Vers un modèle assurant la protection des données dans l'État en réseau: l'aire de partage de renseignements personnels

Pierre TRUDEL

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

Communication à la première Conférence internationale sur la protection des données personnelles dans les États fédéraux et plurinationaux, Barcelone, 4 et 5 octobre 2006

Towards A Model Warranting Data Protection in Networked Administration: The Shared Personal Information Area

Pierre TRUDEL

L.R. Wilson Chair in Information Technology and E-Commerce Law
Public Law Research Center
University of Montréal

Paper Presentedted to the 1st International Conference of Data Protection in Plurinational and Federal States, Barcelona, October 4 and 5, 2006

Table des matières

Introduction 1

A. Une protection mal adaptée aux réalités du gouvernement en ligne 2
   1. De nouvelles circulations de l'information 3
      a) La personnalisation 3
      b) La circulation en réseau et le partage des informations 4
   2. Une normativité en réseau 5

B. Les impératifs de protection de la vie privée dans les réseaux de services publics 7
   1. Une lecture actualisée des principes de protection des renseignements personnels 8
   2. L'impératif de confiance 13

C. Un concept pour assurer l'effectivité du droit de la protection des renseigne-ments personnels dans les réseaux 15
   1. L'aire de partage : définition 17
   2. Le processus de création des aires de partage 17
   3. L'encadrement juridique 18
   4. Les responsabilités 21

Conclusion 22

Table of contents

Introduction 1

A. Protection poorly adapted to governement online 2
   1. New Circulation of information 2
      a) Personalization 3
      b) Circulation in a network and information sharing 4
   2. Normativity in networks 4

B. Privacy protection needs in public service networks 6
   1. An update reading of privacy protection principles 7
   2. The need for trust 11

C. A concept to ensure effective privacy protection in networks 12
   1. A shared area : definition 13
   2. Creation of shared areas 14
   3. The legal framework 15
   4. Responsibilities 17

Conclusion 18

Résumé

L'administration électronique suppose la circulation accrue d'informations sur les personnes. La gestion de l'information est un élément essentiel de l'activité gouvernementale. La tendance de l'évolution législative dans plusieurs pays reflète l'importance de l'information dans le fonctionnement de l'administration publique. 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 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.

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 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. 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.

Le cadre juridique de l'État en réseau devrait être doté d'un mécanisme transparent par lequel le partage de l'information est reconnu, ses risques et enjeux divulgués, discutés et publiquement évalués. 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.

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. 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 véritable protection nécessite un encadrement strict des conditions auxquelles les ministères et autres autorités publiques ou privées accèdent aux renseignements et les utilisent. Si l'on tient à assurer une actualisation pertinente des principes relatifs à la protection des données personnelles dans les contextes diversifiés du gouvernement en ligne, il faut consacrer de l'attention aux règles balisant le droit d'accéder et d'utiliser les données personnelles. Le concept d'aire de partage offre une assise à une régulation de protection de la vie privée fondée sur ces paradigmes.

Abstract

E-government presupposes greater circulation of personal information. Information management is an essential component of government operations, and legislative trends in many countries reflect this. There are numerous advantages to networking activities inherent to such operations. It promotes a individual- or user-centred approach, and facilitates co-operation among a wide range of actors and stakeholders with different statuses. It also accentuates the trend away from the hierarchical model, and enables flexible specialization based on exchanges among different sources of information.

The spread of operations into environments such as the Internet requires a redefinition of the space in which personal information circulates, since that space is increasingly virtual. We have to review the notions that help to identify information that has to be protected because it is private, and information that has to circulate because it plays a role in public affairs or society, or is needed for the effective delivery of public services. This requires identifying the appropriate markers and indicators for protecting privacy without endangering the free circulation of information relevant to the public sphere.

The legal framework of networked government has to have a transparent means of acknowledging information sharing, and of disclosing, discussing and publicly assessing the risks and stakes. Many electronic service delivery models presuppose that private information is kept in an environment in which it is available to other government bodies.

This paper presents the components of an updated framework able to effectively protect privacy in public service networks. Key components of the notion of a shared personal information space are also described, along with principles for setting up and operating such a space.

