l'extérieur du Québec la tâche de les détenir, de les utiliser ou de les communiquer pour son compte »[433].

SECTION 2 – Ententes de partage

Les conditions du partage des renseignements sont habituellement régies par des ententes entre les organismes impliqués.

1 – Ententes de collecte

Suivant le principe général de la confidentialité des renseignements personnels, l'article 64 de la *Loi sur l'accès* limite la collecte des renseignements personnels par un organisme public à ceux qui sont nécessaires à l'exercice des attributions ou à la mise

---

431 *Loi sur l'Accès aux documents des organismes publics et sur la protection des renseignements personnels*, L.R.Q., c. A-2.1, 2006, c. 22, en ligne : <http://canlii.org/fr/qc/legis/lois/lrq-c-a-2.1/derniere/lrq-c-a-2.1.html>.

432 Art. 70.1 al 1, de la *Loi sur l'Accès aux documents des organismes publics et sur la protection des renseignements personnels*, L.R.Q., c. A-2.1, 2006, c. 22, en ligne : <http://canlii.org/fr/qc/legis/lois/lrq-c-a-2.1/derniere/lrq-c-a-2.1.html>.

433 Art. 70.1 al 2, de la *Loi sur l'Accès aux documents des organismes publics et sur la protection des renseignements personnels*, L.R.Q., c. A-2.1, 2006, c. 22, en ligne : <http://canlii.org/fr/qc/legis/lois/lrq-c-a-2.1/derniere/lrq-c-a-2.1.html>.

en œuvre d'un programme dont il a la gestion (art. 64 al.1 de la *Loi sur l'accès*)[434].

Jusqu'en 2006, la *Loi sur l'accès* ne permettait pas explicitement la collecte de renseignements personnels pour un autre organisme public et cela freinait l'implantation de services publics intégrés encouragés par les lois tel le service de guichet unique multiservices (art. 4, *Loi sur Services Québec*) ou le regroupement et la gestion de services par le Centre de services partagés du Québec (art. 5 par. 6 de la *Loi sur le Centre de services partagés du Québec*)[435].

En 2006, les règles de la collecte ont été modifiées afin de faciliter l'offre de services intégrés au citoyen par l'administration publique, offre qui repose sur une plus grande circulation de l'information. Il est désormais possible à un organisme public de recueillir les renseignements personnels qui sont nécessaires à un autre organisme public avec lequel il collabore pour effectuer la prestation de services ou réaliser une mission commune. C'est en ce sens que l'article 64 de la *Loi sur l'accès* a été amendé :

> « **64**. Nul ne peut, au nom d'un organisme public, recueillir un renseignement personnel si cela n'est pas nécessaire à l'exercice des attributions de cet organisme ou à la mise en oeuvre d'un programme dont il a la gestion.
>
> *Demande permise.*
> Un organisme public peut toutefois recueillir un renseignement personnel si cela est nécessaire à l'exercice des attributions ou à la mise en oeuvre d'un programme de l'organisme public avec lequel il collabore pour la prestation de services ou pour la réalisation d'une mission commune.

---

434 Art. 64 al.1 de la *Loi sur l'Accès aux documents des organismes publics et sur la protection des renseignements personnels*, L.R.Q., c. A-2.1, 2006, c. 22, en ligne : <http://canlii.org/fr/qc/legis/lois/lrq-c-a-2.1/derniere/lrq-c-a-2.1.html>.

435 Yves D. DUSSAULT, *Modifications au régime de protection des renseignements personnels*, Texte présenté lors du Colloque du Barreau du Québec intitulé "Vie privée et protection des renseignements personnels", le 23 novembre 2006, p. 10.

Entente écrite.
La collecte visée au deuxième alinéa s'effectue dans le cadre d'une entente écrite transmise à la Commission. L'entente entre en vigueur 30 jours après sa réception par la Commission. »[436]

Donc, suivant certaines conditions, un organisme public peut demander à un autre organisme public de recueillir pour lui des renseignements personnels et ce afin d'éviter la collecte répétitive de renseignements personnels par chacun des organismes publics avec lequel il collabore. Pour ce faire, les organismes doivent collaborer pour la prestation de services ou la réalisation d'une mission commune et la collecte de renseignements personnels qui serviront aux organismes dans ce cadre doit s'effectuer au sein d'une entente écrite transmise à la CAI qui entrera en vigueur 30 jours après sa réception. L'entente n'a pas à faire l'objet d'une autorisation ; la CAI n'a qu'à être informée de l'existence du cadre dans lequel les organismes impliqués recueilleront et partageront des renseignements personnels. Selon les auteurs Doray et Charette,

> « on peut donc penser que les organismes qui sont appelés couramment à collaborer entre eux devraient transmettre à la Commission une entente cadre qui pourra servir éventuellement lorsque des situations particulières requerrant leur collaboration se produiront. Il ne saurait selon nous être requis de soumettre à la Commission une entente pour chaque intervention ponctuelle, d'autant plus que le délai de 30 jours avant l'entrée en vigueur de l'entente risquerait dans bien des cas de compromettre l'efficacité de la collaboration ou de la mission commune »[437].

