CAHIERS DU CENTRE DE RECHERCHES
INFORMATIQUE ET DROIT

DÉFIS DU DROIT À LA PROTECTION DE LA VIE PRIVÉE

CHALLENGES OF PRIVACY AND DATA PROTECTION LAW

Ont contribué à cet ouvrage

Rosa BARCELO
Jon BING
Herbert BURKERT
Cédric BURTON
Cécile DE TERWANGNE
Franck DUMORTIER
Robert GELLMAN
Daphne GILBERT
Steve GILSON
Serge GUTWIRTH
Jean A. M. HERVEG
Peter HUSTINX
Ian R. KERR
Nancy J. KING
Sophie LOUVEAUX
Carter MANNY
Raymond T. NIMMER
Pablo PALAZZI
Maria VERÓNICA PÉREZ ASINARI
Yves POULLET
Oscar Raúl PUCCINELLI
Karen ROSIER
Robert ELLIS SMITH
Daniel J. SOLOVE
Pierre TRUDEL
Jean-Marc VAN GYSEGHEM
Jane K. WINN

sous la coordination de Marie VERÓNICA et Pablo PALAZZI

EXTRAIT

Cahiers du Centre de Recherches Informatique et Droit

HYPOTHÈSES SUR L'ÉVOLUTION DES CONCEPTS DU DROIT DE LA PROTECTION DES DONNÉES PERSONNELLES DANS L'ÉTAT EN RÉSEAU

Pierre TRUDEL

Titulaire de la Chaire L.RM. 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 (*)

Sommaire : I. Introduction. II. La gouvernance. III. L'actualisation des mécanismes de protection des données personnelles. III.1. De nouvelles circulations de l'information. III.1.1. La personnalisation. III.1.2. La circulation en réseau et le partage des informations. III.2. Une normativité en réseau. IV. Les impératifs de protection de la vie privée dans les réseaux du e-gouvernement. IV.1. Une lecture actualisée des principes de protection des renseignements personnels. IV.2. L'impératif de confiance. V. À la recherche de concepts pour assurer l'effectivité du droit de la protection des renseignements personnels dans les réseaux du e-gouvernement. V.1. L'aire de partage : définition. V.2. Le processus de création des aires de partage. V.3. L'encadrement juridique. V.4. Les responsabilités. VI. Conclusion.

Résumé : L'administration électronique suppose la circulation accrue d'informations sur les personnes. Le déroulement en réseau de plusieurs des activités inhérentes aux fonctions de l'État favorise une organisation centrée sur le citoyen ou l'usager. Il facilite le travail coopératif entre une pluralité d'acteurs de statut différent. Il accentue les tendances à se démarquer du modèle hiérarchique. Il permet la spécialisation flexible se fondant sur l'échange entre des pôles agissants de connaissance.

Ces évolutions associées au e-gouvernement requièrent une redéfinition de l'espace dans lequel circulent les renseignements personnels. Il faut 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 assure le bon fonctionnement des services publics. Il faut, à cette fin, identifier les jalons et repères appropriés afin

* Courriel : pierre.trudel@umontreal.ca.

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.

Les éléments d'un cadre actualisé capable d'assurer effectivement la protection des renseignements personnels dans les espaces de réseaux consacrés aux services publics sont présentés. Un grand nombre de modèles de prestations électroniques de services supposent que les renseignements personnels sont conservés de manière à être disponibles dans un environnement d'information accessible à d'autres organismes gouvernementaux. On présente les principaux éléments du concept d'aire de partage d'informations personnelles de même que ses principes de mise en place et de fonctionnement.

Lorsque les renseignements sont dans des environnements d'information auxquels ont accès une pluralité d'organismes gouvernementaux, la protection des renseignements personnels ne résulte plus des limitations intervenant au stade de la collecte ou prohibant la circulation. Une protection effective nécessite un encadrement strict des conditions auxquelles les ministères et autres autorités publiques ou privées accèdent aux renseignements et les utilisent. Le concept d'aire de partage offre une assise à une régulation de protection de la vie privée fondée sur ces paradigmes.

I. INTRODUCTION

Avec l'avènement des réseaux caractéristiques du e-gouvernement, le contexte de la circulation des informations portant sur les personnes connaît des changements significatifs. 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 dépassé par les évolutions qui ne manqueront pas de métamorphoser les conditions de la gestion de l'information.

Kenneth Kernaghan et Justin Gunraj soutiennent que l'adoption croissante par les administrations gouvernementales des technologies de l'information prédispose les organismes publics à changer leurs structures et leurs modes de gestion (1). Un premier facteur de changement induit par les technologies de l'information est la pression engendrée par les lourds investissements et le mouvement conséquent pour une coopération plus intensive entre les organismes gouvernementaux. Un second facteur tient au besoin accru pour de l'expertise de même que des capacités accrues de partager l'information. Cela porte à la création d'entités non ministérielles. Au

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

Canada, on a créé des « agences » qui se présentent comme des structures qui posséderaient des caractéristiques plus adaptées à l'accomplissement de fonctions horizontales. Un troisième facteur de changement serait le déplacement d'une partie du niveau intermédiaire de gestion au profit d'une certaine horizontalisation de la hiérarchie administrative, de l'autorité et des contrôles.

Les systèmes d'information utilisés pour assurer les services publics en ligne se conçoivent désormais comme des réseaux, c'est-à-dire des environnements interconnectés et organisés dans lesquels l'information circule d'un pôle à l'autre, de façon multidirectionnelle et non-hiérarchique (2).

La migration dans les environnements en réseaux de plusieurs activités et services publics requiert de revoir les notions juridiques 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. Les environnements actuels sont des réseaux caractérisés par les interconnections et non les mythiques méga-banques de données que l'on anticipait il y a trois décennies. Mais si on ne prend pas garde de revoir les paradigmes fondant la protection des données personnelles, le maintien des approches actuelles pourrait engendrer la constitution de méga-banques de données.

La virtualisation des échanges se traduit par un phénomène d'interpénétration des environnements. Du fait de la numérisation, des environnements de communication jadis considérés distincts les uns des autres sont désormais rendus techniquement équivalents. La question du cadre juridique appliqué aux espaces d'interactions résultant de cette virtualisation devient un enjeu central. Il faut 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 interactions État-citoyen. Cela 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 insensibles aux frontières ou

(2) Voir : Pierre TRUDEL, *Améliorer la protection de la vie privée dans l'administration électronique : pistes afin d'ajuster le droit aux réalités de l'État en réseau*, réalisé pour le Ministère des relations avec les citoyens et de l'immigration, Montréal, mars 2003, en ligne à<http://www.mrci.gouv.qc.ca/publications/pdf/ViePrivee_AdministrationElectronique_Pierre_Trudel.pdf>.

organigrammes 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 différente de celui constitué par des organismes et ministères indépendants et cloisonnés les uns par rapport autres. La régulation doit s'inscrire au niveau du réseau. Les événements se déroulant dans les espaces réseaux doivent être régis par un cadre juridique assurant la protection et la qualité des informations. Ce type de mutations coïncide avec un redéploiement du rôle et de la configuration de l'État lui-même et entraîne des changements complexes dont la notion de gouvernance cherche à rendre compte.