When data is in an information environment to which a number of government agencies have access, privacy protection can no longer be confined to restrictions on data collection or prohibitions on circulation. Real protection requires strict control of the conditions that have to be met by government departments and other public and private authorities in order to gain access to and use information. If we hope to make appropriate improvements to the principles pertaining to privacy protection in the wide range of government online contexts, we have to focus on the rules governing the right to access and use personal information. The notion of a shared space provides the foundations for privacy protection regulations based on these paradigms.

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.

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[1].

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

Introduction

The advent of e-government networks has resulted in significant changes to the context in which personal information circulates. A privacy protection system that depends on redundant methods is likely to be defeated by the developments that will certainly transform the conditions in which personal information is managed.

The information systems used to deliver public services online are now network-based, in other words, they are inter-connected, structured environments in which information flows from source to source in a multidirectional, non-hierarchical manner.[1]

The migration to networked environments shared by numerous areas of activity and public services requires a review of legal notions. In particular, we have to re-examine the legal notions that define information that has to be protected because it is private, and information that has to circulate because it plays a role in public affairs or society, or is needed for effective delivery of public services. Current environments are networks with inter-connections and not the mythical mega-databases that were predicted three decades ago. However, if we are not careful to examine the paradigms underlying privacy protection, and instead maintain current approaches, such mega-databases could be formed.

As interactions become virtual, environments become inter-penetrated. Owing to digitalization, communications environments that used to be considered separate from one another are now technologically equivalent. The legal framework for the spaces in which interactions now occur is crucial. Regulations have to be designed to protect personal information no matter where it is located in the network environment in which government and individuals interact. This means that protection has to be based on organizational and spatial premises that take into account the way network spaces operate. Governments need regulations that can provide a framework for conduct in virtual spaces that cross barriers and ignore organizational charts. Such regulations must not be based on the idea that public agencies operate in isolation from one another.

In short, the emergence of networked government requires regulations that are not based on the idea that departments and agencies are compartmentalized and independent from one another. Regulation has to be at the network level; events occurring in network spaces have to be regulated by a legal framework that protects and ensures the quality of information.

conduites dans des lieux virtuels insensibles aux frontières ou 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 celle postulant des 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 être régis par un cadre juridique assurant la protection et la qualité des informations.

A. Une protection mal adaptée aux réalités du gouvernement en ligne

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.

Le cadre juridique actuel postule le caractère exceptionnel des transferts de renseignements nominatifs 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 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

A. Protection poorly adapted to government online

Privacy protection mechanisms have to be brought up to date to reflect the current situation in networked government. E-government supposes increased circulation of information. There are many advantages to conducting government activities in a network. It promotes individual- or user-centred services, facilitates collaboration and co-operation among a wide range of stakeholders with different statuses, and enables flexible specialization based on exchanges between sources of information.

The current legal framework postulates that exchanging nominative personal information without the consent of the individuals in question is unusual. However, it is clear that a great deal of personal information is exchanged among some public agencies. Moreover, the current legal framework authorizes the sharing of information, but generally in such a way as to increase duplication. In the end, the result is databases expanded by information obtained from other agencies, and therefore there is duplication, redundancy, and given the longevity of information, always more personal information in government hands.

Unlike what is postulated by current law, in networks privacy protection should suppose the prevention of redundancy and target access to information where it is found in government systems. A legal mechanism has to be established to avoid duplication of personal information. When government services operate in a network, legislation should authorize conditional, regulated access to data held at a given location in the network, so long as such access is authorized by law and no permanent copy of the information is made.

1. New circulation of information

The legal rules inherited from the time when bureaucrats could apply arguments without having to explain them to individuals seem obsolete given present and anticipated networks. E-government supposes taking advantage of more powerful data processing capabilities, sharing information, and personalizing data to obtain services and make decisions. The new ways that information circulates clearly have to take this into account.

A number of trends accompanying the emergence of e-government involve both the personalization and sharing of information. Circulation and sharing of information make it possible to improve service quality and speed. Co-operative work based on information exchange and

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.

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.

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.

