

Immobiliser ou protéger?

Le droit et le développement de services en ligne

Pierre TRUDEL

**titulaire de la Chaire L.R. Wilson sur le
droit des technologies de l'information et
du commerce électronique, CRDP, Faculté
de droit, U de M**

**Le gouvernement en ligne :
Perspectives et orientations**

25 février 2004

Entretiens de la CHAIRE L.R.WILSON SUR LE DROIT DES TECHNOLOGIES DE L'INFORMATION ET DU COMMERCE ÉLECTRONIQUE

**Centre de recherche en droit public
Faculté de droit
Université de Montréal
25 février 2004**



Un cadre juridique à revoir

- nouvelles circulations de l'information
- fondements inadéquats du cadre actuel de la protection
- la recherche de fondement et de concepts
 - adaptés aux environnements-réseaux
 - renforçant l'effectivité de la protection de la vie privée

Cet exposé identifie les approches afin d'assurer effectivement la protection de la vie privée et des renseignements personnels dans le contexte des services en ligne offerts en prenant avantage des fonctionnalités des espaces de réseaux.

Le contexte de la production et de la circulation des informations s'est considérablement modifié au cours des deux dernières décennies.

Le développement de l'État en réseau nécessite de revoir les protections de la vie privée; non pas en érigeant comme un absolu les protections qui prévalaient lorsque les informations personnelles étaient situées quelque part dans un classeur mais en identifiant les conditions d'une réelle protection dans un contexte où les informations relatives aux personnes ont nécessairement vocation à circuler.

Il importe de faire un retour critique sur les fondements des règles de droit telles celles qui concernent la vie privée et d'identifier les ajustements conceptuels qui sont nécessaires afin de garantir une protection vraiment effective de la vie privée.

De nouvelles circulations de l'information

- des réseaux
 - services intégrés
 - organisés selon les situations de vie non les organigrammes
 - prise en charge de fonctions relevant d'une pluralité d'organismes publics
- l'accroissement de la circulation de l'information
 - modifie l'échelle des risques pour la vie privée.

Le contexte de la circulation des informations portant sur les personnes connaît des changements significatifs. Les systèmes d'information utilisés pour assurer les services se conçoivent désormais comme des réseaux. On entend par réseau des environnements interconnectés et organisés dans lesquels l'information circule d'un pôle à l'autre, de façon multidirectionnelle et non-hiérarchique. L'avènement des environnements en réseaux redéfinit les espaces dans lesquels circulent les informations relatives aux personnes. Ce phénomène est particulièrement apparent dans les secteurs où se profilent des projets de mise en place de services intégrés. Le fonctionnement adéquat des services publics requiert des modes efficaces d'échanges et de circulation de l'information et une protection effective du droit à la vie privée des personnes.

Tendances lourdes

- nécessité accrue du partage de l'information
- l'information doit:
 - être disponible *juste à temps*
 - être **de qualité**
- les services personnalisés, diversifiés et livrés avec célérité
- la vie privée doit être protégée contre des risques différents de ceux de l'univers-papier

La gestion collaborative induit des besoins de partager l'information. Les services intégrés comme ceux qui sont organisés autour des situations de vie supposent la capacité d'accéder à des informations détenues en une pluralité de lieux. Sans qu'il soit toujours nécessaire de la conserver et de la dupliquer. La généralisation d'Internet et des plates-formes de partage d'informations met à la portée de tous un ensemble de possibilités d'échange et de diffusion d'informations. Les internautes, citoyens gestionnaires et agents de l'État sont en mesure de communiquer, partager et échanger des informations.

La circulation et le partage des informations permettent d'améliorer la qualité et la célérité des prestations. Le travail coopératif, fondé sur les échanges et le partage de l'information, permet de réduire le nombre de situations dans lesquelles « la main droite de l'État ignore ce que fait la main gauche.... ! » En réduisant la redondance, en limitant les situations dans lesquelles les personnes sont obligées de retransmettre les mêmes informations, on réalise des gains de productivité qui devraient globalement profiter à tous.