II. LA GOUVERNANCE

Les processus associés à la gouvernance peuvent se dérouler dans cet espace qui paraît résulter des interconnexions entre des outils informatiques. Ce que l'on désigne par l'expression cyberespace (3). Les réseaux découlent d'interactions entre personnes poursuivant un but commun. Le phénomène de réseautage suppose l'émergence d'environnements interconnectés unissant les décideurs, les chercheurs, les régulateurs de même que les autres acteurs jouant un rôle dans la gouvernance des espaces au sein desquels se déroulent les activités de gouvernance (4).

La gouvernance est devenue, depuis la décennie 1990, le « mot fétiche censé condenser et résumer à lui seul l'ensemble des transformations qui affectent l'exercice du pouvoir dans les sociétés contemporaines [...] » (5). La notion correspond à la manière d'orienter, de guider, de coordonner les activités d'un pays, d'une région, d'un groupe social ou d'une organisation privée ou publique. Le mot est ancien mais il connaît un regain de popularité depuis une

(3) L'on convient généralement que le mot « cyberspace » (cyberespace en français) a été introduit dans le langage par l'auteur William GIBSON dans son roman *Neuromancien*. Pour Gibson, le « cyberespace », appelé aussi « infosphère », est l'espace virtuel des ordinateurs reliés en réseaux qu'explorent les « cybernautes » dont les systèmes nerveux sont directement branchés sur ceux-ci grâce à une prise fixée sur leur crâne. L'expression est désormais utilisée dans un sens moins péjoratif pour désigner l'espace qui paraît résulter des raccordements entre une multitude d'ordinateurs et autres outils informatiques. Voir Jean-Claude GUÉDON, *Internet le monde en réseau*, Paris, Découvertes, Gallimard, 2000.

(4) Manuel CASTELLS, *La société en réseaux. L'ère de l'information*, Paris, Fayard, 1998. François OST et Michel DE KERCHOVE, *De la pyramide au réseau : pour une théorie dialectique du droit*, Bruxelles, Publications des facultés universitaires Saint-Louis, 2002.

(5) Jacques CHEVALLIER, « La gouvernance, un nouveau paradigme étatique ? », (2003) 105/106 *Revue française d'administration publique*, 203-217, 203.

décennie. Il désigne « un mode de gouvernement organisé sur la base d'une coopération, d'un partenariat ou d'un contrat, entre une pluralité d'acteurs aussi bien publics que privés » (6). La gouvernance renvoie à une idée de réunion, de collaboration de l'ensemble des acteurs de la société quel que soit le niveau. Ainsi, elle se conçoit, selon Thomas B. Riley, comme étant le « résultat de l'interaction du gouvernement, de la fonction publique et des citoyens dans l'ensemble du processus politique ». Selon Andrée Lajoie, s'appuyant sur une étude faite pour la Commission du droit du Canada par Tim Plumptre (7), le concept de gouvernance « concerne tout ce qui a trait aux institutions, aux processus et aux traditions qui interviennent dans les débats d'intérêt public » (8) ce qui inclut le gouvernement et le secteur public, mais aussi la société civile, le secteur privé, les citoyens, les médias, etc. C'est comme s'il importait plus que jamais de reconnaître que le pilotage de la société passe non seulement par les structures de l'État mais par un ensemble beaucoup plus large de lieux de délibération et de pouvoir.

Pour apprécier l'importance du concept dans le contexte du e-gouvernement, il suffit de référer à la nécessité d'associer tous les partenaires pour assurer le développement harmonieux d'un territoire donné (9). S'agissant du e-gouvernement, un ensemble de systèmes de normes se discutent et s'appliquent dans les espaces d'interactions relatifs à la décision et à l'administration publique. Aux réglementations étatiques et professionnelles s'ajoutent des processus ayant vocation à procurer les encadrements pour des activités qui ne peuvent être entièrement régies par les droits territoriaux. La technique et les contraintes qu'elle induit sont aussi source de normativité dans les réseaux. Les normativités juridiques concourent avec les normativités administratives, technologiques et politiques à encadrer les interactions et les échanges d'information au sein de l'appareil gouvernemental. La protection des données personnelles doit être pensée en tenant compte de ces phénomènes qui paraissent inhérents à l'État en réseau.

(6) « Les mots de la gouvernance », *Sciences Humaines Hors série*, n° 44 mars-avril-mai 2004, p. 6; Catherine BARON, « La gouvernance : débats autour d'un concept polysémique », (2003) 54, *Droit et Société*, 329-351.

(7) Tim PLUMPTRE, *Vers un plan de recherche sur la gouvernance*, Commission de réforme du droit du Canada, Ottawa, 1998.

(8) Andrée LAJOIE, *Gouvernance et société civile, Intervention devant la Société royale du Canada*, 20 novembre 1999, tapuscrit, 17 pages.

(9) Jean-Yves PRAX, *Le management territorial à l'ère des réseaux*, Paris, Éditions d'organisation, 2002.

Plus globalement encore, il faut constater que la société de l'information fait éclater et rend de plus en plus obsolètes les fonctionnements cloisonnés, qu'ils soient le fait de l'État lui-même ou de la société civile. Steven Rossel écrit à cet égard que :

> *À mesure que la société devient plus interconnectée, complexe et turbulente, les façons plus traditionnelles de l'organiser et de la gouverner deviennent dépassées. Dans un environnement plus scolarisé, interconnecté et riche en informations, les systèmes gouvernementaux qui reposent sur un flux limité d'informations, y compris la bureaucratie et la démocratie représentative, perdent leur crédibilité et leur autorité* (10).

L'exercice des fonctions gouvernementales passe de plus en plus par une capacité de dialogue avec l'ensemble des participants concernés. Il faut aussi anticiper les conséquences, au plan du droit, des possibilités sans précédent de produire et d'échanger des informations. Le paradigme du « flux limité et contrôlé » d'information fait place au paradigme de la disponibilité illimitée d'information.

Dans l'univers cyberspatial, la gouvernance correspond à la « manière de diriger et d'administrer propre à un gouvernement en ligne, permettant à celui-ci, grâce à l'utilisation d'Internet et des NTIC, d'améliorer les services publics, de développer la responsabilisation et la transparence dans les relations entre les citoyens et l'Administration, tout en favorisant le développement d'une société de l'information et le processus de démocratisation qui l'accompagne » (11).