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.

a) 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

sharing can reduce the number of situations in which "the government's right hand does not know what its left hand is doing!" By reducing redundancy and limiting situations in which people are required to retransmit the same information, productivity is improved, to the benefit of all.

It is increasingly likely that individuals will expect to deal with government in the way that is becoming routine with other goods and services suppliers online. Government will tend to adopt a mode of operation that tries to take advantage of network environments. A branching, collaborative structure will replace the hierarchical edifice of bureaucratic organizations.

a) Personalization

Cyberspace provides new ways to personalize public services as well as the capacity to create numerous artificial persons. Invested with sovereignty and having access to various online tools, users are seen or at least presented as able to choose and negotiate the levels of security and protection that they desire. The rules governing the activities in which users are involved are increasingly seen as part of the product or service offered. These rules are often presented in a personalized manner based on a profile established according to variables recorded when information is exchanged between users and the sites they visit.[2]

Naturally, individuals will expect that the information relevant to their relations with government will be available when needed, and that the information will be appropriate to the purposes for which it is intended. This trend is already clear in the private sector, and will certainly have an impact on expectations with respect to public services.

One of the advantages of network transaction environments is the possibility of matching services with individual preferences. Personalization involves adapting the behaviour of the information environment to the user's expectations, ideally ahead of time. Users' needs must be met, and as quickly as possible. For example, a person who changes addresses could send the relevant information to only one place by performing a single operation that relays it to all the agencies that need to be informed of the change.

In order to offer personalized services based on individual needs, government bodies have to have real-time access to personal information that is normally held by a number of separate components of government. Maintaining a legal regime that prohibits the circulation of personal information makes it difficult to establish integrated services that cannot be mapped onto bureaucratic borders.

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[2].

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

b) 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.

b) Circulation in a network and information sharing

Networked government is based on interconnections. Information is constantly exchanged, and it cannot be assumed that such exchanges take place in a specific physical or organizational location. For example, the WWW's functioning is based on hypertext. This makes possible and creates opportunities for inter-creativity, inter-relations and the mixing of information located in many different places at the same time or even on one or more computer screens, televisions, digital radios or cell phones.

Collaborative management provides opportunities to share information. The spread of shared information platforms places a whole set of information exchange and distribution opportunities within everyone's reach. Cybernauts, individuals and government officials can convey, share and exchange information. In the case of information that is necessarily in the government's possession, the legal framework should regulate only the access conditions for every government official, and not prohibit circulation. This would shift the issue away from whether or not the government can possess certain information, and towards whether or not it has the right to access and use information to make decisions in specific situations.

Interactions in computer networks require different means of identifying people. Since government operations are increasingly networked, information necessarily circulates, and should be available when needed for service delivery. Wider circulation demands precautions because the potential for accumulating and linking information increases. A realistic approach has to be adopted, taking into account both advantages and drawbacks. In this respect, greater protection at the level of access by government departments and agencies is much more effective than what is provided under existing regimes.

2. Normativity in networks

In cyberspace[3] normativity is growingly elaborated in networks. Decentralization is characteristic of networked government: to individuals, government looks more and more like a network with blurred administrative borders. This augments the regulatory responsibilities of those on the front line and also the need to develop appropriate regulatory tools at the local level and in virtual micro-environments.

The normativity of network-based computer communications environments changes the way in which

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.

2. Une normativité en réseau

Dans le cyberespace[3], 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

responsibilities are apportioned. The classical model characteristic of the liberal state, in which every department and agency is supposed to have complete and exclusive control over the information it holds, is gradually being replaced by a model in which information sharing requires new ways of distributing and pooling responsibilities.

A set of normative systems applies in cyberspace. Indeed, cyberspace itself can be seen as an inter-connected set of interacting sources of normativity. It is made up of spaces in which all or some of the norms applying to users prevail. The effectiveness of norms springs either from the fact that they define, even implicitly, the conditions for conducting the activity in question, or from the fact that a government is able to enforce them, as is usually the case in e-government environments.

Cyberspace is also made up of relays through which norms, standards and their consequences are clarified and spread. Rules emanating from sources of normativity are relayed through and spread in the
various virtual spaces. In cyberspace, they co-exist with, and complement or compete with rules from other sources of normativity.