On observe une tendance marquée vers la mise en place d'approches centrées sur le « client ». Le citoyen ou l'administré n'est plus considéré comme un « suspect » potentiel mais plutôt comme un client à qui il convient de procurer les meilleurs services disponibles dans un délai le plus bref possible et en tenant compte de sa situation spécifique. Ces approches procurent plusieurs avantages, mais leur fonctionnement a des exigences. La dispensation de services fonctionnant selon une approche client ou fortement personnalisés suppose la collecte, la détention et l'utilisation importante de renseignements personnels.

Internet et le droit

- processus automatiques et dialogues en ligne
 - guichet automatique ET
 - conseiller de haut niveau
- outils en ligne
 - d'aide à la décision
 - d'information sur les droits et obligations
- du Droit pyramidal au Droit en réseau
 - Imputabilité en silo ou partagée?
 - de la froide hiérarchie au contact direct
 - du commandement autoritaire à la régulation + ou - négociée

On peut retenir une représentation du cyberspace faisant de celui-ci 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. 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 État est en mesure d'exercer une autorité.

Le cyberspace 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 espace virtuels. Elles coexistent dans le cyberspace soit en complémentarité avec d'autres règles soit en concurrence, se proposant à la place de celles qui sont issues d'autres pôles normatifs.

Les réseaux et les interactions qu'ils rendent possibles invitent au développement d'un droit tendant à être conçu selon un modèle contractuel, fondé sur le dialogue entre l'Administration et le citoyen (l'administré).

Alors pour être efficaces, les normes de protection doivent être énoncées dans des nœuds ou pôles de normativité et surtout relayées dans les lieux d'échange.

Cela suppose une régulation au plan de la technique, des intermédiaires et surtout des acteurs eux-mêmes. Notamment une plus grande responsabilisation des acteurs de première ligne.

Tout change

- ...sauf le droit!
- Démarche classique: postuler que les règles actuelles s'appliquent aux nouveaux environnements
- Pourtant, la mise en réseau modifie les conditions concrètes du déroulement des interrelations

On ne peut continuer à se comporter comme si tout avait vocation à changer du fait de l'émergence des réseaux... sauf le droit!

On ne peut se contenter de simplement poser que les règles- le plus souvent conçues pour refléter une époque où tout se passait en silo - vont simplement s'appliquer.

Il importe de tenir compte du fait que les contextes sont modifiés par la mise en réseau.

Approche traditionnelle

- Plaquer les lois sur les nouveaux environnements
 - transposer les exigences du papier au monde virtuel
- ...quitte à multiplier les tracasseries...
 - Ex: exiger des signatures manuscrites afin de confirmer des transactions en ligne
 - exiger le consentement pour toutes sortes de transferts d'informations

Simplement reprendre le libellé des lois actuelles à la manière d'un dogme n'est pas une démarche suffisante. Il en résulte presque toujours une complexification inutile, des tracasseries et complexités inutiles.

Plutôt que de s'épuiser à tenter d'appliquer des mécanismes juridiques conçus pour répondre aux exigences d'un autre contexte technique, il faut revenir aux rationalités des lois et se demander ce que le nouveau contexte change à l'égard des risques et enjeux.

L'approche à retenir

- Revenir aux raisons qui justifient les règles
 - valeurs
 - intérêts à protéger
- Identifier les changements induits par le contexte technique
- Déterminer quelles techniques de régulation assurent la meilleure protection des droits et valeurs

Il s'agit de partir des raisons qui justifient les règles et de se demander si celles-ci sont toujours présentes.

N'y a-t-il pas d'autres enjeux?

Des enjeux sont peut être disparus?

Identifier les techniques conséquentes de réglementation. Adaptées au cyberspace.

Le plus souvent les règles cloisonnées par ministères de même que celles qui sont imposées par les modes de gestion en silo paraîtront dépassées.