Cette notion possède, selon Pierre Lévy, « trois caractéristiques essentielles, qu'il importe de bien saisir si l'on veut en tirer toutes les conclusions concernant les nouvelles formes de gouvernance : l'inclusion, la transparence et l'universalité » (12) :

- **inclusif** : le cyberespace « permet l'expression publique à tous les individus, groupes, institutions et communautés, y compris à des communautés (les communautés virtuelles) qui ne lui préexistaient pas » (13) ;
- **transparence** : le cyberespace autorise « un degré d'accessibilité à l'information supérieur à tout ce qui avait pu être expérimenté auparavant. [...] Cette nouvelle accessibilité de l'information [...] fait perdre une bonne part de leurs privilèges aux élites classiques du pouvoir politique » (14) ;
- **universalité** : le cyberespace « en même temps que d'autres facteurs techniques, économiques ou écologiques, [...] contribue donc à relativiser les frontières des États-nations et même des ensembles géopolitiques [...] » (15).

(10) Steven A. ROSSEL (dir.), *Gouverner dans une société de l'information*, Institut de recherche en politique publique, 1996, p. 93.

(11) OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE, *Grand dictionnaire terminologique*, http://www.granddictionnaire.com/btml/fra/r_motclef/index800_1.asp .

(12) Pierre LÉVY, « Vers la cyberdémocratie », http://www.intervir.org/nl/levy/12.htm

(13) P. LÉVY, *id.*

Au plan du droit, les tendances lourdes induites par ces facteurs accentuent l'importance des droits fondamentaux relatifs à la participation aux espaces publics. Le phénomène suppose l'émergence de stratégies régulatrices qui sont conçues de façon différente de celle qui ont marqué l'État bureaucratique fondé sur l'information portée par le support-papier.

Dans une organisation étatique ainsi constituée en réseaux, l'enjeu auquel le droit vient répondre est celui de la régulation des droits et devoirs relatifs aux épisodes du cycle de vie de l'information. Alors que dans l'univers bureaucratique dominé par le papier, le droit insiste sur la délimitation des droits d'obtenir ou non telle ou telle information, dans l'univers en réseau, le droit tend vers l'organisation d'une régulation des permissions d'accès et d'usage dévolues aux décideurs et aux citoyens.

III. L'ACTUALISATION DES MÉCANISMES DE PROTECTION DES DONNÉES PERSONNELLES

Les mécanismes de protection de la vie privée doivent être actualisés pour refléter les situations qui ont désormais cours dans les États en réseau. 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 permet la spécialisation flexible se fondant sur l'échange entre des pôles agissants de connaissance.

Dans la plupart des pays, le cadre juridique actuel postule le caractère exceptionnel des transferts de renseignements personnels sans le consentement des personnes visées. Mais, en dépit de ce caractère exceptionnel, force est de constater que les transferts de renseignements personnels sont considérables entre certains

(14) P. LÉVY, *id*

(15) P. LÉVY, *id.*

organismes publics. De plus, le cadre juridique actuel autorise le partage de renseignements mais généralement de façon à augmenter la duplication de données d'un organisme vers l'autre. À la fin de l'exercice, on se retrouve avec une banque de données augmentée des renseignements obtenus de l'autre. Il y a donc duplication, redondance et, compte tenu de la persistance de l'information, toujours de plus en plus de renseignements personnels détenus par les Administrations.

Dans le contexte des réseaux, contrairement à ce que postulent les cadres juridiques actuels, la protection des données personnelles suppose de prévenir la redondance et agir sur l'accès aux renseignements où qu'ils se trouvent au sein des réseaux de l'appareil gouvernemental. Il faut mettre en place un mécanisme juridique évitant la duplication des renseignements personnels. Dans le contexte où les services de l'État fonctionnent en réseau la loi devrait autoriser l'accès conditionnel et balisé aux données détenues en quelque point du réseau à la condition que cet accès soit autorisé par la loi et que cela n'emporte pas de copie persistante de l'information.

III.1. De nouvelles circulations de l'information

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. L'administration électronique suppose de tirer avantage des capacités accrues de traiter des informations, de les 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.

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 en ligne. 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.

Un double phénomène de personnalisation et de mise en commun de l'information caractérise plusieurs tendances accompagnant l'émergence de l'administration électronique. 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.

III.1.1. La personnalisation

Le cyberespace permet de nouvelles modalités de personnalisation des services proposés aux citoyens mais aussi une capacité de démultiplication des personnalités. Investi d'une 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 (16).

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 possèdent 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.

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. 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. Par exemple, le citoyen qui change d'adresse pourra 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.

Pour proposer des services personnalisés fondés sur les situations de vie des citoyens, il faut être en mesure d'accéder en temps réel à des renseignements personnels habituellement détenus par une pluralité d'entités distinctes au sein de l'Administration. Le maintien d'un régime juridique prohibant la circulation des renseignements

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

personnels rend problématique la mise en place de services intégrés suivant des catégories qui ne coïncident pas avec les frontières bureaucratiques.

III.1.2. La circulation en réseau et le partage des informations

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.

La gestion collaborative induit des possibilités de partager l'information. La généralisation 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. Pour l'information qui est nécessairement en possession de l'Administration, le cadre juridique devrait s'attacher à en régir les conditions d'accès par chaque agent de l'État plutôt que d'en interdire la circulation. Dans un 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 a le droit d'y accéder et d'en faire usage pour prendre une décision dans une situation spécifique.

Les interactions dans le contexte des réseaux informatiques requièrent des modalités différentes 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. Cela appelle une attitude réaliste tenant compte aussi bien des avantages de la circulation des informations que de ses inconvénients. À cet égard, une protection renforcée au niveau des accès par les Administrations procure une protection de beaucoup supérieure à celle résultant des régimes actuels.

III.2. UNE NORMATIVITÉ EN RÉSEAU

Dans le cyberespace (17), la normativité elle-même s'élabore de plus en plus dans les réseaux. Le phénomène de décentralisation est caractéristique de l'État en réseau : pour le citoyen, l'État se présente de plus en plus comme un réseau maillé dans lequel les frontières administratives ont de moins en moins de pertinence. Ce phénomène favorise un accroissement des responsabilités régulatrices des acteurs en première ligne et accroît la nécessité de développer des outils afin d'assurer le développement d'outils régulateurs appropriés au niveau local et à celui des micros milieux virtuels.