The importance of norms flowing from technological constraints, practice and other sources is clear on the Internet. However, there are also other vessels of normativity, such as the tools, guides and other instruments used to enforce legal principles.

For example, the regulations governing system administrators' information access rights are mechanisms for applying the principles stated in international legislation and documents.

One of the major links between government sources of normativity and cybernauts is liability. Liability provides the framework that circumscribes stakeholders' actions and sets out the scope of their obligations. In the end, it is in order to manage risk and limit their liability that both collective and individual stakeholders adopt codes of conduct. This is how the requirements stated in the sources of normativity are incorporated into environments. For example, the principles stated in sources of normativity, such as legislation and international principles, are conveyed through micro-regulations and self-regulation.

When every department, agency and public servant with access to personal information is accountable for it, they are encouraged to establish measures to anticipate, prevent and reduce risk. In order to manage risk and limit liability, stakeholders can establish strict routine controls over

de l'État libéral où chaque ministère ou entité administrative est réputée 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.

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

access to personal information. Correctly applied, such network normativity should guarantee accountability and provide protection more appropriate for stakeholders who process personal information.

B. Privacy protection needs in public service networks

E-government supposes taking advantage of more effective means of processing and sharing information, and individualizing information use so as to provide services and make decisions. The new flow of information clearly has to be designed in accordance with guidelines such as those stated in OECD principles, which reflect international consensus.

The current framework for privacy protection focuses on compliance with a series of formal procedures. There is little room for assessment of the stakes and context. Rather than leading to the establishment of protection mechanisms based on the postulate that information circulates in networks, the tendency is to insist on maintaining impervious barriers between components of government.

Developing networked government requires reassessing privacy protection, but not by erecting as an absolute the protection that prevailed when personal information was located in filing cabinets. Instead, we have to identify the requirements of real protection in a context in which personal information necessarily has to circulate.

Many electronic service delivery models suppose that personal information is available to other components of government in an electronic environment. Such sharing therefore has to be anticipated and provided with a framework so that the information can be used only for purposes compatible with service delivery requirements. Individuals also have to be informed about what happens to the information they entrust to government.

Under existing regulations, if a department or agency gathers personal information, then it possesses that information. The department or agency is allowed to gather information only if it proves that doing so is necessary given its mandate and the services it has to provide. However, once a department or agency has obtained personal information, there are in practice few guarantees that the information will not be used without the individual's knowledge or even for purposes other than those for which it was gathered. The public body has exclusive ownership of the information that it has gathered. The information is under its control even though in some circumstances the data may be physically located

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.

B. Les impératifs de protection de la vie privée dans les réseaux de services publics

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 sont accessibles à l'extérieur des locaux contrôlés par le ministère ou l'organisme. Il existe des dispositions pour le partage de renseignements personnels, mais ce partage est inhabituel.

outside of the premises controlled by the department or agency. There are provisions for sharing personal information, but such sharing is unusual.

We therefore need a legal framework based on a concept that guarantees protection of personal information when it is located in an information environment to which a number of departments and agencies have access for the purpose of delivering public services alone or in partnership. This requires identifying the conceptual changes needed to guarantee effective privacy protection. Thus, an updated reading of the fundamental principles of privacy protection is required.

1. An updated reading of privacy protection principles

The development of networked services requires an update of the principles that provide the framework for processing personal information.

The OECD sets out the following principles:[4]
- Collection limitation;
- Purpose specification;
- Openness;
- Individual participation;
- Accountability;
- Use limitation;
- Data quality;
- Security safeguards.

It is important to identify how these principles have to be understood and applied in order to provide real privacy protection in network environments with growing flows of information.

Limiting data collection supposes the establishment of decision-making processes that use the minimum personal information necessary to deliver services or make decisions in a network environment. Concretely, frameworks for decision-making have to require justification of why the information is needed before any personal information is gathered.

In a network environment, the **need for collection** has to be considered in relation to the set of services concerned. Once the information is gathered, the need to keep it can be assessed in accordance with its relevance to the set of decision-making processes in question. Consequently, there is overlap between the principles pertaining to data preservation and collection and those concerning purpose specification. The principle of purpose specification is thus strengthened: when purposes are strictly defined,

ments 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.