---

436 Art. 64 de la *Loi sur l'Accès aux documents des organismes publics et sur la protection des renseignements personnels*, L.R.Q., c. A-2.1, 2006, c. 22, en ligne : <http://canlii.org/fr/qc/legis/lois/lrq-c-a-2.1/derniere/lrq-c-a-2.1.html>.

437 Raymond DORAY et François CHARETTE, *Accès à l'information, Loi annotée, Jurisprudence Analyse et commentaires*, volume 1, mis à jour au 10 décembre 2008, Cowansville, Éditions Yvon Blais, 2001, p. III/64-9.

Ce type de collecte doit faire l'objet d'une inscription au registre suivant 67.3[438] de la *Loi sur l'accès* et est soumise aux obligations d'informer la personne concernée selon l'article 65 de la même loi[439].

Cette collaboration en matière de collecte de renseignements personnels implique, selon Doray et Charette, que ces renseignements soient partagés, si nécessaire, entre les organismes qui collaborent à la prestation de services. L'article 62 de la *Loi sur l'accès*[440] permet de déterminer qui au sein des divers organismes impliqués serait autorisé à prendre connaissance des renseignements étant donné qu'ils sont nécessaires à l'exercice de leurs fonctions. Et rien n'interdit, selon ces auteurs, l'application de cet article 64 al. 2 de la *Loi sur l'accès*[441] à plus de deux organismes publics[442]. Donc, l'article 64 al. 2 sus mentionné permet la col-

---

438 Art. 67.3 de la *Loi sur l'Accès aux documents des organismes publics et sur la protection des renseignements personnels*, L.R.Q., c. A-2.1, 2006, c. 22. en ligne : <http://canlii.org/fr/qc/legis/lois/lrq-c-a-2.1/derniere/lrq-c-a-2.1.html>. Dans le cas d'une entente portant sur la collecte de renseignements personnels, le registre comprend :

1° le nom de l'organisme pour lequel les renseignements sont recueillis ;

2° l'identification du programme ou de l'attribution pour lequel les renseignements sont nécessaires ;

3° la nature ou le type de la prestation de service ou de la mission ;

4° la nature ou le type de renseignements recueillis ;

5° la fin pour laquelle ces renseignements sont recueillis ;

6° la catégorie de personnes, au sein de l'organisme qui recueille les renseignements et au sein de l'organisme receveur, qui a accès aux renseignements.

439 Art. 65 de la *Loi sur l'Accès aux documents des organismes publics et sur la protection des renseignements personnels*, L.R.Q., c. A-2.1, 2006, c. 22, en ligne : <http://canlii.org/fr/qc/legis/lois/lrq-c-a-2.1/derniere/lrq-c-a-2.1.html>.

440 Art. 62 de la *Loi sur l'Accès aux documents des organismes publics et sur la protection des renseignements personnels*, L.R.Q., c. A-2.1, 2006, c. 22, en ligne : <http://canlii.org/fr/qc/legis/lois/lrq-c-a-2.1/derniere/lrq-c-a-2.1.html>.

441 Art. 64 al.2 de la *Loi sur l'Accès aux documents des organismes publics et sur la protection des renseignements personnels*, L.R.Q., c. A-2.1, 2006, c. 22, en ligne : <http://canlii.org/fr/qc/legis/lois/lrq-c-a-2.1/derniere/lrq-c-a-2.1.html>.

442 Raymond DORAY et François CHARETTE, *Accès à l'information, Loi annotée, Jurisprudence Analyse et commentaires*, volume 1, mis à jour au 10 décembre 2008, Cowansville, Éditions Yvon Blais, 2001, p. III/64-8.

lecte et le partage de renseignements personnels lorsqu'il y a collaboration entre organismes pour la prestation de services.

2 – Ententes de communication

Au Québec, le régime des ententes de partage de renseignements personnels est défini plus précisément aux articles 67.2 et suivants de la *Loi sur l'accès*[443].

Des ententes doivent encadrer la transmission d'informations personnelles aux fins de l'accomplissement d'un mandat ou d'un contrat de service. L'article 67.2 de la *Loi sur l'accès* prévoit qu'un organisme public peut, sans le consentement de la personne concernée, communiquer un renseignement personnel à toute personne ou organisme si cette communication est nécessaire à **l'exercice d'un mandat ou à l'exécution d'un contrat de service ou d'entreprise** confié par l'organisme public à cette personne ou à cet organisme. Dans un tel cas, l'organisme public doit : premièrement, confier ce mandat ou le contrat par écrit et deuxièmement y consigner un ensemble d'indications. L'organisme doit indiquer, dans ce mandat ou contrat, les dispositions de la loi qui s'appliquent au renseignement qui a été communiqué ainsi que les mesures qu'il faut prendre pour en assurer le caractère confidentiel et pour que ce renseignement ne soit utilisé que dans l'exercice du mandat ou l'exécution du contrat. Il faut préciser que les renseignements personnels seront détruits après l'expiration du mandat. En outre, l'organisme public doit, avant la communication, obtenir un engagement de confidentialité complété par toute personne à qui le renseignement peut être communiqué, à moins que le responsable de la protection des renseignements personnels n'estime que cela ne soit pas nécessaire. Une personne ou un organisme qui exerce un tel mandat ou qui exécute un tel contrat de service doit aviser, sans délai, le responsable de toute violation ou tentative de violation par toute

---

443 Art. 67.2 de la *Loi sur l'Accès aux documents des organismes publics et sur la protection des renseignements personnels*, L.R.Q., c. A-2.1, 2006, c. 22, en ligne : <http://canlii.org/fr/qc/legis/lois/lrq-c-a-2.1/derniere/lrq-c-a-2.1.html>.

personne de l'une ou l'autre des obligations relatives à la confidentialité du renseignement communiqué et doit également permettre au responsable d'effectuer toute vérification relative à cette confidentialité.

Le registre consignant les ententes de partage d'informations personnelles comprend des précisions sur :

1° la nature ou le type des renseignements communiqués ;

2° la personne ou l'organisme qui reçoit cette communication ;

3° la fin pour laquelle ce renseignement est communiqué et l'indication, le cas échéant, qu'il s'agit d'une communication visée à l'article 70.1 ;

4° la raison justifiant cette communication ;

Par cet article 67.2, le législateur a voulu, selon Doray et Charette, « que les organismes publics, en raison de la confidentialité des renseignements personnels, ne soient pas empêchés de confier à des tiers ou à d'autres organismes publics des tâches qu'ils ne sont pas en mesure d'accomplir eux-mêmes ou que d'autres pourraient effectuer à meilleur coût, de manière plus efficace ou avec une expertise appropriée. »[444] Donc, cette communication de renseignements personnels prévue à 67.2 de la *Loi sur l'accès* est entourée de conditions : le mandat ou le contrat de service doit être confié par écrit, il doit contenir les diverses mentions relatives à la protection des renseignements personnels[445], la communication doit être inscrite dans le registre et donc sujette au pouvoir de vérification a posteriori de la CAI. La communication ne nécessite pas le consentement de la personne, ni d'avis ou d'entente préalable à la CAI, mais plutôt une inscription dans le

---

444 Raymond DORAY et François CHARETTE, *Accès à l'information, loi annotée, jurisprudence et commentaires*, Cowansville, Éditions Yvon Blais, 2002, p. III/67.2.2.

445 Sauf si le mandat ou le contrat de service lie deux organismes publics (art. 67.2 al. 3 de la *Loi sur l'Accès aux documents des organismes publics et sur la protection des renseignements personnels*, L.R.Q., c. A-2.1, 2006, c. 22, en ligne : <http://canlii.org/fr/qc/legis/lois/lrq-c-a-2.1/derniere/lrq-c-a-2.1.html>).

registre (donc sujette au pouvoir de vérification a posteriori de la CAI)[446].

---

[446] L'article 69.0.0.17 de la *Loi sur le ministère du Revenu* introduit aussi des règles concernant la communication de renseignements fiscaux lors de l'octroi de contrats de services. La personne qui exécute le contrat est assujettie à des obligations telles prendre des mesures nécessaires pour assurer la confidentialité du renseignement communiqué, compléter un engagement de confidentialité, n'utiliser le renseignement que dans l'exécution du contrat, ne pas transporter de renseignements à l'extérieur des locaux du ministère du Revenu lorsque le contrat est exécuté dans les locaux de celui-ci, etc. Le contrat doit également faire l'objet d'une inscription dans un registre, qui est accessible à la personne qui en fait la demande. Lors de l'adoption du projet de loi, le ministre du Revenu, M. Guy Julien mentionnait « que l'octroi de ces contrats sera rigoureusement gouverné par des règles strictes relatives aux renseignements fiscaux, règles de protection qui, je me permets de le rappeler, sont beaucoup plus exigeantes que celles prévues par la Loi sur l'accès. » (*Journal des débats*, 36e législature, 2e session, 7 mai 2002).

Quant à la LSSSS, les nouveaux articles 27.1 et 27.2 permettent la communication de renseignements contenus dans le dossier de l'usager à toute personne si cela est nécessaire à l'exercice d'un mandat ou à l'exécution contrat de service suivant un certain nombre de balises devant impérativement être précisées et mises en place avant que les renseignements ne puissent circuler. Par exemple, le mandat ou le contrat doit être par écrit et à durée déterminée ; des clauses contractuelles sont obligatoires sous peine de nullité pour couvrir la cueillette, la circulation et la durée de conservation des renseignements ainsi que les obligations de l'exécutant ; le tiers retenu par la personne ou l'organisme doit être soumis aux mêmes obligations que l'exécutant et enfin, la tenue d'un registre est obligatoire. Ces nouvelles dispositions s'appliquent dans les circonstances suivantes : lors de mandat ou de contrat de service à durée déterminée sauf la prestation de certains services de santé et services sociaux, lors de l'agrément des services (art. 107.1 LSSSS), lors de la dispensation, pour le compte de l'établissement, de certains services de santé ou services sociaux requis par un usager de cet établissement, lors de la préparation centralisée de certains médicaments (108 al. 3 LSSSS) et lors de la gestion des ressources informationnelles ou support technologique (art. 520.3.1 LSSSS). Pour plus de détails, voir Christiane LEPAGE, « La protection de l'information confidentielle dans le contexte de la « réingénierie » » dans Service de la formation continue du Barreau du Québec, Après le projet de loi 83 : un nouveau réseau de la santé, volume 260, Cowansville, Éditions Yvon Blais, 2006, p. 220-237.

Lors de la modification de cet article en 2006, la CAI s'est inquiétée que cette disposition ouvre la porte à l'échange de renseignements personnels sans aucune intervention de sa part chaque fois qu'un contrat de service est conclu entre deux organismes publics[447] :

> La CAI estime que l'article 67.2 pourra servir de plus en plus à appuyer la légalité des communications de renseignements personnels entre organismes publics. Avec le temps, les mécanismes de communication de renseignements personnels établis par les articles 68 et 68.1, mécanismes où l'avis de la CAI est requis, risquent peu à peu d'être écartés. Ces préoccupations de la CAI s'appuient également sur l'adoption récente de la *Loi sur Services Québec* et de la *Loi sur le Centre de services partagés du Québec*.

En effet, la communication de renseignements personnels aux fins de comparaison de fichiers (**art. 68.1** de la *Loi sur l'accès*[448]) et la communication administrative (**art. 68** de la *Loi sur l'accès*[449]) nécessitent une entente écrite soumise à la CAI[450]. Ainsi,

---

447 C.A.I., Mémoire de la Commission d'accès à l'information concernant le projet de loi non 86, présenté à la Commission parlementaire de la culture, septembre 2005, p. 12 et 13.

448 Art. 68.1 de la *Loi sur l'Accès aux documents des organismes publics et sur la protection des renseignements personnels*, L.R.Q., c. A-2.1, 2006, c. 22, en ligne : <http://canlii.org/fr/qc/legis/lois/lrq-c-a-2.1/derniere/lrq-c-a-2.1.html>.

449 Art. 68 de la *Loi sur l'Accès aux documents des organismes publics et sur la protection des renseignements personnels*, L.R.Q., c. A-2.1, 2006, c. 22, en ligne : <http://canlii.org/fr/qc/legis/lois/lrq-c-a-2.1/derniere/lrq-c-a-2.1.html>.

450 Quoique circonscrites, il existe plusieurs exceptions à la règle de confidentialité des renseignements contenus dans un dossier fiscal. Essentiellement, les articles 69.0.1 et 69.1 de la *Loi sur le ministère du Revenu* précisent les personnes et organismes à qui peuvent être communiqués des renseignements fiscaux à certaines conditions mais sans le consentement de la personne concernée (ex : contrôleur des finances, vérificateur général, ministre des Finances, ministre des Ressources naturelles et de la Faune, Commission des normes du travail, ministre de l'Emploi et de la Solidarité sociale, Protecteur du citoyen, Institut de la statistique du Québec, Régie de l'assurance maladie du Québec, Régie des rentes du Québec, ministre de l'Éducation, Commission des transports du Québec, Régie de l'énergie, Société de

l'article 68 par. (1°) de la *Loi sur l'accès*[451] indique qu'un organisme public peut communiquer un renseignement personnel « à un organisme d'un autre gouvernement lorsque cette communication est **nécessaire à l'exercice des attributions de l'organisme receveur ou à la mise en œuvre d'un programme dont cet organisme a la gestion** ». Dans le même esprit, l'article 68 par. (1.1°) de la même loi[452] prévoit qu'un organisme public peut communiquer un renseignement personnel « à un organisme d'un autre gouvernement lorsque la communication est manifestement au **bénéfice de la personne concernée** ». Rappelons également que l'article 68 par. (3°) de ladite loi[453] autorise la communication d'un

---

l'assurance automobile du Québec, ministre de l'agriculture, des Pêcheries et de l'Alimentation, ministre ou organisme à qui incombe la responsabilité de rendre une décision pour l'application d'une loi fiscale…) Ces personnes ou ces organismes sont assujettis à des règles qui limitent à des fins précises la communication et l'utilisation de tels renseignements. Généralement, ces communications ne peuvent se faire que dans le cadre d'une entente écrite soumise à la C.A.I. pour avis (art. 69.8). L'entente, ou s'il n'y a pas d'entente, toute communication de fichiers de renseignements personnels, doit être inscrite dans un registre (art. 71.0.7). Le ministre doit informer annuellement la personne au sujet de laquelle il recueille des renseignements de la possibilité que des renseignements soient transmis à d'autres personnes conformément à la présente loi. (art. 70.1).

Aussi, un organisme doit fournir au ministre tout renseignement si cela est nécessaire à l'application ou à l'exécution d'une loi fiscale et le ministre doit dresser un plan d'utilisation de tout fichier de renseignements à des fins de comparaison, de couplage ou d'appariement et le soumettre pour avis à la C.A.I. (art. 71 et 71.0.3). La demande de fichiers de renseignements doit être inscrite dans un registre (art. 71.0.7). Le ministre doit informer annuellement la personne concernée de la possibilité que des comparaisons, des couplages ou des appariements de fichiers de renseignements soient effectués dans le cadre de l'application d'une loi fiscale (art. 70.1).

451 Art. 68 (1) de la *Loi sur l'Accès aux documents des organismes publics et sur la protection des renseignements personnels*, L.R.Q., c. A-2.1, 2006, c. 22, en ligne : <http://canlii.org/fr/qc/legis/lois/lrq-c-a-2.1/derniere/lrq-c-a-2.1.html>.

452 Art. 68 (1.1) de la *Loi sur l'Accès aux documents des organismes publics et sur la protection des renseignements personnels*, L.R.Q., c. A-2.1, 2006, c. 22, en ligne : <http://canlii.org/fr/qc/legis/lois/lrq-c-a-2.1/derniere/lrq-c-a-2.1.html>.

453 Art. 68 (3) de la *Loi sur l'Accès aux documents des organismes publics et sur la protection des renseignements personnels*, L.R.Q., c. A-2.1, 2006, c. 22, en ligne : <http://canlii.org/fr/qc/legis/lois/lrq-c-a-2.1/derniere/lrq-c-a-2.1.html>.

renseignement personnel « à une personne ou à un organisme si cette communication est nécessaire dans le cadre de la prestation d'un service à rendre à la personne concernée par un organisme public, notamment aux fins de **l'identification de cette personne** ».

Dans ces cas susmentionnés, la communication s'effectue dans le cadre d'une entente écrite. Cette entente doit être soumise à la Commission pour avis[454]. Lorsqu'elle est appelée à donner son avis à l'égard d'une entente de partage de renseignements personnels, la Commission doit prendre en considération la conformité de l'entente aux conditions visées à l'article 68 ou à l'article 68.1 de la *Loi sur l'accès*[455], c'est-à-dire que le partage porte bien sur une situation ou la communication est nécessaire à l'exercice des attributions de l'organisme receveur ou à la mise en œuvre d'un programme dont cet organisme a la gestion. Dans d'autres situations, il faudra s'assurer que la communication est au bénéfice de la personne concerné ou est nécessaire à l'application d'une loi.

La loi commande également à la Commission de considérer l'impact de la communication du renseignement sur la vie privée de la personne concernée, le cas échéant, par rapport à la nécessité du renseignement pour l'organisme ou la personne qui en reçoit communication.

La Commission doit rendre un avis motivé dans un délai d'au plus 60 jours de la réception de la demande d'avis accompagnée de l'entente. Si la demande est modifiée pendant ce délai, celui-ci court à compter de la dernière demande. Si le traitement de la demande d'avis dans ce délai ne lui paraît pas possible sans nuire au déroulement normal des activités de la Commission, le président peut, avant l'expiration de ce délai, le prolonger d'une période

---

454 Art. 70 de la *Loi sur l'Accès aux documents des organismes publics et sur la protection des renseignements personnels*, L.R.Q., c. A-2.1, 2006, c. 22, en ligne : <http://canlii.org/fr/qc/legis/lois/lrq-c-a-2.1/derniere/lrq-c-a-2.1.html>.

455 Art. 68 et 68.1 de la *Loi sur l'Accès aux documents des organismes publics et sur la protection des renseignements personnels*, L.R.Q., c. A-2.1, 2006, c. 22, en ligne : <http://canlii.org/fr/qc/legis/lois/lrq-c-a-2.1/derniere/lrq-c-a-2.1.html>.

n'excédant pas 20 jours. Il doit alors en donner avis aux parties à l'entente dans le délai de 60 jours.

L'entente entre en vigueur sur avis favorable de la Commission ou à toute date ultérieure prévue à l'entente. La Commission doit rendre publics cette entente ainsi que son avis. À défaut d'avis dans le délai prévu, les parties à l'entente sont autorisées à procéder à son exécution.

En cas d'avis défavorable de la Commission, le gouvernement peut, sur demande, approuver cette entente et fixer les conditions applicables. Avant d'approuver l'entente, le gouvernement publie à la Gazette officielle du Québec l'entente et, le cas échéant, les conditions qu'il entend fixer avec un avis qu'il pourra approuver l'entente à l'expiration d'un délai de 30 jours de cette publication et que tout intéressé peut, durant ce délai, transmettre des commentaires à la personne qui y est désignée. L'entente entre en vigueur le jour de son approbation ou à toute date ultérieure fixée par le gouvernement ou prévue à l'entente. Une telle entente ainsi que l'avis de la Commission et l'approbation du gouvernement sont déposés à l'Assemblée nationale dans les 30 jours de cette approbation si l'Assemblée est en session ou, si elle ne siège pas, dans les 30 jours de la reprise de ses travaux. Le gouvernement peut révoquer en tout temps une telle entente[456].

Bien qu'ils aient un droit d'accès aux registres compilant les ententes de partage de renseignements personnels, les citoyens ne sont pas systématiquement informés des conséquences que de telles ententes peuvent avoir sur la communication secondaire de renseignements personnels qu'ils sont appelés à fournir. Il n'y a pas de processus public d'évaluation afin d'apprécier les impacts, les risques et enjeux que ces échanges peuvent comporter.

Il nous semble par ailleurs important de souligner qu'au niveau fédéral, l'article 4.1.3 de l'Annexe 1 de PIPEDA impose à l'« organisation » (en l'occurrence l'administration) qui « est responsable

[456] Art. 70 de la *Loi sur l'Accès aux documents des organismes publics et sur la protection des renseignements personnels*, L.R.Q., c. A-2.1, 2006, c. 22, en ligne : <http://canlii.org/fr/qc/legis/lois/lrq-c-a-2.1/derniere/lrq-c-a-2.1.html>.

ou qui a la garde des renseignements personnels » de « fournir un degré comparable de protection aux renseignements qui sont en cours de traitement par une tierce partie » et ce « par voie contractuelle ou autre »[457].

Cette disposition pourrait nous faire penser qu'elle recoupe quelque peu le contenu des articles 67.2 et suivants de la *Loi sur l'accès* en ce qui concerne les protections d'ordre contractuel et les ententes de communication conclues avec la CAI. Néanmoins, cet article ne représente pas la portée généralisée de la mesure disponible dans la loi provinciale et il n'existe pas, au meilleure de notre connaissance, d'équivalent ni dans PIPEDA ni dans d'autres lois.

Conclusion

Les précédents développements ont donc pour vertu de se prononcer sur le fait qu'en dépit du besoin accru en circulation des renseignements personnels, les lois visant à la protection de ces derniers disposent assurément de la souplesse nécessaire pour ce faire. Cette souplesse est surtout le fruit de règles interprétatives pluriséculaires qui sont pleinement capables de qualifier certaines opérations au-delà des opérations correspondantes dans les lois sur la protection des renseignements personnels. En revanche, la souplesse qui a été introduite par les lois, paradoxalement, n'est pas pleinement utilisable dans le cas des prestations en ligne qui nous intéressent. D'une part, le consentement est trop souvent la voie d'entrée vers une utilisation des données d'un individu sans que celui-ci n'ai pleinement conscience de ce à quoi il consent. D'autre part, plusieurs des autorisations ponctuelles que l'on trouve dans les lois étudiées sont à la fois, en certains cas, lourdes d'utilisation, et selon nous, de toutes les manières, en bien des cas, non nécessaires étant donné la réponse apportée dans la Partie 1 relative à l'interprétation.

---

[457] L'Annexe 1 de la *Loi sur la protection des renseignements personnels et les documents électroniques* (PIPEDA), en ligne : <http://www.canlii.ca/fr/ca/legis/lois/lc-2000-c-5/derniere/lc-2000-c-5.html>.

Mais de manière plus générale, de cette revue du cadre juridique relatif à la protection des renseignements personnels dans les services publics en ligne, il nous est possible de faire ressortir certains éléments d'un cadre juridique efficace pour la protection des renseignements personnels dans les plateformes de services gouvernementaux en ligne :

- **Reconnaître** les caractéristiques associées aux rôles et fonctions assurées par les différents acteurs dans la circulation des renseignements personnels.

  La circulation des renseignements personnels n'emporte pas toujours que ceux-ci sont communiqués. L'univers d'Internet présente un ensemble de cas de figure dans lesquels les différentes entités tiennent des rôles diversifiés. Par exemple, plutôt que de plaquer des consentements à tout propos comme si tous et chacun des acteurs avaient le droit de s'approprier les renseignements personnels qui transitent, il faut s'assurer que les obligations associées aux différents rôles tenus par chacune des entités soient explicites.

- **Assurer** que toutes les entités qui interviennent dans les différentes situations de partage de renseignements personnels soient tenues à des obligations de reddition de comptes de leurs faits et gestes, compte tenu du rôle qu'ils tiennent à l'égard de ces renseignements.

- **Informer** adéquatement les usagers de la nature des environnements dans lesquels ils interagissent et des risques inhérents à ceux-ci.

- **Requérir** le consentement à la communication des renseignements personnels uniquement dans les situations dans lesquelles il y a effectivement une communication de ces renseignements à une autre entité et que cette communication n'est pas inhérente à l'activité même dans laquelle sont communiquées les informations.

TABLEAU RÉCAPITULATIF DES OPÉRATIONS SUSCEPTIBLES DE SURVENIR LORS DE LA CIRCULATION DE RENSEIGNENTS PERSONNELS

Archiver	Activité consistant à préserver le **contenu intellectuel** de documents, et ce, de façon **permanente**. (ce terme n'existe en tant que tel dans aucune des lois concernant la protection des renseignements personnels objet de la présente étude)
Collecte	La collecte de renseignements personnels s'entend comme une opération par laquelle des renseignements sont placés sous le contrôle d'une entité qui du fait de cette opération acquiert, à l'égard des documents ou renseignements, le droit d'en prendre connaissance. Pour qu'il y ait « collecte » de renseignements ou de documents, il faut que ces documents ou renseignements aient été communiqués à une entité, ou à une personne qui a le **droit** d'en prendre connaissance. **(Voir notamment les articles 65 et 67.3 de la Loi sur l'Accès aux documents des organismes publics et sur la protection des renseignements personnels,** L.R.Q. c. A-2.1, 2006, c. 22. en ligne : <http://canlii.org/fr/qc/legis/lois/lrq-c-a-2.1/derniere/lrq-c-a-2.1.html>, **et l'article 7(3) c1) ii) de Loi sur la protection des renseignements personnels et les documents électroniques (PIPEDA) et les articles 4.2 à 4.2.6 et 4.3, 4.3.1, 4.3.3 et 4.3.7 de l'Annexe 1 de ladite loi** disponible à http ://www.canlii.ca/fr/ca/legis/lois/lc-2000-c-5/derniere/lc-2000-c-5.html. **et l'article 14 de Loi sur la Protection des renseignements personnels dans le secteur privé,** L.R.Q. c. P-39.1 disponible à http ://canlii.ca/fr/qc/legis/lois/lrq-c-p-39.1/derniere/lrq-c-p-39.1.html**)**

Communication	Communiquer un renseignement ou un document implique de conférer un droit de prendre **connaissance** de la teneur du document ou du renseignement. Si le document est mis en possession physique ou juridique d'une entité, cela ne signifie pas pour autant que celle-ci ait obtenu communication du document ou du renseignement. **(Voir notamment les articles 65, 67, 67.2, 67.3, 68, 68.1 et 88 de la Loi sur l'Accès aux documents des organismes publics et sur la protection des renseignements personnels,** L.R.Q. c. A-2.1, 2006, c. 22. en ligne : <http://canlii.org/fr/qc/legis/lois/lrq-c-a-2.1/derniere/lrq-c-a-2.1.html>, **et l'article 7(3) a) , c1) ii) et f) de Loi sur la protection des renseignements personnels et les documents électroniques (PIPEDA) et les articles 4.2.6, 4.3, 4.3.1, 4.3.3, 4.5 et 4.7.1 de l'Annexe 1 de ladite loi** en ligne : <http://www.canlii.ca/fr/ca/legis/lois/lc-2000-c-5/derniere/lc-2000-c-5.html>. **et l'article 14 de Loi sur la Protection des renseignements personnels dans le secteur privé,** L.R.Q. c. P-39.1 en ligne : <http://canlii.ca/fr/qc/legis/lois/lrq-c-p-39.1/derniere/lrq-c-p-39.1.html> **et les articles 22, 27, 28, 34 et 36 de la Loi concernant le cadre juridique des technologies de l'information.** L.R.Q. c. C-1.1, en ligne : <http://www.canlii.org///qc/legis/loi/c-1.1/20080818/tout.html>**)**

Conservation	La **conservation** est l'action de maintenir l'intégrité d'un document, que celui-ci contienne – ou non – des renseignements personnels, et ce, durant toute la durée active du document afin que ce dernier demeure accessible. **(Voir notamment les articles 7(3) g) de Loi sur la protection des renseignements personnels et les documents électroniques (PIPEDA) et les articles 4.2.6, 4.5, 4.5.2 et 4.7.2 de l'Annexe 1 de ladite loi** en ligne : <http://www.canlii.ca/fr/ca/legis/lois/lc-2000-c-5/derniere/lc-2000-c-5.html>. **et les articles 22 et 26 de la Loi concernant le cadre juridique des technologies de l'information.** L.R.Q. c. C-1.1, en ligne : <http://www.canlii.org///qc/legis/loi/c-1.1/20080818/tout.html>**)**
Détention	La détention est un terme qui émane non pas du domaine de la gestion documentaire mais de la protection des renseignements personnels. Elle correspond à la situation selon laquelle un organisme est **responsable juridiquement** du support sur lequel est consigné un ou des renseignements personnels. Le terme de détention, dans une perspective de gestion documentaire – et non de mise en application du devoir de transparence en fonction des dispositions de la *Loi sur l'accès* – doit être distingué de la possession physique que ne signifie plus grand chose dans une perspective de gestion électronique. **(Voir notamment l'article 1 al.1 de la Loi sur l'Accès aux documents des organismes publics et sur la protection des renseignements personnels,** L.R.Q. c. A-2.1, 2006, c. 22. en ligne : <http://canlii.org/fr/qc/legis/lois/lrq-c-a-2.1/derniere/lrq-c-a-2.1.html>)

Donner accès

L'accès à des renseignements personnels est assujetti à des limites et il importe de se dissocier de la croyance correspondant à un certain « sens commun » selon laquelle dès lors qu'on est en « possession » physique d'un document, on a le droit d'en prendre connaissance. L'article 25 de la *Loi concernant le cadre juridique des technologies de l'information* réaffirme au contraire que l'obligation de contrôler doit être effectuée par la personne responsable, personne qui n'est pas forcément celle qui gère « physiquement » le document en cause. Cette Loi lui impose plutôt l'obligation de voir à ce que les moyens technologiques convenus soient mis en place pour en assurer la sécurité, en préserver l'intégrité et, le cas échéant, en protéger la confidentialité.

(Voir notamment l'article 63.1 de la Loi sur l'Accès aux documents des organismes publics et sur la protection des renseignements personnels, L.R.Q. c. A-2.1, 2006, c. 22. en ligne : <http://canlii.org/fr/qc/legis/lois/lrq-c-a-2.1/derniere/lrq-c-a-2.1.html>, **et l'article 4.7.3 de l'Annexe 1de Loi sur la protection des renseignements personnels et les documents électroniques (PIPEDA)** disponible à http://www.canlii.ca/fr/ca/legis/lois/lc-2000-c-5/derniere/lc-2000-c-5.html.**et l'article 25 de la Loi concernant le cadre juridique des technologies de l'information.** L.R.Q. c. C-1.1, en ligne : <http://www.canlii.org///qc/legis/loi/c-1.1/20080818/tout.html>**)**

Garde

La garde telle que décrite à l'article 26 de la *Loi concernant le cadre juridique des technologies de l'information* est une sous-catégorie de la conservation qui dispose de mesures de sécurité passablement plus rigoureuses que la seule obligation du respect de l'intégrité que l'on retrouve à l'article 22 de la même loi. L'opération de garde constitue donc une hypothèse de conservation à laquelle on associe une obligation sécuritaire de la part du prestataire suite à l'information en ce sens faite par l'intéressé.
(Voir notamment les articles 22, et 26 de la Loi concernant le cadre juridique des technologies de l'information. L.R.Q. c. C-1.1, en ligne : <http://www.canlii.org///qc/legis/loi/c-1.1/20080818/tout.html>**)**

Hébergement

Le terme d'hébergement, ni défini ni évoqué dans aucune loi, correspond à la réalisation d'une activité de conservation par un tiers, et ce, relativement à une réalité assez précise à savoir celle pour un prestataire de mettre à disposition des internautes des espaces web conçus et gérés par ces mêmes tiers.
(ce terme n'existe en tant que tel dans aucune des lois concernant la protection des renseignements personnels objet de la présente étude)

Possession

Le terme de **possession** est un terme uniquement générique qui ne bénéficie d'aucune utilisation à proprement parler dans les lois et qui ne correspond non plus à aucune signification particulière sur le plan technique. De ce fait, l'on devrait sans doute éviter de l'utiliser. Il semblerait néanmoins avoir une compréhension très globale.
(Voir notamment l'article 4.1.3 de l'Annexe 1 de Loi sur la protection des renseignements personnels et les documents électroniques (PIPEDA) disponible à http ://www.canlii.ca/fr/ca/legis/lois/lc-2000-c-5/derniere/lc-2000-c-5.html.**)**

Transmission Transmettre un document, c'est l'expédier d'un point d'expédition à un point de réception. C'est le faire passer **techniquement** d'un point à l'autre. En d'autres mots, et pour reprendre une image préalablement évoquée, la transmission est au « support » ce que la communication est à l'« information ».
(Voir notamment les articles 28, 34 et 36 de la Loi concernant le cadre juridique des technologies de l'information. L.R.Q. c. C-1.1, en ligne : <http://www.canlii.org///qc/legis/loi/c-1.1/20080818/tout.html>**)**

Utilisation Utiliser des renseignements personnels implique d'en avoir **connaissance** et de décider d'agir ou non à la lumière de la connaissance que ces renseignements confèrent.
(**Voir notamment les articles 55, 59, 63.1, 65.1, 67.2, 67.3, 68, et 72 de la Loi sur l'Accès aux documents des organismes publics et sur la protection des renseignements personnels,** L.R.Q. c. A-2.1, 2006, c. 22. en ligne : <http://canlii.org/fr/qc/legis/lois/lrq-c-a-2.1/derniere/lrq-c-a-2.1.html>, **et les articles 4(1), 4(1)a) , 4(1)b), 4(2), 4(2)b), 4(2)c), 5(3), 7(2), 7(2)a), 7(2)b), 7(2)c), et 7(4) de Loi sur la protection des renseignements personnels et les documents électroniques (PIPEDA) et les articles 4.2.4, 4.2.6, 4.3, 4.3.1, 4.3.2, 4.3.3, 4.3.7 a) et b), 4.5, 4.6.1 et 4.7.1 de l'Annexe 1 de ladite loi** disponible à http ://www.canlii.ca/fr/ca/legis/lois/lc-2000-c-5/derniere/lc-2000-c-5.html.
et les articles 11 et 14 de Loi sur la Protection des renseignements personnels dans le secteur privé, L.R.Q. c. P-39.1 en ligne : <http://canlii.ca/fr/qc/legis/lois/lrq-c-p-39.1/derniere/lrq-c-p-39.1.html>
et les articles 19 et 22 de la Loi concernant le cadre juridique des technologies de l'information. L.R.Q. c. C-1.1, en ligne : <http://www.canlii.org///qc/legis/loi/c-1.1/20080818/tout.html>