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

Un ensemble de systèmes de normes s'appliquent dans le cyberespace. On peut retenir une représentation du cyberespace faisant de celui-ci un ensemble interconnecté constitué de pôles interagissants de normativités. Il est constitué d'espaces dans lesquels prévalent en tout ou en partie des normes qui s'imposent aux usagers. Les normes peuvent s'imposer soit en raison de leur capacité à définir, même implicitement, les conditions de l'exercice des activités soit parce qu'un État est en mesure d'exercer une autorité comme c'est habituellement le cas dans les environnements de e-gouvernement.

Le cyberespace est aussi constitué de relais par lesquels s'explicitent et se diffusent les normativités et les conséquences de celles-ci. Les règles émanant des pôles de normativité se relayent et se diffusent dans les différents espaces virtuels. Elles coexistent dans le cyberespace soit en complémentarité avec d'autres règles soit en concurrence, se proposant à la place de celles qui sont issues d'autres pôles normatifs.

(17) Pierre TRUDEL, « Quel droit et quelle régulation dans le cyberespace ? », *Sociologie et sociétés*, vol. 32, n° 2, automne 2000, 189-209, http://www.erudit.org/erudit/socsoc/v32n02/trudel/trudel.pdf; Pierre TRUDEL, « Un 'droit en réseau' pour le réseau : le contrôle des communications et la responsabilité sur Internet », dans INSTITUT CANADIEN D'ÉTUDES JURIDIQUES SUPÉRIEURES, *Droits de la personne : Éthique et mondialisation*, Cowansville, Éditions Yvon Blais, 2004, pp. 221-262.

Dans le cyberespace, on relève l'importance des pôles de normativité que constituent les règles découlant de la technique de même que les diverses normativités pratiquées, à titre d'usage ou autrement- sur Internet. Mais il existe aussi des relais de normativité qui sont les outils, guides et autres instruments assurant l'application effective des principes du droit...

Par exemple, les règles relatives aux droits d'accès aux informations par les administrateurs de systèmes constituent des mécanismes de mise en œuvre des principes énoncés dans les lois et les textes internationaux.

L'un des relais majeurs entre les pôles étatiques de normativité et les acteurs du cyberespace est fourni par les régimes de responsabilité. Pour les acteurs, la responsabilité fournit le cadre délimitant leurs actions et prescrivant l'étendue de leurs obligations. C'est en somme afin de gérer leurs risques et limiter la mise en cause possible de leur responsabilité que les acteurs, tant collectifs qu'individuels, se donnent des règles de conduite. Ainsi se relaient les exigences énoncées dans les pôles de normativité. Au niveau de chaque environnement, les principes énoncés dans les pôles de normativité comme les lois et principes internationaux sont relayés en micro-régulation ou en auto réglementation.

En responsabilisant chacun des ministères, organismes publics ou fonctionnaires susceptibles de prendre connaissance d'informations personnelles, on incite ces derniers à mettre en place les mesures nécessaires afin d'anticiper les risques, les prévenir et éventuellement les réduire. Pour gérer leurs risques et baliser leur responsabilité, ils pourront instaurer des mesures de contrôle au jour le jour afin de contrôler strictement les accès au quotidien aux renseignements personnels. Cette normativité en réseau, si elle est correctement appliquée devrait au final garantir une responsabilisation et une protection mieux ciblée des acteurs ayant à traiter les renseignements personnels.

IV. LES IMPÉRATIFS DE PROTECTION DE LA VIE PRIVÉE DANS LES RÉSEAUX DU E-GOUVERNEMENT

L'administration électronique suppose de tirer avantage des capacités accrues de traiter des informations, de les 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 les balises énoncées notamment

dans les principes formulés par l'OCDE. Ces principes reflètent les consensus internationaux à cet égard.

Le cadre actuel de la protection de la vie privée et des renseignements personnels insiste sur le respect d'une série de procédures formelles. Il y a peu de place laissée à l'appréciation des enjeux et du contexte. Plutôt que d'inciter à la mise en place de mécanismes de protection fondés sur le postulat que l'information circule dans des réseaux, on tend à insister sur le respect de l'étanchéité entre les organisations.

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.

Un grand nombre de modèles de prestations électroniques de services supposent que les renseignements personnels sont conservés de manière à être disponibles dans un environnement d'information accessible à d'autres composantes de l'Administration. Il faut donc anticiper ce partage et l'encadrer de manière à ce que les renseignements ne puissent servir qu'à des fins compatibles avec les exigences des ensembles de services et de prestations. Il importe également d'informer les citoyens de ce qu'il advient des renseignements qu'ils confient à l'État.

En vertu des règles actuelles, les renseignements personnels sont détenus par le ministère qui les a recueillis. Ce dernier ne peut collecter ces renseignements sans démontrer que cela est nécessaire, compte tenu des mandats et services qui sont concernés. Mais une fois qu'un ministère a obtenu et détient des renseignements personnels, il existe en pratique peu de garanties que ceux-ci ne seront pas utilisés à l'insu du citoyen ou même utilisés à des fins qui n'étaient pas prévues lors de la collecte. L'organisme public a la possession exclusive des renseignements qu'il a recueillis. Ces derniers sont sous son contrôle bien qu'en certaines circonstances les informations peuvent se trouver physiquement en dehors des lieux contrôlés par l'organisme détenteur. Des dispositions permettent le partage des renseignements personnels, mais ce partage a un caractère exceptionnel.

Il est donc nécessaire de formuler un cadre juridique reposant sur un concept qui garantit la protection des renseignements personnels lorsque ceux-ci sont déposés dans un environnement d'information accessible à une pluralité de ministères ou autres organismes publics,

afin de leur permettre d'assurer seuls ou en partenariat un ensemble de services aux citoyens. Il importe d'identifier les ajustements conceptuels qui sont nécessaires afin de garantir une protection vraiment effective de la vie privée. Pour cela, une lecture actualisée des principes fondamentaux de la protection des renseignements personnels s'avère nécessaire.

IV.1. UNE LECTURE ACTUALISÉE DES PRINCIPES DE PROTECTION DES RENSEIGNEMENTS PERSONNELS

Le développement de services en réseaux nécessite une réactualisation des principes encadrant le traitement des renseignements personnels.

Les principes énoncés par l'OCDE (18) sont les suivants :

- limitation en matière de collecte ;
- spécification des finalités ;
- transparence ;
- participation individuelle ;
- responsabilité ;
- limitation de l'utilisation ;
- qualité des données ;
- garanties de sécurité.

Il importe de déterminer comment, dans les environnements en réseau caractérisés par le partage accru de l'information, ces principes doivent être compris et appliqués afin d'assurer une réelle protection de la vie privée.

La limitation en matière de collecte suppose de mettre en place des processus décisionnels qui feront usage du minimum d'informations personnelles nécessaires afin d'assurer les prestations ou la prise de décision dans un environnement en réseau. Concrètement, les cadres décisionnels doivent imposer l'obligation de justifier le pourquoi de la collecte de chaque catégorie de renseignement personnel.