Un exemple: la vie privée

- Pour protéger: il faut une analyse qui
 - revient aux fondements et
 - réévalue les méthodes de protection
- Permet une adaptation du droit qui renforce les protections... sans accentuer les blocages
- Or, le cadre actuel.....

a priori, la circulation de l'information est suspecte

- elle est confondue avec le « couplage » les méga-banques de données et la « surveillance »
- peu d'importance pour les valeurs au nom desquelles circule l'information

Le trait commun de plusieurs approches est le peu de cas ou le traitement cavalier qu'elles font des valeurs au nom desquelles certaines informations ont vocation à circuler. On en vient à prohiber la circulation de données publiques au nom d'extrapolations alarmistes.

Seuls semblent compter les dangers, généralement hypothétiques, qui pourraient exister pour la protection de la vie privée. Le biais est troublant et profondément incompatible avec l'idée selon laquelle tous les droits et libertés connaissent des balises découlant de l'exercice d'autres droits.

Un système de protection des renseignements personnels qui compterait sur le maintien de méthodes redondantes pour assurer la protection de la vie privée des personnes est susceptible de se voir complètement dépassé par les évolutions qui ne manqueront pas de métamorphoser les conditions de la gestion de l'information.

rigidification du principe de finalité

- tendance à en faire un principe limitant les usages possibles des informations personnelles.
- **conséquence:** forcer à la redondance - il faut redemander, redemander et redemander les mêmes informations -
- celles qui sont disponibles ont été recueillies pour d'autres fins.
- *Résultat: collecte excessive d'infos personnelles*

Le principe de finalité pose que l'on ne peut recueillir et utiliser l'information que pour des fins compatibles avec celles de la collecte initiale. La rigidité donnée au principe a contribué à immobiliser l'information personnelle. On a eu tendance à en faire un principe limitant les usages possibles de ces informations personnelles. Cela a eu souvent pour conséquence de forcer à la redondance : les organismes doivent redemander et redemander les mêmes informations car celles qui sont disponibles ont été recueillies pour d'autres fins.

Le principe de finalité est bien davantage lié au maintien de la qualité de l'information.

Une information peut très bien convenir pour répondre à un besoin. Elle sera inadéquate, voire franchement contre-indiquée, pour répondre à un autre type de besoin. Dans l'univers des réseaux où l'information est persistante et circulante, il importe de revenir aux fondements véritables du principe de finalité. Il s'agit d'assurer que les informations utilisées sont de qualité adéquate pour servir aux fins envisagées, non ériger la redondance en garantie de la vie privée !

statisme de l'information

- si l'information ne circule pas, la vie privée est sauve!
- la circulation de l'information est assimilée au couplage et aux menaces de surveillance...
- ...alors qu'elle pourrait réduire les risques

Il y a 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. Aussi, a-t-on vu la Commission émettre des avis dans lesquels elle demande une démonstration de la nécessité du transfert ou du partage de l'information. Les renseignements personnels demeurent associés à l'établissement entendu comme lieu physique. Plusieurs avis de la Commission montrent des réticences à admettre que les informations d'un organisme pourraient être partagées. Des dispositions sont pourtant prévues dans la loi pour permettre et encadrer le partage d'informations. Elles ont été assorties d'exigences, non prévues dans la loi, de démontrer la nécessité des partages et des transferts.

Pourtant, la notion de nécessité retenue par la Commission et la Cour du Québec dans des décisions d'adjudication ne renvoie pas à une condition *sine qua non* pour l'accomplissement des devoirs et fonctions de l'organisme. Il suffit d'établir que le renseignement est raisonnablement requis, compte tenu de l'ensemble des contraintes dans lesquelles évolue l'organisme. Raymond Doray et François Charrette concluent de ces décisions que « serait nécessaire au sens de l'article 64, un renseignement requis pour répondre aux besoins de l'organisme, c'est-à-dire à la bonne marche de ses attributions ou d'un programme dont il a la gestion ».

multiplication des lois d'exceptions

- de plus en plus de lois dérogatoires
 - pour rétablir les équilibres rompus en matière de protection des renseignements personnels
- au Québec, une loi a été adoptée afin de permettre la circulation d'informations de manière à prévenir les suicides
- le droit à la vie privée l'emporte sur le droit à la vie!