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[4] sont les suivants :
- limitation en matière de collecte;
- spécification des finalités;
- transparence;

collection is limited to the information that it truly indispensable for the benefits and services concerned.

More than ever, government is in a position to tell every individual what information it has on him or her, and which information it intends to use to make a given decision. The individual is now able to take action and require that information be withdrawn or added. Consequently, the rule preventing the circulation and re-use of information, so that it cannot be diverted from its original purpose, has to be re-evaluated in light of the greater dialogue made possible by networks.

The spread of networks requires that we assess needs in all situations involving information environments. Naturally, needs always have to be assessed with respect to the legitimacy of gathering and retaining information, as is required by current principles. However, there has to be a way of ensuring that only relevant and authorized information is used in a given decision-making process. This calls for an approach in which the need to retain information is considered separately from the need for access when making a decision or delivering a benefit.

The purpose specification principle states that personal information can be gathered and used only for purposes compatible with those of the initial collection. This principle is linked with the data quality principle. The OECD expresses this principle in the following manner:

> Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up to date.[5]

In a network environment, the purpose issue presupposes that the information is already available, in other words that it has already been gathered. It is not with respect to data preservation that the purpose specification principle applies, but with respect to access to and use of information. In a network, the principle of control at the level of access rights ensures purpose compliance. Within a government body, access to information should be permitted only for authorized purposes and in the course of an activity related to such a purpose. Purposes have to be seen in the framework of the set of services offered.

Compliance with the **purpose** supposes that the user is in fact aware of the family of purposes for which the information will be used. The notion of purpose thus has to be centred on the user and not on government structures. For example, a user who enters into a relationship with the departments and agencies responsible for implementing income security legislation has to know

- 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 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

that the information he or she provides will circulate and be used to implement the legislation, no matter whether the body that applies the legislation is a department or another public agency.

Information on the **purposes** for which information is held has to be available at all times. It has to be repeated every time data is gathered. Moreover, in order to comply with the use limitation principle, information environments should provide well-defined families of services. This ensures that personal information is used for purposes related to and compatible with the initial reasons for collecting the information.

Openness is an essential condition for credibility and trust in network environments. Users have to be able to know with whom they are dealing and how the information process works. Thus, public assessment of information environments and information sharing for electronic service delivery purposes is crucial. The stakes and risks associated with networking electronic services have to be disclosed, debated and assessed publicly.

When personal data is available on a network, every department and agency has to ensure that the information to which it has access is of appropriate **quality**, given service delivery requirements and the context. Network technology's potential for direct dialogue between government and users should be used to ensure quality. It is becoming easier to base protection of individuals on the individual's right to dialogue with the decision makers responsible for identifying his or her rights and duties.

In this respect, the principle of **individual participation** in decisions concerning personal information processing takes on a whole new meaning. In networks, it is possible to present information and have it checked in real time by the person concerned. Data **quality** can also be improved if the department or agency verifies information when it delivers a specific service. It is now possible to guarantee that the information really has the qualities required for making the decision or delivering the service in question.

Data quality is crucial to service delivery and decision-making: information has to be accurate, specific, legally authorized and unambiguous. The legitimacy of circulating such personal information can be strengthened if decision-making processes require that every time there is a decision to be made concerning an individual, that person must be presented (online or by other means) with the information on which the decision is to be based. Individuals should also be able to review and, if required, correct personal information. The right to rectification would thus gain real meaning.

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.[5]

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

The legal framework applicable in networks should therefore require the organization to ensure the accuracy of data. Whenever personal information is used, public bodies should check the information with the individual concerned. Data quality can be ensured if the information is made available so that the individuals concerned can check and, if necessary, rectify it.

With respect to **accountability**, every public body with access to personal data in a network can be considered the legal holder of the data. When information is held by more than one body, every partner is considered the legal holder of the documents and personal information in the databases to which it has access.

This makes every body accountable for the confidentiality of personal information; the bodies shoulder the responsibility jointly. If there are many bodies, they should decide how to divide the responsibilities among themselves.