Dans un environnement en réseau, la **nécessité de la collecte** doit s'envisager au regard de l'ensemble des familles de prestations qui sont concernées par les informations. Une fois l'information collectée, la nécessité de sa conservation s'apprécie en référence à un ensemble de

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

processus de décision susceptibles d'être réalisés en ayant recours à une donnée personnelle. Par conséquent, le principe de retenue en matière de collecte et le principe de spécification des finalités se recoupent. Le principe relatif à la spécification des finalités est aussi renforcé : en spécifiant le plus strictement possible les finalités, on se trouvera en situation où la collecte est limitée aux informations effectivement indispensables aux fins poursuivies au plan de l'ensemble des prestations et services concernés.

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

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

> *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* (19).

Dans le contexte d'un environnement en réseau, la question des finalités se pose en tenant compte que les informations peuvent être là disponibles, déjà recueillies : ce n'est plus au regard de la détention que s'applique l'exigence du respect de la finalité mais plutôt au

(19) OCDE, *Lignes directrices régissant la protection de la vie privée et des flux transfrontières de données de caractère personnel*, Paris, OCDE, 2002, < http://www.oecd.publications.gfinb.com/cgi-bin/ OECDBook Shop.storefront/EN/product/932002012P1 >.

regard de l'accès et de l'utilisation du renseignement. Dans un réseau, le principe du contrôle au niveau du droit d'accès vient assurer le respect des finalités. Au sein d'un organisme gouvernemental, l'accès à un renseignement n'est licite que pour une finalité autorisée et lorsqu'on accomplit une activité s'inscrivant dans le cadre de la finalité. Les finalités doivent être envisagées dans le cadre de l'ensemble des services qui ont vocation à être proposés à l'usager.

Le respect de la **finalité** suppose que l'usager ait effectivement connaissance des familles de finalités auxquelles serviront les informations. La notion de finalité doit désormais être axée sur l'usager, non sur les structures gouvernementales. Par exemple, l'usager qui entre en relation avec les ministères chargés de l'application des lois sur la sécurité du revenu doit savoir que les informations qu'il fournit circuleront et seront utilisées aux fins d'assurer l'application des lois relatives à la sécurité du revenu et ce, peu importe que l'une relève d'un ministère et l'autre d'un organisme public tiers.

Il faut que l'information sur les **finalités** des informations détenues soit constamment disponible. Cette information doit être rappelée lors de chaque collecte. Pour respecter le principe de la limitation de l'utilisation, les environnements d'information devraient desservir des familles délimitées de prestations : ce qui assure que les renseignements personnels ne seront utilisés qu'à des fins apparentées et compatibles avec celles de la collecte initiale.

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

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

À cet égard, le principe de la **participation individuelle** de la personne concernée dans les décisions relatives au traitement des renseignements personnels acquiert dans les réseaux une portée renouvelée. Dans les réseaux, il est possible de présenter l'information que l'on possède et de la valider en temps réel avec la personne concernée. La garantie de la **qualité** des données sera du même coup renforcée par la validation que l'organisme effectue de l'information lors d'une prestation spécifique. Il est désormais possible de garantir que l'information utilisée possède réellement les qualités requises pour servir à la décision ou à la prestation visée.

La qualité des données s'apprécie à l'égard des prestations et décisions à être accomplies avec les renseignements : il faut garantir que les renseignements utilisés pour rendre le service ou effectuer la prestation sont exacts, précis, autorisés par les lois et ne présentent pas d'équivoque. La légitimité de pareilles circulations d'informations personnelles serait 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. Le droit de rectification prend ainsi tout son sens.

Le cadre juridique applicable dans les réseaux devrait donc faire obligation à l'organisme de s'assurer de l'exactitude des informations. Lors de toute utilisation de renseignements personnels, les organismes publics doivent valider auprès de l'intéressé les informations auxquelles ils ont eu accès. Lorsque cela est nécessaire pour assurer la qualité des données, les informations doivent être rendues disponibles afin que les personnes concernées puissent en vérifier la teneur et, le cas échéant, exercer leur droit de rectification.

S'agissant de la **responsabilité**, chaque organisme public susceptible d'accéder à des données personnelles au sein d'un réseau peut être considéré comme en étant le détenteur juridique. Lorsque les renseignements sont détenus par une pluralité d'organismes, chaque partenaire est considéré comme détenteur juridique des documents et des renseignements personnels consignés dans l'une ou l'autre des banques de données auxquelles il a accès.

À ce titre, chaque organisme est responsable de la confidentialité des renseignements et l'ensemble des organismes en répondent solidairement. Comme il y a pluralité d'organismes, ces derniers auront à déterminer comment se répartiront les responsabilités de l'un et l'autre des participants.

Des règles devraient encadrer l'action des gestionnaires. Il importe en effet de préciser les obligations et délimiter la responsabilité des gestionnaires quant aux exigences de confidentialité et de sécurité. Il est en effet nécessaire que soient précisées les normes à la lumière desquelles seront évalués le comportement et la responsabilité des citoyens. Il en est aussi de même des rapports devant s'établir entre le citoyen-utilisateur et le gestionnaire du réseau.

La **sécurité** tant physique que logique est évidemment une exigence essentielle pour tout environnement de services fonctionnant en réseau. C'est une obligation de l'ensemble des détenteurs de renseignements personnels. Le cadre juridique doit donc fonctionner de manière à inciter les responsables à prendre les mesures afin de garantir la sécurité des informations sur les personnes. Afin de développer une « culture de la sécurité », il importe, comme cela est exprimé dans les *Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information. Vers une culture de la sécurité* (20), que les principes suivants soient pris en considération :

- **sensibilisation** : les parties prenantes doivent être sensibilisées au besoin d'assurer la sécurité des systèmes et réseaux d'information et aux actions qu'elles peuvent entreprendre pour renforcer la sécurité ;
- **responsabilité** : les parties prenantes sont responsables de la sécurité des systèmes et réseaux d'information ;
- **réaction** : les parties prenantes doivent agir avec promptitude et dans un esprit de coopération pour prévenir, détecter et répondre aux incidents de sécurité ;
- **éthique** : les parties prenantes doivent respecter les intérêts légitimes des autres parties prenantes ;
- **démocratie** : la sécurité des systèmes et réseaux d'information doit être compatible avec les valeurs fondamentales d'une société démocratique ;
- **évaluation** des risques : les parties prenantes doivent procéder à des évaluations des risques ;
- **conception** et mise en œuvre de la sécurité : les parties prenantes doivent intégrer la sécurité en tant qu'élément essentiel des systèmes et réseaux d'information ;

(20) ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUE, *Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information. Vers une culture de la sécurité*, 2002, < www.oecd.org/dataoecd/58/62/1946930.doc >.