Au Québec, une loi a été adoptée afin de permettre la circulation d'informations de manière à prévenir les suicides. Cette loi a ajouté l'article 59.1 à la Loi d'accès prévoyant que :

Un organisme public peut communiquer un renseignement nominatif, sans le consentement des personnes concernées, en vue de prévenir un acte de violence, dont un suicide lorsqu'il existe un motif raisonnable de croire qu'un danger imminent de mort ou de blessures graves menace une personne ou un groupe de personnes identifiable. [Loi modifiant diverses dispositions législatives eu égard à la divulgation de renseignements nominatifs en vue d'assurer la protection des personnes, L.Q., 2001, c. 78.]

Que l'on en soit venu à une telle solution pour rendre juridiquement possible ce qui aurait été, dans une interprétation raisonnable et nuancée de la loi, un motif légitime de donner accès à des informations personnelles illustre à quel point on en est venu à une conception rigide du droit de la protection des renseignements personnels. Jusqu'à cet amendement, la notion de renseignements personnels était lue de manière à faire prévaloir la protection des renseignements nominatifs sur la protection de la vie ! L'interprétation qui en a été donnée de même que les exigences que l'on a développées à l'égard de son application ont fait en sorte que cette législation paraît beaucoup moins adaptable qu'on aurait pu le croire lors de sa mise en vigueur.

crispation sur les moyens

- Attachement aux cloisonnements hérités de l'univers fondé sur le papier
 - l'univers « en silo » est érigé en dogme
 - le réseau est suspect...
 - pourtant.....le cloisonnement est un moyen, souvent par défaut....de protéger, non une fin en soi...
 - multiplication des incantations pour assurer le respect d'exigences dépassées même si cela est absurde....

Il y a 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. Aussi, a-t-on vu la Commission émettre des avis dans lesquels elle demande une démonstration de la nécessité du transfert ou du partage de l'information. Les renseignements personnels demeurent associés à l'établissement entendu comme lieu physique. Plusieurs avis de la Commission montrent des réticences à admettre que les informations d'un organisme pourraient être partagées. Des dispositions sont pourtant prévues dans la loi pour permettre et encadrer le partage d'informations. Elles ont été assorties d'exigences, non prévues dans la loi, de démontrer la nécessité des partages et des transferts.

Dans son *Guide en matière de protection des renseignements personnels dans le développement des systèmes d'information*, la CAI écrit : *En dépit du mouvement de concentration des traitements et des données qui s'opère au sein des organisations publiques, la gestion des renseignements personnels ne doit pas s'opposer à l'idée de cloisonnement de l'information ...* À la page 14 de son guide, la CAI affirme : *Les principes...reprennent chacun à leur manière l'idée que la dispersion des renseignements personnels et le cloisonnement administratif des organismes détenant ces mêmes renseignements représentent les meilleurs gages de confidentialité;*

Pourtant, le principe selon lequel l'information doit demeurer au sein de l'entité qui l'a recueillie et pour ses fins est un moyen de protection, pas une fin en soi.

Mythologie du « consentement »

- Le recours au consentement : un palliatif à la rigidité du cadre de protection
- Devant la domination des interprétations rigides, on tend à rechercher des consentements
- à « gérer » le consentement....
- même lorsque cela est factice...

L'obligation d'obtenir le consentement servait à l'origine à baliser le droit de procéder à des interventions médicales. En l'important dans le champ de la protection des renseignements personnels le procédé a induit une rigueur à l'origine conçue pour encadrer les interventions pouvant avoir des conséquences infiniment plus drastiques ! Les exigences au sujet du caractère libre, éclairé, non équivoque et consigné par écrit pouvaient fort bien se comprendre lorsqu'il s'agit de porter atteinte à l'intégrité physique d'une personne. Est-ce adapté aux transferts d'informations, dont plusieurs sont effectués dans l'intérêt même du citoyen ?

Cette exigence de consentement a engendré un dysfonctionnement particulièrement visible lorsque vient le temps de penser la circulation de l'information dans les réseaux. Pour contourner la difficulté découlant du caractère excessivement englobant de la notion de renseignements personnels, on a vu se développer des pratiques fondées sur une véritable mythologie du consentement "libre et éclairé." On parle maintenant de « gérer le consentement » comme si cela était toujours une exigence de la loi. En réalité, hormis certaines interprétations contestables, il n'est pas nécessaire d'obtenir un consentement aussi tatillon pour chaque mouvement d'information personnelle. On en vient à se demander si les ressources qu'on se croit obligé de consacrer à la gestion des consentements ne seraient mieux investies dans une gestion plus serrée des informations personnelles, en fonction des risques posés par celles-ci.

Pour une approche actualisée pour protéger la vie privée dans les réseaux

- d'une protection formaliste
 - basée sur les règles tatillonnes, d'application mécanique
- à une protection effective - mieux ciblée

Le cadre actuel de la protection de la vie privée et des renseignements personnels insiste sur le respect d'une série de procédures formelles. Il y a peu de place laissée à l'appréciation des enjeux et du contexte. Issue d'une conception quasi-théologique des « menaces pour la protection de la vie personnelle » le cadre actuel est d'une part inutilement rigide alors qu'il laisse pratiquement incontrôlé les véritables activités de surveillance, celles contre lesquelles il est supposé avoir été mis en place.

Ainsi, l'on multiplie les règles tatillonnes sans se soucier des véritables enjeux.

Alors même que l'on s'inquiète tant au sujet des périls que ferait courir la circulation des données personnelles, les activités de surveillance - les véritables celles-là - semblent s'exercer sans que cela paraisse contrevenir aux lois sur la protection de la vie privée. Par exemple, alors que l'article 36 (4) du Code civil du Québec déclare que le fait de « surveiller la vie privée d'une personne par quelque moyen » peut être constitutif d'une atteinte à la vie privée, il est de notoriété publique que des agences font commerce d'investiguer sur les gens, les surveillent et collectent de l'information sur leur compte.

Des fondements plus cohérents

- Le principe de finalité : revenir au fondement de base - la qualité
- La confiance
 - via la transparence
 - l'information
 - le dialogue avec les personnes concernées
- L'effectivité des protections
 - plutôt que des protection formalistes et légalistes

Il faut s'attacher à appliquer les principes de la protection de la vie privée en tenant compte des contextes variés du cyberspace qui n'est pas réductible à un ensemble de banques de données isolées les unes des autres et invariablement susceptibles de servir à la surveillance des personnes. En l'état actuel de la législation québécoise, tous les renseignements personnels sont traités sur le même pied. Il est de plus en plus manifeste que cette approche globalisante est irréaliste en certains contextes, qu'elle protège ce qui n'a pas besoin de protection et pire, qu'elle laisse sans protection, des volets entiers de la vie privée des citoyens.

Ainsi, plutôt que de se crisper sur une règle de respect des finalités appliquée de façon statique, il faut revenir au fondement du principe de finalité et l'appliquer de manière à promouvoir l'obligation de faire usage d'information présentant les qualités appropriées pour les fins auxquelles on veut les utiliser.

Il faut surtout revoir les approches afin d'accroître l'effectivité des protections plutôt que de s'en remettre à une protection formaliste qu'on n'a pas les moyens d'appliquer.

Un cadre juridique assurant une protection effective de la vie privée dans les réseaux

- Mieux cibler les périls et enjeux
 - remplacer les scénarios catastrophes ...
 - par une **démarche publique de divulgation et de prise en charge des risques**
 - en expliquant ce qu'on fait de l'information personnelle
- Les informations « de surveillance » sont distinctes des autres informations personnelles

L'avènement de l'administration électronique ne doit pas engendrer d'accroissement des activités de surveillance de l'État. Ces activités relèvent en principe des forces de police et sont encadrées en conséquence. Il ne revient pas aux organismes publics chargés de procurer les prestations prévues par les lois d'implanter des systèmes ou des opérations de surveillance des citoyens.

Le régime des informations utilisées à des fins de surveillance policière est en grande partie déterminé par le droit criminel et pénal relevant du Parlement fédéral. Il faut assurément rechercher la mise en place de balises au droit des forces policières de collecter, de détenir et d'échanger des informations sur les personnes. Mais ce n'est certainement pas en rendant plus difficile la gestion des informations dans les réseaux chargés d'assurer les prestations de services aux citoyens que l'on obtiendra ce résultat.

Assurer un environnement de confiance

- Des garanties quant à la qualité des informations personnelles
 - la qualité de l'information utilisée
 - la maîtrise des données personnelles
 - le dialogue entre la personne concernée et les organismes publics
- Des moyens de protection plus efficaces de la vie privée dans les réseaux

La confiance est une composante essentielle de tout cadre de gestion des informations portant sur les personnes. Tout au long du cycle de traitement de l'information, il faut garantir un environnement dans lequel l'utilisateur/citoyen est véritablement en confiance. C'est dès l'étape de la cueillette que se construit le lien de confiance essentiel à la bonne gestion de l'information. La cueillette et le traitement de l'information doivent se faire dans un climat de transparence. En misant sur l'information de l'utilisateur à l'égard de ce qu'il advient de l'information qu'il confie à l'État, on tisse un climat de confiance. Plus les informations demandées sont susceptibles d'être sensibles, plus il faut multiplier les précautions afin de garantir le niveau de confiance nécessaire. Par exemple, les données personnelles recueillies lors du recensement sont assorties de règles très strictes : elles ne peuvent être utilisées à quelques autres fins. Lorsque des garanties sont données, il faut impérativement qu'elles soient respectées et que des mesures garantissent un tel respect.

Le développement de services en réseaux appelle à une relecture de la notion de finalité. Ce qui importe désormais est que l'utilisateur soit informé des familles de finalités auxquelles serviront les informations. La notion de finalité doit en effet être axée sur l'utilisateur, non sur les structures gouvernementales.

Des espaces de confiance

- un ensemble de mécanismes balisant la **circulation** de l'information dans des espaces régulés
 - pour l'accomplissement de prestations conçues en fonction des personnes - non des organigrammes
- et en délimite les usages
- organiser l'espace au sein duquel les informations peuvent circuler
- les protections sont modulées en fonction des risques *évalués*, non des scénarios catastrophe

Si les organismes publics travaillent en réseaux et collaborent d'avantage afin de proposer des services à la carte et personnalisés, il faut que l'information puisse circuler de manière conséquente. Cela appelle la mise en place des outils nécessaires pour procurer les garanties et les protections que requiert l'information portant sur les personnes. Dans un tel contexte, la notion de domaine de confiance prend une importance considérable.

Par domaine de confiance, on entend un ensemble de mécanismes balisant la circulation de l'information et en délimite les usages. La notion vise à organiser l'espace au sein duquel les informations peuvent circuler. Il s'agit de disposer d'un cadre permettant de définir les droits et les responsabilités relatives à l'information sur les personnes lorsque celle-ci se trouve dans un réseau. La notion de domaine de confiance a d'abord été mise de l'avant dans le champ du commerce électronique, particulièrement dans la littérature relative à la sécurité. Elle renvoie à la nécessité que les protagonistes se sentent en confiance pour que des transactions significatives se déroulent dans un environnement électronique. L'une des dimensions les plus cruciales de l'établissement d'un domaine de confiance est d'identifier l'autorité responsable du service ou de l'échange. Si, dans un contexte d'État en silo où l'information demeure en principe cloisonnée dans l'organisme public qui l'a recueillie, dans un État en réseau, l'information circule entre les organismes afin d'offrir des bouquets de prestations électroniques. Alors, il pourra être nécessaire d'identifier le statut juridique et les responsabilités liées à un domaine de confiance déterminé.

Le droit à une technologie compatible avec la protection de la vie privée

- prise en compte des impératifs de protection dès la conception des systèmes
- la sécurité : une condition nécessaire mais insuffisante
- l'obligation d'évaluer les risques et de spécifier les mesures pour leur prise en charge

La protection effective de la vie privée appelle le développement d'un droit à ce que soient mis en place des environnements technologiques qui accroissent la protection de la vie privée plutôt que de la diminuer. Les décideurs publics et les entreprises privées pourraient se voir imposer l'obligation de démontrer que la technologie qui est mise en place est la plus respectueuse pour la vie privée. Pour y arriver, il faudrait qu'il existe une obligation de planifier la mise en place de technologies en tenant compte des dimensions juridiques. Ce n'est pas toujours ainsi que sont planifiés les systèmes d'information. Très souvent, les environnements d'information sont développés sans se soucier des dimensions juridiques et présentés ensuite comme une sorte de situation inévitable à laquelle il faut s'adapter. S'il est un domaine où le droit devrait jouer un plus grand rôle, c'est au niveau des balises lors du développement d'environnements d'information.

Une protection effective

- la répression *a posteriori* des abus
 - une répression *a posteriori* efficace est plus utile qu'une réglementation *a priori* stricte non-appliquée
 - monitoring des accès
- des mécanismes effectifs de sanction des droits
 - notamment des mécanismes en ligne de gestion des conflits
 - sanctions disciplinaires

Il y a des informations portant sur les personnes et qui ont de l'importance pour d'autres. Par exemple, il existe des informations à caractère public qui peuvent être consultées afin de prendre une décision éclairée. Le seul fait que de telles informations présentent une possibilité d'être utilisées de manière abusive ne doit pas conduire à les censurer à titre préventif. À l'égard des possibilités d'usage abusif des informations publiques, il faut plutôt organiser des mécanismes efficaces de sanction une fois avérés les usages abusifs. Une telle approche évite de censurer les informations de manière préventive mais réserve des sanctions dissuasives pour les situations où il y a usage abusif de données.

L'efficacité de la protection de la vie privée est tributaire de l'existence de possibilités réelles d'exercice des recours lorsqu'il y a eu violation.

La généralisation des activités dans les réseaux doit s'accompagner de la mise en place d'outils appropriés, préférablement situés au sein même de ces environnements afin d'assurer l'exercice efficace des droits des personnes. On voit mal comment il sera possible de maintenir un processus judiciaire ou quasi-judiciaire opérant à la vitesse de l'escargot alors que les transactions s'effectuent à la vitesse de la lumière! Dans la mise en place des systèmes d'information inhérents à l'administration électronique, il faut assurer la mise en place de mécanismes assurant le respect effectif de la vie privée de même que les correctifs qui peuvent se révéler nécessaires à l'usage.

Conclusion

- prendre acte des mutations que la généralisation des environnements en réseaux provoque dans les conditions de production et de circulation des informations.
- ces mutations affectent particulièrement les environnements destinés à procurer les services intégrés

En somme, les citoyens trouveront légitime que les informations nécessaires à l'application de familles de services circulent dans des environnements où elles pourront être partagées et réutilisées. Ils seront d'autant plus enclins à trouver légitime une telle circulation que cela paraît clairement nécessaire à l'accomplissement d'un ensemble de missions complémentaires ou interreliées.

La légitimité de pareilles circulations d'informations personnelles est renforcée lorsque les processus de décision imposent qu'à chaque fois que l'on entend prendre une décision au sujet d'une personne, on lui présente- en ligne ou autrement- l'information sur laquelle on entend se fonder.

Le citoyen se trouve à même de réviser et, le cas échéant de rectifier les informations personnelles. Ainsi, l'effort est mis, non plus sur la collecte redondante des informations mais sur les assurances effectives permettant de garantir que l'information sera de qualité pour les fins spécifiques auxquelles elle est destinée.

Dans un contexte de réseau

- cesser de confiner les renseignements nominatifs dans les « silos » mais favoriser leur circulation encadrée
 - saisie unique
 - usages multiples, justifiés et ciblés
- dans des espaces de circulation dignes de confiance
- dotés d'un statut garantissant que les informations seront de qualité et qu'elles ne seront utilisées qu'aux fins compatibles.

Assurer la possibilité de transiger sans s'identifier dans toutes les situations où l'identification n'est pas nécessaire. Par contre, il arrivera souvent que la fourniture de services publics nécessite, dans l'intérêt même des citoyens, que l'on exige des informations permettant de disposer d'une certitude raisonnable quant à l'identité de la personne ou de son droit à un bien ou à un service gouvernemental.

D'autre part, les informations portant sur les personnes ne peuvent être toujours envisagées comme relevant d'un droit de veto de la personne concernée. Ces informations possèdent des dimensions sociales qui intéressent les autres. Dans plusieurs situations, les tiers ont un intérêt tout à fait légitime à connaître des informations sur nous. Oublier cela c'est nier le caractère social de l'être humain. Le défi est de lutter efficacement contre les usages abusifs des informations portant sur autrui, non de conférer un droit de veto susceptible d'être exercé de façon préjudiciable au bon fonctionnement des services.

Renforcer le statut des informations sensibles

- celles qui portent directement sur la vie privée des personnes
 - dossier médical
 - dossier détenu par l'établissement de soins
 - secret professionnel
- ces informations ne circulent que dans des domaines spécifiques et moyennant des encadrements stricts.

Les données sensibles sont celles qui concernent effectivement la vie privée des personnes. Par exemple, les données relatives à l'état de santé ou le dossier fiscal d'un individu. De telles données ne peuvent circuler que dans un domaine de confiance bien délimité, par exemple au sein du réseau socio-sanitaire. Un haut niveau de protection doit être garanti à ces données. Leur circulation doit être conditionnelle au respect d'un ensemble de conditions très strictes. Les échanges de ces données n'ont lieu qu'au sein d'un même domaine de confiance, par exemple, le domaine de confiance des autorités fiscales. Il devrait être interdit de les transmettre en dehors du domaine de confiance concerné.

Merci!

Pierre Trudel, professeur
Titulaire de la Chaire L.R. Wilson sur le droit des technologies de l'information et du commerce électronique
Centre de recherche en droit public, Faculté de droit
Université de Montréal
C.P. 6128, succursale Centre-ville
Montréal (Québec) Canada H3C 3J7
Tél : (514) 343-6263
Fax : (514) 343-7508
Courriel : pierre.trudel@umontreal.ca
URL: <http://www.crdp.umontreal.ca>

Repères bibliographiques

COMMISSION D'ACCÈS À L'INFORMATION, Guide en matière de protection des renseignements personnels dans le développement des systèmes d'information, décembre 2002, < http://www.cai.gouv.qc.ca/fra/biblio_fr/bib_pub_fr.htm > p. 12.

SECRÉTARIAT DU CONSEIL DU TRÉSOR, Architecture gouvernementale de la sécurité de l'information numérique, architecture-cible globale, sommaire, Québec, Sous secrétariat à l'inforoute gouvernementale et aux ressources informationnelles, septembre 2001. < www.autoroute.gouv.qc.ca/publica/pdf/agsin-ciblesom.pdf >

Cynthia Chassigneux, Claudine Fecteau, Bartha Maria Knoppers, Pierre Trudel, *L'encadrement juridique de la protection des renseignements personnels dans le secteur de la santé et des services sociaux*, Université de Montréal, Centre de Recherche en Droit Public, Juin 2001.

Pierre TRUDEL, « Quel droit et quelle régulation dans le cyberspace? » *Sociologie et sociétés*, vol. 32, no 2, automne 2000, 189-209. < <http://www.erudit.org/erudit/socsoc/v32n02/trudel/trudel.pdf> >

Pierre Trudel, « La protection de la vie privée dans les systèmes d'information relatifs à la santé. Ajuster les concepts aux réalités des réseaux, » dans Christian HERVÉ, Bartha-Maria KNOPPERS et Patrick A. Molinari, *Les pratiques de recherche biomédicales visitées par la bioéthique*, Paris, Dalloz, 2003, 163-176.