Managers should be guided by rules that specify their obligations and delimit their responsibility with respect to confidentiality and security. Standards have to be defined so that the behaviour and responsibility of individuals can be assessed. The same applies to relations between individual-users and network managers.

Both physical and software **security** is obviously an essential requirement for every networked service delivery environment. It is an obligation for all holders of personal information. The legal framework therefore has to lead those responsible to take action to guarantee the security of information on individuals. As the *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*[6] state, in order to develop a "security culture" the following principles have to be taken into consideration:

- **Awareness**: Participants should be aware of the need for security of information systems and networks and what they can do to enhance security;
- **Responsibility**: All participants are responsible for the security of information systems and networks;
- **Response**: Participants should act in a timely and co-operative manner to prevent, detect and respond to security incidents;
- **Ethics**: Participants should respect the legitimate interests of others;
- **Democracy**: The security of information systems and networks should be compatible with essential values of a democratic society;
- **Risk assessment**: Participants should conduct risk assessments;

l'utilisation, les environnements d'information devraient desservir des familles délimitées de prestations : ce qui assure que les renseignements personnels seront utilisés qu'à des fins apparentées et compatibles avec celles de la collecte initiale.

La **transparence** est une condition essentielle de la crédibilité et de la confiance dans les environnements en réseau. L'usager doit être en mesure de savoir à qui il a affaire et comment est conçu le processus informationnel dans lequel il est engagé. À cet égard, l'évaluation publique des environnements d'information ou des 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

- **Security design and implementation**: Participants should incorporate security as an essential element of information systems and networks;
- **Security management**: Participants should adopt a comprehensive approach to security management;
- **Reassessment**: Participants should review and reassess the security of information systems and networks, and make appropriate modifications to security policies, practices, measures and procedures.

In addition to a security culture, there must also be a set of processes able to prevent and especially solve problems as soon as something endangers the information process.

2. The need for trust

Management of personal information is a crucial factor in inspiring the trust necessary in relations between government and individuals. This is why gathering and processing personal information has to be accompanied by guarantees of trust. In a network environment, trust is built by ensuring a high degree of transparency. Users have to be informed clearly and openly, promises have to be kept and strong guarantees have to be provided with respect to possible uses of information.

Trust is an essential component of any framework for managing personal information. Throughout the information processing cycle, an environment has to be provided in which the user/individual has real trust. Indeed, trust has to be fostered from the collection stage on: information gathering and processing have to be transparent. This is essential for good information management. By focussing on the user's awareness of what happens to the information entrusted to the state, an atmosphere of trust is created. The more sensitive the information, the more precautions must be taken in order to guarantee the level of trust required. For example, in Canada, personal information gathered during a census is subject to very strict rules: it cannot be used for any other purpose. When promises are made, they absolutely have to be kept and this requires that appropriate measures be taken.

However, as soon as tagged personal information circulates in a network, the very establishment of the network environment in which the information circulates has to be transparent and result from a public assessment of risks and stakes. In order to obtain the legitimacy and trust essential to the acceptability of circulation of personal information, all stakes and concerns have to be taken into consideration. Individuals' questions have to be answered. Michel Dorais notes that, in decisions involving risk assessment,

…the nature of the decision-making process becomes more important. The legitimacy of the decision-making process

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 évaluées 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*

becomes the key to the right decision. Such "good decisions" are the only ones that will be acceptable. The others will be defeated by political pressure, some form of vote or the constant swing of an inextricable legal web.[7]

Christine Noiville notes that an explanatory and deliberative component has to be included in the process when decisions are made that involve risks to be shouldered by the community. She writes:

Remember: a risk is not acceptable in itself. It becomes so through the prism of debate, which confers legitimacy on it. Acceptability is not an essence that imposes itself on he who is confronted with a risk. [...] *Thus, because an "acceptable risk" is not a given but the fruit of constant reassessment, the meaning that it should be given should be negotiated as much as possible.*[8]

This author is referring to environmental impact assessment when she argues for the need for public consultation. However, the establishment of environments in which personal information circulates seems to raise similar problems.

The concerns of pressure groups and individuals with respect to information environments for processing personal information resemble those pertaining to the environmental impact of a project. People worry about precautions, unforeseen consequences, and specific problems that could be experienced by some people. They seek assurances that precautions will be taken, impact assessed, and controls established to prevent mishaps.