- **gestion** de la sécurité : les parties prenantes doivent adopter une approche globale de la gestion de la sécurité ;
- **réévaluation** : les parties prenantes doivent examiner et réévaluer la sécurité des systèmes et réseaux d'information et introduire les modifications appropriées dans leurs politiques, pratiques, mesures et procédures de sécurité.

Outre une culture de la sécurité, il faut un ensemble de processus capables de prévenir les attaques et surtout d'y remédier aussitôt que se produit un évènement qui met en péril les processus d'information.

IV.2. L'IMPÉRATIF DE CONFIANCE

La gestion des informations sur les personnes est 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.

La confiance est un élément essentiel 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. Dès l'étape de la collecte, se construit le lien de confiance essentiel à la bonne gestion de l'information. La collecte 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, au Canada, les données personnelles recueillies lors du recensement sont assorties de règles très strictes : elles ne peuvent être utilisées à d'autres fins. Lorsque des garanties sont données, il faut impérativement qu'elles soient respectées et que des mesures appropriées garantissent un tel respect.

Mais dès lors que les informations personnelles ont vocation à circuler de façon balisée dans un réseau, il devient nécessaire que l'établissement même de l'environnement en réseau au sein duquel circuleront les informations soit établi de façon transparente et à la suite d'un processus public d'évaluation des enjeux et des risques. Pour procurer la légitimité et la confiance essentielle à l'acceptabilité

des modes de circulation de renseignements personnels, il importe que tous les enjeux, toutes les appréhensions soient pris en considération. Il faut que les questions que se posent les citoyens reçoivent des réponses. Michel Dorais relève que dans des décisions comportant des choix et l'appréciation de risques :

> *[...] la nature du processus décisionnel prend de l'importance. La légitimité du processus décisionnel devient la clef qui ouvre la voie vers la bonne décision. Ces « bonnes décisions » sont les seules qui seront acceptables; les autres se verront écrasées par la pression politique, un scrutin quelconque ou par le balancement incessant d'un filet juridique aux mailles inextricables* (21).

Christine Noiville constate que la prise de décision à l'égard de phénomènes comportant des risques à être assumés par la collectivité doit comporter une dimension explicative et délibérative. Elle écrit :

> *Rappelons-le : un risque n'est pas en soi acceptable, il le devient par le prisme du débat, qui lui donne sa légitimité. L'acceptabilité n'est pas une essence qui s'imposerait à celui qui est confronté au risque. [...]. Ainsi, parce que le « risque acceptable » n'est pas un « donné » mais le fruit d'une appréciation à chaque fois renouvelée, le sens qu'il convient de lui attribuer doit autant que possible être négocié* (22).

L'évaluation que cette auteure fait de la nécessité de la consultation publique s'inscrit dans le contexte de l'évaluation environnementale des projets. Mais la mise en place d'environnements de circulation de renseignements personnels paraît relever d'une problématique analogue.

Ce qui préoccupe les groupes de pression et les citoyens lors de la mise en place d'environnements d'information où sont traités des renseignements personnels ressemble à ce qui préoccupe lorsqu'on s'interroge sur les impacts environnementaux d'un projet. On s'inquiète des précautions qui ont été prises, des conséquences non prévues, des problèmes particuliers que pourraient vivre certaines personnes. On cherche à être rassuré à l'égard des précautions, des analyses d'impacts et des mesures de contrôle qui préviendront les possibles dérives.

Pourtant, on sait que les organismes publics promoteurs de projets anticipent ces préoccupations et ont à cœur de concevoir des services et des prestations qui assurent un niveau élevé de protection. Le processus public permet de porter ces précautions à la connaissance

(21) Michel DORAIS, « L'évaluation environnementale : les conséquences de l'émergence de la démocratie procédurale », *Optimum*, hiver 1994-1995, pp. 38-41, p. 38.

(22) Christine NOIVILLE, *Du bon gouvernement des risques*, Paris, PUF, « Les voies du droit », 2003, p. 120.

publique. Il permet un débat éclairé sur les choix à faire et un regard critique sur les choix qui ont été faits. C'est le meilleur antidote aux discours alarmistes, habituellement construits sur des suppositions catastrophistes et des procès d'intention.

Il est donc nécessaire de formuler un cadre juridique reposant sur un concept qui garantit la protection des renseignements personnels lorsque ceux-ci sont déposés dans un environnement d'information accessible à une pluralité de ministères ou autres entités de service public, afin de leur permettre d'assurer seuls ou en partenariat un ensemble de services aux citoyens. Un tel cadre doit être établi moyennant un processus par lequel les enjeux et risques de même que les précautions mises en place sont publiquement divulgués et débattus.

V. À LA RECHERCHE DE CONCEPTS POUR ASSURER L'EFFECTIVITÉ DU DROIT DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS DANS LES RÉSEAUX DU E-GOUVERNEMENT

Dès lors que la circulation d'informations personnelles entre les organismes cesse d'avoir un caractère exceptionnel, il vaut mieux disposer d'un cadre juridique résolument axé sur les conditions à respecter lors du déploiement de prestations de services en ligne de même que sur les garanties devant accompagner la mise en place des espaces de circulation des renseignements personnels. Au plan juridique, les espaces-réseaux dans lesquels circulent des données personnelles doivent être encadrés par des règles qui viendront préciser le partage des responsabilités. En somme, il s'agit de mettre en place les règles désignant celui qui répond des informations ainsi partagées en réseau.

Lorsque les renseignements sont dans des environnements d'information auxquels ont accès une pluralité de ministères ou autres organismes ou entités publics, la protection des renseignements personnels ne résulte plus des limitations intervenant au stade de la collecte ou prohibant la circulation. Une véritable protection nécessite un encadrement strict des conditions auxquelles il est licite d'accéder aux renseignements de même que les conditions de leur utilisation. D'où la nécessité de **dissocier la possession de l'information et le droit d'y accéder et d'en faire usage**.

Dans la plupart des modèles de prestations de services intégrés, l'information nécessaire est en principe disponible à l'entité qui l'a recueilli initialement. Mais une partie ou certains éléments de l'information peut être disponible dans d'autres organismes; il importe

alors de baliser le droit d'y accéder. Il faut que tous les organismes n'accèdent à l'information que pour des fins légitimes et nécessaires à la réalisation de la prestation concernée.

