GOUVERNEMENT ÉLECTRONIQUE ET INTERCONNEXION DE FICHIERS ADMINISTRATIFS DANS L'ÉTAT EN RÉSEAU

Pierre Trudel*

Sommaire

* Pierre Trudel, professeur titulaire de la Chaire L. R. Wilson sur le droit des technologies de l'information et du commerce électronique <chairelrwilson.net >, Centre de recherche en droit public, Faculté de droit, Université de Montréal, <pierre.trudel@umontreal.ca>.
Article reçu le 31.05.2007

La mutation de l'État découle notamment de l'avènement des technologies de réseaux. L'avènement du e-gouvernement est emblématique des mutations induites dans le droit par le recours aux technologies de l'information afin d'assurer le fonctionnement des services gouvernementaux. L'univers postmoderne caractéristique des pays touchés par la révolution numérique à des échos dans la morphologie du droit[1]. Il en résulte une redéfinition des conditions de l'intervention juridique et des façons de concevoir le droit. Une telle redéfinition concerne au premier chef les pratiques relatives à la protection des données personnelles détenues par l'Administration.

La présente étude est réalisée selon la perspective canadienne. Le Canada est un État fédéral. Les textes constitutionnels partagent la totalité des pouvoirs d'adopter des lois entre le Parlement fédéral et les législatures des provinces[2]. En accord avec la tradition de gouvernement parlementaire britannique introduite au Canada au XVIII^e^ siècle, les ministères sont responsables des documents et informations qui sont en leur possession. L'avènement des services en ligne présente un défi additionnel : celui d'assurer des services intégrés à l'égard de matières qui peuvent relever de la compétence d'entités appartenant à des niveaux multiples de gouvernement.

Envisagées du point de vue des citoyens et des administrés, les interactions avec les instances étatiques relevant du Parlement fédéral et des législatures provinciales supposent de multiples échanges d'information. Par exemple, pour se procurer un passeport, le citoyen canadien doit présenter des informations permettant de confirmer sa citoyenneté. Pour ce faire, il sera nécessaire de produire un document de l'état civil émanant habituellement d'autorités relevant des provinces. Cela n'est qu'un exemple des multiples situations dans lesquelles sont impliquées une pluralité d'instances gouvernementales relevant de l'état fédéral ou d'une province. Dans leurs champs respectifs de compétences, les provinces et le Parlement fédéral ont adopté des lois relatives à la protection des données personnelles. La protection des données personnelles est régie par des textes qui distinguent entre le secteur privé et le secteur public. Les mécanismes de protection minimales sont édictés dans les textes relatifs au secteur privé. Des

1. Jacques Chevallier, *L'État post-moderne*, 2e édition, Paris LGDJ, 2004 ; Charles-Albert Morand, *Le droit néo-moderne des politiques publiques*, Paris LGDJ, 2000.

2. Henri Brun et Guy Tremblay, *Droit constitutionnel*, 3e édition, Cowansville, Éditions Yvon Blais, 1997, p. 457 et ss.

protections renforcées découlent des lois s'appliquant aux entités relevant de l'État ou du secteur public.

Afin de rendre compte des cadres juridiques relatifs à l'interconnexion des fichiers administratifs dans l'État en réseau, il importe dans un premier temps de rappeler les impératifs du gouvernement en ligne. Ensuite, il est fait état des exigences relatives à la protection des renseignements personnels pour enfin présenter le régime juridique des échanges de données prévu par les lois sur la protection des données personnelles. Dans une dernière partie, sont présentés des modèles émergents de mécanismes juridiques destinés à assurer le partage balisé des données personnelles entre une pluralité d'entités de l'État.

1. Les impératifs du gouvernement en ligne

Les enjeux clés qui marquent le développement du droit relatif au e-gouvernement concernent l'ajustement des principes juridiques ayant vocation à encadrer les interactions en ligne. Le cadre juridique du e-gouvernement est marqué par les visions managériales de l'État[3]. Les politiques d'implantation du gouvernement en ligne ou du « gouvernement en direct » sont conçues selon une logique de reconfiguration de l'offre des services de l'État en fonction d'une approche fondée sur le citoyen envisagé comme un « client ».

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[4]. 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. Un second facteur tient au besoin accru pour de l'expertise de même que des capacités accrues de partager l'information. Cela porte à

3. Jacques Chevallier, « La juridicisation des préceptes managériaux », [1993] 11 *Politique et management public*, 111-134.

4. Kenneth Kernaghan and Justin Gunraj, « Integrating information technology into public administration : Conceptual and practical considerations,» [2004] *47 Canadian Public Administration*, 525-546.

la création d'entités non ministérielles; c'est ainsi qu'au Canada, on a créé des « agences » se présentant comme des structures qui posséderaient des caractéristiques plus adaptées à l'accomplissement de fonctions horizontales. Un troisième facteur de changement serait le déplacement d'une partie du niveau intermédiaire de gestion au profit d'une 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 données personnelles détenues par l'Administration gouvernementale.

Les interconnexions sont une composante marquante de l'État en réseau. Les échanges d'information y sont constants et il ne peut être tenu pour acquis que ces échanges se déroulent sur un espace territorial ou organisationnel déterminé. Par exemple, le fonctionnement de la plupart des services en ligne est fondé sur l'hypertexte. Cela permet et généralise les possibilités d'intercréativité, d'interrelations, et de croisement d'informations. Les informations sont désormais situées à la fois ici et ailleurs dans un même temps, voire sur un même ou sur plusieurs écrans d'ordinateurs, de téléviseurs, de radios numériques ou de téléphones portables. Un tel environnement suppose un partage accru mais balisé d'informations.

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. Cela invite à une attitude réaliste tenant compte aussi bien des avantages de la circulation des informations que de ses inconvénients.

2. Les impératifs de protection de la vie privée et des données personnelles

La protection de la vie privée et des données personnelles est usuellement identifiée comme l'un des enjeux majeurs du développement du e-gouvernement. Au niveau fédéral, la *Loi sur la protection de renseignements personnels,* entrée en vigueur le 1er juillet 1983, organise la protection des renseignements personnels dans le secteur public fédéral[5]. Elle poursuit le double objectif de protéger les renseignements personnels[6], en limitant leur collecte, leur utilisation et leur communication, et d'assurer le droit d'accès et de correction des individus aux renseignements personnels les concernant[7] qui sont détenus par des organisations fédérales. Elle s'applique donc aux institutions fédérales, c'est-à-dire à tout ministère ou département d'État relevant du gouvernement du Canada, ou tout organisme figurant à l'annexe de la loi ce qui représente quelque 150 ministères et organismes fédéraux.

---

5. *Loi sur la protection des renseignements personnels*, L.R., 1985, ch. P-21.

6. L'expression « renseignements personnels », définie à l'article 3 de la loi, est interprétée comme suit dans *Dagg c. Canada (Ministre des Finances)*, [1995] 3 C.F. 199 (C.A.) et dans *Canada (Commissaire à l'information) c. Canada (Commissaire de la Gendarmerie royale du Canada)*, [2003] 1 R.C.S. 66: Les renseignements personnels s'entendent de tout renseignements concernant un individu identifiable relatifs à ses caractéristiques personnelles, à son éducation, à son dossier médical, à son casier judiciaire, à tout numéro ou symbole ou toute autre indication identificatrice, son adresse, ses empreintes digitales, son groupe sanguin, ses opinions ou ses idées personnelles, toute correspondance de nature implicitement ou explicitement privée ou confidentielle, des idées ou opinions d'autrui sur lui, son nom, lorsque celui-ci est mentionné avec d'autres renseignements le concernant ou lorsque la seule divulgation du nom révélerait des renseignements à son sujet. Dans la loi québécoise, la notion de renseignement personnel connaît une portée très large. L'article 54 indique que « dans un document sont personnels les renseignements qui concernent une personne physique et permettent de l'identifier » et ce sont ces renseignements qui sont déclarés par la loi « confidentiels à moins que leur divulgation ne soit autorisée par la personne qu'ils concernent ».