Yet, we know that public agencies do not promote projects without first anticipating such concerns and that their aim is to design and provide benefits and services that ensure a high level of protection. A public process can raise public awareness of such precautions. It makes it possible to have an informed debate on current choices and to examine past choices critically. It is the best antidote to alarmist discourse, which is usually based on catastrophic assumptions and unfounded suspicions.

Therefore it is necessary to formulate a legal framework based on a concept that guarantees protection of personal data when such data is held in an information environment that can be accessed by a number of departments or other public service bodies for the purpose of providing a set of public services alone or in partnership. The framework has to be established through a process in which stakes and risks as well as precautions are publicly disclosed and debated.

C. A concept to ensure effective privacy protection in networks

As soon as the circulation of personal information among government bodies ceases to be exceptional, it is better to

des systèmes et réseaux d'information. Vers une culture de la sécurité[6], 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 évaluation 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;
- **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.

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.

have a legal framework that focuses on the conditions to be met when delivering services online, and on the guarantees that have to accompany the establishment of spaces where personal data circulates. At the legal level, the network spaces in which personal information circulates have to be regulated by rules that stipulate how responsibilities are shared. In short, rules have to be established to identify who is accountable for information shared in the network.

When data is in information environments that are accessed by a number of departments, agencies or public bodies, restrictions on collection and prohibitions on circulation no longer suffice to protect privacy. Real protection requires strict regulation of when it is legal to access information and how data may be used. This entails the need to **dissociate possession of information from the right to access and use it**.

In most integrated service delivery models, information is in principle available to the body that initially gathered it. However, part or some components of the information can be available to other bodies, so it is important to control access rights. None of the bodies should be able to access information except for legitimate reasons that are necessary for the service delivery in question.

Of course, though the information may be held in an environment to which a number of bodies have access, that in itself does not give the bodies access rights to it. **The accent is thus shifted towards the right to use personal information and away from the possession or holding of that information.** Thus, there is a dissociation of the physical holding of information by a body and the body's right to access and use it. If it shares a networked area, then a department or agency holds a set of data together with other bodies. However, it does not have the right to access the information unless specific conditions are fulfilled.

Protection measures should thus be designed to ensure that personal information is truly used for legitimate purposes; their goal should not be to prevent data circulation. By regulating the access rights of departments and agencies to information in an environment, protection can be strengthened without immobilizing personal data.

1. A shared area: definition

The notion of a **shared personal information area** can be defined as follows:

> An information environment in which personal information required to deliver a set of services to individuals can be made available to various bodies. The services or benefits are

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 quelques 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.*[7]

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.*[8]

complementary and providing them requires information held by a number of departments and other bodies.

The notion covers a set of mechanisms controlling the circulation of information and delimiting the uses that can be made of it. The purpose is to structure the space in which information can circulate by establishing a framework that defines rights and responsibilities pertaining to personal information located in a network.

In most integrated service delivery models, required information is in principle available to the body that initially gathered it. However, part or some components of the information can be available in other departments or agencies. Thus, access rights have to be defined. No organization should be able to access the information for any reason other than purposes that are legitimate and necessary for delivering the benefit in question, and nothing more.

Safeguards thus have to be designed not to prevent the circulation of personal information but to ensure that it is used for legitimate purposes.

2. Creation of shared areas

Establishing a shared personal information area necessarily requires co-operation among bodies that deliver complementary services. Such co-operation also has to be part of the general service delivery framework.

The circulation of personal information in networks raises concerns. It will be accepted and considered legitimate only if the public is confident that the information is protected and used only for the purposes stated.

Shared personal information areas can be employed in the delivery of both universal benefits for all individuals and limited, targeted services for only a few hundred people. In order to be appropriate for such a wide range of situations, the consultation process has to include both large-scale debates on social issues and more targeted projects concerning more limited stakes. A flexible consultation process should be preferred over one that is so cumbersome that it would be virtually impossible to establish shared areas.