Certes, du fait de sa détention dans un environnement d'information accessible à une pluralité d'entités, l'information leur est disponible, mais cela ne leur confère pas, en soi, le droit d'y accéder. **L'accent est alors déplacé vers le droit de faire usage des renseignements personnels plutôt que sur la seule possession ou détention de ces derniers**. Il y a donc dissociation entre la détention physique d'une information par une entité et le droit de cette dernière d'y accéder ou d'en faire usage. Du fait de sa participation à un espace en réseau, un ministère ou autre entité publique détient un ensemble d'informations en commun avec d'autres entités. Toutefois, il n'a droit d'accéder à ces informations que si un ensemble de conditions sont réunies.

Les protections sont ainsi conçues de manière à garantir que les renseignements personnels seront effectivement utilisés pour des fins licites, plutôt que pour empêcher leur circulation. En encadrant le droit des ministères et autres entités d'accéder aux informations versées dans un environnement d'information, la protection sera mieux assurée sans pour autant immobiliser les renseignements personnels.

V.1. L'AIRE DE PARTAGE : DÉFINITION

La notion ***d'aire de partage de renseignements personnels*** peut être définie de la façon suivante.

Un environnement d'information dans lequel des renseignements personnels nécessaires à la délivrance d'un ensemble de services accomplis au bénéfice des citoyens peuvent être rendus disponibles à différentes entités. Ces services ou prestations ont un caractère complémentaire et leur accomplissement nécessite des informations détenues par une pluralité de ministères et autres entités.

La notion vise un ensemble de mécanismes balisant la circulation de l'information et délimitant les usages qui peuvent en être faits. Elle 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 relatifs à l'information sur les personnes lorsque l'information se trouve dans un réseau.

Dans la plupart des modèles de prestations de services intégrés, l'information nécessaire est en principe disponible à l'organisme qui l'a recueilli initialement. Mais une partie ou certains éléments de l'information peut être disponible dans d'autres organismes; il importe alors de baliser le droit d'y accéder. Il faut que tous ces organismes n'accèdent à l'information que pour des fins légitimes et nécessaires à la réalisation de la prestation concernée, pas plus.

Les protections sont ainsi conçues de manière à garantir que les renseignements personnels seront effectivement utilisés pour des fins licites, plutôt que pour empêcher leur circulation.

V.2. LE PROCESSUS DE CRÉATION DES AIRES DE PARTAGE

L'instauration d'une aire de partage de renseignements personnels procède nécessairement d'une concertation entre une pluralité d'entités concernées par l'accomplissement de prestations complémentaires de services. Cette concertation doit aussi s'inscrire dans le cadre global mis en place afin de développer les prestations de services.

La circulation des renseignements personnels dans les réseaux soulève des appréhensions. Elle sera acceptée et considérée comme légitime à la condition que le public ait l'assurance que l'information est protégée et utilisée seulement pour les fins déterminées.

Les aires de partage de renseignements personnels peuvent concerner aussi bien des prestations à caractère universel, touchant l'ensemble des citoyens, que des services localisés et ciblés pouvant ne concerner que quelques centaines de personnes. Pour convenir à une telle diversité de situations, il faut un processus de consultation capable d'encadrer à la fois des débats à grande échelle sur les enjeux de société et des projets plus ciblés comportant des enjeux plus limités. Un processus de consultation à géométrie variable doit être privilégié à un processus trop lourd qui rendrait quasi impraticable la mise en place d'aires de partage.

Les cas de figure possibles d'espaces de circulation de renseignements personnels sont nombreux. Selon les secteurs d'activités desquels relèvent les renseignements concernés, des enjeux différents pourront se soulever. Les échanges d'informations relatives aux personnes soulèvent des frayeurs différentes de même que des appréciations diversifiées des dangers et des risques qui pourraient résulter de la mise en place des aires de partage.

Il faut un cadre juridique susceptible de convenir à une grande variété d'espaces possibles de détention et de circulation de renseignements personnels. Les espaces de circulation seront délimités en fonction des risques et enjeux jugés acceptables à la suite d'un

processus de consultation publique. Ce processus vise à poser ouvertement les enjeux, les avantages et les précautions relatifs aux prestations électroniques envisagées et aux partages de renseignements qui sont projetés.

Les analogies entre les problématiques de protection des renseignements personnels et les autres enjeux sociaux, pour lesquels on a jugé nécessaire d'instituer des processus de consultation publique, désignent les différentes approches possibles afin de déterminer le cadre qu'il conviendrait de retenir pour le processus de consultation publique associé à la mise en place d'aires de partage de renseignements personnels.

V.3. L'ENCADREMENT JURIDIQUE

Pour délimiter ces aires de partage, 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.

Le cadre juridique doit nécessairement respecter les principes fondamentaux en matière de protection des renseignements personnels. Ces principes sont énoncés non seulement dans la législation mais résultent de documents internationaux auxquels il importe de se conformer. Il doit garantir une protection de bout en bout et assurer que seules les informations autorisées seront utilisées lors de chacune des prestations électroniques de service.

Les responsables et les responsabilités qui leur incombent doivent être identifiés. Il faut, en tout temps, être en mesure de connaître qui répond des informations personnelles détenues dans l'aire de partage et quels sont ses devoirs. En outre :

- l'aire de partage s'établit au moyen d'une entente à caractère public soumise préalablement à consultation; sa mise en œuvre est effectuée conformément aux conditions d'un décret du pouvoir exécutif;
- le processus public assure la transparence et l'évaluation publique et contradictoire des enjeux et risques. Lors de chaque interaction, les citoyens sont informés ou ont accès aux informations à l'égard de ce qu'il advient de leurs renseignements personnels.

Les ministères et autres entités peuvent modifier l'aire de partage afin d'assurer une prestation optimale de services et respecter les

impératifs des lois et autres règles qui encadrent leur activité. Les modifications substantielles doivent aussi être soumises au processus s'appliquant lors de la création de l'aire de circulation.

En tant qu'espace régulé, l'aire de partage est nécessairement balisée par les finalités de la famille de services et prestations pour lesquelles elle est établie. Le citoyen est informé de sa vocation, de sa portée et de sa teneur. Une liste des usages possibles des informations est continuellement disponible en ligne ou autrement.

Ces espaces de circulation sont délimités par les protections physiques et logiques de même que par les droits et autorisations d'accès. De tels espaces se balisent en fonction des sujets sur lesquels portent les informations qui y circulent, celles qu'il est licite d'y faire figurer et celles qui ne peuvent y figurer.

L'accès par un organisme à une aire de partage est réservé aux prestations électroniques fonctionnant suivant des pratiques en vertu desquelles toute information portant sur une personne est divulguée (ou rendue disponible) à cette dernière sur demande ou à chaque fois qu'une décision doit être prise concernant cette personne. La personne peut alors s'opposer à ce qu'une information soit utilisée, si celle-ci est équivoque ou ne possède pas les qualités requises.

Les actes d'établissement ou ententes relatifs à la mise en place d'une aire de partage de renseignements personnels prévoient des dispositions sur des matières telles que les suivantes :

- préciser les finalités auxquelles peuvent servir les informations incluses dans l'aire ;
- identifier les catégories de personnes qui peuvent avoir accès aux informations de même que la nature de leur droit d'accès ;
- préciser les conditions d'utilisation des informations ;
- préciser les moyens par lesquels les informations personnelles sont validées auprès des personnes concernées lors d'une décision ;
- déterminer les responsabilités respectives incombant aux entités partenaires à l'aire de partage de renseignements personnels.

En plus, l'aire est sécurisée par un ensemble de protections spécifiées dans l'entente de création. Ces protections découlent de mesures telles que :

- le contrôle des droits d'accès; contrôle effectué, *a priori*, par l'obligation de mettre en place une politique et une liste des droits d'accès puis, *a posteriori*, par la vérification

systématique ou aléatoire des accès et, pour certaines informations sensibles, la journalistique des accès ;

- le contrôle des décisions rendues suite à l'usage de renseignements ;
- la validation de l'information à être utilisée pour accomplir une prestation pour le citoyen.

Les conditions de mise en place des aires de partage doivent prévoir un régime de gestion des conditions moyennant lesquelles un organisme et les individus qui y oeuvrent peuvent y accéder licitement. L'accès doit être licite aux termes de la loi, compte tenu de la finalité pour laquelle le renseignement est recherché, ou moyennant le consentement général ou spécifique de l'usager.

L'entente doit identifier les obligations des entités qui exercent le contrôle sur l'information de même que les obligations de ceux qui ont droit d'accéder aux informations. Le détenteur physique ou juridique de l'information doit s'assurer de la validité du droit d'accès.

L'entente de création de l'aire de partage identifie les moyens qui sont mis en œuvre afin d'assurer la circulation sécurisée de ces renseignements dans cet espace. À l'égard de certains renseignements, l'entente peut même prévoir l'obligation de demander le consentement de la personne concernée avant d'y accéder. Mais alors, il s'agit d'un consentement qui a son véritable sens : il vise à assurer un véritable droit de maîtrise de la personne sur certaines informations qu'il n'est pas, par ailleurs, tenu de divulguer en vertu d'exigences prévues par les lois. En somme, au plan juridique, l'aire de partage est un espace régulé alors qu'au plan technique, c'est un espace normé.

V.4. Les responsabilités

L'aire de partage est un espace virtuel constitué de gisements d'informations et de relais de communications. Chaque entité qui est partie à une entente relative à une aire de partage peut être considérée comme étant le détenteur juridique des renseignements. Dès lors qu'on exerce la maîtrise d'une donnée personnelle, on en répond.

À ce titre, chaque organisme est responsable de la confidentialité des renseignements. Comme il y a pluralité d'organismes, ces derniers pourront déterminer, dans l'entente relative à l'aire de partage, comment se répartiront les responsabilités de l'une et l'autre des entités participantes.

Dans une aire de partage, il y a des maîtriseurs d'information, créateurs, décideurs et contrôleurs. Les responsabilités des différents acteurs ne tiennent pas tellement à leur rôle officiel mais plutôt au

degré de contrôle et de maîtrise qu'ils exercent ou qu'ils sont réputés exercer sur l'information et les communications qui se déroulent dans les réseaux ou sur la partie de ceux-ci sur lesquels ils ont une certaine maîtrise.

La maîtrise de l'information emporte des devoirs. Ces devoirs incombent à celui qui produit l'information et la traite. Mais les devoirs ont une intensité différente selon que l'on exerce la maîtrise de l'information ou que l'on ait simplement connaissance de celle-ci.

Lorsqu'une entité exerce la maîtrise d'un renseignement personnel, elle doit s'assurer d'en préserver l'intégrité, elle doit s'assurer que seuls ceux qui y ont droit puissent y avoir accès, elle doit veiller à ce que les renseignements soient modifiés dans le respect de la loi. Elle doit évidemment mettre en place les mesures de sécurité et autres précautions afin d'assurer la conservation de l'information.

Ainsi, les personnes qui ont la maîtrise de l'information ont habituellement à en répondre. Pour les acteurs qui n'ont pas de droit de maîtrise sur l'information, leur responsabilité découle de la démonstration qu'ils avaient connaissance de l'information. Alors, ils sont susceptibles d'en supporter la responsabilité. Par contraste, l'intermédiaire passif tel que l'intermédiaire agissant comme transmetteur n'est pas, en principe, responsable des actions accomplies par autrui au moyen des documents qu'il transmet ou qu'il conserve durant le cours normal de la transmission et pendant le temps nécessaire pour en assurer l'efficacité.

VI. Conclusion

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. Il importe donc de voir à l'actualisation des moyens par lesquels on assure la protection de la vie privée et des renseignements personnels. Ces moyens doivent être conséquents avec les caractéristiques des environnements en réseau. Se contenter de reconduire les méthodes de régulation qui prévalaient dans l'univers de l'administration publique conçue en silo est probablement le moyen le plus sûr d'affaiblir la protection de la vie privée.

Dans ce texte, nous avons présenté un modèle possible d'évolution du droit de la protection des données personnelles reflétant les

impératifs, exigences et risques qui caractérisent les environnements en réseaux.

Ce modèle permet de penser et de situer les processus et les principes devant être mis en place lorsque vient le temps de mettre en ligne des services publics nécessitant l'accès et le traitement de renseignements personnels. En instituant un mécanisme qui régule et contrôle les accès aux données personnelles par toute entité partenaire dans un réseau, on accroît la protection effective des données personnelles tout en créant les conditions d'une meilleure responsabilisation de l'ensemble des acteurs.

L'état en réseau appelle des fondements qui se conçoivent de façon différente de ceux qui relèvent de l'État-papier. En particulier l'impératif de confiance prend une place considérable dans un univers où les renseignements sur les personnes sont disponibles dans un environnement interconnecté. Pour que soit préservé le lien de confiance entre l'État et le citoyen, il importe de cadrer la protection de manière à garantir que chaque accès à un renseignement portant sur une personne identifiable n'a lieu que pour des motifs autorisés par la loi. L'interaction plus intense rendue possible dans les environnements en réseau permet de mieux respecter l'impératif de la qualité de l'information.

La notion d'aire de partage au plan juridique un espace régulé et au plan technique un espace normé procure ce concept à partir duquel s'articulent les droits et obligations de l'ensemble de partenaires du e-gouvernement. Le concept permet de situer les protections qui doivent être assurées à l'égard des données personnelles de même que les responsabilités respectives de tous ceux qui en ont la maîtrise au sein d'un espace en réseau.

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.