7. Ces deux objectifs sont énoncés dans ces décisions: *Dagg c. Canada (Ministre des Finances)*, [1997] 2 R.C.S. 403; *Lavigne c. Canada (Commissariat aux langues officielles)*, [2002] 2 R.C.S. 773

Les provinces et les territoires ont également adopté des lois sur la protection des renseignements personnels[8]. À l'instar de la législation fédérale, ces lois régissent la collecte, l'utilisation et la communication des renseignements personnels détenus par les organismes relevant des gouvernements provinciaux comme les gouvernements locaux. Elles confèrent aux personnes le droit de demander accès aux renseignements personnels les concernant et celui de les rectifier s'il y a lieu. La surveillance de l'application de ces lois est généralement assurée par un commissaire, un ombudsman ou une Commission indépendante qui est doté du pouvoir de recevoir les plaintes et de mener des enquêtes[9].

De ces textes législatifs, tant au niveau fédéral que provincial, ressortent différents principes relatifs au consentement, à la limitation de la cueillette, de l'utilisation et de la communication de renseignements personnels, aux droits d'accès et de correction des individus concernés par les renseignements et enfin, à l'exercice de recours indépendants.

Les exceptions au principe de la confidentialité des renseignements personnels sont limitées aux cas où les renseignements sont nécessaires pour lutter contre le crime, aux situations d'urgence mettant la sécurité ou la vie de la personne concernée en danger et à des fins d'étude ou de recherche. Les autres exceptions importantes à la confidentialité des renseignements personnels sont celles ayant trait aux ententes de transfert de tels renseignements entre organismes. Ce sont ces mécanismes qui paraissent avoir vocation à évoluer afin de refléter les impératifs de l'État en réseau.

---

8. Voici les principaux textes pour chacune des provinces et territoires: **Québec:** *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, (L.R.Q., c. A-2.1) ; **Ontario:** *Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c. F.31; *Municipal Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c. M.56; **Colombie-Britannique:** *Freedom of Information and Protection of Privacy Act*, R.S.B.C. 1996, c. 165; **Alberta:** *Freedom of Information and Protection of Privacy Act*, R.S.A 2000, c. F-25; **Saskatchewan:** *Freedom of Information and Protection of Privacy Act*, S.S. 1990-91, c. F-22.01; *The Local Authority Freedom of Information and the Protection of Privacy Act,* S.S. 1990-91, c. L-27.1; **Manitoba:** *Freedom of Information and Protection of Privacy Act*, S.M. 1997, c. 50; **Ile-du-Prince-Édouard:** Freedom of Information and Protection of Privacy Act, S.P.E. I. 2001, c. 37; **Nouveau-Brunswick:** *Protection of personal Information Act*, S.N.B. 1998, c. P-19.1; **Nouvelle-Écosse:** *Freedom of Information and Protection of Privacy Act,* S.N.S. 1993, c. 5; **Terre-Neuve, Labrador:** *Access to information and Protection of Privacy Act*, S.N. 2002, c. A-1.1; **Yukon:** *Access to information and Protection of Privacy Act*, R.S.Y 2002, c.1; **Nunavut:** *Access to Information and Protection of Privacy Act (Nunavut)*, S.N.W.T. 1994, c. 20; **Territoires du Nord-Ouest:** *Access to Information and Protection of Privacy Act*, S.N.W.T. 1994, c. 20.

9. Voir pour une description de l'ensemble des lois canadiennes sur la protection des renseignements personnels : Barbara McIsaac, Rick Shields and Kris Klein, *The law of privacy in Canada*, looseleaf edition, vol. 1, Scarborough (Ont.), Thomson/Carswell, 2000.

3. Le partages de données personnelles entre les administrations

Les législations relatives à la protection des données personnelles détenues 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[10]. À la lumière de l'expérience de l'application des lois sur la protection des données personnelles, 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.

La circulation des données personnelles entre les entités gouvernementales est régie soit par des dispositions de la loi habilitant la transmission à des conditions qui y sont précisées soit par des ententes ou encore par la règle du consentement explicite de la personne concernée par les données.

Trois mécanismes sont prévus pour encadrer le partage de renseignements personnels entre les entités gouvernementales. Évidemment, la communication peut aussi être autorisée par la personne concernée. Mais il y a des habilitations prévues expressément par les lois en vertu desquelles des renseignements personnels peuvent être communiqués à d'autres Administrations. Un ensemble de règles encadrent les ententes de partage de renseignements personnels entre les entités gouvernementales.

3.1. La communication effectuée avec le consentement de la personne concernée

Le consentement est la manifestation de la volonté d'une personne de souscrire à un acte juridique. À l'égard de renseignements personnels, le consentement porte sur l'usage qui peut en être fait. Le consentement est nécessaire pour autoriser l'usage de renseignements personnels lors des différentes étapes de leur

10. Raymond Doray et François Charette, *Accès à l'information, Loi annotée, Jurisprudence Analyse et commentaires*, Cowansville, Éditions Yvon Blais, 2001, mis à jour au 15 novembre 2006, p. III/59-2.

cycle de vie. Pour être valable le consentement doit être manifeste, libre et éclairé, donné à des fins spécifiques, pour une durée déterminée et exprimé par la personne concernée.

Pour être valable, le consentement doit être donné par la personne concernée. Cette dernière doit être capable, c'est-à-dire ayant la faculté d'être titulaire de droits et de les exercer elle-même. Toutefois, pour parer aux conséquences de l'âge et à toute détérioration de l'état physique ou mental de la personne concernée, des mesures de protection ont été prévues visant à garantir les intérêts des mineurs et de certains majeurs. Dans ce cas, le consentement est donné par des tiers. Le consentement peut évidemment être sollicité et obtenu en ligne. D'ailleurs, l'un des avantages les plus prometteurs associé aux prestations électroniques de services publics est la capacité accrue de dialogue entre le citoyen-usager et l'Administration lors des interactions se déroulant en ligne.

Le consentement doit être libre et éclairé. Cela signifie qu'il doit être donné en dehors de toute contrainte et en connaissance de cause. Par conséquent, l'entité qui recueille des renseignements personnels a l'obligation d'informer l'intéressé de tous les faits pertinents relatifs aux activités pour lesquelles on sollicite son accord. L'exigence du caractère manifeste signifie que le consentement peut être donné verbalement ou par écrit, mais à condition qu'il soit évident et clair que la personne a acquiescé à l'usage ou à la divulgation d'informations[11].

Le consentement est donné à des fins spécifiques et pour une durée limitée. Une fois l'objet accompli, les renseignements personnels ne devraient plus être utilisés, sauf à obtenir de nouveau le consentement de la personne concernée ou de toute autre personne autorisée par la loi. Il en va de même si le détenteur des renseignements personnels veut utiliser ces derniers pour une autre fin que celle prévue initialement.

---

11. La *Loi sur la protection des renseignements personnels et les documents électroniques* prévoit à l'article 4.3.7 de l'annexe 1 que le consentement, nécessaire dès la collecte des renseignements personnels, peut revêtir différentes formes, étant entendu selon l'article 4.3.4 de l'annexe que « la forme du consentement que l'organisme cherche à obtenir peut varier selon les circonstances et la nature des renseignements ». Ainsi, le consentement devra être explicite si les renseignements sont considérés comme sensibles. Un consentement implicite sera normalement jugé suffisant si les renseignements sont jugés moins sensibles. La loi précise cependant que tous les renseignements peuvent devenir sensibles suivant la collecte. Il semble donc que l'appréciation du degré de sensibilité des renseignements soit laissée aux organismes qui les recueillent.

Toutefois, l'exigence du consentement connaît des exceptions lors du transfert ou de la communication des renseignements personnels. Des dispositions législatives ou l'ordre d'un tribunal peuvent permettre la divulgation ou le transfert de renseignements sans que le consentement ne soit requis.

3.2. Les habilitations générales à partager des informations personnelles

Les organismes publics sont habilités par les lois à partager des renseignements personnels dans les cas où les renseignements sont nécessaires pour lutter contre le crime[12] ou dans des situations d'urgence mettant la sécurité ou la vie de la personne concernée en danger.

Des dispositions prévoient qu'un organisme public peut communiquer, à toute personne ou à un autre organisme public, un renseignement nominatif, 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 nominatif 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.*

Au lendemain de la mise en vigueur de la Loi, la Commission d'accès a eu 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 »[13]. Les amendements insérés en 2006 ont mis fin à cette tendance en introduisant la précision selon

12. Robert Frater, « Should the left hand get what the right hand got ? Government information sharing, criminal investigation, and privacy rights », [2003] 20 *Supreme court Law Rev.*, 197-212.

13. Raymond Doray et François Charette, *Accès à l'information, loi annotée, jurisprudence et commentaires*, Cowansville, Éditions Yvon Blais, 2002, p. III/67-2.

laquelle il n'est pas nécessaire que la communication soit prévue expressément par la loi.

Parmi les exceptions prévues au caractère confidentiel des renseignements personnels, il y a les dispositions autorisant la communication à un organisme d'un autre gouvernement. L'alinéa 68(1°) de la loi québécoise 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».

L'alinéa 68 (1.1°) 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 ». De même, l'alinéa 68(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.*

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»[14]. Si l'organisme public estime que les renseignements privés «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»[15].

3.3. Les ententes de partage

Les conditions du partage des renseignements sont habituellement régies par des ententes entre les organismes impliqués. Seule la loi québécoise précise les

---

14. Art. 70.1 al 1, *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, (L.R.Q. A-2.1)

15. Art. 70.1 al 2, *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, (L.R.Q. A-2.1)

éléments qui doivent figurer dans de telles ententes. Pour les accords et les arrangements pouvant intervenir entre le gouvernement du Canada et le gouvernement d'une des provinces, le secrétariat du conseil du trésor du Canada a émis des lignes directrices à l'intention des ministères et organismes fédéraux concernant les éléments que doivent contenir ces ententes[16]. Les ententes de partage de renseignements personnels doivent comprendre :

- une description des renseignements personnels à échanger;
- les objectifs pour lesquels les renseignements sont échangés et utilisés;
- un énoncé de toutes les mesures de protection administratives, techniques et matérielles nécessaires à la protection du caractère confidentiel des renseignements, surtout en ce qui concerne leur usage et leur communication;
- un énoncé précisant si les renseignements reçus par l'institution fédérale seront assujettis aux dispositions de la *Loi sur la protection des renseignements personnels* (par exemple, est-ce que les individus concernés peuvent avoir accès aux renseignements, et, sinon, quelles sont les exceptions recommandées par l'institution qui fournit les renseignements);
- un énoncé précisant si les renseignements communiqués par l'institution fédérale seront assujettis aux dispositions de la *Loi sur la protection des renseignements personnels* (par exemple, si l'institution qui reçoit les renseignements peut y donner accès aux individus concernés, et, sinon, quelles sont les exceptions recommandées);
- un énoncé indiquant que l'échange de renseignements prendra fin si le bénéficiaire communique de façon inopportune les renseignements personnels échangés;
- le nom, le titre et la signature de l'agent autorisé de l'institution qui fournit les renseignements personnels et de celle qui les reçoit, ainsi que la date de l'entente.

Au Québec, le régime des ententes de partage de renseignements personnels est défini plus précisément aux articles 67 et suivants de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements person-*

16. Canada, Secrétariat du Conseil du Trésor, *Politiques et Lignes directrices* : *Formulaires - Protection des renseignements personnels - 3-05*. En ligne : http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_128/siglist_f.asp.

nels. Des ententes doivent encadrer la transmission d'informations personnelles aux fins de l'accomplissement d'un mandat. Les articles 67.2 et 67.3 prévoient qu'un organisme public peut, sans le consentement de la personne concernée, communiquer un renseignement nominatif à toute personne ou organisme si cette communication est nécessaire à l'exercice d'un mandat confié par l'organisme public à cette personne ou à cet organisme. Dans un tel cas, l'organisme public doit: premièrement confier ce mandat par écrit et deuxièmement y consigner un ensemble d'indications. L'organisme doit indiquer, dans ce mandat, les dispositions de la loi qui s'appliquent au renseignement qui a été communiqué ainsi que les mesures qu'il faut prendre pour que ce renseignement ne soit utilisé que dans l'exercice du mandat. 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 estime que cela n'est pas nécessaire. Une personne ou un organisme qui exerce un mandat ou qui exécute un contrat de service visé au premier alinéa doit aviser sans délai le responsable de toute violation ou tentative de violation par toute 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;

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.

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.

Le registre est accessible à toute personne qui en fait la demande sauf à l'égard des renseignements personnels dont la confirmation de l'existence peut être refusée en vertu des dispositions de la loi protégeant les renseignements détenus par les forces de police. (art. 67.4)

Comme on l'a vu, des dispositions autorisent la communication de renseignements personnels à un organisme d'un autre gouvernement. Ainsi, l'alinéa 68(1°) 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'alinéa 68 (1.1°) 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'alinéa 68(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».

Dans les trois cas susmentionnés, la communication s'effectue dans le cadre d'une entente écrite. Cette entente doit être soumise à la Commission

pour avis[17]. 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, 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 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

17. Art. 70, *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, (L.R.Q. A-2.1)

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[18].

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.

Lorsque les transferts sont autorisés, ils emportent la possibilité pour un organisme public receveur de devenir détenteur de la totalité des renseignements concernés. Par exemple au Québec, où existent des dispositions plus détaillées, ce processus d'approbation par la Commission, lorsqu'il a lieu, n'est pas précédé d'un débat public et contradictoire. La Commission reçoit une demande et donne un avis habituellement à partir des informations qui lui ont été fournies par le ministère ou organisme concerné. Il n'y a pas d'audience publique au cours de laquelle l'organisme public et les intéressés pourraient débattre des enjeux. Un tel processus laisse peu de place à l'évaluation publique des enjeux et des risques.

4. Le modèle du réseau pour rendre compte de la protection des droits dans les services transgouvernementaux

Envisagé selon le point de vue du citoyen, l'État se présente de plus en plus comme un réseau dans lequel les frontières administratives paraissent avoir de moins en moins de pertinence. Ce phénomène favorise un accroissement des responsabilités régulatrices des acteurs en première ligne et accroît la nécessité de développer des outils afin d'assurer le développement d'outils régulateurs appropriés au niveau local et à celui des micros milieux virtuels.

18. Art. 70, *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, (L.R.Q. A-2.1)

Le réseau se substitue de plus en plus aux institutions hiérarchisées comme lieu de conception et d'énonciation de la normativité. Au sein des réseaux s'élaborent des principes qui doivent habituellement être relayés par d'autres lieux de normativité. D'où l'idée d'une régulation relayée dans plusieurs vecteurs. Cette tendance laisse penser que les institutions rompues aux modes souples de régulation sont les plus susceptibles d'agir avec efficacité dans les univers numériques de l'État en ligne.

Le réseau suppose l'émergence d'environnements interconnectés unissant les décideurs, les chercheurs, les régulateurs de même que les autres acteurs jouant un rôle dans la gouvernance des espaces au sein desquels se déroulent les activités de gouvernance[19]. C'est bien ce que l'on retrouve dans les environnements d'interaction entre l'Administration et les citoyens. Dans son « modèle intégré du gouvernement électronique », Réjean Roy inclut les dimensions juridiques au nombre des éléments du cadre commun de gouvernance du gouvernement électronique[20]. Les normativités juridiques concourent avec les normativités administratives, technologiques et politiques à encadrer les interactions et les échanges d'information au sein de l'appareil gouvernemental.

Ce type de modèle rend compte de la dimension réseautique du e-gouvernement, du fait que l'espace auquel on a affaire est un ensemble interconnecté constitué de pôles interagissants de normativités. Il est constitué d'espaces dans lesquels prévalent en tout ou en partie des normes qui s'imposent aux usagers et autres partenaires. Les normes peuvent s'imposer soit en raison de leur capacité à définir, même implicitement, les conditions de l'exercice des activités, soit parce qu'un participant est en mesure d'exercer une autorité. Cet espace est aussi constitué de relais par lesquels s'explicitent et se diffusent les normativités et les conséquences de celles-ci. Les règles émanant des pôles de normativité se relayent et se diffusent dans les différents espaces virtuels. Elles coexistent soit en complémentarité avec d'autres règles soit en concurrence, se proposant à la place de celles qui sont issues d'autres pôles normatifs[21].

---

19. Manuel Castells, *La société en réseaux. L'ère de l'information*, Paris, Fayard, 1998; François Ost et Michel de Kerchove, *De la pyramide au réseau : pour une théorie dialectique du droit*, Bruxelles, Publications des facultés universitaires Saint-Louis, 2002.

20. Réjean Roy, *Vers un modèle intégré de gouvernement électronique*, Québec, CEFRIO, 2005, p. 6, < http:// www.cefrio.qc.ca/Actes/acte_06.cfm >.

21. Pierre Trudel, « Un 'droit en réseau ' pour le réseau : le contrôle des communications et la responsabilité sur internet, » dans Institut Canadien D'Études Juridiques Supérieures, *Droits de la personne : Éthique et mondialisation,* Cowansville, Éditions Yvon Blais, 2004, pp. 221-262.

La normativité en réseau caractéristique des environnements fondés sur l'usage des réseaux de communication informatique emporte des changements dans les façons de concevoir la répartition des responsabilités[22]. Le modèle classique, caractéristique de l'État libéral où chaque ministère ou entité administrative est réputé avoir le contrôle entier et exclusif de ses informations, est graduellement supplanté par un modèle où le partage des informations appelle la mise en place de nouveaux modes de répartition et de partage des responsabilités.

Alors que dans l'univers bureaucratique dominé par le papier, le droit insiste sur la délimitation des droits d'obtenir ou non telle ou telle information, dans l'univers en réseau, le droit tend vers l'organisation d'une régulation des permissions d'accès et d'usage dévolues aux décideurs et aux citoyens.

Une tendance semble se profiler vers une évolution des conceptions présidant à l'interprétation des principes fondamentaux relatifs à la gestion des données personnelles. Ainsi, la limitation en matière de collecte suppose la mise en place de processus décisionnels qui feront usage du minimum d'informations personnelles nécessaires afin d'assurer les prestations ou la prise de décision. Il faut être en mesure de justifier le pourquoi de la collecte de chaque renseignement personnel.

Dans un environnement en réseau, la nécessité de la collecte doit s'envisager au regard de l'ensemble des familles de prestations concernées par les informations. Une fois l'information collectée, la nécessité de sa conservation s'apprécie au regard d'un ensemble de processus de décision susceptibles d'être réalisés en ayant recours à une donnée personnelle. Le principe de retenue en matière de collecte et le principe de spécification des finalités se recoupent. Le principe relatif à la spécification des finalités est aussi renforcé: en spécifiant le plus strictement possible les finalités, on se trouvera en situation où la collecte est limitée aux informations effectivement indispensables aux fins poursuivies au plan de l'ensemble des prestations et services devant être assurés au sein d'un réseau.

La règle empêchant la circulation et la réutilisation des informations pour le motif que celles-ci pourraient être détournées de leur finalité, doit être relue

22. Sur les mutations du modèle pyramidal vers un droit en réseau voir : Antoine Bailleux, « À la recherche des formes du droit : de la pyramide au réseau, » [2005] 55 *R.I.E.J.*, 91-115.

dans le contexte de dialogue accru que permet le réseau. Plus que jamais, l'Administration est en mesure d'indiquer à chaque administré quelles sont les informations qu'il possède sur son compte, lesquelles il entend utiliser afin de prendre une décision. Le citoyen est désormais en mesure d'interagir et d'exiger le retrait et l'ajout d'informations.

La généralisation des réseaux conduit à apprécier la nécessité à l'égard de l'ensemble des situations concernées par un environnement d'information. Certes, il faut toujours considérer la nécessité au plan de la légitimité de la collecte et de la détention d'informations, comme cela est exigé par les principes actuels. Mais il faut assurer que seules les informations pertinentes et autorisées sont utilisées dans le cadre d'un processus décisionnel spécifique. Cela appelle une démarche dans laquelle sont dissociées, d'une part, la question de la nécessité de la détention de l'information et, d'autre part, l'appréciation de la nécessité d'y accéder pour une décision ou prestation déterminée.

Le principe de finalité pose que l'on ne peut recueillir et utiliser les renseignements personnels que pour des fins compatibles avec celles de la collecte initiale. Le principe de finalité est lié au maintien de la qualité de l'information. Dans les principes de l'OCDE, cette exigence est exprimée ainsi :

> *Les données de caractère personnel devraient être pertinentes par rapport aux finalités en vue desquelles elles doivent être utilisées et, dans la mesure où ces finalités l'exigent, elles devraient être exactes, complètes et tenues à jour.*[23]

Dans le contexte d'un environnement en réseau, la question des finalités se pose en tenant compte que les informations peuvent être là disponibles, déjà recueillies : ce n'est plus au regard de la détention que s'applique l'exigence du respect de la finalité mais plutôt au regard de l'accès et de l'utilisation du renseignement. Dans un réseau, le principe du contrôle au niveau du droit d'accès vient assurer le respect des finalités. L'accès à un renseignement n'est licite que pour une finalité autorisée et lorsqu'on accomplit une activité s'inscrivant dans le cadre de la finalité.

---

23. OCDE, *Lignes directrices régissant la protection de la vie privée et des flux transfrontières de données de caractère personnel*, Paris, OCDE, 2002, <http://www.oecdpublications.gfinb.com/cgibin/OECDBook Shop.storefront/EN/product/932002012P1.

Le respect du principe de finalité, suppose que l'usager ait effectivement connaissance des familles de finalités auxquelles serviront les informations au sein des réseaux de services publics. La notion de finalité doit désormais être axée sur l'usager, non sur les structures gouvernementales. Par exemple, l'usager qui entre en relation avec les ministères chargés de l'application des lois sur la sécurité du revenu doit savoir que les informations qu'il fournit circuleront et seront utilisées aux fins d'assurer l'application des lois relatives à la sécurité du revenu et ce, peu importe que l'une relève d'un ministère et l'autre d'un organisme public tiers. Il faut que l'information sur les finalités des informations détenues soit constamment disponible et portée à la connaissance de l'usager lors de chaque collecte. Pour respecter le principe de la limitation de l'utilisation, les environnements d'information devraient desservir des familles délimitées de prestations : ce qui assure que les renseignements personnels seront utilisés qu'à des fins apparentées et compatibles avec celles de la collecte initiale.

La transparence est une condition essentielle de la crédibilité et de la confiance dans les environnements en réseau. L'usager doit être en mesure de savoir à qui il a affaire et comment est conçu le processus informationnel dans lequel il est engagé. À cet égard, l'évaluation publique des environnements d'information ou des partages d'informations à des fins de prestations électroniques prend une importance accrue. Les enjeux et les risques associés à des prestations électroniques que l'on projette de proposer en réseau doivent être publiquement divulgués, débattus et leurs risques publiquement évalués.

La qualité des données s'apprécie à l'égard des prestations à être accomplies: il faut garantir que les renseignements utilisés pour effectuer la prestation sont exacts, précis, autorisés par les lois et ne présentent pas d'équivoque. La légitimité de pareilles circulations d'informations personnelles est renforcée lorsque le citoyen se trouve à même de réviser et, le cas échéant, de rectifier en ligne ou autrement les informations qui le concernent. Le droit de rectification – pour l'heure si peu exercé – prend alors tout son sens.

Comme les données personnelles sont disponibles en réseau, chaque organisme doit s'assurer que l'information à laquelle il a droit d'accéder, afin d'accomplir une prestation relative à une personne, est de qualité adéquate, compte tenu des exigences et du contexte de la prestation. Pour assurer la qualité, il faut tabler sur le potentiel de dialogue en direct entre l'Administration et l'usager que recèlent les technologies de réseau.

À cet égard, le principe de la participation individuelle de la personne concernée dans les décisions relatives au traitement des renseignements personnels acquiert dans les réseaux une portée renouvelée. Dans les réseaux, il est possible de présenter l'information que l'on détient et de la valider en temps réel avec la personne concernée. La garantie de la qualité des données sera du même coup renforcée par la validation que l'organisme effectue de l'information lors d'une prestation spécifique.

S'agissant de la responsabilité, chaque organisme public susceptible d'accéder à des données personnelles au sein d'un réseau peut être considéré comme en étant le détenteur juridique. À ce titre, chaque organisme est responsable de la confidentialité des renseignements et l'ensemble des organismes en répondent solidairement. Comme il y a pluralité d'organismes, ces derniers auront à déterminer comment se répartiront les responsabilités de l'un et l'autre des participants. Il importe en effet de préciser les obligations et délimiter la responsabilité des gestionnaires quant aux exigences de confidentialité et de sécurité. Il est en effet nécessaire que soient précisées les normes à la lumière desquelles seront évaluées le comportement et la responsabilité des citoyens de même que celle du gestionnaire.

La sécurité tant physique que logique est évidemment une exigence essentielle pour tout environnement fonctionnant en réseau. Le cadre juridique doit inciter les responsables à prendre les mesures afin de garantir la sécurité des informations sur les personnes. Outre une culture de la sécurité, il faut un ensemble de processus capables de prévenir les attaques et surtout d'y remédier aussitôt que se produit un évènement qui met en péril les processus de traitement.

Ainsi, lorsque les données sont dans des environnements d'information auxquels ont accès une pluralité de ministères ou autres organismes ou entités publics, la protection des renseignements personnels ne résulte plus des limitations intervenant au stade de la collecte ou prohibant la circulation. La véritable protection procède d'un encadrement strict des conditions auxquelles il est licite d'accéder aux renseignements de même que les conditions de leur utilisation. Le cadre juridique doit dissocier la possession de l'information et le droit d'y accéder et d'en faire usage.

Certes, du fait de sa détention dans un environnement d'information accessible à une pluralité d'entités, l'information leur est disponible, mais cela ne

confère pas, en soi, le droit d'y accéder. L'accent est ainsi déplacé vers le droit de faire usage des renseignements personnels plutôt que sur la seule possession ou détention de ces derniers. Il y a dissociation entre la détention physique d'une information par une entité et le droit de cette dernière d'y accéder ou d'en faire usage. Du fait de sa participation à espace en réseau, un ministère ou autre entité publique détient un ensemble d'informations en commun avec d'autres entités. Toutefois, il n'a droit d'accéder à ces informations que si cela est nécessaire à l'accomplissement d'une prestation visée par l'acte constitutif de l'aire de partage.

En fin de compte, dans le contexte du e-gouvernement, les protections doivent être conçues de manière à garantir que les renseignements personnels seront effectivement utilisés pour des fins licites, plutôt que pour empêcher leur circulation. Des modèles commencent à émerger afin de structurer les modes de protection dans des environnements en réseaux. Au Canada, on évoque les aires de partage, un concept qui se conjugue suivant des modalités à géométrie variable selon le degré de sensibilité des données et on commence à prendre la mesure de modèles fondés sur la maitrise, par l'usager, des informations.

4.1. Les aires de partage de données personnelles

Dès lors que la circulation de données personnelles entre les organismes publics cesse d'avoir un caractère exceptionnel, il vaut mieux disposer d'un cadre juridique résolument axé sur les conditions à respecter lors du déploiement de prestations de services en ligne. Il faut aussi des garanties lors de la mise en place des espaces de circulation des données personnelles. Au plan juridique, les espaces-réseaux dans lesquels circulent des données personnelles doivent être encadrés par des règles précisant les responsabilités de l'ensemble des entités concernées. En somme, il s'agit de mettre en place les règles désignant celui qui répond des informations ainsi partagées en réseau. Pour ce faire, il importe de revoir les prémisses sur lesquelles reposent la plupart des lois sur la protection des données personnelles qui reflètent souvent le postulat que la protection des données est assurée par leur confinement.

L'aire de partage est l'une des notions mises de l'avant afin de penser les nouveaux modes de partage d'information dans les environnements en réseau. L'aire de partage peut être définie comme un environnement d'information

dans lequel des données personnelles nécessaires à la délivrance d'un ensemble de services accomplis au bénéfice des citoyens peuvent être rendus disponibles à différentes entités[24]. Ces services ou prestations ont un caractère complémentaire et leur accomplissement nécessite des informations détenues par une pluralité d'entités liées par une entente. La notion fournit un concept adapté aux réalités des réseaux et permet de concevoir les droits et obligations de l'ensemble de partenaires du e-gouvernement.

Le concept renvoie à un ensemble de mécanismes balisant la circulation de l'information et en délimitant les usages. Il s'agit d'organiser l'espace au sein duquel les données peuvent circuler. Le cadre qui en découle définit les droits et les responsabilités. Les protections sont conçues de manière à garantir que les données seront effectivement utilisées pour des fins licites, plutôt que pour empêcher leur circulation.

4.2. Les répertoires de renseignements personnels sur la santé disponibles en ligne avec l'accord du patient

Selon des conditions différentes, les dispositions introduites dans les législations de plusieurs pays organisent l'hébergement et la circulation contrôlée des données de santé à des fins de soins. Par exemple, dans les législations françaises et québécoises, il est institué un régime juridique pour des environnements d'information dans lesquels des données personnelles nécessaires à la délivrance d'un ensemble de services accomplis au bénéfice des citoyens peuvent être rendus disponibles à différentes entités. Les informations ne sont disponibles que pour des services ou prestations de santé ayant un caractère complémentaire. Cette disponibilité des informations pour une pluralité d'entités –comme les médecins, les autres professionnels de la santé ou les hôpitaux– est assortie de conditions strictes.

En droit français c'est la *Loi relative aux droits des malades*[25] qui introduit l'article L. 1111-8 au *Code de la santé publique*. Cette disposition qui organise le

24. En ce sens, voir : Pierre Trudel, « Renforcer la protection de la vie privée dans l'État en réseau; l'aire de partage de données personnelles, » [2004] 110, *Revue française d'administration publique* 257-266.

25. Loi no 2002-303 du 4 mars 2002, J.O. 5 mars 2002.

régime juridique du contrat d'hébergement. Aux termes de l'article L.1111-8 « la prestation d'hébergement fait l'objet d'un contrat ». Elle dispose que :

> *Les professionnels de la santé ou les établissements de santé ou la personne concernée peuvent déposer des données de santé à caractère personnel, recueillies ou produites à l'occasion des activités de prévention, de diagnostic ou de soins, auprès des personnes physiques ou morales agréées à cet effet.*

La détention matérielle des données étant transférée à l'hébergeur, celui-ci se trouve en position de dépositaire. Seuls les hébergeurs agréés sont autorisés à conclure des contrats d'hébergement. Pour l'hébergeur, le défaut d'agrément expose à une sanction pénale et à la nullité du contrat. Les parties au contrat sont les professionnels de la santé, les établissements de santé et la personne concernée. L'accord de cette dernière est une condition de validité du contrat. Isabelle Vacarie écrit que:

> *Pour chaque patient hospitalisé dans un établissement de santé public ou privé, le Code de la santé publique prescrit la constitution d'un dossier médical et sa conservation. Mais le Code autorise l'externalisation des dossiers auprès d'un hébergeur. À cet égard, le code précise que « cet hébergement de données ne peut avoir lieu qu'avec le consentement exprès de la personne concernée ». Son accord est donc une condition de validité du contrat. Le contrat comporte des obligations essentielles. L'hébergeur assume une obligation de restitution des données. En tant que dépositaire, l'hébergeur assume une obligation de non utilisation des données. Il ne peut en forcer le secret.*[26]

Le statut de l'hébergeur est régi par des dispositions d'ordre public : celui-ci ne peut recevoir des données que s'il a été agréé et il est astreint au secret professionnel. Ainsi, le « dépositaire naturel » des dossiers médicaux et l'hébergeur sont assujettis à un même corps de règles d'ordre public. Un décret précise les conditions de l'agrément et les contrôles exercés à l'égard des hébergeurs de données de santé. Le décret indique six conditions à remplir pour demander l'agrément. Ainsi, les contrats entre hébergeur et clients doivent comporter des clauses obligatoires et les hébergeurs doivent élaborer et respecter une politique de confidentialité et de sécurité.

---

26. Isabelle Vacarie, « L'hébergement des données de santé : entre contrat et statut », (2002) 38 (4) R.D. *Sanit. Soc*, 695, p. 698.

Pour le Québec, c'est la *Loi modifiant la Loi sur les services de santé et les services sociaux*[27] qui introduit un régime juridique complet pour les services régionaux de conservation de certains renseignements aux fins de la prestation de services de santé. Ces dispositions instituent un titre II intitulé « Services régionaux de conservation de certains renseignements aux fins de la prestation de services de santé »[28].

L'article 520.5 de la *Loi sur les services de santé et des services sociaux* énonce des finalités-objectifs que visent les services régionaux de conservation de renseignements de santé. Les objectifs sont précisés à l'article 520.5. Il s'agit de fournir aux intervenants habilités de l'information pertinente, organisée, intégrée et à jour afin de faciliter la prise de connaissance rapide des renseignements de santé d'une personne au moment de sa prise en charge ou lors de toute prestation de services de santé rendus par ces intervenants, en continuité et en complémentarité avec ceux dispensés par d'autres intervenants. L'autre finalité mentionnée dans la Loi est d'assurer l'efficacité de la communication ultérieure des renseignements conservés par une agence ou un établissement autorisé à des intervenants habilités, aux seules fins de la prestation de services de santé.

La personne dispose un droit d'accès aux renseignements qui la concernent; elle peut demander que les renseignements inexacts, incomplets ou équivoques de même que ceux dont la collecte ou la communication n'est pas autorisée soient rectifiés. La Loi ménage aussi les recours à l'égard des entités mandatées pour assurer la conservation des renseignements. Est aussi affirmé, le principe de la responsabilité et de l'imputabilité de l'entité autorisée et des autres entités qui assurent le fonctionnement des services de conservation. Enfin, les entités responsables doivent mettre en place un ensemble de mécanismes visant à assurer la disponibilité, l'intégrité, la confidentialité, l'accessibilité et l'irrévocabilité des renseignements détenus ou conservés. Selon le cas, il y a obligation de pourvoir à l'authentification de l'identité des personnes habilitées.

---

27. *Loi modifiant la Loi sur les services de santé et les services sociaux et d'autres dispositions législatives*, L.Q., 2005, c. 32, art. 189.

28. Pierre, Trudel, « Aperçu du cadre juridique des services d'hébergement de données de santé », dans Barreau du Québec, *Après le projet 83 : un nouveau réseau de la santé*, Formation continue, volume 260, Cowansville, Éditions Yvon Blais, 2006.

Seuls les intervenants habilités ont accès aux renseignements confiés aux services régionaux et uniquement pour des fins strictement délimitées. Ces services de conservation ne peuvent être mis en place que moyennant une autorisation du ministre.

Des conditions strictes s'appliquent au regard des mesures à prendre pour assurer la confidentialité et la sécurité des renseignements pendant tout leur cycle de vie. Tout accès aux renseignements doit être journalisé et les journaux doivent être surveillés afin de détecter les accès non autorisés. Des mécanismes de contrôle interne afin d'assurer le respect des obligations doivent être mis en place. Il est interdit de confier à un tiers la prestation des services de conservation mais il est possible pour un établissement autorisé de confier à un tiers un contrat de service relatif à l'installation, à l'entretien ou à la réparation de tout support technologique utilisé aux fins des services de conservation.

Toute personne assurée auprès de la Régie de l'assurance-maladie, âgée de plus de quatorze ans peut donner son consentement à ce que les renseignements soient versés auprès des centres de conservation. Elle doit alors être informée au préalable sur les objectifs et finalités poursuivies de même que sur les modalités de fonctionnement concernant l'accès, l'utilisation, la communication, la conservation et la destruction des renseignements conservés. On doit lui spécifier que le consentement emporte une autorisation relative à tout intervenant habilité de transmettre selon son profil d'accès de recevoir. Un tel consentement est renouvelable. Il peut être révoqué en tout temps sur demande et l'est de plein droit dès lorsqu'une personne n'est plus assurée

La révocation du consentement aux termes de l'article 520.23 a pour conséquence de rendre inactifs les renseignements préalablement conservés. Ceux-ci ne peuvent être détruits avant cinq ans suivant leur inscription. Il est interdit de transmettre ces renseignements à un intervenant qui ne rend pas à une personne des services de santé ou exerce à l'égard d'une personne des fonctions de contrôle ou d'expertise. Il est pareillement prohibé de transmettre les renseignements hébergés à un assureur ou à un employeur et de recevoir extrait ou copie de renseignements conservé. Interdiction est faite à quiconque d'avoir accès à ces renseignements, un extrait ou une copie pour la conclusion de tout contrat exigeant l'évaluation de l'état de santé d'une personne tel contrat d'assurance ou d'embauche ou à tout autre moment. Les renseignements conservés ne peuvent être communiqués à quiconque et ce même avec le consentement de la personne concernée.

4.3. Les répertoires et espaces virtuels sous la maîtrise des usagers

Le développement d'applications sur Internet qui réservent à l'usager un haut niveau de maîtrise sur les informations laisse envisager de nouveux modes de partage de renseignements personnels. Il est en effet envisageable de mettre en place des espaces personnalisés placés en partie ou en totalité sous la maîtrise du citoyen et pouvant être utilisés lors des interactions de ce dernier avec l'Administration. De tels espaces informatiques placés sous la maîtrise de l'usager, au moyen d'un réseau informatique, lui permettent de placer des documents dans un espace sous son contrôle. Ils se distinguent des « guichets uniques » qui sont habituellement des sites fédérant des services de provenance multiple. La notion d'espace citoyen renvoie plutôt à des espaces virtuels dans lesquels il est loisible à l'usager de verser, de conserver, d'autoriser la consultation ou la transmission de renseignements aux fins d'asurer la réalisation de prestations électroniques de services.

Le modèle reflète une tendance associée à ce que l'on désigne par le Web 2.0, soit une grande maîtrise par l'usager de l'information archivée et rendue disponible à autrui selon ses choix. La mise en place de ces types d'environnements en ligne permettant d'échanger et de partager des documents technologiques est préconisée psr ceux qui souhaitent assurer une protection des documents détnus par l'état et par le citoyen aux fins de prestations électroniques de service. Par exemple, le Rapport sur le gouvernement en ligne *Vers un Québec branché pour ses citoyens* mettait de l'avant l'idée d'une « page citoyenne »[29]. Dans cet espace accessible en ligne, le citoyen pourrait avoir accès aux informations qui le concernent, y consigner des documents relatifs aux relations qu'il entretient avec les divers services et autoriser la transmission de documents requis pour l'accomplissement de prestations en ligne.

Mais à ce jour, il reste beaucoup à faire afin de caractériser les divers types d'espaces en ligne placés sous la maîtrise du citoyen et lui permettant de consigner des documents technologiques et, moyennant son accord, de rendre ces derniers disponibles à d'autres entités notamment les ministères et organismes publics dans le cadre d'une prestation de service.

---

29. Henri-François Gautrin, *Rapport sur le gouvernement en ligne, vers un Québec branché pour ses citoyens*, Québec, juin 2004, p. 49.

Conclusion

Dans l'État en réseau, les informations sont essentiellement circulantes, disponibles au moment où elles doivent l'être pour accomplir une prestation de service. Cela circulation nécessite des précautions car les potentialités d'accumulation et de couplage des informations peuvent s'accroître. Or, l'attachement d'une partie de la population à certaines règles telles que celles qui prescrivent les exigences d'obtenir le « consentement libre et éclairé » pour chaque mouvement d'information personnelle semble difficile à concilier avec la mise en place d'un cadre juridique reflétant les caractéristiques des réseaux et pour cette raison ne saurait tenir lieu de cadr juridique assurant la protection de la vie privée dans l'État en réseau.

La détention dans un environnement d'information accessible à une pluralité d'organismes publics, afin de leur permettre d'assurer seuls ou en partenariat un ensemble de services aux citoyens n'est envisageable que si de fortes garanties assurent la protection de la vie privée. La formulation d'un tel cadre juridique suppose une lecture actualisée des principes fondamentaux de la protection des renseignements personnels. Une protection située au niveau des accès par les Administrations procure une protection de beaucoup supérieure à celle que l'on peut espérer des régimes actuels découlant des lois relatives à la protection des données personnelles.

Le réseautage des données administratives porte à une relecture des principes de protection afin d'assurer une gestion pleinement compatible avec les exigences, risques et enjeux posés par les réseaux et les exigences de la protection effective des droits des personnes. Pour tenir compte des enjeux au regard de la protection des informations personnelles, il faut poser un regard lucide sur les risques qui découlent aussi bien de la nature sensible des données et du contexte inhérent aux réseaux. Les mécanismes juridiques doivent procurer à la fois une protection effective sans entraver la circulation de l'information qui est inhérente à la mise en place de services en réseaux.

Les modèles émergents pour formuler les encadrements des usages partagés des données personnelles témoigne des voies qu'emprunte l'adaptation du droit aux impératifs de la virtualisation. On peut y lire l'allure que prend la modernisation des mécanismes de protection – fondés sur le paradigme des dossiers consignés sur papier en les resituant dans un cadre assurant à la fois la mo-

bilité et la confidentialité de l'information. Sont aussi conciliées les exigences nouvelles relatives à la qualité de l'information requise pour assurer des services publics.

Les cadres juridiques qui tendront à s'implanter dans l'État en réseau doivent garantir aussi bien la pleine disponibilité des données à tous ceux qui doivent y avoir accès que leur protection à l'égard des autres utilisations. C'est dire combien la mise en œuvre de modèles innovateurs de partage de données personnelles constitue un enjeu majeur du déploiement des services en ligne et de la modernisation des services publics.

RÉSUMÉ

Revista catalana de dret públic, 35, ISSN 1885-5709, 2007
Source de la classification: Classification Décimale Universelle (CDU)
Source des descripteurs: mots-clés facilités par les auteurs

35:004
Pierre Trudel, professeur titulaire de la Chaire L. R. Wilson sur le droit des technologies de l'information et du commerce électronique

fr Gouvernement électronique et interconnexion de fichiers administratifs dans l'État en réseau
p. 247-280

Les possibilités offertes par les réseaux permettent la mise en place de plusieurs applications de gestion afin d'offrir aux citoyens une gamme étendue de service en ligne. Mais le fonctionnement optimal de la plupart des services en ligne requiert que les renseignements personnels puissent être partagés entre une pluralité d'entités relevant de divers niveaux de gouvernement. Au Canada, la constitution fédérale répartit les pouvoirs de faire des lois entre le Parlement et le gouvernement central et les législatures et gouvernements provinciaux. Un grand nombre de services peuvent nécessiter des informations personnelles en possession de l'un ou l'autre des gouvernements. Cette tendance à la collaboration nécessite un partage des renseignements personnel. La généralisation des plates-formes de partage d'information permet de situer le citoyen au cœur des décisions. Elle soulève néanmoins des interrogations quant à la protection des renseignements personnels devant nécessairement être partgés entre les multiples instances gouvernementales.

L'article expose le cadre juridique qui prévaut au Canada afin d'encadrer les partages d'informations personnelles entre les instances gouvernementales. Outre les partages autorisés via le consenement donné par la personne concernée, les lois imposent ou permettent le partage des renseignements personnels entre les administrations. La plupart du temps, ces partages sont régis par des ententes dont les conditions essentielles sont prescrites par des textes législatifs ou des politiques.

Il est aussi fait état de la nécessité de concevoir des règles afin de faire en sorte que les renseignements personnels, qui doivent être disponibles à tout moment pour assurer la qualité des services et des prestations, soient protégés peu importe où ils se trouvent au sein d'un environnement en réseau voué aux interactions État-citoyen. Sont examinés des modèles émergents comportant de nouvelles façons de régir les partages d'informations sur les personnes. Ainsi, il est fait mention de l'aire de partage un environnement d'information dans lequel des données personnelles nécessaires à la délivrance d'un ensemble de services accomplis au bénéfice des citoyens peuvent être rendus disponibles à diffé-

rentes entités. On examine aussi le modèle des centres d'hébergement de données de santé pour enfin esquisser les tendances récentes vers la mise en place de répertoires et espaces personnels placés sous la maîtrise des usagers eux-mêmes. L'article conclut en insistant sur la nécessité d'assurer l'adéquation du droit de la protection des données personnelles aux réalités des réseaux du e-gouvernement et de concevoir lucidement les droits et obligations de l'ensemble des partenaires du e-gouvernement.

Mots-clés: e-gouvernement ; protection des données personnelles ; partage d'information.

RESUM

Revista catalana de dret públic, 35, ISSN 1885-5709, 2007
Font de la classificació: Classificació Decimal Universal (CDU)
Font dels descriptors: paraules clau facilitades pels autors

35:004
Pierre Trudel, professor titular de la Càtedra L. R. Wilson sobre Dret de les Tecnologies de la Informació i el Comerç Electrònic

fr Gouvernement électronique et interconnexion de fichiers administratifs dans l'État en réseau

ca Administració electrònica i interconnexió de fitxers administratius a l'Estat en xarxa

p. 247-280

Les possibilitats que ofereixen les xarxes permeten posar en marxa diverses aplicacions de gestió per tal d'oferir als ciutadans una gamma amplia de serveis en línia. Però el funcionament òptim de la majoria dels serveis en línia requereix que les dades de caràcter personal puguin compartir-se entre una pluralitat d'entitats que depenen de diversos nivells del govern. Al Canadà, la Constitució federal distribueix el poder de dictar lleis entre el Parlament i el Govern central i les legislatures i els governs provincials. Un gran nombre de serveis poden requerir informació personal que estigui en possessió d'un o d'altre govern. Aquesta tendència a la col·laboració requereix que es comparteixin dades de caràcter personal. La generalització de les plataformes de compartició d'informació permet situar el ciutadà al centre de les decisions. Provoca, però, interrogants en relació amb la protecció de les dades de caràcter personal en haver de ser compartides entre múltiples instàncies governamentals.

L'article exposa el marc jurídic prevalent al Canadà per emmarcar la compartició d'informació personal entre les instàncies governamentals. Més enllà de les comparticions autoritzades pel consentiment atorgat per l'interessat, les lleis imposen o permeten la compartició de dades personals entre les administracions. En la majoria de casos, aquestes comparticions es regeixen per acords, les condicions essencials dels quals estan prescrites per textos legislatius o per polítiques.

També s'ha de tenir en compte la necessitat de concebre regles perquè les dades personals, que han d'estar disponibles en tot moment per assegurar la qualitat dels serveis i de les prestacions, estiguin protegides independentment d'on es trobin al si d'un context en xarxa consagrat a les interaccions Estat-ciutadà. S'examinen els models emergents que comporten noves formes de regir la compartició d'informació sobre les persones. Així, es menciona l'àrea de compartició d'un context d'informació en el qual les dades de caràcter personal necessàries per a l'expedició d'un conjunt de serveis en benefici dels ciutadans poden estar disponibles per a diferents entitats. S'examina també el model dels centres d'allotjament de dades de salut i, finalment, s'esbossen les tendències actuals sobre l'aplicació de repertoris i espais personals situats sota el control dels mateixos usuaris. L'article conclou insistint en la necessitat d'assegurar l'adequació del dret de la protecció de les dades de caràcter personal a les realitats de les xarxes de l'Administració electrònica i de concebre lúcidament els drets i les obligacions del conjunt de socis de l'Administració electrònica.

Paraules clau: Administració electrònica; protecció de dades de caràcter personal; compartició de la informació.

RESUMEN

Revista catalana de dret públic, 35, ISSN 1885-5709, 2007
Fuente de la clasificación: Clasificación Decimal Universal (CDU)
Fuente de los descriptores: palabras clave facilitadas por los autores

35:004
Pierre Trudel, profesor titular de la Cátedra L. R. Wilson sobre Derecho de las Tecnologías de la Información y el Comercio Electrónico

fr Gouvernement électronique et interconnexion de fichiers administratifs dans l'État en réseau
es Administración electrónica e interconexión de ficheros administrativos en el Estado en red
p. 247-280

Las posibilidades que ofrecen las redes permiten poner en marcha diversas aplicaciones de gestión con el fin de ofrecer a los ciudadanos una gama amplia de servicios en línea. Pero el funcionamiento óptimo de la mayoría de los servicios en línea requiere que los datos de carácter personal puedan compartirse entre una pluralidad de entidades que dependen de diversos niveles del gobierno. En Canadá, la Constitución federal distribuye el poder de dictar leyes entre el Parlamento y el Gobierno central y las legislaturas y los gobiernos provinciales. Un gran número de servicios pueden requerir información personal que esté en posesión de uno o de otro gobierno. Esta tendencia a la colaboración requiere que se compartan datos de carácter personal. La generalización de las plataformas de compartición de información permite situar al ciudadano en el centro de las decisiones. Provoca, sin embargo, interrogantes en relación con la protección de los datos de carácter personal al tener que ser compartida entre múltiples instancias gubernamentales.

El artículo expone el marco jurídico existente en el Canadá para enmarcar la compartición de información personal entre las instancias gubernamentales. Más allá de las comparticiones autorizadas por el consentimiento otorgado por el interesado, las leyes imponen o permiten la compartición de datos personales entre las administraciones. En la mayoría de casos, estas comparticiones se rigen por acuerdos, cuyas condiciones esenciales están prescritas por textos legislativos o por políticas.También se debe tener en cuenta la necesidad de concebir reglas para que los datos personales, que tienen que estar disponibles en todo momento para asegurar la calidad de los servicios y de las prestaciones, estén protegidos independientemente de donde se encuentren en el seno de un contexto en red consagrado a las interacciones Estado-ciudadano. Se examinan los modelos emergentes que comportan nuevas formas de regir la compartición de información sobre las personas. Así, se menciona el área de compartición de un contexto de información en el cual los datos de carácter personal necesarios para la expedición de un conjunto de servicios en beneficio de los ciudadanos pueden estar disponibles para diferentes entidades. Se examina también el modelo de los centros de alojamiento de datos de salud y por último se esbozan las tendencias actuales sobre la aplicación de repertorios y espacios personales situados bajo el control de los propios usuarios. El artículo concluye insistiendo en la necesidad de asegurar la adecuación del derecho de la protección de los datos de carácter personal a las realidades de las redes de la Administración electrónica y de concebir lúcidamente los derechos y obligaciones del conjunto de socios de la Administración electrónica.

Palabras clave: Administración electrónica; protección de datos de carácter personal; compartición de la información.

ABSTRACT

Revista catalana de dret públic, 35, ISSN 1885-5709, 2007
Classification source: Universal Decimal Classification (UDC)
Key words source: Key words are given by the authors

35:004
Pierre Trudel, holder of the L. R. Wilson Chair in Information Technologies and E-Commerce Law

fr Gouvernement électronique et interconnexion de fichiers administratifs dans l'État en réseau
en Electronic Administration and the Interconnection of Administrative Files to the Networked State
p. 247-280

The possibilities offered the networks make it possible to implement various management applications in order to provide citizens with a wide range of on-line services. However, for the majority of on-line services to function optimally, personal data must be shared among multiple entities in different governmental hierarchies. In Canada, the federal Constitution distributes the power of enacting laws between the Parliament and the central government and the legislatures and the provincial governments. A large number of services may require personal information that might be in the possession of one level of government or another. This tendency towards collaboration requires the sharing of personal data. The generalization of the information-sharing platforms makes it possible to situate the citizenry at the heart of the debate. It does, however, raise questions with regard to the protection of personal data when such data must be shared among multiple government agencies.

The article sets forth the prevalent legal framework in Canada for approaching the sharing of personal information among governmental agencies. Beyond the authorization of sharing through the consent granted by the party concerned, the laws impose and allow for the sharing of personal data among governmental agencies. In most cases, this sharing is governed by agreements whose essential conditions are prescribed by legislative texts or policies.

One should also take into consideration the need to design regulations so that personal data, which must always be available in order to insure the quality of service, are protected independently of where they may be located in the network of interactions between the state and the citizen. Emerging models that entail new ways of governing the sharing of information on people are examined. Thus, mention is made of the area of sharing of an information context in which the personal data necessary for the provision of a set of services on behalf of the citizenry may be available to different entities. The model of hosting centers for health data is also examined, and finally, current tendencies on the

application of personal repertoires and spaces under the control of the users themselves are outlined. The article concludes by emphasizing the need to insure the adaptation of the right to the protection of personal data to the realities of electronic administration networks and the need to view the rights and obligations of all the actors in electronic administration with lucidity.

Key words: Electronic administration; protection of personal data; information sharing.