Many different shared personal information areas are possible. Depending on the activities in which the information is used, different issues can arise. The prospect of establishing shared personal information areas raises various fears, and people assess dangers and risks differently.

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 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.

C. Un concept pour assurer l'effectivité du droit de la protection des renseignements personnels dans les réseaux

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

We need a legal framework that can cover a great variety of possible areas in which personal information can be held and circulate. Circulation spaces have to be delimited in accordance with the risks and stakes that are considered acceptable following a public consultation process. The purpose of such a process has to be to openly describe the stakes, advantages and precautions related to planned electronic service delivery and information sharing.

There are analogies between privacy protection problems and other social issues on which public consultation is deemed necessary. Such analogies can be used to identify possible approaches and processes for public consultation on the establishment of shared personal information areas.

3. The legal framework

In order to delimit shared areas, we have to identify different levels of protection that should be implemented in accordance with the degree of sensitivity of the personal information. Public information has to be distinguished from personal information that does not include names, nominative information and information that is sensitive, in other words, that touches the heart of an individual's private life.

The legal framework has to respect the basic principles of privacy protection. The principles are not only stated in legislation but also follow from international documents with which we have to comply. The framework has to provide protection at all levels, and ensure that only authorized information is used in electronic service delivery.

Those responsible and their responsibilities have to be identified. It must always be possible to know who is accountable for the personal information in the shared area, as well as the related responsibilities. Thus,

- The shared area has to be established through a public agreement that is first subject to consultation; its implementation has to comply with the conditions contained in an executive order;
- The public process has to ensure transparency, and public and adversarial assessment of issues and risks. Every time there is interaction, individuals have to be informed or given access to information on what happens to their personal information.

Departments and other bodies should be able to change a shared area so as to provide optimal service delivery and carry out their mandates in compliance with legislation and regulations. Major changes must also be submitted to the process applying when the shared area is created.

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 les 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 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

As a regulated space, a shared area necessarily has to be defined by the purposes of the family of services and benefits for which it is established. Individuals have to be informed of its purpose, scope and content. A list of possible ways that the information could be used should always be available online or elsewhere.

Such circulation spaces have to be delimited by protective measures that are both physical and software-based, as well as by access rights and authorization. The spaces must be controlled in accordance with the content of the information circulating, and information that can legitimately appear must be differentiated from and that which cannot.

A department or agency should have access to a shared area only if the electronic service delivery procedures require that the personal information be disclosed (or made available) to the individual concerned on demand or every time a decision has to be made concerning him or her. The person can then challenge use of the information if it is ambiguous or inappropriate.

Acts and agreements pertaining to the establishment of a shared personal information area should include provisions on the following:

- The purposes for which information in the area can be used;
- The categories of persons who can access information and the nature of their access rights;
- The conditions on use of information;
- The means by which personal information is verified with the people concerned when a decision is to be made;
- The responsibilities of the bodies that are partners in the shared personal information area.

Moreover, the area should be protected by a set of specific measures in its founding agreement. The protective measures should include:

- Control of access rights, which is *a priori* contained in the obligation to establish a policy and list of access rights, and *a posteriori* by the systematic or random verification of access and, for some sensitive information, verification of the daily access log;
- Auditing of decisions made on the basis of information;
- Verification of the information to be used to provide public services.

The conditions for establishing shared areas have to provide for a system for managing legitimate access to data. This has to be done both for the government body as a whole and for the individuals working for it. Access has

d'information, la protection sera mieux assurée sans pour autant immobiliser les renseignements personnels.

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 fait. 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 relatives à l'information sur les personnes lorsque celle-ci 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 recueillie 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.

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

to be lawful given the purpose for which the information is sought and in accordance with the user's general or specific consent.

The agreement has to identify the obligations of the entities that control the information and the obligations of those who have the right to access it. The physical or legal holder of the information has to verify access rights.

The agreement that creates the shared area should identify the means that will be employed to ensure secure information circulation in the area. The agreement can even require the consent of the individual concerned before access is granted to some kinds of information. Such consent has to have its real meaning: it has to entail that a person confers a real right of control over some information that he or she is not required to disclose by law. In short, on the legal level, the shared area is a regulated space, whereas on the technological level is it a space with norms.

4. