Centre de recherche en droit public
Chaire L.R. Wilson sur le droit des technologies de
l'information et du commerce électronique
Faculté de droit
Université de Montréal

Améliorer la protection de la vie privée dans l'administration électronique : pistes afin d'ajuster le droit aux réalités de l'État en réseau

par

Pierre TRUDEL

Courriel : pierre.trudel@umontreal.ca

Mars 2003

Améliorer la protection de la vie privée dans l'administration électronique : pistes afin d'ajuster le droit aux réalités de l'État en réseau

Pierre TRUDEL[*]

Table des matières

---

[*] 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. Ce rapport a été rédigé à la demande du Ministère des relations avec les citoyens et de l'immigration du Québec. L'auteur a bénéficié de l'aide de France Abran et Richard Langelier, agents de recherche au Centre de recherche en droit public. Marc Lafrance et Robert Parent du Ministère des relations avec les citoyens et de l'immigration ont formulé d'utiles commentaires sur une version antérieure de texte. L'auteur demeure toutefois l'unique responsable des lacunes qui subsistent dans ce texte.

Sommaire

Ce rapport identifie les changements dans les approches pour assurer effectivement la protection de la vie privée et des renseignements personnels dans le contexte des services publics offerts dans les 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.

On rappelle les traits qui caractérisent l'administration électronique. On constate que l'État en réseau suppose un partage accru de l'information de même qu'il permet une plus grande personnalisation des rapports entre le citoyen et l'administration. Du coup on peut tabler sur un potentiel accru de dialogue entre l'État et les citoyens. Un tel dialogue est un atout majeur dans l'accroissement de l'effectivité du droit à la vie privée. L'intensification de la circulation de l'information portant sur les personnes n'emporte pas en soi une plus grande surveillance : il importe de distinguer les informations servant à la surveillance policière de celles utilisées pour assurer les services aux citoyens.

On passe ensuite en revue les fondements et l'application du droit relatif à la protection des renseignements personnels. On fait le constat que plusieurs fondements qui sous-tendent le droit actuel de la protection des renseignements personnels ne tiennent plus dans le contexte des réseaux. Les conceptions selon lesquelles le droit de la protection des renseignements personnels répond à des dangers de surveillance sont aujourd'hui dépassées et portent à orienter les protections sur les mauvaises cibles.

Le ciblage défectueux du droit de la protection des renseignements personnels affaiblit la protection de la vie privée des personnes. Non seulement se trouve-t-on à nier la légitimité de la circulation de certaines informations dans les espaces publics, mais l'extension indue du principe de finalité et surtout l'interprétation rudimentaire qui en a été retenue porte à privilégier une protection purement formelle des renseignements personnels en imposant des barrières, souvent artificielles et tatillonnes à la circulation de l'information sans gain pour la protection de la vie privée. Devant les rigidités découlant de ces interprétations abusives, tant les administrations que les législateurs ont été amenés à recourir à des expédients comme le développement de pratiques de gestion du consentement et on a multiplié les lois d'exception, affaiblissant ainsi la protection des renseignements personnels.

Il faut actualiser les approches afin de protéger effectivement la vie privée dans les réseaux. Le cadre juridique doit assurer la dévolution des efforts conséquents à l'égard des informations personnelles présentant des enjeux significatifs pour la vie privée. Il faut recentrer le cadre juridique de manière à accroître les garanties de qualité de l'information utilisée pour assurer la prestation des services aux citoyens. Dans l'univers des réseaux, l'information est persistante et circulante. Il importe de revenir aux fondements véritables du principe de finalité : assurer que les informations utilisées sont de qualité adéquate pour servir aux fins envisagées, non ériger la redondance en garantie de la vie privée !

Le rapport expose comment concevoir des droits actualisés afin de protéger efficacement la vie privée dans le contexte des réseaux de service publics. Une telle reconceptualisation doit évidemment faire une distinction entre les informations de police et celles qui sont requises pour assurer les services aux citoyens. À toutes les étapes du cycle de gestion de l'information, il importe de garantir un environnement de confiance. Le cadre juridique devrait aussi assurer un niveau adéquat de maîtrise des informations personnelles de même que reconnaître le droit à une technologie compatible avec le respect de la vie privée.

Au plan des moyens d'assurer les protections appropriées, il est recommandé d'inscrire dans la législation la notion de domaine de confiance en tant qu'entité, pouvant être de forme diversifiée, au sein de laquelle peuvent circuler des renseignements personnels moyennant des conditions prédéfinies. Les efforts de protection doivent être modulés aux différences de sensibilité des informations. Il faut reconnaître le droit des citoyens à une technologie compatible avec la protection de la vie privée et mettre en place des mécanismes effectifs de sanction des droits.

La modernisation effective du droit de la protection des renseignements personnels passe par une relecture critique des applications qui en a été faite et une évaluation lucide des contextes dans lesquels circulent désormais les informations. Ce serait affaiblir le droit à la vie privée que de se réfugier dans une frileuse défense des façons de faire héritées des époques antérieures puisque cela accroît les risques d'une protection purement formelle, passant à côté des véritables périls.

Introduction

Le contexte de la circulation des informations portant sur les personnes connaît des changements significatifs. Les systèmes d'information utilisés pour assurer les services publics 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 le secteur public où se profilent de plus en plus des projets de mise en place de services publics en ligne voire de « gouvernement électronique ». 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.

Le droit de la protection des renseignements personnels dans les organismes publics apparaît de plus en plus comme un droit à renouveler. Plusieurs évolutions ont marqué le fonctionnement des États modernes[1] depuis la mise en place des lois d'accès au cours de la décennie 1970-1980. Il existe une abondante littérature vantant les bienfaits que les technologies de l'information pourraient procurer à l'administration au plan de son efficacité. Plusieurs préoccupations sont soulevées au sujet des périls que l'implantation des technologies de l'information dans l'administration publique pourrait comporter pour la protection de la vie privée. On a parfois l'impression d'être pris entre ces deux extrêmes que sont d'une part, le discours promotionnel au sujet des merveilles des technologies de l'information et, d'autre part le discours alarmiste au sujet des dangers réels ou supposés pour la vie privée. Entre ces deux dérives, il reste peu de place pour envisager comment devrait être redéfini un ensemble de droits susceptibles de garantir, dans le contexte nouveau des technologies de l'information, une véritable protection des droits des citoyens.

La migration dans les environnements-réseaux de plusieurs activités et services publics requiert de revoir les notions permettant de déterminer ce qui doit être protégé comme relevant de la vie privée et l'information qui doit circuler puisqu'elle participe à l'espace public, contribue au déroulement de la vie sociale et permet d'assurer les meilleurs services aux citoyens. Il devient aussi nécessaire de préciser les critères permettant de distinguer les informations vraiment susceptibles d'usages attentatoires à la vie privée des personnes de celles qui relèvent des conditions inhérentes à la vie en société.

En particulier, il importe de distinguer l'État contrainte et l'État prestataire de services. L'État-contrainte –celui qui assure les fonctions de police est doté d'un régime juridique spécifique pour les informations sur les personnes. Une part importante du cadre juridique de l'État-contrainte relève du droit criminel et est de ce fait sous la juridiction des autorités fédérales. Ce cadre juridique ne doit pas être confondu avec celui qui s'applique à l'État fournissant des services aux citoyens : c'est principalement à ces fonctions que s'appliquent les lois sur les renseignements personnels dont il sera ici question. La généralisation des activités susceptibles de se dérouler désormais de plus en plus dans des environnements comme Internet requiert une redéfinition de

---

[1] Voir en général : Miriam LIPS, « Designing Electronic Government Around the World. Policy Developements in the USA, Singapore, and Australia », (2000) 7 *EDI Law Review*, 199-216.

l'espace dans lequel circulent les renseignements personnels avec la place accrue que prend désormais le virtuel. Ce rapport expose :

- les fondements, principes et valeurs caractéristiques des approches actuelles en matière de protection des renseignements personnels et leur pertinence dans le contexte des réseaux;

- les conséquences des modifications induites par la généralisation des réseaux sur la production et la circulation des informations relatives aux personnes;

- ce que révèle l'analyse des tendances des législations des autres états occidentaux;

- les avantages et les limites des définitions actuelles et des règles découlant du cadre juridique en matière de renseignements personnels, notamment dans les situations d'interactions dans des réseaux;

- les avenues pour de nouvelles approches en matière de protection de la vie privée dans le monde en réseaux.

La gestion de l'information est un élément essentiel de l'activité gouvernementale. La *Loi sur l'administration publique* reflète l'importance de l'information dans le fonctionnement de l'administration. L'administration électronique suppose la circulation accrue d'informations. Le déroulement en réseau de plusieurs des activités inhérentes aux fonctions de l'État comporte plusieurs avantages. Il favorise une organisation centrée sur le citoyen ou l'usager; il facilite la collaboration et le travail coopératif entre une pluralité d'acteurs, de statut différent. Il favorise une organisation se démarquant du modèle hiérarchique. Il permet la spécialisation flexible se fondant sur l'échange entre des pôles agissants de connaissance.

Le Québec s'est doté d'une politique afin de faire profiter la société des avantages que laissent prévoir les technologies de l'information pour l'amélioration générale des conditions de vie. Ainsi, la politique sur l'Autoroute de l'information affirme que :

> […] *c'est d'abord par la généralisation du commerce électronique que l'économie québécoise pourra le plus profiter de l'apport des inforoutes. C'est dans ce but que le gouvernement étendra l'usage de l'inforoute à l'essentiel de ses échanges et de ses transactions avec les entreprises, qu'il prendra les moyens requis pour soutenir le déploiement du commerce électronique dans les entreprises, par la formation, l'information et le soutien technique, et qu'il prendra les mesures requises pour l'établissement d'un environnement électronique sécuritaire, notamment par l'élaboration d'une politique en matière de cryptographie.*
>
> *Le Québec a joué un rôle de pionnier dans l'établissement d'un cadre législatif et réglementaire en ce qui concerne le respect de la vie privée et la protection des renseignements personnels, et ce, autant dans le secteur public que dans le secteur privé. Cette attitude de la société québécoise doit se refléter sur l'inforoute.*[2]

---

[2] Politique québécoise de l'autoroute de l'information, version abrégée, < http://www.autoroute.gouv.qc.ca/politique/sommaire.html >

Des initiatives innovatrices ont été mises en place pour favoriser l'application des principes de protection de la vie privée et des renseignements personnels dans les contextes caractéristiques des inforoutes. Ainsi, des lois ont été adoptées afin d'actualiser les règles devant assurer l'encadrement des activités se déroulant dans les réseaux.

La généralisation des activités susceptibles de se dérouler désormais de plus en plus dans des environnements comme Internet requiert une redéfinition de l'espace dans lequel circulent les renseignements personnels avec la place accrue que prend désormais le virtuel. Il devient en effet nécessaire de revoir les notions qui aident à déterminer ce qui doit être protégé comme relevant de la vie privée et l'information qui doit circuler puisqu'elle participe à l'espace public, contribue au déroulement de la vie sociale ou à assurer le bon fonctionnement des services publics.

Le défi est donc de définir des modalités de la circulation des informations dans les réseaux qui tiennent compte à la fois :

- de la nécessité d'assurer la protection de la vie privée, et ce, compte tenu des changements quantitatifs et qualitatifs que le cyberespace induit quant aux dangers pour la vie privée;

- de la nécessité de la libre circulation des informations qui témoignent de la participation à la vie sociale des personnes. C'est ce dernier impératif qui est habituellement oublié par plusieurs auteurs et groupes de pression s'intéressant à la protection des renseignements personnels.

Il faut à cette fin, identifier les jalons et repères appropriés afin d'assurer la protection de la vie privée sans pour autant mettre en péril la libre circulation de l'information afférente à l'espace public. Plusieurs écrits sur la protection des renseignements personnels font fi du caractère social de certaines informations relatives aux personnes.

La rituelle référence à quelques sondages faisant état du fait que les populations s'inquiètent à propos de leur vie privée tient habituellement lieu de justification aux interprétations rigides des règles relatives à la protection des renseignements personnels.

Les analyses des périls réels ou appréhendés pour la vie privée que présentent les technologies de l'information ne procurent pas toujours des approches respectueuses des équilibres à préserver entre les droits. Il y a une tendance à y substituer une conception des droits posant la vie privée comme un absolu. Ces démarches ne permettent pas un renouvellement approprié du cadre juridique de la protection des renseignements personnels dans les contextes qui prévalent désormais. Il faut aborder la question de la protection des renseignements personnels dans le contexte de l'État en réseau de façon moins alarmiste. Il importe de laisser de côté certaines idées reçues et non encore vérifié au sujet des périls qui pourraient en résulter pour la vie privée. Plutôt que de postuler que l'État cherche constamment à « surveiller » les citoyens, il faut s'interroger sur les précautions à prendre, compte tenu des risques de dérive dans des environnements voués à servir les citoyens.

Dans une première partie, on passe en revue le phénomène de l'administration électronique, ses principales caractéristiques au plan de l'information sur les personnes de même que les éléments

principaux du cadre juridique destiné à faciliter la mise en place des services électroniques de l'État.

Dans la seconde partie, l'on propose une revue critique plusieurs concepts fondateurs du droit de la protection des renseignements personnels. On démontre que ceux-ci doivent être adaptés aux exigences découlant de la généralisation des réseaux. On relève le caractère trop simplificateur de la notion de renseignements personnels, les effets pervers du paradigme de la « surveillance » qui est sous-jacent à l'interprétation dominante du droit actuel de la protection des données personnelles. Ce paradigme mené à des interprétations englobantes de ce que recouvre la notion de renseignements personnels. Il a favorisé une interprétation rigide de plusieurs notions de même qu'une tendance à complexifier ou interdire la circulation des informations. Des expédients ont dû être surdéveloppés afin de pallier à ces dérives au plan de l'interprétation des lois sur la protection des renseignements personnels. Le résultat de cette évolution est une complexité inutile et coûteuse au plan de la protection de la vie privée.

Enfin, dans la troisième partie, sont présentés les éléments d'un cadre actualisé capable d'assurer effectivement la protection des renseignements personnels dans les espaces de réseaux consacrés aux services publics.

I- L'administration électronique

Les environnements de réseaux induisent des changements dans les conditions de la circulation des informations. Le caractère interactif du réseau et ses conséquences sur les risques qui en résultent pour la vie privée est ainsi mis en relief par Yves Poullet :

> *L'interactivité des réseaux et leur utilisation de plus en plus banalisée expliquent que nous soyons les premiers auteurs des traces qu'en permanence nous créons, tantôt par le dialogue avec un site web, tantôt par le déplacement de notre voiture équipée d'un GPS, tantôt par l'utilisation de mobilophones désormais reliés à Internet.*[3]

Les informations circulent de moins en moins dans des banques de données localisées et de plus en plus dans des environnements réseaux. Cela emporte des conséquences sur les approches à privilégier pour assurer l'équilibre entre la protection de la vie privée des personnes et les impératifs d'efficacité des systèmes de gestion des divers services publics.

La notion d'administration électronique est une réalité en devenir dans la plupart des pays développés. La Banque mondiale en propose la définition suivante :

> *E-Government refers to the use by government agencies of information technologies (such as Wide Area Networks, the Internet, and mobile computing) that have the ability to transform relations with citizens, businesses, and other arms of government. These technologies can serve a variety of different ends : better delivery of government services to citizens, improved interactions with business and industry, citizen empowerment through access to information, or more efficient government management. The resulting*

---

[3] Yves POULLET « Internet et vie privée : entre risques et espoirs », (2001) 120 *Journal des tribunaux* 155.

> *benefits can be less corruption, increased transparency, greater convenience, revenue growth, and/or cost reductions.*[4]

L'expression renvoie évidemment aux changements que la généralisation des technologies de l'information induit dans l'administration publique. Dominique Gerbod et Fabien Paquet relèvent deux tendances fondamentales qui leur semblent caractériser l'administration électronique[5]. Il s'agit de l'orientation vers le citoyen et la gestion collaborative.

Orientée vers le citoyen, l'administration électronique vise à profiter des possibilités des technologies de l'information pour rapprocher le citoyen de l'administration, faciliter les démarches et les interactions que ce dernier entretient avec les administrations gouvernementales. Ces dernières fonctionnent de plus en plus en étroite relation.

Fruit d'une réflexion menée en France sur les conditions de la mise en place de l'Administration électronique, le Rapport Lasserre constate que dans les réseaux, l'information peut circuler de manière à accroître le dialogue entre l'État et les administrés. Le rapport fait valoir que :

> *Dans un modèle d'organisation administrative cloisonnée, l'information était un enjeu de pouvoir que les services ne partageaient qu'avec réticences. Le développement des réseaux permet au contraire de nouvelles circulations de l'information, à partir du moment où quelques grands principes seront définis pour la valider et la diffuser.*[6]

De nouvelles situations appellent une circulation différente de l'information. L'information personnelle n'est plus tant un outil de contrôle mais plutôt un élément de processus décisionnels multiples conçus suivant une perspective de service à rendre au citoyen. Ce constat met en relief la distinction qui existe entre les informations recueillies et détenues à des fins de prévention du crime et celles qui servent à assurer la prestation des services.

Alors que les craintes souvent exprimées portent sur les collectes et usages d'informations pour des fins policières, ce sont souvent les lois sur la protection des renseignements personnels relatives aux renseignements utilisés pour assurer les services qui sont ciblés par ceux qui ont des inquiétudes au sujet de la protection de la vie privée. Ces craintes légitimes de surveillance sont ainsi dirigées vers les mauvaises cibles ; elles induisent ainsi à rechercher des mesures donnant lieu à des rigidités entravant les activités qui ne relèvent pas des fonctions policières ou de surveillance de l'État. L'amélioration de la protection de la vie privée nécessite de bien cibler les périls à encadrer.

---

4 World Bank Group, A Definition of E-Government, < http://www1.worldbank.org/publicsector/egov/definition.htm >

5 Dominique GERBOD et Fabien PAQUET, *Les clés de l'e-administration, vade mecum de l'administration électronique*, Colombelle, Éditions EMS, 2001, 347 p.

6 *L'État et les technologies de l'information et de la communication, Vers une administration « à accès pluriel »,* Paris, La documentation française, 2000, Introduction,.

A) De nouvelles circulations de l'information

L'administration électronique suppose de tirer avantage des capacités accrues de traiter des informations, de la partager et d'en particulariser les usages afin de procurer des services ou de prendre des décisions. Ces nouvelles circulations d'information doivent évidemment s'envisager moyennant des balises. Toutefois, on aurait tort de mésestimer le potentiel de dialogue en direct entre l'Administration et l'usager que recèlent les technologies de réseau. De plus en plus, il paraît possible de fonder la protection des personnes sur un droit du citoyen à un dialogue avec les décideurs chargés de déterminer ses droits et obligations. Les règles de droit héritées de l'époque où la bureaucratie pouvait appliquer des raisonnements sans avoir à s'en expliquer avec le citoyen paraissent dépassées dans le contexte actuel et prévisible du développement des réseaux.

1. Le réseautage, la circulation et le partage des informations

Les interactions dans le contexte des réseaux informatiques requièrent des modalités différentes d'identification des personnes. 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 dans les réseaux informatiques que dans les échanges prenant place ailleurs que dans le cyberespace. Cela appelle une attitude réaliste tenant compte aussi bien des avantages de la circulation des informations que de ses inconvénients.

La gestion collaborative induit des besoins de partager l'information. 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. Dans un pareil contexte, 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 à le droit d'en faire usage pour prendre une décision dans une situation spécifique.

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. 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.

2. La personnalisation

La personnalisation consiste à adapter le comportement de l'environnement d'information aux attentes de l'utilisateur, l'idéal étant de les précéder. L'utilisateur doit trouver satisfaction, et le

plus rapidement possible. Les experts du marketing voient dans cette technique une arme puissante au champ d'action très étendu, mais c'est une technique difficile à maîtriser. Il ne suffit pas de demander à l'utilisateur de définir ses préférences et de décliner son profil. Il faut adapter les services en conséquence. Les méthodes de marketing qui conviennent aux besoins des entreprises commerciales ne répondent pas nécessairement aux exigences de la fourniture des services publics. Ces derniers sont en effet encadrés par un régime juridique reflétant divers équilibres à maintenir. Il faut donc se méfier des discours promotionnels et de certaines méthodes et applications « d'affaires » qui font très souvent abstraction des exigences juridiques des activités assurées par les organismes publics.

L'un des avantages des environnements de transactions sur des réseaux est la possibilité de moduler les services proposés en tenant compte des préférences des personnes. Par exemple, le citoyen qui change d'adresse pourra trouver avantageux de transmettre l'information pertinente en un seul lieu et lors d'une seule opération afin qu'elle soit relayée à tous les organismes qui doivent être informés du changement. C'est là une opération qui ne pose pas, en soi, de menaces à la vie privée et qui permet de simplifier les démarches du citoyen avec l'administration. Une telle opération est toutefois difficile, voire impossible si l'on persiste à maintenir un cloisonnement rigide de l'information entre les organismes. On érige alors en dogme ce qui est une entrave.

Dans plusieurs organismes du secteur public, 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. Pour éviter que les informations personnelles ne soient divulguées à des tiers, il faut habituellement pouvoir identifier les personnes avec lesquelles on est en interaction de façon suffisamment précise. Plus les environnements d'administration électroniques sont construits à partir du citoyen-client moins les structures et organigrammes des organismes publics ont de pertinence. En passant d'un état en silo en un État en réseau, les frontières administratives tendent à s'estomper au profit d'une organisation en réseaux.

Il est à prévoir que le citoyen s'attendra à ce que les informations pertinentes aux rapports qu'il entretient avec l'État soient disponibles au moment où elles sont nécessaires et que ces informations aient les qualités appropriées pour les fins auxquelles elles doivent servir. Une telle tendance s'observe déjà dans le secteur privé ; elle ne manquera pas d'influer sur les attentes à l'égard du service public.

Ce double phénomène de personnalisation et de mise en commun de l'information caractérise plusieurs tendances accompagnant l'émergence de l'administration électronique. D'une part, il est de plus en plus prévisible que les citoyens s'attendront à interagir avec l'État comme ils sont en voie de s'habituer à le faire avec les autres prestataires de biens et de services. D'autre part, l'état tendra à adopter un fonctionnement qui visera à prendre avantage des environnements en

réseaux. Une structure arborescente et collaborative tendant à se substituer à la structure hiérarchique caractérisant les organisations bureaucratiques.

Il faudra que le cadre juridique soit adapté à ces modifications de logique. Au Québec cette adaptation est commencée comme en témoignent l'entrée en vigueur de lois reflétant ces tendances lourdes.

B) Un cadre juridique anticipant l'administration en réseaux

Les mutations vers l'administration électronique sont enclenchées depuis déjà quelques années au gouvernement du Québec. Ainsi, des lois ont été mises en place afin de favoriser et d'encadrer les mutations prévisibles que l'administration publique est appelée à connaître. Au nombre de ces pièces législatives, il faut signaler la *Loi sur l'administration publique* de même que la *Loi concernant le cadre juridique des technologies de l'information*.

1. La Loi sur l'administration publique

Adoptée en mai 2000, la *Loi sur l'administration publique*[7] énonce les grands objectifs devant présider au déploiement des services gouvernementaux. Au plan des ressources informationnelles, la loi prévoit que celles-ci doivent être gérées de façon à :

1° utiliser de façon optimale les possibilités des technologies de l'information et des communications comme moyen de gestion des ressources humaines, budgétaires et matérielles;

2° contribuer à l'atteinte des objectifs d'accessibilité et de simplification des services aux citoyens;

3° favoriser la concertation entre les ministères et organismes et le partage de leur expertise et de leurs ressources.

Lors de l'entrée en vigueur de cette loi en mai 2000, on a souligné le fait que les technologies de l'information et des télécommunications seront essentielles pour concrétiser le nouveau cadre de gestion, puisqu'elles fourniront notamment aux gestionnaires des outils pour analyser plus rapidement les situations et ainsi, réduire le processus bureaucratique. La loi prévoit également que les ressources informationnelles seront utilisées aux fins de simplifier et de rendre plus accessibles les services à la population et aux entreprises[8].

---

7 *Loi sur l'administration publique*, L.R..Q., c. A-6.01, < http://www.canlii.org/qc/loi/a6.01/tout.html >.

8 Voir : *Communiqué : Adoption de la Loi sur l'administration publique - Pour de meilleurs services aux citoyens, l'Administration gouvernementale québécoise aura un nouveau cadre de gestion*, < http://communiques.gouv.qc.ca/gouvqc/communiques/GPQF/Mai2000/26/c8676.html >

2. La Loi concernant le cadre juridique des technologies de l'information

La *Loi concernant le cadre juridique des technologies de l'information*[9] est d'application générale. Elle implante dans notre droit, les conditions de la mise en place de plusieurs éléments de l'État en réseau. Elle vient préciser le droit relatif aux documents consignés sur divers supports comme ceux qui reposent sur le recours aux technologies de l'information. Elle apporte des ajustements à plusieurs notions fondamentales du droit québécois afin de rendre celui-ci pleinement compatible avec l'usage sécuritaire des technologies de l'information.

La loi organise le statut juridique des documents, peu importe leur support. Elle est fondée sur la notion de document qui est l'objet commun entre l'univers de l'écrit sur papier et l'univers de l'écrit sur des supports résultant de l'usage des technologies de l'information.

La loi prévoit des règles relativement à l'établissement de documents sur divers supports, au transfert de l'information d'un document d'un support à un autre, aux conditions de l'intégrité des documents tout au long de leur vie, au lien entre une personne et un document, ainsi qu'à la certification. Elle met en place des protections spécifiques pour les renseignements personnels et apporte des précisions sur les conditions de la responsabilité des prestataires de services.

Un premier objet de la loi est d'ailleurs d'assurer la sécurité juridique des communications effectuées par les personnes, les associations, les sociétés ou l'État au moyen de documents quels qu'en soient les supports. On précise les précautions à prendre afin de conserver la validité juridique des documents tout au long de leur cycle de vie.

Le second objet de la loi est d'assurer la cohérence des règles de droit et leur application aux communications effectuées au moyen de documents qui sont sur des supports faisant appel aux technologies de l'information. On vise tous les supports qu'ils soient électroniques, magnétiques, optiques, sans fil ou autres ou faisant appel à une combinaison de technologies.

Un troisième objet de la loi est d'assurer l'équivalence fonctionnelle des documents et leur valeur juridique, quels que soient les supports des documents, ainsi que l'interchangeabilité des supports et des technologies qui les portent. La loi indique comment les situations juridiques connues dans le monde des documents sur papier se transposent dans un univers où l'on fait usage de documents s'appuyant sur les technologies. On se fonde sur les fonctions accomplies par les différents gestes et processus de production et de circulation des documents.

La *Loi concernant le cadre juridique des technologies de l'information* prévoit un ensemble de mesures pour protéger la vie privée dans les réseaux. Ainsi, la loi fait obligation, lors de chaque phase du cycle de vie d'un document, de prendre les précautions de nature à garantir la protection des informations confidentielles, dont les renseignements personnels. La protection des renseignements personnels et confidentiels doit être assurée avant de détruire un document dont la loi exige la *conservation* et qui ont fait l'objet d'un transfert[10].

---

[9] *Loi concernant le cadre juridique des technologies de l'information*, L.Q. 2001 c. 32, < http://www.autoroute.gouv.qc.ca/loi_en_ligne/index.html >

[10] *Loi concernant le cadre juridique des technologies de l'information*, L.Q. 2001 c. 32, art. 20.

La *consultation* de documents technologiques qui portent des renseignements confidentiels est également assortie de protection; la personne responsable de l'accès à ces documents doit prendre des mesures de sécurité propres à en assurer la confidentialité[11]. La protection de la confidentialité d'un document technologique doit être maintenue y compris dans un contexte où la *garde* du document est confiée à un prestataire de services[12]. De même, les renseignements déclarés confidentiels par la loi doivent être protégés en cours de *transmission* d'un document, y compris sur les réseaux de communication et ce, par un moyen approprié au mode de transmission retenu[13].

Des balises sont aussi édictées à l'égard de l'usage de mécanismes d'identification et de vérification de l'identité de même qu'à l'égard de l'activité de certification. À l'égard de ces activités, ont été mises en place des mesures de protection de la vie privée et de contrôle de l'accès à l'information jugée sensible. Toutefois, la *Loi concernant le cadre juridique des technologies de l'information* ne modifie pas les notions relatives à la protection des renseignements personnels. Elle vise primordialement à assurer que les principes des lois québécoises en matière de protection des renseignements personnels trouvent effectivement application dans toutes les situations utilisant des documents sur support-papier ou sur d'autres supports.

Avec les innovations législatives des années récentes, le Québec a anticipé les changements découlant de la plus grande disponibilité des environnements en réseaux pour assurer la fourniture des services publics. Il reste à mettre en place un cadre vraiment efficace pour assurer effectivement la protection de la vie privée des personnes.

---

11 *Loi concernant le cadre juridique des technologies de l'information*, L.Q. 2001 c. 32, art.25.

12 *Loi concernant le cadre juridique des technologies de l'information*, L.Q. 2001 c. 32, art. 26.

13 *Loi concernant le cadre juridique des technologies de l'information*, L.Q. 2001 c. 32, art. 34.

II- La protection des renseignements personnels

L'accroissement de la circulation de l'information modifie l'échelle des risques pour la protection des personnes. La généralisation des réseaux induit des mutations au niveau de la raison d'être des règles de droit. D'où les revendications constantes, dans la plupart des pays développés pour un renforcement de la protection de la vie privée des personnes lors de la mise en place des environnements de traitement de l'information. Au nombre des motifs justifiant la mise en place de lois qui viennent baliser ce qui peut être fait et ce qui doit être évité lors du déploiement des environnements d'information, il y a la protection de la dignité des personnes et du droit à la vie privée.

Il faut renforcer la protection de la vie privée. 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 le tiroir d'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.

Le droit relatif à la protection des renseignements personnels existe depuis près de trois décennies. Principalement issu d'un mouvement véhiculant les appréhensions à l'égard des périls de l'informatique centralisée, il s'est construit en forme de rempart contre les risques de surveillance par les autorités étatiques. Ses fondements ont fait l'objet de peu de débats. Un auteur a même avancé qu'il s'agissait de « législation symbolique » caractérisée notamment par un faible ancrage sur la demande sociale[14].

Dans la plupart des pays, la communauté juridique, les juges et les médias ont montré une tendance à adhérer à une vision quasi théologique du droit relatif à la protection des renseignements personnels. Peu de questions ou de débats ont été soulevés sur ses fondements et finalités. On a presque unanimement pris pour acquis que ce droit était justifié et que les techniques utilisées par les législateurs puis par les instances de régulation étaient généralement appropriées.

Afin de garantir l'effectivité du régime de protection de la vie privée dans le contexte des environnements ouverts, il faut revoir certaines des prémisses fondant le régime actuel de la protection des renseignements personnels. Ce n'est plus tant contre les risques de surveillance qu'il faut diriger le cadre juridique de la protection des renseignements personnels mais plutôt vers l'utilisation adéquate et balisée de l'information relative aux personnes dans un monde où cette information circule de plus en plus. Ce n'est plus en mettant des entraves à la circulation de l'information qu'on assurera le respect de la vie privée mais en encadrant de façon appropriée, la collecte, l'utilisation, la circulation et le maintien de la qualité de l'information portant sur les personnes.

---

[14] Pierre SADRAN, « De l'efficacité des politiques symboliques : l'accès à l'information et la transparence administrative, » dans Pierre TRUDEL (éd.) *Accès à l'information et protection des renseignements personnels*, Montréal, P.U.M., 1984, p.29.

A) Des fondements devenus inadéquats

Le droit de la protection des renseignements personnels a été conçu pour protéger la vie privée des personnes contre les écueils que laissait entrevoir l'utilisation des technologies de l'information à des fins de surveillance. À l'usage, il s'est avéré que le droit de la protection des renseignements personnels ne vise pas tant à contrer la surveillance que d'assurer la qualité de l'information dans le cadre des processus décisionnels.

Mais la persistance du paradigme de la surveillance a conduit à étendre la portée et l'interprétation de certaines notions au point de transformer ce qui devait protéger la vie privée en une protection tous azimuts de la vie personnelle. Il en résulte un ensemble de malentendus, de blocages et une complexification des processus de gestion de l'information sans gain pour la protection de la vie privée.

1. Le droit à la vie privée

Le droit à la vie privée connaît un sens qui varie selon les époques et les cultures. Dans les sociétés contemporaines, il recouvre tout ce qui a trait à l'identité, à la santé, aux mœurs, à la correspondance, à l'image, à la vie familiale, conjugale et sentimentale, etc.[15] Les activités effectuées dans le cadre de la vie publique en sont exclues, bien qu'il soit souvent difficile d'établir une frontière précise entre ce qui relève de la sphère d'intimité de la personne et ce qui peut licitement être laissé exposé au regard d'autrui[16]. Au Québec, le législateur à assuré, dès 1982, la protection des renseignements personnels afin de garantir la relation de confiance devant s'instaurer entre les citoyens et les différents services offerts par l'État. Le législateur étendu l'exigence à toute personne avec les articles 37 à 41 du Code civil et aux entreprises avec la *Loi sur la protection des renseignements personnels dans le secteur privé*.

Le droit à la vie privée varie en fonction du contexte, des époques, des moeurs et, surtout, de la position occupée par les personnes dans la société. Pour établir s'il y a atteinte à la vie privée, il est nécessaire de déterminer si une divulgation d'information ou une intrusion porte sur un élément de la vie privée. Le domaine de la vie privée regroupe certains types d'informations qui y sont, en principe, rattachées. Le domaine de la vie privée connaît aussi des variations selon les qualités et la situation des personnes. On identifie traditionnellement deux grands volets à la vie privée. Le premier réfère aux faits et aux aspects de la vie d'une personne qui sont inclus dans un domaine protégé. Il permet d'identifier les éléments considérés comme inclus dans le domaine de la vie privée d'une personne, à une époque donnée. Mais le contenu concret de ce domaine varie suivant les personnes, la position qu'elles occupent dans la société et d'autres circonstances. C'est le volet qui prend en considération les personnes visées. Ce volet

---

15 Pierre KAYSER, *La protection de la vie privée par le droit- Protection du secret de la vie privée*, 3e édition, Paris, Économica, 1995; François RIGAUX, *La protection de la vie privée et des autres biens de la personnalité*, Paris, LGDJ, 1990 ; Martin MICHAUD, *Le droit au respect de la vie privée dans le contexte médiatique: de Warren et Brandeis à l'inforoute*, Montréal, Wilson & Lafleur, 1996.

16 Pierre TRUDEL et France ABRAN, *Droit du public à l'information et vie privée : deux droits irréconciliables ?*, Montréal, Les Éditions Thémis, 1992.

contextuel permet d'apprécier le contenu du domaine de la vie privée en fonction des circonstances, notamment la participation de l'individu à la vie de la collectivité[17].

Le droit à la protection des renseignements personnels constitue une facette des régimes de protection de la vie privée. Il existe une étroite relation entre les règles relatives à la protection des données personnelles et la possibilité effective pour une personne de maîtriser la circulation de l'information la concernant.

2. Une simplification

À ce jour, les régimes de protection de la vie privée dans les technologies de l'information ont été construits sur la notion de renseignements personnels. La notion de renseignements personnels ou de renseignements nominatifs est née d'un souci de simplification. Pour contourner les difficultés de dégager ce qui doit rester dans le secret au nom du droit à la vie privée, on a opté pour une notion qui confond « renseignements qui identifient une personne » avec les « renseignements sur sa vie privée. »

L'adoption de la notion de renseignements personnels dans plusieurs législations procédait d'un souci de disposer d'une définition claire des renseignements portant sur les personnes et qui devaient êtres protégés. On cherchait à s'affranchir des difficultés découlant du caractère fluctuant et contextuel de la notion de vie privée. C'est apparemment à un souci de simplicité que répondait l'adoption de cette notion. Si l'on convenait que plusieurs renseignements personnels relatifs à une personne relevaient de sa vie privée, il était aussi entendu que tous les renseignements sur une personne ne relèvent pas de sa vie privée. C'est sur cette distinction qu'est fondé l'article 55 de la Loi d'accès suivant lequel « Un renseignement personnel qui a un caractère public en vertu de la loi n'est pas nominatif. » Malgré cela, on a peu à peu laissé de côté les nuances qui caractérisaient jusque-là le concept de vie privée.

Le résultat de ce glissement a été d'assimiler tout renseignement sur une personne à sa vie privée et de protéger cette dernière en censurant sans distinction, tous les renseignements relatifs à une personne. Les craintes que s'instaurent des pratiques de « surveillance » ont accentué la distorsion introduite dans le droit à des fins de commodité. On en est venu à considérer que tout renseignement concernant une personne identifiable était un renseignement pouvant avoir un rapport avec la vie privée de cette dernière.

3. La crainte de la « surveillance »

Les lois sur la protection des renseignements personnels ont été conçues à partir du postulat que l'informatique est un outil capable de servir à des activités de surveillance des personnes. On a pris pour acquis que les outils informatiques peuvent être utilisés pour accroître la surveillance et qu'ils le seront nécessairement. Pourtant, les sociétés ayant érigé la surveillance en mode de gouvernement comme l'ancienne République démocratique allemande n'utilisaient pas les outils informatiques. Il faut sans doute convenir que ce qui fait qu'une société se transforme en société

---

[17] Patrick A. MOLINARI et Pierre TRUDEL, «Le droit au respect de l'honneur, de la réputation et de la vie privée : Aspects généraux et applications», dans Barreau du Québec, Formation permanente, *Application des chartes des droits et libertés en matière civile*, Cowansville, Éditions Yvon Blais, 1988, 197p. 211.

de surveillance et en État totalitaire ne tient pas seulement à la disponibilité d'outils informatiques. Des facteurs plus globaux permettent d'expliquer l'avènement des tendances à la surveillance par les États ou par les entreprises. La seule disponibilité d'une technologie n'emporte pas automatiquement des usages abusifs.

Les craintes de surveillance doivent être relativisées car elles mènent à confondre les mesures inhérentes au bon fonctionnement de la démocratie avec les véritables menaces à la vie privée. Lorsqu'on rappelle les distinctions qui existent entre les mesures de surveillance et la fourniture de services publics, on retrouve une perspective plus réaliste des enjeux.

a. Distinguer les informations de police des informations de gestion

Les informations de police sont régies par un ensemble de règles spécifiques. Par exemple, l'article 80 de la Loi d'accès prévoit l'établissement de fichiers confidentiels non accessibles aux personnes fichées. Il énonce que :

> *80. Le gouvernement peut, par décret, autoriser un organisme public à établir un fichier confidentiel*
>
> *Un fichier confidentiel est un fichier constitué principalement de renseignements nominatifs destinés à être utilisés par une personne qui, en vertu de la loi, est chargée de prévenir, détecter ou réprimer le crime ou les infractions aux lois.*

Par leur nature même, les informations recueillies dans le cadre d'activités de détection du crime ne sauraient être accessibles aux personnes concernées. Un régime spécifique et des balises sévères doivent évidemment encadrer la collecte, l'usage et la détention de telles informations. Les dispositions du *Code criminel* et des autres lois pénales prévoient des garanties à cet égard.

Certes, on peut avoir des craintes à l'égard de certaines pratiques policières. On peut légitimement s'inquiéter de ce qu'il advient des informations sur les citoyens que détiennent les forces de l'ordre. Mais ces inquiétudes devraient s'exprimer à l'égard des lois pénales et des lois de police et non à l'égard des lois encadrant la gestion des services publics aux citoyens. Si des dangers existent qui peuvent découler des abus possibles des forces policières, qu'on intervienne à ce niveau. On ne parviendra pas à remédier à ce genre de problèmes en surmultipliant les entraves au niveau des lois régissant la prestation des services publics. Ces dernières n'ont pas pour objet de servir à la surveillance des citoyens et elles sont d'ailleurs pourvues de balises s'opposant à de pareilles dérives. Dans la mesure où les lois prévoient des garanties raisonnables à l'égard de la vie privée, on ne devrait pas imputer aux lois visant à encadrer la fourniture des services et prestations aux citoyens, des velléités de « surveillance » semblables à celles que certaines lois de police pourraient laisser craindre.

b. Le contrôle de gestion n'est pas de la surveillance

Il est inhérent au respect de l'état de droit que l'administration effectue des contrôles aux fins de s'assurer que seules les personnes qui y ont droit obtiennent un service ou une prestation de l'État. Invoquer le droit à la vie privée à l'encontre de mesures raisonnables de contrôles de gestion revient à placer celui-ci au-dessus des exigences élémentaires de l'état de droit.

Il est en effet du devoir de l'Administration publique de s'assurer qu'il n'y a pas d'évasion fiscale ou que seules les personnes répondant aux exigences prévues par la loi reçoivent une prestation de l'État. Désigner comme de la surveillance les mesures raisonnables de contrôles de gestion destinés à garantir le bon fonctionnement des programmes gouvernementaux est un abus de langage. Ce sont au contraire des mesures destinées à garantir les droits des citoyens à ce que les services publics soient gérés conformément à la loi. En confondant de pareilles mesures avec des activités de surveillance, on oublie les impératifs de bonne gestion des fonds publics.

c. S'éloigner des extrapolations apocalyptiques

S'agissant des informations personnelles détenues par les organismes publics aux fins d'offrir des services aux citoyens, la quasi-totalité des affirmations au sujet des dangers et risques de surveillance pour les personnes est fondée sur des extrapolations alarmistes. Habituellement, l'argument est fondé sur la prise en compte du potentiel des technologies de l'information. On escompte que le potentiel d'abus sera nécessairement et universellement réalisé et on réclame des obligations générales en conséquence. Ces extrapolations se fondent sur le constat de la plus grande capacité d'agglomérer et de recouper des informations, la puissance des outils de recherche, la persistance de l'information, etc. De ces constats, on relève les inquiétudes que des usages malveillants en viennent à constituer des périls pour la liberté des personnes.

S'il était si évident que les outils de traitement de l'information donnent effectivement lieu à de la surveillance, cela se verrait. Depuis le temps qu'il est fait usage des technologies de l'information, il devrait être possible de documenter, à tout le moins d'illustrer par des situations réelles, les écueils qui peuvent découler de certaines utilisations des technologies de l'information. Mais, à ce jour, les cas connus de surveillance relèvent plutôt de l'anecdote. La plupart concernent les opérations de surveillance policières qui échappent à toutes fins pratiques à la portée des lois sur la protection des renseignements personnels. On retrouve quelques incidents ayant eu pour conséquence de laisser circuler des informations personnelles de façon inappropriée. Mais c'est en vain que l'on cherchera des pratiques généralisées de surveillance des personnes, sauf à donner au mot surveillance un sens plus étendu que celui qu'il a.

Devant les possibilités théoriques que procurent les technologies de l'information, on en vient à une utilisation des notions de surveillance, non plus pour désigner les activités de surveillance qui se déroulent effectivement mais les activités de surveillance qui pourraient devenir possibles si des informations étaient traitées de façon malveillante. On entre alors dans un cycle d'auto-justification… Ayant proclamé de tels dangers, l'on cite ensuite des sondages qui tendent à indiquer que les citoyens ont cru à ces pronostics et s'inquiètent des dangers pour la vie privée susceptibles de découler de l'accroissement des traitements d'informations personnelles.

Malgré la rareté des tentatives d'en vérifier l'application réelle, le paradigme de la « surveillance » s'est traduit par une constante rigidification et bureaucratisation des mesures de protection des renseignements personnels. Pour éviter la surveillance, il fallait que l'information soit confinée à l'organisme qui l'a collecté, qu'elle ne circule que moyennant consentement éclairé de l'intéressé et ce peu importe le degré de sensibilité de l'information. Le dossier médical d'une personne est mis sur le même pied que son adresse de courriel! Pour prévenir la surveillance, il faut éviter que l'information ne circule. On va donc préférer la redondance à la réutilisation de l'information. Peu importe que le citoyen soit obligé de recommencer les mêmes

démarches plusieurs fois ! Pourvu que l'information soit confinée dans autant d'alcôves administratives et qu'elle ne serve qu'à une seule finalité !

À une époque où se généralise l'usage des technologies de l'information, il faut des fondements plus solides et mieux ciblés. On ne peut se limiter à reconduire indéfiniment les frayeurs d'une époque où l'on confondait l'usage des technologies avec les usages abusifs dont elles peuvent faire l'objet. Le prix à payer pour des mesures aussi mal ciblées pourrait être un affaiblissement des protections de la vie privée. Par contre, il y a des écueils - réels ceux-là - qui doivent être pris en compte afin de disposer de réseaux assurant une réelle protection des personnes.

d. Mieux cibler les périls

Plusieurs interprétations des lois sur les informations personnelles sont essentiellement fondées sur des craintes et des extrapolations. Daniel J. Solove relève que les appréhensions à leur égard ne sont pas adéquatement articulées. Il écrit que :

> *Altough the problem of databases is undestood as one concern over privacy, beyond this, the problem is often not well defined. How much weight should our vague appehensions be given, especially considering the tremendous utility, profit and efficiency of using databases?*[18]

Solove répond à cette question en soutenant que :

> *The answer to this question depends upon how the privacy problem of databases is conceptualized. Unfortunately, so far, the problem has not been adequately articulated.*

C'est que les médias, les décideurs politiques et les juristes décrivent les problèmes engendrés par le traitement de l'information relative aux personnes en se fondant sur la métaphore du Big Brother telle qu'elle est utilisée dans le roman *1984* de George Orwell. Une littérature foisonnante justifie la nécessité des lois sur la protection des renseignements personnels en se fondant sur les possibilités que s'instaure une société de surveillance semblable à celle décrite par Orwell dans son célèbre roman.

La fascination que suscite souvent la technologie ou encore, la frayeur qu'elle inspire à plusieurs caractérise - et de façon nettement dominante- les analyses et les discours au sujet des menaces et des risques que les technologies représentent pour les personnes. Mais comme on se représente le traitement de l'information comme menant invariablement à la surveillance, on en déduit que la généralisation des outils capables de servir à de telles fins va nécessairement engendrer de plus grandes menaces. Lucas, Devèze et Frayssinet, écrivent à cet égard que :

> [...] *les nouvelles technologies constituent un puissant outil bureaucratique et technocratique devenu essentiel pour la rationalisation de la gestion publique, l'action de la police et de la justice, la conduite des politiques publiques (santé, emploi, aides*

---

[18] Daniel J. SOLOVE, « Privacy and Power : Computer Databases and Metaphors for Information Privacy, » [2001] 53 *Stanford L. R.,* 1393, p. 1395.

> *publiques…), la lutte contre les fraudes, la prévision. Pratiquement toutes les actions administratives passent par un fichage.*[19]

Ces analyses reflètent de ce que Daniel J. Solove appelle la « métaphore du Big Brother ». Mais, lorsqu'on y regarde de près, la protection des renseignements personnels ne répond pas à des dangers de surveillance. Elle vise plutôt à assurer que les informations sur les personnes soient de qualité.

Dans les argumentations justifiant les mesures de contrôle des renseignements personnels, on prend acte des possibilités offertes par la technique et on conclut aussitôt à l'éventualité d'usages abusifs. On invoque machinalement les supposés risques de surveillance ou les dramatiques « vols d'identité » ou pareilles fantasmagories illustrées par la littérature ou une certaine cinématographie. Par contre, lorsque vient le temps de documenter les dangers qui guettent effectivement les personnes du fait de la circulation des données personnelles, on évoque, non plus des problématiques de surveillance, mais plutôt des problématiques tenant à la qualité des informations lors des processus décisionnels. On fait alors le constat que :

> *Le danger provient du caractère inadéquat, équivoque, imprécis, disproportionné de l'information collectée parfois de manière déloyale par rapport à une finalité critiquable qui peut s'abriter derrière un argumentaire la présentant de manière favorable.*[20]

Dans cet esprit, on souligne le fait qu'il n'y a pas de « données anodines ». Lucas, Devèze et Frayssinet relèvent que :

> *La pratique démontre qu'il n'y a pas de données anodines et que la notion de données sensibles (santé, opinion politique ou syndicale, vie privée) définie a priori doit être considérée de manière relative; après tout, les sociétés de vente par correspondance ne demandent pas l'âge de leurs clientes car cela est mal perçu; mais grâce aux tables d'attribution des prénoms de l'INSEE, elles déduisent avec une forte probabilité l'âge des personnes.*[21]

Suivant un tel raisonnement, même le prénom d'une personne serait une information pouvant relever de sa vie privée en ce que cela permettrait de connaître son âge par recoupement. Mais l'âge que l'on attribuerait à la personne dans une telle situation est celui que permettrait d'évaluer le processus de comparaison avec une donnée à caractère historique : les tables annuelles d'attribution des prénoms. Il serait ainsi possible de savoir qu'une Nathalie est possiblement née entre 1965 et 1972. On voit que ce qui pose ici problème n'est pas tant la menace à la vie privée car on ne divulgue pas l'âge effectif de la personne. On a plutôt ici une donnée à caractère probabiliste fondée sur le fait qu'une personne née entre telle et telle année a beaucoup de chances de porter tel ou tel prénom. Il serait évidemment absurde d'utiliser de

---

[19] André LUCAS, Jean DEVÈZE et Jean FRAYSINNET, *Droit de l'informatique et de l'Internet*, Paris PUF coll. Thémis Droit privée, 2001, p. 10.

[20] André LUCAS, Jean DEVÈZE et Jean FRAYSINNET, *Droit de l'informatique et de l'Internet*, Paris PUF coll. Thémis. n° 18.

[21] André LUCAS, Jean DEVÈZE et Jean FRAYSINNET, *Droit de l'informatique et de l'Internet*, Paris PUF coll. Thémis n° 19.

telles informations afin de prendre une décision significative à l'égard d'une personne. On constate que nous ne sommes pas ici en présence d'une atteinte à la vie privée. C'est plutôt un problème de qualité d'information. Si cette information sur l'âge des personnes obtenue via ce genre de recoupement est possiblement suffisante pour mener des opérations de ciblage en marketing, elle est nettement insuffisante pour prendre la moindre décision à propos d'un individu.

L'exemple est extrême mais il illustre la nécessité de fonder la protection des renseignements personnels non sur les risques de surveillance, mais en donnant plus d'importance aux garanties de qualité de l'information. L'exemple illustre aussi les écueils de confondre toutes les informations relatives à une personne et la vie privée de cette dernière. Enfin, il met en lumière le fait que les problèmes auxquels vient répondre le droit de la protection des renseignements personnels sont souvent des problèmes de qualité de l'information utilisée dans les processus décisionnels concernant les individus plutôt que des actions de surveillance.

Une autre situation vécue par plusieurs contribue à faire ressortir l'importance de bien cibler les mesures de protection des renseignements personnels. Nombreux sont ceux qui se sont fait refuser une carte de crédit au motif « qu'un jugement a été prononcé contre eux ». Dans certaines situations, il s'agissait de personnes impliquées dans une affaire judiciaire en leur seule qualité professionnelle ! Par exemple, un arbitre intimé dans un recours intenté contre une décision ! Ce phénomène met en lumière la possibilité que certaines maisons d'évaluation de crédit ne prennent pas les précautions suffisantes afin de vérifier la nature des condamnations dont une personne aurait été l'objet. Voilà bien un problème de qualité de l'information : on utilise de façon inadéquate une information par ailleurs vraie et publique.

On observe une tendance à invoquer les usages abusifs ou incompétents d'information pour en justifier la censure. Il est dangereux d'invoquer des situations de traitement inadéquat pour justifier la censure généralisée des informations sur les condamnations judiciaires ou sur d'autres sujets. Certes, il peut s'avérer plus difficile d'adopter des mesures qui imposeraient des normes de qualité dans le domaine de l'évaluation de crédit. Mais dans un monde où presque toute l'information est susceptible de circuler en réseau, il devient impossible de s'en remettre à une approche postulant de possibles utilisations fautives des informations. À la limite, aucune information ne pourrait circuler puisque toutes sont susceptibles d'usages abusifs ou inappropriés. Plutôt que persister dans une telle approche restrictive, il faut renforcer les règles afin d'assurer que seule l'information présentant les qualités requises sera utilisée afin de prendre des décisions plutôt que de prétexter le risque d'usages maladroits, incompétents ou malhonnêtes d'informations pour prohiber a priori la circulation d'information.

Les dangers découlant des traitements de données personnelles sont perçus à deux niveaux. Au niveau des représentations globales, on évoque le spectre de la surveillance. Mais comme il est généralement difficile de donner de la substance, de documenter les situations où la surveillance aurait été effectivement faite à partir de banques de données, on évoque en fait les problèmes mettant en cause la qualité des données pour justifier la protection des renseignements personnels. Ce phénomène de glissement met en lumière le caractère inadéquat du paradigme de la surveillance inspiré du roman *1984* de Georges Orwell afin de justifier les mesures de protection des renseignements personnels. Par contre, il révèle un autre paradigme, beaucoup plus pertinent : celui du roman de Kafka *Le Procès*. Ce qui pose problème ce n'est pas tant le risque de surveillance mais bien l'utilisation inadéquate, incompétente, aveugle de données

personnelles. Dans le contexte de l'État fournissant des services aux citoyens, c'est le fait que les conclusions soient tirées de données qui ne présentent pas les qualités requises pour y donner ouverture qui est le danger redouté. En somme, c'est la façon dont l'information est utilisée, la question de savoir si elle possède les qualités appropriées aux usages qu'on veut en faire qui pose des difficultés et qui appelle un cadre de gestion et de protection.

Le glissement que l'on observe à l'égard de la portée de la notion de renseignements personnels paraît résulter de la crainte certes réelle, que des recoupements d'informations sur une personne permettent de profiler et de révéler des informations sur la vie privée des personnes. Mais le recours à la notion de renseignements personnels comme notion de substitution à celle de droit à la vie privée n'a pas été accompagné de réflexions sur les distinctions qu'il convenait de faire entre d'une part les informations personnelles rattachées effectivement au champ de la vie privée d'une personne et celles qui portent plutôt sur les dimensions sociales de l'individu, qui concernent les rapports qui le rattachent à la société par opposition à ce qui relève de son intimité et de sa dignité. Il n'y a pas eu non plus de réflexions sérieuses sur les mérites des approches utilisées afin de prévenir les atteintes aux droits des personnes. Par exemple, on a eu tendance, en ces matières à retenir des approches de confinement a priori de l'information plutôt que la mise en place de mesures de sanctions une fois les atteintes constatées.

Ce phénomène est probablement une conséquence des représentations dominantes ayant émergé lors de l'avènement puis de la généralisation de l'informatique pour traiter des informations relatives aux personnes. Les analystes qui ont jeté un regard critique sur l'informatisation ont adhéré, pour la plupart, au paradigme de la surveillance. Pour eux, l'informatique accroît les possibilités de surveillance des personnes. Là résideraient ses effets liberticides. Le mouvement de la protection des renseignements personnels est largement issu de cette mouvance. Mais il est devenu contre-productif de maintenir des fondements aussi mal ciblés. D'ailleurs, devant ce ciblage défectueux et les difficultés qu'il pose, on a eu tendance à opter pour une sorte de fuite en avant en élargissant la notion de renseignements personnels au point d'en faire une protection généralisée de la vie personnelle.

4. Une fuite en avant : de la vie privée à la « vie personnelle »

Du glissement alimenté par la crainte de la « surveillance » ont découlé toutes sortes de revendications afin de protéger ce qui ne relève pas toujours de la vie privée. Cela se comprend : lorsqu'on craint la surveillance, on s'inquiète de tout ce qui peut survenir à l'égard de toutes les informations qui nous touchent. Il n'est pas surprenant que certains en soient venus à envisager l'avènement d'Internet, voire tout environnement électronique, comme donnant ouverture à la mise en place de vastes activités de surveillance. Cela explique l'émergence de la tendance de plus en plus marquée à rechercher, non plus la protection de la vie privée, mais plutôt la protection de la « vie personnelle. »

En soi, un très grand nombre d'usages d'informations personnelles ne sont pas une violation de la vie privée. Il devient en effet difficile de justifier, au nom de la vie privée, les mesures relatives à certaines informations dont la circulation est inhérente à la vie sociale. C'est probablement pour cette raison que certains se sont rabattus sur une notion extrêmement vague et d'une ampleur encore indéterminée : la notion de vie personnelle. Cette notion paraît répondre aux difficultés conceptuelles découlant de la fragilité des fondements sur lesquels reposent les mesures de contrôle des informations personnelles ne se rattachant pas à la vie privée.

La crainte que les informations soient utilisées de manière inadéquate porte à rechercher une protection pour toutes les informations relatives à une personne. Dès lors que l'on postule qu'il n'y a pas d'informations anodines, que le couplage peut permettre de dresser des profils à partir des traces les plus anodines, on ne peut plus faire la distinction entre les informations relevant du domaine public et celles qui relèvent de la vie privée. Il devient du coup plus difficile d'asseoir les fondements des régimes de protection des renseignements personnels uniquement sur un souci de protéger la vie privée. Étant donné les perceptions des risques susceptibles de découler des recoupements d'information, on en est venu à trouver naturel que le droit sanctionne toute circulation d'information *a priori*, sans égard à la faute, sans égard au fait que la vie privée des personnes a été ou non violée, ou qu'un dommage a été effectivement causé.

D'où cette revendication pour la reconnaissance d'un « droit à la vie personnelle ». C'est ainsi que Frayssinet fait valoir que « l'atteinte ne concerne pas que la vie privée (…) mais tous les aspects de la vie personnelle »[22].

Il en résulte une kyrielle de revendications ayant l'apparence d'une quête généralisée d'un droit de veto à l'égard de toutes les informations sur les personnes, y compris celles qui étaient il n'y a pas si longtemps perçues comme relevant des inconvénients normaux de la vie en société. Par exemple, on invoque le droit de ne pas recevoir des dépliants publicitaires etc. ou de sollicitations par courriel. Ces craintes, en partie justifiées, entraînent des revendications pour mettre en place des contrôles à l'égard de toutes sortes de situations mettant en cause des informations personnelles. À bien des égards, les revendications pour renforcer la protection des renseignements personnels sont parfois devenues des revendications pour protéger d'inconvénients inhérents à la vie sociale, non pour assurer la protection de la vie privée. C'est une approche incompatible avec les exigences d'une société démocratique car elle nie l'exercice des autres droits fondamentaux comme la liberté d'expression ou les exigences de saine gestion des services publics.

La notion de « protection de la vie personnelle » ne comporte pas de contours définis; elle paraît pour l'essentiel renvoyer aux préférences des individus. Il est difficile de voir où s'arrête une telle notion. Si la notion veut dégager une aire de protection afin d'assurer l'intimité des individus de même que la possibilité d'exercer un contrôle sur leur vie, elle se confond avec la notion de vie privée, une notion toutefois délimitée par les impératifs de la vie en société. Si la notion de « vie personnelle » va plus loin que le droit à la vie privée pour ériger au rang de droit tout ce qui, au fil de leurs sensibilités, peut déranger les personnes, la notion est étrangère à notre droit, elle n'est reconnue nulle part dans des lois ou les textes constitutionnels. Il serait dangereux de fonder un droit sur une notion aussi tributaire des sensibilités variables, voire arbitraires des individus.

Au surplus, la notion de « vie personnelle » laisse peu de place aux impératifs de la vie en société, au fait que l'information doit pouvoir circuler et que cette circulation, en pratique, est rarement préjudiciable. Si tout n'est qu'affaire de choix individuels, il reste peu de place pour la

---

[22] Jean FRAYSSINET, « La protection des données personnelles est-elle assurée sur Internet ? », Texte présenté au colloque international *Droit de l'Internet, approches européennes et internationales*, septembre 2001, http://droit-internet-2001.univ-paris1.fr/pdf/vf/Frayssinet.pdf. Voir aussi André LUCAS, Jean DEVÈZE et Jean FRAYSINNET, *Droit de l'informatique et de l'Internet*, Paris PUF coll. Thémis droit privé, 2002, n° 50.

circulation de l'information qui répondrait à des impératifs de la collectivité. Enfin, si toutes les activités humaines significatives supposent désormais l'usage des réseaux, il faudra bien convenir qu'il faut un cadre juridique suffisamment nuancé pour assurer les équilibres entre les divers droits mis en cause dans les interactions sociales. C'est sans doute dans ce contexte que la notion de « vie personnelle » paraît une notion trop rudimentaire pour servir de cadre de réflexion. Pire encore, par la négation des autres valeurs inhérentes à la démocratie qu'elle comporte nécessairement, la notion recèle une tendance au totalitarisme de même qu'au recul de l'état de droit.

Enfin, ce genre de dérive emporte une importante distraction de ressources vers la protection des désirs individuels relevant habituellement du caprice alors qu'elle laisse le champ libre à des pratiques autrement plus attentatoires à la vie privée. Par exemple, on multiplie les précautions afin de préserver les citoyens du fléau du télémarketing alors que peu est fait pour encadrer les activités de surveillance, notamment par les agences d'investigation.

5. Les véritables activités de surveillance demeurent

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.

Yves Boisvert fait écho à ce paradoxe dans un commentaire sur une affaire d'espionnage, présumément à des fins politiques, d'un dirigeant d'une société d'État :

> *On s'entend tous : enquêter sur la vie privée des gens, en plus d'être probablement illégal, ce n'est pas une façon très jolie de faire de la politique.*
>
> *Les éditoriaux, les partis politiques, les avocats : tout le monde est d'accord : ça ne se fait pas de fouiller dans les poubelles des gens. Même le Parti libéral, que l'on accuse d'avoir participé à une enquête privée sur Gaétan Frigon, réclame une enquête publique sur sa propre conduite pour se dédouaner!*
>
> *Tout le monde est contre, donc. Fort bien.*
>
> *Peut-on m'expliquer alors comment il se fait que les «agences d'investigation» sont si nombreuses? Il suffit d'ouvrir les Pages Jaunes : on en compte une quarantaine dans la région de Montréal.*
>
> *Que font-elles? Elles trouvent des gens, elles les filent, elles les écoutent, elles prennent des photos, des vidéos, trouvent des documents... Il y en a qui posent des micros, ou qui en tendent.*[23]

---

[23] Yves BOISVERT, « Vie privée et hypocrisie », *La Presse*, 30 mars 2002, < http://www.cyberpresse.ca/reseau/chroniqueurs/yboisvert/yboi_102030082367.html >

Le phénomène de la surveillance sur les lieux de travail est une autre illustration des contradictions de l'approche actuelle en matière de protection des renseignements personnels. Dans une décision, la Cour d'appel du Québec confirmait que les employeurs peuvent, lorsqu'ils ont des motifs sérieux, surveiller leurs employés, même dans leur vie privée[24]. La même contradiction se retrouve dans la jurisprudence de la Commission d'accès à l'information. D'une part, celle-ci a jugé qu'une municipalité ne pouvait recueillir des informations sur support vidéo car l'enregistrement des images captées par des caméras de surveillance n'apporte rien de plus à la protection du public que ce que la simple présence des caméras n'assure déjà[25]. Par contre, la Commission a reconnu qu'un organisme public peut recourir aux services d'un enquêteur et capter des images d'un employé afin de vérifier si celui-ci s'adonne à des activités incompatibles avec son état de santé[26]. Le paradoxe est troublant : la surveillance est *a priori* fautive. Mais elle devient licite lorsque l'on peut faire valoir des motifs, même d'intérêt privé, pour la légitimer après-coup. En somme, il est interdit de surveiller les personnes sauf si cette surveillance permet de recueillir des informations révélant un comportement fautif de la personne surveillée. On conviendra en effet que si une surveillance ne révèle rien de fautif, il y a fort peu d'intérêt à s'y livrer ! Alors, c'est peut-être qu'elle n'est pas si illicite que cela !

Ces contradictions mettent en évidence le fait que le droit à la protection de la vie privée, et du coup le droit de la protection des renseignements personnels ne peut être posé en absolu. Il y a des intérêts légitimes à la circulation de l'information sur les personnes. Celle-ci n'est pas toujours fautive. Plutôt que de construire un cadre juridique qui reflète cela, certains ont eu tendance à se réfugier dans une conception absolutiste de la protection des renseignements personnels, quitte à laisser de côté les conséquences absurdes de cette approche. Le résultat est que la protection des renseignements personnels porte ses exigences sur des cibles faciles, comme les services gouvernementaux et ne s'intéresse que rarement aux véritables périls pour la protection de la vie privée. Ainsi, on impose des exigences strictes pour la mise en place des services gouvernementaux et on se limite à quelques mises en garde au sujet des dangers découlant des véritables activités de surveillance.

Ces contradictions indiquent qu'il est nécessaire de reconnaître la légitimité de certaines activités de surveillance. Actuellement, le cadre juridique nie a priori la légitimité de la surveillance ce qui n'empêche pas ensuite de la trouver licite lorsque cela paraît commode afin de découvrir la vérité. Ne vaudrait-il pas mieux identifier les balises moyennant lesquelles il est licite de surveiller, sur les lieux de travail ou ailleurs ? La protection de vie privée se trouverait du coup renforcée.

Pour disposer d'un cadre juridique cohérent et prévisible, il est nécessaire de bien articuler les fondements et les valeurs au nom desquelles le droit est protégé. À défaut de cela, on court le risque de se retrouver avec une protection factice de la vie privée, une protection qui ne jouera plus dès qu'elle portera sur des enjeux cruciaux.

---

[24] *Syndicat des travailleurs de Bridgestone-Firestone de Joliette (CSN)* c. *Me Gilles Trudeau/Firestone Canada inc*, CA Montréal, 30 août 1999, J.E., 99-1554.

[25] *Ligue des droits et libertés et ville de Sherbrooke*, Rapport d'enquête du 25 novembre 1992.

[26] *Eppell*. C. *Commission de la santé et de la sécurité du travail*, [2000] C.A.I., 194. Voir sur cette contradiction : Raymond DORAY et François CHARETTE, *Accès à l'information, loi annotée, jurisprudence, analyse et commentaires*, Cowansville, Éditions Yvon Blais, p. 64-7.

B) Une application de plus en plus laborieuse

La protection des renseignements personnels a connu une telle étendue que son application s'avère de plus en plus laborieuse. Les dysfonctionnements sont encore plus visibles dans les situations où l'information doit circuler pour assurer un processus décisionnel de plus en plus centré sur le citoyen-client.

1. La négation de la légitimité des espaces publics

La portée étendue conférée à la notion de renseignements personnels a transformé des renseignements ayant un caractère public en des renseignements devant être traités comme s'ils étaient confidentiels. Il y a dans ces démarches une négation de l'équilibre que le législateur avait pourtant pris soin de ménager entre les impératifs de protection de la vie privée et la nécessité de laisser circuler certaines informations relatives aux personnes.

Dans son enquête au sujet des activités de généalogie, la Commission d'accès porte un œil *a priori* sévère sur une activité licite que l'on a tenue, à toutes les époques, comme relevant de la tâche d'écrire l'histoire. Dans une liste de questions publiées en vue d'une audience publique sur la généalogie, la Commission présente la problématique comme si elle postulait le caractère illégitime de la recherche généalogique[27]. Elle invite ainsi à commenter l'affirmation suivant laquelle « les généalogistes prétendent que les actes de l'État civil pour la période de 1926 à 1993, contrôlés par le directeur de l'État civil depuis 1994, ont un caractère public ». Il est pourtant établi depuis longtemps que les actes de l'État civil ont, par leur nature même un caractère public. Le reste des questions posées montre un parti pris surprenant de la part d'un organisme public. On parle de rassurer la population qu'« il n'y aura pas d'atteinte à la vie privée par la communication de renseignements personnels le concernant ou, le cas échéant, de ses héritiers ». C'est en vain que l'on cherche dans cette façon de la Commission de poser les problèmes posés par la généalogie, un mince indice que la démarche généalogique peut possiblement être légitime ! Pourtant, on ne retrouve pas de décisions judiciaires ayant conclu que la recherche généalogique est une atteinte à la vie privée.

Il est étonnant de voir la Commission d'accès se mettre à enquêter avec une approche aussi négative sur les recherches en généalogie, comme si celles-ci donnaient lieu régulièrement à des violations de la vie privée. Comment expliquer que l'on ne démontre pas le même zèle à l'égard des pratiques des agences d'investigation ou de l'espionnage et la surveillance des personnes ? Tout se passe comme si le droit à la protection des renseignements personnels était protégé uniquement lorsqu'il soulève des enjeux modestes, voire insignifiants. Il cède le pas dès lors qu'il heurte un intérêt jugé plus important.

L'Avis préliminaire de la CAI sur les infrastructures à clés publiques[28] est encore plus préoccupant tant il paraît procéder d'une panique au sujet de la nature et des finalités des listes

---

27 COMMISSION D'ACCÈS À L'INFORMATION, *Consultation publique renseignements personnels – généalogie, les questions*, février 2002.

28 COMMISSION D'ACCÈS À L'INFORMATION, *Avis de pertinence sur la solution intérimaire de l'infrastructure à clés publiques gouvernementale du secrétariat du Conseil du trésor*, août 2001, < http://www.cai.gouv.qc.ca/fra/docu/a011107.pdf >

de personnes possédant un certificat dans le contexte d'une ICP. Ainsi, négligeant complètement le caractère public[29] des informations consignées dans un répertoire associé à une infrastructure à clé publique, l'*Avis de pertinence sur la solution intérimaire de l'infrastructure à clés publiques gouvernementales du secrétariat du Conseil du Trésor* affirme péremptoirement que « L'utilisation d'ICP implique pour les individus et organisations une cueillette d'informations additionnelles et une surveillance de leurs actions » (nous soulignons). Qu'il existe des risques pour la protection de la vie privée résultant de ce genre d'infrastructure est évidemment possible. Mais de poser *a priori* que la surveillance est une conséquence découlant nécessairement de l'utilisation d'une ICP relève du domaine de l'affirmation gratuite. Mais l'affirmation est révélatrice d'un état d'esprit : ce qui est redouté, parfois sans égard à l'examen des faits mis en cause, c'est la surveillance.

Pourtant, l'article 55 de la Loi d'accès[30] précise « qu'un renseignement personnel qui a un caractère public en vertu de la loi n'est pas nominatif. » Au départ, ces renseignements sont régis par un principe de libre de circulation. C'est aller à l'encontre de la loi que de se mettre à imposer des limites à la circulation de renseignements que le législateur a pris le soin de soustraire au régime des renseignements nominatifs.

Ces craintes de la « surveillance » conduisent à l'imposition d'une restriction encore plus drastique des possibilités d'accéder à des renseignements en se fondant sur les finalités, réelles ou supposées sous-jacentes à leur caractère public. Les informations à caractère public sont de plus en plus censurées au motif qu'il existe des risques – le plus souvent hypothétiques - que certaines d'entre elles soient utilisées de manière fautive.

L'ampleur de la dérive au sujet des informations à caractère public est particulièrement préoccupante car ici, on restreint l'accès à l'information à caractère public sans appeler à un débat public, celui auquel plusieurs avis de la Commission appellent lorsque sont mis de l'avant des projets de modifications de la législation sur la protection des renseignements personnels. Dans son *Avis relatif à la diffusion sur Internet de renseignements contenus dans les demandes de permis de construction*[31], la Commission prend sur elle de restreindre la notion de renseignements à caractère public au motif, pourtant non prévu dans la loi, que ces renseignements à caractère public une fois sur Internet pourraient devenir accessibles à des millions d'Internautes et que cela pourrait faire du Québec « un paradis du marketing direct. » On peut certes en avoir contre le marketing direct et trouver désagréable de recevoir des publicités non-sollicitées. C'est, à ce jour, matière de préférences personnelles. L'activité de marketing direct n'est pas illégale au Québec. Il est surprenant qu'un organisme public chargé d'appliquer la loi se permette de poser de tels jugements de valeur au sujet d'une activité en elle-même licite.

---

[29] L'article 50, 2e al. de la *Loi concernant le cadre juridique des technologies de l'information* affirme le caractère public du répertoire.

[30] *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, L.R.Q., c. A-2.1, ci-après citée Loi sur l'accès.

[31] COMMISSION D'ACCÈS À L'INFORMATION, *Avis relatif à la diffusion via intranet et Internet par la ville de Gatineau des renseignements contenus dans les demandes de permis de construction, mai 1999*, < http://www.cai.gouv.qc.ca/fra/docu/a990534.pdf >

Outre le fait que l'avis est construit sur un ensemble de suppositions, il faut relever que la Commission prend sur elle d'imposer des obligations relativement à la finalité des informations à caractère public. Elle affirme que « même si la loi est muette à ce sujet, on peut tout de même cerner l'objectif visé par une telle disposition. » Elle ajoute ainsi à la loi en y incluant une sorte de limite intangible au caractère public des renseignements fondée sur leur finalité supposée. Ce procédé est très inquiétant : on se met ainsi à poser des jugements de valeur au sujet de tout un ensemble possible d'usages d'informations publiques. Consulter le rôle d'évaluation pour prendre connaissance du fait que telle ou telle personne possède tant d'immeubles dans une ville est-il illégitime ? Il n'y a rien dans notre droit qui décrète que le fait qu'une personne soit propriétaire d'un immeuble, voire de plusieurs, relève de sa vie privée. Par contre, le droit sanctionne déjà -et à juste titre- la diffusion abusive de telles informations lorsque cela résulte d'un geste malveillant. En fait, on est ici en présence de renseignements qui ne sont pas des renseignements nominatifs et qui ne sont absolument pas assujettis aux exigences prévues par la loi. Lorsqu'on pose de pareils jugements de valeur sur les usages de certaines informations publiques, on porte gravement atteinte au droit à l'information. Un tel droit, comme les autres droits fondamentaux, ne devrait être restreint que lorsque des périls identifiables sont démontrés et alors des mesures ciblées devraient être prises, non des interdits à caractère universel.

Cette dérive a même été reprise dans la *Loi concernant le cadre juridique des technologies de l'information*. Cette loi impose un mécanisme de censure des documents publics comportant des renseignements personnels. L'article 24 de cette loi se lit comme suit :

> *L'utilisation de fonctions de recherche extensive dans un document technologique qui contient des renseignements personnels et qui, pour une finalité particulière est rendu public doit être restreinte à cette finalité. Pour ce faire, la personne responsable de l'accès à ce document doit voir à ce que soient mis en place les moyens technologiques appropriés. Elle peut, en outre, eu égard aux critères élaborés en vertu du paragraphe 2° de l'article 68, fixer des conditions pour l'utilisation de ces fonctions de recherche.*

Cette disposition vise des informations qui ont un caractère public; elle ne concerne pas les renseignements à caractère privé. Elle permet de restreindre l'utilisation des fonctions de recherche extensive à l'égard des documents technologiques comportant des renseignements personnels et rendus publics pour une finalité particulière. On veut ainsi éviter, par exemple, les consultations de banques de données à l'aide de moteurs de recherche afin de repérer des renseignements personnels pour des fins autres que celles pour lesquelles ils ont été recueillis ou diffusés.

On soutient parfois que ce genre de mesure se justifie du fait que dans l'univers des documents sur papier, la recherche est souvent longue puisque les documents publics doivent être examinés un à un. Pour les documents technologiques, les possibilités de recherche sont démultipliées, ce qui peut laisser craindre des abus. Devant cette possibilité hypothétique d'abus, la solution retenue est d'imposer la mise en place de moyens technologiques pour assurer la protection des renseignements personnels contenus dans ces documents publics. Et cette protection est de limiter l'accès uniquement aux fins pour lesquelles un document est rendu public comme si ces fins étaient connues et spécifiées. Voilà qui témoigne d'une tendance à nier le caractère social des informations portant sur les personnes. Les décideurs vont devoir se mettre à spécifier les finalités du caractère public d'une information. Il est difficile de concevoir comment une telle démarche est possible sans porter un jugement *a priori* sur la légitimité de certaines recherches;

sans parler de la difficulté de déterminer, en l'absence de texte législatif, ce qui constitue la finalité du caractère public d'une information. En fait, lorsqu'une information est à caractère public, elle est de libre parcours, sauf à démontrer qu'on en fait un usage fautif ou contraire à une loi. On ne peut présumer, sans nier le caractère public d'une information, qu'une information ne doit servir qu'à certaines fins et pas à d'autres. La seule limite légitime à l'usage d'une information à caractère public est le caractère abusif de l'usage : postuler a priori que des usages seraient abusifs laisse fort peu de place au droit à l'information.

Avec l'approche que reflète les politiques de la CAI de même que l'article 24 de la *Loi concernant le cadre juridique des technologies de l'information*, il n'y a plus d'informations à caractère public : il n'y a que des informations qui peuvent circuler pour des fins prédéterminées par les autorités publiques ou privées et ce, au gré de procès d'intention sur de possibles usages malveillants. Dans un État qui a pourtant été l'un des premiers à proclamer, à l'article 44 de la *Charte des droits et libertés de la personne* le droit à l'information, le dérapage est de grande ampleur.

Le trait commun de ces approches est le peu de cas ou le traitement cavalier qu'elles font des valeurs au nom desquelles certaines informations ont un caractère public. 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. Il serait légitime de la part d'un groupe de pression, on peut se demander s'il revient à un organisme public de se faire l'apôtre d'une conception aussi peu équilibrée des droits fondamentaux. Une autre faiblesse de ces analyses tient au fait qu'elles prennent peu d'intérêt pour l'analyse des alternatives aux mesures préconisées qui sont invariablement de retrancher – parfois au gré de demandes plus ou moins justifiées - des informations du domaine public. D'une part, on prête des finalités déterminées à des renseignements qui sont de libre parcours sous réserve d'abus et on postule qu'un renseignement ne peut avoir qu'une finalité fixe. Ces approches révèlent une rigidification à l'égard de la notion de finalité.

2. La rigidification du principe de finalité

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. Dans les principes de l'OCDE, le principe est ainsi exprimé :

> *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.*[32]

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 !

Lucas, Devèze et Frayssinet rappellent ainsi la raison d'être du principe de finalité :

> *Plus que la nature ou la signification première de l'information ou de la technique utilisée, le danger est dans les finalités des usages des données personnelles. La finalité doit être légitime pour le gestionnaire des informations, utile ou nécessaire pour la personne concernée qui a besoin d'information préalable, d'une capacité de choix éclairé et personnel pour déterminer son autonomie informationnelle.*[33]

D'un principe conçu pour procurer des balises au droit de traiter des informations personnelles obtenues d'une personne, on en a fait un principe justificatif de la censure imposée à la circulation des informations. Au nom des possibles et hypothétiques détournements d'informations sur des personnes, on a construit un régime de contrôle des informations afin de les soustraire aux usages non-prévus initialement et les assujettir, comme si ces informations relevaient de l'intimité, à un droit de veto des personnes ou des bureaucraties.

Le principe de finalité est né d'une démarche où il s'agissait principalement de sanctionner après-coup des usages abusifs. Il trouvait application une fois que l'on avait constaté que des informations étaient utilisées et que se posait la question de savoir si cela correspondait bien aux fins pour lesquelles le renseignement avait été recueilli. On a fait de ce principe une règle s'appliquant *a priori* même aux renseignements ayant un caractère public.

Pourtant, le principe de finalité n'a de sens que dans le cadre d'une évaluation du caractère fautif de l'utilisation d'une information. Il y a en effet de sous-jacent aux interdits de changement de finalités, un souci de prévenir les changements significatifs et préjudiciables dans les usages des informations. Dans un mode d'informatique centralisée ou l'usager n'a pas accès, il faut un moyen afin de garantir que des informations équivoques ne seront pas utilisées afin de prendre des décisions. Car, les changements dans les usages d'informations posent des problèmes de qualité d'information. Ce qui est problématique dans l'utilisation d'une information pour des finalités différentes de celles pour lesquelles elle avait été recueillie, c'est le risque que cette information soit de piètre qualité pour les nouvelles fins auxquelles on souhaite l'utiliser. Faute d'être en mesure de promouvoir des moyens afin de garantir que l'information utilisée pour

---

[32] OCDE, *Lignes directrices régissant la protection de la vie privée et des flux transfrontières de données de caractère personnel*, Paris, OCDE, 2002, < http://oecdpublications.gfi-nb.com/cgibin/OECDBookShop.storefront/EN/product/932002012P1 >

[33] André LUCAS, Jean DEVÈZE et Jean FRAYSINNET, *Droit de l'informatique et de l'Internet*, Paris PUF coll. Thémis droit privé, 2002, n° 11.

prendre des décisions relatives à une personne sera de qualité, on en est venu à interdire les changements de finalité.

Mais le contexte des réseaux permettant communication en temps réel change la donne. Il devient désormais possible d'assurer un contrôle de qualité de l'information en présentant, à chaque fois qu'on entend en faire usage, l'information à la personne concernée. Elle est alors en mesure de la valider. Il n'est plus nécessaire de se contraindre à la redondance. En accroissant la transparence des processus décisionnels, il est possible de mettre en place des garanties de qualité de l'information, compte tenu de finalités variables, sans pour autant subir le carcan d'une règle en vertu de laquelle toute information est réputée n'être détenue que pour une seule finalité.

Face aux risques que les informations utilisées pour une prise de décision soient inadéquates, on doit envisager de renforcer les mécanismes tendant à assurer la qualité de l'information plutôt que d'en empêcher platement la circulation. Le contrôle de finalité doit par conséquent être envisagé comme un contrôle de qualité : à chaque fois qu'on utilise une information, il faut la valider au regard des décisions pour lesquelles on entend l'utiliser. Dans plusieurs situations, cela peut se faire en présentant l'information à la personne concernée et lui demander de la valider et le cas échéant de la rectifier.

3. Le statisme de l'information

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 êtres 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.

L'article 66 de la Loi d'accès reconnaît qu'un organisme a le droit de recueillir des renseignements nominatifs déjà colligés auprès d'une entreprise. L'article 67 prévoit qu'il peut obtenir un renseignement nominatif de toute personne ou d'un autre organisme dès lors que cela est nécessaire à l'application d'une loi au Québec. Malgré cela, la Commission d'accès s'attache au principe de non-communication des renseignements personnels entre les organismes. Dans plusieurs avis, elle a exigé une démonstration de la nécessité des informations pour l'organisme, voire même que l'on démontre qu'il n'y a pas d'autres moyens d'assurer l'application des lois. En août 2002, devant le congrès de l'IFIP, la présidente de la CAI érigeait même en principe une règle à ce jour non mentionnée dans la loi selon laquelle il y aurait lieu, lors de partages d'informations de « respecter le cloisonnement administratif entre les différents organismes »[34].

---

[34] « Gouvernement en ligne et respect de la vie privée », allocution de Mme Jennifer Stoddart au 17e congrès de l'IFIP, Montréal, 27 août 2002, < http://www.cai.gouv.qc.ca/fra/actualite_fr/act_com_fr.htm >

Pourtant, la notion de nécessité retenue par la Commission[35] et la Cour du Québec[36] 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 Charette 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 »[37].

Mais la Commission d'accès a appliqué, notamment dans ses avis et recommandations portant sur des projets de modernisation des systèmes d'information une conception beaucoup plus stricte de la notion de nécessité. Doray et Charette observent que : « On retrouve depuis lors dans les décisions de la Commission une assimilation de l'adjectif «nécessaire» aux termes «indispensable», «essentiel», «obligatoire» et à l'expression «dont l'organisme ne peut se passer» »[38].

La Commission a eu souvent l'occasion de rappeler[39], qu'elle n'est pas liée par les écrits et les opinions de son personnel administratif, professionnel ou juridique dans ses fonctions d'adjudication. Il n'en reste pas moins que plusieurs avis de la Commission procèdent d'une conception très stricte de la nécessité. Parfois, on cherche à déterminer dans l'abstrait, ce qui est nécessaire à l'exercice d'une fonction ou à l'accomplissement d'une prestation. On évalue des projets entiers en fonction de critères qui ne sont pas nécessairement conformes à ceux que suivrait la Commission si elle était appelée à se prononcer dans un cas réel de plainte pour non-respect de la loi.

Mais comme le mentionne le juge Claude Filion dans la décision *Société de transport de la Ville de Laval c. X*,[40] le principe d'interprétation (…) « voulant que la nécessité doit être évaluée relativement aux fins pour lesquelles un renseignement est requis, est conforme à la lettre et à l'esprit de la loi. Il ne s'agit pas de déterminer ce qu'est la nécessité en soi, mais plutôt de chercher, dans le contexte de la protection des renseignements personnels, et pour chaque situation, ce qui est nécessaire à l'accomplissement de chaque fin particulière pour laquelle un organisme public plaide la nécessité. »

---

35 *Bellerose* c. *Université de Montréal*, [1986] C.A.I. 236.

36 *Bellerose* c. *Université de Montréal*, [1988] C.A.I. 377 (C.Q.).

37 Raymond DORAY et François CHARETTE, *Accès à l'information, loi annotée, jurisprudence , analyse et commentaires*, Cowansville, Éditions Yvon Blais, p. III/ 64-3.

38 Raymond DORAY et François CHARETTE, *Accès à l'information, loi annotée, jurisprudence , analyse et commentaires*, Cowansville, Éditions Yvon Blais, p. III 64-3.

39 *X.* c. *Société de transport de la Ville de Laval*, C.A.I., n° 99-15 58, 15 avril 2001. Voir sur cette décision : Raymond DORAY et François CHARETTE, *Accès à l'information, loi annotée, jurisprudence, analyse et commentaires*, Cowansville, Éditions Yvon Blais, p. III/ 64-4.

40 *Société de transport de la Ville de Laval c. X, (2003-02-21) QCCQ 500-02-094423-014, < http://www.canlii.org/qc/jug/qccq/2003/2003qccq11657.html >.*

4. Le recours au consentement comme palliatif à la rigidité

C'est au prix de contorsions et d'artifices que l'on parvient à concilier la conception de la protection des renseignements personnels qui tend à se développer au Québec, avec les exigences d'un fonctionnement réaliste des environnements d'information. Parmi les contorsions les plus apparentes, il y a celles auxquelles a donné lieu la pratique relative au « consentement libre et éclairé. »

Il convient de rappeler le libellé de l'article 53 de la Loi d'accès :

> *Les renseignements nominatifs sont confidentiels sauf dans les cas suivants :*
>
> *1° leur divulgation est autorisée par la personne qu'ils concernent; si cette personne est mineure, l'autorisation peut également être donnée par le titulaire de l'autorité parentale;*
>
> […]

On constate que la Loi d'accès ne traite pas du consentement, elle parle plutôt d'autorisation par la personne concernée. Alors que pour la collecte, la loi régissant les organismes publics n'exige pas de consentement, l'autorisation de divulgation peut découler des circonstances ou du contexte dans lequel se déroule la relation entre la personne et l'organisme. Le consentement nécessite, quant à lui, un acte juridique spécifique. Malgré cette disposition explicite de la Loi d'accès, la Commission a imposé, pour son application article des exigences qui ne figurent pourtant que dans la *Loi sur la protection des renseignements personnels dans le secteur privé*[41]. Elle s'est ainsi mise à subordonner la divulgation de renseignements personnels au consentement manifeste, libre, éclairé, donné à des fins spécifiques par la personne concernée. Pourtant, l'exigence mentionnée dans la Loi sur l'accès est celle d'une autorisation, qui pourrait être implicite ou simplement découler du contexte. Cette exigence de consentement et la lourdeur qui l'accompagne est devenue, sans que la loi l'ait prévu, une exigence fondamentale dans le cycle de gestion des renseignements personnels au sein des organismes publics. En décembre 2002, la Commission d'accès en faisait encore une exigence dans son *Guide en matière de protection des renseignements personnels dans le développement des systèmes d'information* : « *6.3 Le consentement à la communication provient directement de la personne concernée. 6.4 Vous consignez les preuves de consentement à la communication et les échangez entre parties communicantes. 6.5 Vous validez la signature du consentement à la communication »*[42].

L'effet pervers de ce genre de dérive est de faire porter les efforts sur la recherche et la gestion du consentement plutôt que sur la protection effective de la vie privée des personnes.

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

---

41 L.R.Q., c. P-39.1

42 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 >

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 une exigence de la loi. En réalité, c'est le fruit d'une interprétation éminemment contestable de la Commission d'accès. On en vient à se demander si les ressources qu'on se croit obligé de consacrer à la gestion des consentements seraient mieux investies dans une gestion plus serrée des informations personnelles, en fonction des risques posés par celles-ci.

En France, la CNIL relève les malentendus que la généralisation des recours au consentement pourrait introduire dans la gestion de l'information par les organismes publics. Dans son 22e rapport d'activités 2001, la Commission écrit : « Promouvoir le consentement ne risque-t-il pas de donner à croire que chacun serait libre de ne pas figurer dans un fichier fiscal, un fichier de police, un fichier de gestion administrative ? Ce serait tromper nos concitoyens sur la réalité de leurs droits et peut-être sur l'essentiel de ce qui constitue le lien social qui contraint à devoir concilier vie privée et d'autres valeurs d'intérêt général […] ». Et la CNIL d'ajouter qu'« en sens inverse, promouvoir le consentement, ne peut-il aboutir à anéantir des garanties d'intérêt public au motif que les personnes auraient consenti ? »[43].

Ces dérives autour de la notion de consentement sont révélatrices du fait que, bien souvent, on a perdu de vue la raison d'être de la protection des renseignements personnels. D'une finalité de protéger la vie privée on est passé à celle de donner suite à un plus ou moins mythique « droit de veto » de la personne sur les informations la touchant. On se trouve ainsi à omettre le caractère social de certaines informations relatives aux personnes et en assujettir la circulation à un droit de veto de l'individu concerné. Le consentement, qui était au départ un moyen d'assurer au sujet la maîtrise nécessaire sur les renseignements relevant de sa vie privée, est devenu une fin en soi, quitte à ce qu'il soit perverti ou banalisé afin de contourner les rigidités résultant d'une conception trop englobante de la protection des renseignements personnels.

Cette conception a eu pour conséquence de faire porter de plus en plus la protection sur le consentement de l'intéressé. Plutôt que de mettre en place les mécanismes assurant la protection de ce qui relève de la vie privée et la circulation de ce qui relève de l'espace collectif, on a transformé la protection des renseignements personnels en un droit de veto. L'avènement des environnements de réseaux de même que les mutations des finalités auxquelles les informations peuvent être utilisées ont fait en sorte que pour assurer le fonctionnement efficace des systèmes, il fallait nécessairement se munir d'un consentement large. La pratique s'est ainsi répandue de

---

[43] Commission nationale de l'informatique et des libertés, *22e rapport d'activités 2001*, Paris, La documentation française, 2002, p. 108 et 109, < http://www.ladocumentationfrancaise.fr/BRP/024000377/0000.pdf >

faire signer des consentements aux personnes afin de se prémunir contre les éventuelles contestations. Armés de la légitimité d'un consentement « libre et éclairé », certains services publics ou entreprises pourraient se mettre à recueillir plus d'informations que nécessaire. Comme le tout se fait dans un contexte de contrat d'adhésion, il est irréaliste d'imaginer que les personnes seront prêtes à se priver des services parce qu'on leur réclame trop d'informations personnelles. Ce phénomène est d'ailleurs un indice que les individus savent que la circulation des informations sur leur personne est inhérente à la vie sociale et que sa circulation n'emporte pas les conséquences apocalyptiques que certains se plaisent à imaginer.

5. La multiplication des lois d'exceptions

La rigidité de l'application des règles en matière de protection des renseignements personnels de même que l'extension excessive de certaines notions ont rompu l'équilibre. C'est sans doute pour cette raison que le Parlement se trouve de plus en plus dans l'obligation d'intervenir au moyen de lois afin de rétablir les équilibres rompus en matière de protection des renseignements personnels.

Herbert Burkert constate que dans plusieurs pays, se sont multipliées les lois d'exception, venant sectoriellement restreindre ou baliser le droit à la protection des renseignements personnels. Il écrit qu' :

> *Il est en effet qu'à considérer l'ensemble des textes législatifs émis depuis la promulgation des premières lois sur la protection des données, pour se rendre compte qu'ils comportent une multitude de textes sectoriels. Tous ne prennent pas la forme de lois spéciales; certains se présentent sous forme de simples amendements ou compléments. Cette législation, et tout particulièrement celle relative au traitement des données détenues par le secteur public, a globalement limité la portée des principes généraux en la matière en introduisant ce que l'on a vu comme des compromis entre le respect de la vie privée et les nécessités de l'intérêt public. Et s'il est vrai que les individus sont attachés au respect de leur vie privée, ils s'en détachent rapidement dès lors qu'ils sont appelés à choisir entre confidentialité et sécurité- qu'il s'agisse de sécurité sociale ou publique.*[44]

Cette tendance à la multiplication de lois venant apporter des ajustements sectoriels au droit de la protection des données personnelles est un indice du caractère inadéquat des mécanismes généraux. Le cadre juridique général de la protection est trop rigide, ou perçu comme tel pour accommoder les autres impératifs.

Pour illustrer l'ampleur de la dérive à laquelle on doit remédier, rappelons qu'au Québec, une loi a été adoptée afin de permettre la circulation d'informations de manière à rendre possible les mesures de prévention des suicides ou autres actes de violence contre une personne identifiable[45]. Cette loi a ajouté l'article 59.1 à la Loi d'accès prévoyant que :

---

[44] Herbert BURKERT, « Progrès technologiques, protection de la vie privée et responsabilité politique, 89 *Revue française d'administration publique*, janvier-mars 1999, pp. 119-129, p. 125.

[45] *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. < http://publicationsduquebec.gouv.qc.ca

> *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.*

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.

Pourtant, il aurait été possible de lire la loi en convenant que les informations portant sur une personne ne sont pas toujours relatives à sa vie privée entendue comme le rempart de sa dignité. On aurait pu donner un sens au fait que la loi est rédigée de manière à distinguer les informations servant à rendre des services aux citoyens et les activités ayant pour objectif de les surveiller. Plusieurs informations se rattachent à la personne en tant qu'élément constitutif de la société. Et ces informations appellent un régime qui ne peut être entièrement tributaire du veto de l'intéressé. Si l'on peut convenir de la nécessité d'assurer la capacité de la personne de contrôler la circulation des informations portant sur sa vie privée, il en va tout autrement pour les informations qui sont des manifestations de sa participation à la vie sociale, qui concernent son appartenance à une communauté ou encore, qui sont utilisées dans son propre intérêt. Si l'on comprend ainsi le régime de la protection des renseignements personnels, il devient possible de l'adapter et de renforcer les protections de la vie privée. Si on persiste à en faire un droit des personnes à faire prévaloir leurs préférences, on va devoir surmultiplier les situations pour lesquelles tous conviendront que l'intérêt social doit l'emporter et se résoudre à adopter de plus en plus de lois d'exception.

/fr/cgi/telecharge.cgi/180F0206.PDF?table=gazette_pdf&doc=180F0206.PDF&gazette=4&fichier=180F0206.PDF >

III- Des droits actualisés pour protéger la vie privée dans les réseaux

Devant les carences que présente le droit relatif à la protection des renseignements personnels, il faut identifier des voies qui permettront une mise à niveau avec les impératifs contemporains de meilleure circulation de l'information tout en renforçant le niveau de protection de la vie privée des personnes. Il est nécessaire d'actualiser les droits des personnes afin d'assurer une protection effective de la vie privée. Mais une telle démarche doit être menée selon une approche assurant à la fois une réelle protection de la dignité des personnes et la libre circulation des informations relevant de l'espace social. Pour organiser le cadre juridique des informations personnelles dans les réseaux, il faut reconnaître les caractéristiques de ces environnements et structurer ceux qui servent à dispenser les services publics de manière à pouvoir y appliquer des règles de protection appropriées.

L'administration électronique se conçoit dans un environnement caractérisé par l'interconnexion et la dématérialisation. Les interactions prennent place dans un environnement décentralisé et de plus en plus personnalisé. En même temps, le contexte découlant de l'interconnexion apparemment infinie des ordinateurs est universel. Il se caractérise par l'interpénétration d'univers qu'on avait l'habitude de traiter comme distincts. Et tout cela se déroule à un rythme accéléré, à l'image des vitesses de traitement de l'information désormais possibles[46].

L'État en réseau est fondé sur les interconnexions. 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 du www est fondé sur l'hypertexte. Cela permet et généralise les possibilités d'intercréativité, d'interrelations, le croisement d'informations situées 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.

Le phénomène de décentralisation est aussi caractéristique de l'État en réseau : pour le citoyen, l'État en réseau se présente de plus en plus comme un réseau maillé dans lequel les frontières administratives ont peu 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.

L'environnement décentralisé et personnalisable que constitue le cyberespace appelle l'émergence de nouvelles formes de coopération. L'usager est actif, les environnements virtuels en font un souverain à la fois émetteur, volontaire ou involontaire, et un récepteur[47]. Il faut donc envisager la construction des repères de la confiance et concevoir les modalités du partage de l'information ainsi que les obligations de rendre compte. Ces phénomènes laissent deviner l'apparition de nouvelles formes et méthodes de régulation.

Le cyberespace permet de nouvelles modalités de personnalisation des services proposés aux consommateurs mais aussi une capacité de démultiplication des personnalités. Investi d'une

---

46 François DENIEUL, *Internet et les sept piliers du XXI^e siècle*, Paris Connaissance partagée, 1999, p. 9 ss.

47 Pierre TRUDEL, « Quel droit et quelle régulation pour le cyberespace ?», (2000) *Sociologie et Société,* vol. 32, n^o 2, < http://www.erudit.org/revue/socsoc/2000/v32/n2/index.html >.

souveraineté et ayant vocation à recourir à différents outils en ligne, l'usager est perçu ou à tout le moins présenté comme étant en position de choisir, puis de négocier les niveaux de sécurité et de protection qu'il veut avoir. Les règles du jeu qui encadrent les activités auxquelles il prend part sont de plus en plus envisagées comme une composante du produit et du service qui lui est proposé. Ces règles se présentent souvent de façon personnalisée, modelées sur le profil établi en fonction de différentes variables prises en compte à l'occasion des échanges d'information qui ont lieu lors des interactions entre l'usager et les sites qu'il visite[48].

À l'égard des services offerts par l'État aux citoyens, ces caractéristiques ont des conséquences. On ne peut plus simplement postuler que les services publics agissent unilatéralement. L'environnement en réseaux permet des dialogues multiples. Plus que jamais, l'État est en position 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, ou l'administré, est désormais en mesure d'interagir et d'exiger le retrait et l'ajout d'informations. Par conséquent, 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 dans le contexte de dialogue accru que permet le réseau.

La virtualisation des échanges se traduit également par un phénomène d'interpénétration des entreprises et des environnements. Cette interpénétration des environnements de communication jadis considérés distincts les uns des autres est favorisée par la numérisation. Cette dernière permet de réaliser différentes activités par un traitement de l'information reposant sur des traitements informatiques de données désormais rendues techniquement équivalentes. Se pose ainsi la question du cadre juridique appliqué aux espaces d'interactions résultant de cette virtualisation. Il faut pareillement concevoir des règles pour faire en sorte que les informations personnelles soient protégées où qu'elles se trouvent au sein d'un environnement de réseau voué aux services gouvernementaux et aux interactions État-citoyen.

Dans un univers où les regroupements d'intérêts ne sont plus tributaires de la distance physique, le rôle des communautés, leurs capacités d'auto-organisation et d'autorégulation permettent d'envisager l'émergence d'une normativité propre à assurer la gestion des interactions ainsi rendues possibles. Dans de telles situations, il est normal que l'information pertinente aux groupes et au bon déroulement de ses activités puisse circuler.

L'accélération de la circulation des informations et les conséquences qui en résultent en termes d'accélération des échanges appellent souvent des modalités conséquentes au plan des encadrements normatifs. L'instantanéité des activités dans les environnements-réseaux s'oppose de plus en plus à la valorisation de la stabilité et du conformisme si cher à certaines communautés bureaucratiques. Cette accélération appelle la conception de cadres normatifs reflétant cette vélocité de l'information, non des normes pour figer l'information sous le prétexte de la protéger.

Ainsi décrit, l'espace virtuel paraît universel et difficilement réductible à une division spatiale ou organisationnelle. Au plan du droit de la protection des renseignements personnels, ce

---

[48] Paul M. SCHWARTZ, « Privacy and Democracy in Cyberspace », (1999) 52 *Vanderbilt L.R.*, 1609-1702, pp. 1621-1632.

phénomène emporte la nécessité de concevoir la protection des personnes en se fondant sur des repères organisationnels et spatiaux capables de rendre compte du fonctionnement des espaces de réseaux. Au niveau d'un gouvernement, il faut des règles capables d'assurer l'encadrement des conduites dans des lieux virtuels et non plus au sein d'organismes publics considérés isolément les uns des autres.

En somme, l'émergence de l'État en réseau appelle un environnement régulé de façon passablement différente que celle reposant sur le postulat d'organismes et ministères indépendants et cloisonnés les uns des autres. La régulation doit se situer au niveau du réseau. Les événements se déroulant dans les espaces réseaux doivent bénéficier d'un cadre juridique assurant la protection et la qualité des informations. Mais aussi, le cyberespace est un environnement technique. Construit essentiellement en fonction des capacités de communiquer dont sont désormais pourvus les outils informatiques, son cadre normatif paraît fortement influencé par les choix que la technique reflète, permet ou interdit.

A) Des fondements plus cohérents

Il faut recentrer les fondements de la protection des renseignements personnels. En faisant une distinction entre les informations policières et les informations nécessaires à la fourniture de services publics, il devient possible de s'affranchir de l'imagerie de la « surveillance » qui caractérise jusqu'ici les approches en matière de protection de renseignements sur les personnes. C'est la qualité de l'information qui devient le fil conducteur. Ce qui fonde la protection des renseignements personnels, c'est la garantie de la qualité de l'information. En s'affranchissant des imageries de la « surveillance, » et en mettant l'accent sur la qualité des services publics, c'est un état d'esprit renouvelé qui est recherché.

Les principes fondamentaux du droit de la protection des renseignements personnels n'ont pas en soi à être remis en cause. Ces principes composent la structure d'instruments internationaux de protection des données personnelles comme les *Lignes directrices de l'OCDE*, la *Convention européenne* et la *Directive de la Commission européenne*, mais également de plusieurs législations nationales[49]. Il s'agit des principes suivants :

- le principe de justification sociale,
- le principe de la limitation en matière de collecte,
- le principe de la qualité des données,
- le principe de la spécification des finalités,
- le principe de la limitation de l'utilisation,
- le principe des garanties de sécurité,
- le principe de la transparence,
- le principe de la détention limitée dans le temps,
- le principe de la responsabilité et
- le principe de la participation individuelle.[50]

---

[49] L.R.Q., c. P-39.1.

[50] Voir sur ces principes en particulier et sur la protection des renseignements personnels en général Karim BENYEKHLEF, *La protection de la vie privée dans les échanges internationaux d'information*, Montréal, Éditions Thémis, 1992.

Mais il faut s'attacher à appliquer les principes de la protection de la vie privée en tenant compte des contextes variés du cyberespace 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.

Il importe désormais de faire la part des choses entre les informations de surveillance et les informations visant le service au citoyen. Il faut assurer un haut degré de confiance d'un bout à l'autre des environnements transactionnels utilisés par l'État. Le cadre juridique doit s'attacher à assurer la qualité de l'information, compte tenu de chaque contexte d'utilisation. Enfin, cela suppose de garantir, mais aussi de compter sur un plus haut degré de maîtrise, par l'individu, des données le concernant.

1. 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.

2. Assurer un environnement de confiance

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'usager/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'usager 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'êtres 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 appropriées garantissent un tel respect.

Par contre, le développement de services en réseaux appelle à une relecture de la notion de finalité. Ce qui importe désormais est que l'usager soit informé des familles de finalités

auxquelles serviront les informations. La notion de finalité doit en effet 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 fiscales doit savoir que les informations qu'il fournit circuleront et seront utilisées aux fins d'assurer l'application des lois fiscales. Le lien de confiance serait lourdement hypothéqué si de pareilles informations pouvaient être utilisées à des fins d'évaluation médicale ou lorsque la personne postule un emploi!

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. 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.

La gestion des informations sur les personnes se révèle ainsi comme une composante majeure de la confiance inhérente aux relations entre l'État et le citoyen. C'est pourquoi la cueillette et le traitement d'informations personnelles doivent être assortis de garanties de confiance. La confiance dans l'environnement de réseaux se construit en assurant un haut niveau de transparence : il faut informer clairement et franchement l'usager, il faut tenir parole et fournir des garanties solides quant à l'usage possible des informations.

D'autre part, la tendance à l'impartition ne doit pas faire perdre à l'État la maîtrise effective des informations personnelles. L'intervention du secteur privé, notamment lorsqu'il est décidé de procéder à l'impartition de certaines tâches, doit se faire moyennant un encadrement strict. Ainsi, le recours, par les organismes publics, aux services de fournisseurs d'applications en ligne doit pareillement être encadré. L'implication d'une entité privée dans le traitement, la transmission, l'archivage ou la confection des informations ne devrait pas modifier les responsabilités des organismes à l'égard des informations personnelles ou même entraîner une réduction du niveau de protection des informations.

D'ailleurs, l'article 26 de la *Loi concernant le cadre juridique des technologies de l'information* requiert de toute personne qui confie un document technologique à un prestataire qui doit en assurer la garde d'informer ce prestataire des protections que requiert le document en ce qui a trait à la confidentialité de l'information. Le prestataire est tenu d'en assurer la sécurité, d'en préserver l'intégrité et d'en protéger la confidentialité.

3. Des garanties quant à la qualité des informations personnelles

Dans un monde où l'information a vocation à circuler de plus en plus, le défi est d'assurer que l'information sera de qualité adéquate pour chacune des utilisations. La circulation des informations doit donc être assortie de garanties à l'égard de la qualité des informations. La qualité est une composante du lien de confiance qui doit nécessairement exister entre l'usager et l'administration. Si le citoyen n'a pas la certitude que tout est mis en œuvre afin d'assurer que

les décisions sont prises avec les informations de la plus grande qualité possible, il n'aura pas confiance.

Le droit intervient pour identifier la qualité des informations à utiliser. Par exemple, dans plusieurs situations, le droit exige que l'identification des personnes s'effectue au moyen d'informations présentant certains seuils de précision ou garanties de fiabilité. Pour obtenir un passeport canadien, il faut fournir un document de l'état civil, un formulaire et une déclaration d'un répondant. Toutes ces informations visent à assurer la qualité de l'identification de la personne qui demande un passeport. De la même façon, le droit prescrit des seuils de qualité pour autoriser l'utilisation de certaines informations.

Au nombre des exigences de qualité technique de l'information les plus souvent mentionnées, il y a l'intégrité technique de l'information. La valeur juridique d'un document, c'est-à-dire sa capacité de constituer une preuve, dépend de son intégrité. Au Québec, l'article 6 de la *Loi sur le cadre juridique des technologies de l'information*[51] vient expliciter les critères d'intégrité d'un document, qui sont les mêmes que ceux reconnus habituellement au support papier. En application du principe d'équivalence fonctionnelle, on a transposé les critères qui sont utilisés afin de déterminer ce qui permet de conclure à l'intégrité à l'égard d'un document sur un support papier.

Dans la plupart des situations, la qualité de l'information s'apprécie en fonction du contexte. Une information peut répondre convenablement à un besoin alors qu'elle sera nettement insuffisante, voire contre-indiquée, dans un autre contexte. Dans le contexte des interactions entre l'État et le citoyen au sein des réseaux, il devient possible d'évaluer, de concert avec la personne concernée, si l'information répond aux exigences qualitatives requises pour la décision qui doit être prise.

C'est donc en organisant des processus de dialogue entre les administrations et les usagers que l'on peut obtenir une application des plus hauts standards de qualité. C'est dire l'importance renouvelée de garantir aux individus un niveau adéquat de maîtrise des données les concernant.

4. La maîtrise des données personnelles

La protection de la vie privée et des informations personnelles suppose de reconnaître à la personne concernée un droit d'exercer un certain contrôle sur ce qu'il advient des renseignements la concernant. Mais ce droit de contrôle n'a jamais été et ne saurait être absolu. Lucas, Devèze et Frayssinet rappellent qu'« il n'y a pas de vie sociale sans échanges de données personnelles ». Ces auteurs ajoutent qu'« une personne est non seulement un être physique et psychique mais aussi un être informationnel (…). » Il faut donc poser le principe en convenant de ses limites. Le rapport Truche rappelle que « le principe de maîtrise des données personnelles ne saurait être posé en absolu »[52]. La CNIL exprime aussi des réserves au sujet d'un droit de

---

51 L.Q. 2001, c. 32, en ligne avec annotations à < http://www.autoroute.gouv.qc.ca/loi_en_ligne > .

52 Pierre TRUCHE, Jean-Paul FAUGÈRE et Patrice FLICHY, *Administration électronique et protection des données personnelles livre blanc,* Rapport au ministre de la fonction publique et de la réforme de l'État, Paris, La documentation française, 2002, p. 77.
< http://www.ladocumentationfrancaise.fr/brp/notices/024000100.shtml >

maîtrise des données personnelles en rappelant que ce qui est essentiel, c'est que les données soient de qualité. Dans son 22e rapport d'activité, la CNIL écrit que :

> *Mais ne peut-on soutenir que si le droit d'accès est peu exercé, en pratique, c'est qu'au fond l'essentiel pour nos concitoyens n'est pas tant de vérifier la teneur des données qu'ils ont le plus souvent communiquées eux-mêmes à l'administration concernée, que d'avoir la garantie que ces données ne seront pas détournées de la finalité initiale, communiquées à des tiers qui n'ont pas à en connaître ou leur serait opposables de nombreuses années après.*[53]

Le droit de contrôle des données peut être conçu comme un droit s'exerçant *a priori*. Il peut aussi s'exercer *a posteriori*, lorsqu'un usage inadéquat a été fait d'une information et qu'il convient de le rectifier. Ainsi un droit de contrôle *a priori* peut être exercé par la personne concernée à l'égard de toutes les informations personnelles circulant au sein d'un domaines de confiance. Il devrait être possible d'exercer un droit d'accès et de vérification des informations circulant dans un domaine de confiance et d'éventuellement demander des correctifs. Il devrait également être possible, en tout temps, de s'assurer de la qualité des informations utilisées pour prendre une décision à son sujet.

La mise en place de prestations électroniques de services peut être une excellente occasion d'accroître le niveau de maîtrise de l'usager sur ses données personnelles. En garantissant un droit d'accès et de validation des informations relatives à une transaction ou à une décision, on procure au citoyen un droit de maîtrise continu et ciblé sur ses données personnelles. En plus, on améliore la qualité de l'information utilisée pour assurer la prestation des services publics.

B) Des moyens de protection plus efficaces de la vie privée dans les réseaux

La clé du succès de l'administration électronique réside dans sa capacité d'inspirer confiance. Des moyens de protection conséquents doivent être mis en place. Pour exiger légitimement des citoyens qu'ils laissent circuler des informations qui les concernent dans des réseaux, l'État doit être hautement crédible. Il faut donc organiser des espaces virtuels de confiance au sein desquels les informations pourront circuler moyennant des garanties strictes de qualité et des balises en limitant la collecte et les usages.

Le cadre juridique de la protection des renseignements personnels doit être conçu à partir d'une désignation de domaines parmi les espaces en réseau au sein duquel se déroulent les interactions. Dans ces domaines, l'information n'entre et sort que moyennant des conditions strictes ; elle y circule moyennant des conditions définies et dont est informé l'intéressé.

1. Des domaines de confiance

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

---

[53] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, *22e rapport d'activités 2001*, Paris, La documentation française, 2002, p. 108, < http://www.ladocumentationfrancaise.fr/BRP/024000377/0000.pdf >.

conséquente. Le cadre juridique de la protection des renseignements personnels doit prévoir des concepts qui pourront assurer à la fois la circulation des informations et les balises à cette circulation. Il faut aussi pouvoir situer les responsabilités, non plus seulement en fonction de la possession d'un renseignement personnel par un organisme déterminé, mais dans une situation où il est disponible simultanément pour une pluralité d'organismes. Cela appelle la mise en place des outils nécessaires pour procurer les garanties et les protections que requiert l'information portant sur les personnes. La notion de domaine de confiance paraît susceptible de contribuer à l'organisation du cadre juridique de cet espace indivis de production et de circulation d'informations sur les personnes.

Par domaine de confiance, on entend un ensemble de mécanismes balisant la circulation de l'information et en délimitant 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. Le Conseil du trésor reconnaît la notion dans le cadre de l'architecture gouvernementale de l'information et en fait une composante de l'approche en matière de sécurité[54].

L'une des dimensions les plus cruciales de l'établissement d'un domaine de confiance est d'identifier, parfois d'organiser, l'autorité responsable du service ou de l'échange. Dans un contexte d'État en silo, 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 tel espace de circulation.

Pour les fins de la législation sur la protection des renseignements personnels, la notion de domaine de confiance pourrait être définie comme : « Un ensemble d'organismes publics liés par une entente d'échange et de partage de renseignements nominatifs ». La loi devrait prescrire la teneur et les conditions de telles ententes. De telles ententes devraient avoir un caractère public et être accessibles au public.

Les domaines de confiance peuvent se concevoir suivant différents modèles et cas de figure.

Un premier cas de figure est fourni par la grappe d'informations. Des organismes partagent des informations qui sont détenues par l'un des organismes participants au domaine de confiance. Dans un tel modèle, les informations sont partagées par un ensemble d'organismes publics. Elles sont détenues dans un organisme mais rendues accessibles à d'autres.

---

[54] 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 resources informationnelles, septembre 2001. < www.autoroute.gouv.qc.ca/publica/pdf/agsin-ciblesom.pdf >

Le modèle dit du « bureau de poste » évoque la notion de dépôt dans lequel sont déposées des informations qui sont ensuite transmises aux organismes participants concernés. Dans un autre cas de figure, les informations sont confiées à un tiers qui les garde à la disposition du destinataire qui vient les y recueillir. Une fois les informations transmises, elles ne sont qu'en possession des organismes destinataires.

Dans le modèle de l' « application service provider, » les renseignements personnels sont confiés à un tiers qui agit pour le compte de l'organisme public. Alors ce dernier n'est pas dégagé des responsabilités qui lui incombent à l'égard des dossiers des personnes.

On peut aussi imaginer le modèle itinérant soit celui dans lequel l'information personnelle est répartie dans une pluralité de lieux réunis en réseaux. Ainsi, les informations concernant une personne peuvent être consignées dans plusieurs documents résidant sur des supports situés en divers lieux.

C'est une situation mentionnée à l'article 4 de la *Loi concernant le cadre juridique des technologies de l'information* qui prévoit que :

> ***4.*** *Un document technologique, dont l'information est fragmentée et répartie sur un ou plusieurs supports situés en un ou plusieurs emplacements, doit être considéré comme formant un tout, lorsque des éléments logiques structurants permettent d'en relier les fragments, directement ou par référence, et que ces éléments assurent à la fois l'intégrité de chacun des fragments d'information et l'intégrité de la reconstitution du document antérieur à la fragmentation et à la répartition.*

Par conséquent, un dossier d'une personne dans un cadre où l'information est répartie sera réputé constituer un tout si les deux conditions suivantes sont réunies :

- les éléments logiques structurants permettent d'en relier les fragments, directement ou par référence, et

- ces éléments assurent à la fois l'intégrité de chacun des fragments d'information et l'intégrité de la reconstitution du document antérieur à la fragmentation et à la répartition.

Le droit québécois reconnaît donc d'ores et déjà qu'un dossier, voire un document, peut être réparti sur une pluralité de lieux et de supports.

Au plan juridique, les domaines de confiance doivent être encadrés par des règles qui viendront préciser le partage des responsabilités relativement aux informations. On devra aussi déterminer qui répond des informations qui sont ainsi partagées en réseau. En somme, il s'agit de mettre en place les règles définissant les responsabilités.

Pour délimiter ces domaines de confiance, il faut identifier des niveaux de protection différenciés qui devront trouver application en fonction du degré de sensibilité de l'information personnelle. Il faut distinguer les informations à caractère public, les informations des personnes échangées de façon anonyme, les informations nominatives et celles qui sont sensibles, qui touchent au cœur de la vie privée des personnes.

Une fois identifiés les niveaux de protection, de même que les catégories d'information, il faut structurer les responsabilités.

La responsabilité d'un domaine de confiance pourra être confiée à un organisme : une pluralité d'entités lui confient des responsabilités générales ou spécifiques à l'égard d'un corpus d'informations.

L'article 26 de la *Loi sur le cadre juridique des technologies de l'information* impose des obligations lorsqu'un responsable d'un document le confie à un prestataire. Il prévoit que :

> *Quiconque confie un document technologique à un prestataire de services pour qu'il en assure la garde est, au préalable, tenu d'informer le prestataire quant à la protection que requiert le document en ce qui a trait à la confidentialité de l'information et quant aux personnes qui sont habilitées à en prendre connaissance.*
>
> *Le prestataire de services est tenu, durant la période où il a la garde du document, de voir à ce que les moyens technologiques convenus soient mis en place pour en assurer la sécurité, en préserver l'intégrité et, le cas échéant, en protéger la confidentialité et en interdire l'accès à toute personne qui n'est pas habilitée à en prendre connaissance. Il doit de même assurer le respect de tout autre obligation prévue dans la loi relativement à la conservation du document.*

La responsabilité du domaine de confiance peut incomber à une entité spécifiquement établie à cette fin qui répond des obligations à respecter à l'égard des renseignements personnels. Une telle entité pour avoir la personnalité juridique ou être une société constituée d'organismes publics participant. Ce qui importe, au-delà de la forme juridique, c'est la transparence des droits et des responsabilités de même que la capacité d'identifier - en tout temps - qui est imputable pour les informations.

2. Moduler les efforts de protection aux différences de sensibilité des informations

La généralisation des environnements et réseaux de traitement de l'information est telle qu'elle permet d'entrevoir que la quasi-totalité des informations concernant chaque individu peut s'y retrouver. Pour protéger efficacement les informations relatives aux personnes, il faut apporter des distinctions. Même si toutes les informations relatives à une personne ont un statut semblable, elles ne présentent pas tous les mêmes risques ou les mêmes enjeux. Une véritable protection des personnes requiert de consacrer plus d'efforts à protéger les informations hautement sensibles. Il serait dommage de maintenir une interprétation du cadre juridique imposant de divertir des ressources à protéger ce qui est en pratique dérisoire au point d'en manquer afin de protéger ce qui comporte des enjeux importants.

La protection des informations n'est pas une activité gratuite; si elle est menée avec soin, elle suppose des coûts et des efforts qui doivent être justifiés. Il serait en effet absurde de consacrer autant d'efforts pour assurer la protection de la confidentialité de l'adresse de courriel d'une personne que l'on en consacre afin d'assurer la confidentialité de son dossier fiscal. Toutes les informations personnelles ne présentent pas le même niveau de risque. Dans les réseaux, l'information doit pouvoir circuler; toutefois, les personnes doivent être assurées d'une

protection efficace, comte tenu des risques et enjeux associés aux différentes informations qui les concernent.

Il faut donc concevoir le cadre de la protection des renseignements personnels en considérant que les citoyens interagissent avec un ensemble d'organismes publics. Ces interactions doivent être situées dans des sphères d'interaction. Ces sphères d'interaction devant fonctionner en conformité avec des normes garantissant les usages appropriés et licites de l'information de même que l'acheminement des informations nominatives uniquement vers les services publics concernés.

L'anonymat

Une première catégorie d'informations relève des situations où il n'est pas nécessaire de recueillir des informations qui identifient la personne. Ce n'est pas tant une catégorie qu'une conséquence de l'obligation de retenue dans la collecte d'informations. Si on ne collecte pas d'information nominative, il n'est plus nécessaire d'en assurer la protection. C'est autant de ressources gagnées pour assurer la protection qui convient aux données nominatives.

En dehors du monde virtuel, on n'est pas toujours placé dans la situation de devoir livrer toute une batterie d'informations sur soi-même pour accéder aux services. De la même façon, on ne collecte pas d'information à l'insu des personnes (sauf pour les fins de lutte contre la criminalité, etc.). La plupart des transactions de dimensions modestes ou payables au comptant peuvent se faire dans un relatif anonymat. Le principe de la retenue dans la collecte des renseignements personnels mène à reconnaître le droit d'agir sous l'anonymat pour toutes les interactions qui ne requièrent pas une identification.

Il importe en effet d'assurer, dans les environnements de prestation électroniques, une diversité d'options relatives à l'identification, qui soit comparable à celles qui existent dans le monde non virtuel. *A priori*, il n'y a pas de raison d'exiger un quantum d'informations plus considérable pour des transactions d'importance et d'enjeux similaires pour le seul motif que l'une est réalisée sur Internet et l'autre dans un établissement ayant pignon sur rue. Il s'agit donc d'appliquer le principe selon lequel seules les informations légitimement nécessaires au déroulement de la transaction doivent être exigées et utilisées.

Un tel principe se concilie mal avec une pratique qui prétendrait imposer un niveau identique d'exigences relatives à l'identification pour toutes les situations, même les plus banales. Il appelle plutôt la mise en place d'approches offrant un large spectre d'options en matière d'identification des personnes. Il s'oppose évidemment à ce que des informations identifiant une personne soient collectées à l'insu de l'intéressé.

Mais à l'inverse, il faut convenir que certaines transactions nécessitent l'identification plus complète de la personne. Comme dans le monde physique, il peut arriver que les services publics concernés requièrent le quantum d'informations qui est justifié par les risques qui y sont associés. S'imaginer qu'il en soit autrement relève de l'angélisme. En revanche, il faut poser le principe que les parties ne peuvent exiger que les informations dont on peut démontrer la nécessité, compte tenu de la finalité de l'échange.

Les informations à caractère public

Les informations à caractère public ont vocation à circuler. Elles sont régies par un régime de liberté de circulation. Des limites existent toutefois afin de prévenir et surtout de sanctionner un usage abusif de ces données à caractère public.

Il existe des informations qui relèvent de notre participation à la vie sociale. Dans les sociétés contemporaines, certaines informations sont l'affaire de tous : il est absurde de postuler que les caprices d'une personne l'emportent sur les impératifs de la protection de la santé publique ou les intérêts des autres membres de la famille. À l'égard de l'information qui concerne les autres, il est contraire aux principes démocratiques d'appliquer un régime de censure préalable. Le plus souvent, la censure de ces informations est revendiquée afin d'éviter que l'on fasse des usages préjudiciables de telles informations : on postule quelques hypothèses d'usage abusif, souvent à partir de cas isolés et on en déduit des justifications pour un régime général de censure. Il faut s'éloigner de cette tendance consistant à recourir à des techniques de censure de l'information sous le prétexte que cette information est susceptible d'être utilisée à mauvais escient. C'est une démarche dangereuse en matière d'information que de postuler un emploi abusif et de fonder le cadre juridique sur cette possibilité, souvent hypothétique, d'abus.

Il faut protéger uniquement ce qui relève vraiment de la vie privée, par opposition à un désir d'immuniser contre tous les inconvénients de la vie en société. Il faut s'y prendre en faisant un usage rationnel de l'ensemble des techniques de régulation disponibles dans les environnements de réseaux. Il faut réprimer les abus dont peuvent faire l'objet les informations publiques par des interventions après-coup plutôt que de censurer toutes les informations publiques sous le prétexte que certaines d'entre elles pourraient être utilisées de façon abusive.

S'il faut assurer plus que jamais la protection de la vie privée, il importe de le faire de manière à protéger ce qui est vraiment nécessaire à la préservation de la dignité des personnes. Il faut se garder de confondre le droit à la vie privée avec un droit d'être préservé de tous les inconforts pouvant résulter de la vie en société. Il faut poser d'entrée de jeu qu'il y a une limite à cette revendication souvent affirmée d'empêcher les autres de nous parler ou de parler de nous!

À l'égard des informations qui concernent une pluralité de personnes, telles que la plupart des informations personnelles, il faut préférer une approche en deux volets. Il faut premièrement assurer une protection renforcée pour tout ce qui concerne les informations relatives à l'intimité qui n'ont pas de rapport avec la santé du public ou ne concernent pas les tiers. Mais il faut en second lieu assurer un régime de libre circulation pour les données publiques, y compris celles qui concernent d'autres personnes pouvant avoir un intérêt légitime à y accéder. À l'égard des informations à caractère public, il faut garantir que les usages abusifs seront effectivement sanctionnés. Mais les sanctions ne doivent intervenir qu'une fois les abus constatés.

Les informations nominatives

Une autre catégorie de données personnelles est celle des informations nominatives, celles qui concernent une personne et permettent de l'identifier ou de connaître des éléments de sa vie privée. Ces données ne portent pas sur des aspects sensibles de la vie des personnes mais peuvent néanmoins révéler des détails relevant de la liberté des individus de mener leur vie personnelle.

Ces données devraient pouvoir librement circuler mais uniquement au sein de domaines de confiance spécifiés lors de la collecte et des échanges.

Ainsi, l'actuel article 53 de la Loi d'accès se lirait comme suit :

> ***53.*** *Les renseignements nominatifs ne peuvent être transmis qu'au sein d'un domaine de confiance précisé lors de la collecte.*
>
> *1° leur divulgation en dehors des domaines de confiance peut être autorisée par la personne qu'ils concernent; si cette personne est mineure, l'autorisation peut également être donnée par le titulaire de l'autorité parentale;*
>
> *2° Les renseignements nominatifs qui portent sur un renseignement obtenu dans l'exercice d'une fonction d'adjudication par un organisme public exerçant des fonctions quasi judiciaires ne sont pas confidentiels; ils demeurent cependant confidentiels si l'organisme les a obtenus alors qu'il siégeait à huis clos ou s'ils sont visés par une ordonnance de non-divulgation, de non-publication ou de non-diffusion.*

Après avoir fait l'objet d'une étude d'impact, les systèmes de gestion d'information faisant partie d'un domaine de confiance spécifique pourraient collecter et traiter les informations nominatives. Ces informations pourraient en principe être communiquées au sein du domaine de confiance déterminé. Elles pourraient être communiquées au sein d'un autre domaine de confiance moyennant le consentement de l'intéressé. Des normes détermineraient les précautions à mettre en place de façon à assurer la qualité des informations lorsque celles-ci sont utilisées.

Les données sensibles

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 sociosanitaire. 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.

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

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.

La sécurité : une condition nécessaire mais insuffisante

La sécurité n'égale pas automatiquement protection de la vie privée. Il est évident que la protection de la vie privée suppose que les informations et les systèmes soient dotés des caractéristiques assurant la sécurité physique et logique des informations. Mais la protection de la vie privée requiert des démarches allant largement au-delà de celles qui sont nécessaires afin de sécuriser un système d'information, un réseau ou un domaine de confiance.

L'obligation d'évaluer les risques et de spécifier les mesures pour leur prise en charge

On peut certes convenir que l'emploi des technologies de l'information modifie l'échelle des risques associés à la circulation des informations. Ce phénomène requiert une démarche d'évaluation des risques, non de prendre pour acquis le pire des scénarios afin de déterminer le niveau de protection que la loi devrait exiger.

Ceux qui mettent en place des environnements technologiques devraient avoir l'obligation de démontrer que ceux-ci fonctionnent dans le respect de la vie privée, entendue comme protégeant la dignité. En particulier, il n'y a pas de raisons pour qu'il incombe aux personnes de prendre les moyens et faire les démarches pour assurer le respect de leur vie privée : le devoir de protéger la vie privée des personnes est plus facile à assumer au niveau de la mise en œuvre et du déploiement des environnements. Cela est particulièrement vrai dans les environnements voués au service public.

Mais cela nécessite la mise en place d'un processus cohérent d'évaluation préalable des systèmes. Une telle évaluation ne devrait pas se fonder sur des scénarios catastrophes mais devrait plutôt avoir pour finalité de vérifier si les choix ont été effectués de manière à respecter les principes énoncés dans la loi. Par la suite, lorsque sont signalées des situations attentatoires à la vie privée, le pouvoir d'enquête de la Commission d'accès devrait viser à documenter les incidents afin d'éviter qu'ils se reproduisent.

C) La répression *a posteriori* des abus

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.

D) Des mécanismes effectifs de sanction des droits

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. Le principe est ainsi décrit par Yves Poullet :

> […] *dans la même mesure où Internet facilite, pour les fournisseurs de services de communications électroniques, la collecte et le traitement des données, ceux-ci doivent permettre à l'utilisateur de profiter du même médium pour l'exercice plus aisé de leurs droits.*[55]

Il s'agit d'utiliser les environnements électroniques pour assurer l'efficacité de l'exercice des droits des personnes. Yves Poullet explicite ainsi comment ce concept pourrait contribuer à assurer une application plus efficace du droit à la vie privée :

> […] *le droit d'une personne concernée peut s'exercer plus aisément par un simple clic sur un sigle permettant l'accès direct à un 'privacy statement'* […] *La personne concernée peut être amenée à exercer son droit au consentement ou son droit d'opposition directement en ligne. En ce qui concerne le droit d'accès proprement dit, c'est-à-dire le droit de connaître les données enregistrées, leur origine, la logique du traitement, etc.* […] *on peut même imaginer qu'il s'exerce en ligne par une demande signée électroniquement. Enfin, le droit de recourir en cas de contestation relative à la pertinence ou la qualité d'une donnée* […] *pourquoi ne pas permettre son exercice, voire sa résolution, par des mécanismes électroniques de saisine et de règlements des conflits.*[56]

La généralisation des activités dans les réseaux doit s'accompagner de la mise en place d'outils appropriés, préférablement située 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.

---

[55] Yves POULLET « Internet et vie privée : entre risques et espoirs », (2001) 120 *Journal des tribunaux* 155.

[56] Yves POULLET « Internet et vie privée : entre risques et espoirs », (2001) 120 *Journal des tribunaux* 155.

Conclusion

Lucas, Devèze et Frayssinet rappelent que :

> *C'est entre le discours parfois paranoïaque qui voit Big Brother partout et celui lénifiant ou intéressé qui refuse de voir les réalités et les potentialités de la technique en face, que doit se situer l'analyse raisonnée des dangers pour les droits et libertés des personnes engendrée par les nouvelles technologies de l'information et de la communication.*[57]

Il a été ici question du défi d'assurer l'ajustement du cadre normatif de la protection de la vie privée afin de le rendre efficace dans les environnements de réseaux.

Il faut 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 se consacrant aux services publics. Elles appellent la mise en place d'un cadre efficace pour assurer la protection des droits des citoyens. Ce n'est pas en laissant persister un cadre juridique agissant comme un blocage des changements qui doivent accompagner l'avènement de l'État en réseau qu'on assure la protection effective de la vie privée. Il faut, au contraire, recentrer le cadre juridique de l'information sur les personnes de manière à protéger effectivement la vie privée dans les contextes diversifiés des réseaux.

Les conceptions fondées sur la suprématie de la vie privée sans égard à la nécessité d'articuler ce droit avec les impératifs de l'exercice des autres droits, constituent des approches dangereuses pour le développement d'un droit des environnements de réseaux qui soit vraiment cohérent avec les principes démocratiques. Ces conceptions rendent plus difficile la réflexion sur les moyens pour assurer la protection effective de la vie privée. Avec ce genre de conceptions dès que l'on pointe du doigt l'inadéquation des techniques juridiques visant à assurer la protection de la vie privée, on est soupçonné d'hostilité à l'égard de la vie privée elle-même. Pourtant, il est nécessaire d'examiner sereinement les techniques permettant d'assurer une protection équilibrée de la vie privée des personnes vivant en société et des autres valeurs qui contribuent, elles aussi, à assurer la dignité humaine.

Nous avons vu qu'il faut concevoir le cadre de la protection de la vie privée dans les réseaux en distinguant entre elles les diverses informations susceptibles de circuler. Il faut 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

---

[57] André LUCAS, Jean DEVÈZE et Jean FRAYSINNET, *Droit de l'informatique et de l'Internet*, Paris PUF coll. Thémis n^{o} 7.

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 publics.

Dans un grand nombre de situations, il faudra assurer à la fois la protection des informations portant sur les personnes de même que leur circulation afin de rendre les services auxquels le citoyen est en droit de s'attendre. Pour permettre cette adaptation, il faut confiner les renseignements nominatifs, non plus dans les organismes publics définis étroitement mais plutôt dans des domaines de confiance dotés d'un statut garantissant que les informations seront de qualité et qu'elles ne seront utilisées qu'aux fins compatibles.

Enfin, il faut renforcer le statut des informations sensibles, celles qui portent directement sur la vie privée des personnes. Il faut que ces informations ne circulent que dans des domaines de confiance spécifiques et moyennant des encadrements stricts.

La modernisation effective du droit de la protection des renseignements personnels passe par une relecture critique des applications qui en a été faite et une évaluation lucide des contextes dans lesquels circulent les informations. Ce serait affaiblir ce droit que de se réfugier dans une frileuse défense des façons de faire héritées des époques antérieures puisque cela accroît les risques d'une protection purement formelle, passant à côté des véritables périls.

La généralisation des environnements de réseaux ne laisse guère le choix : il devient de plus en plus urgent d'ajuster un régime de protection de la vie des personnes qui reflète toute la complexité du cyberespace. La démarche doit être menée en reconnaissant le fait que l'information sur les personnes n'a jamais été et ne peut être détachée de l'environnement global dans lequel évoluent les personnes. C'est de cette façon qu'il faut envisager la modernisation du régime de protection de la vie privée pour l'État en réseaux.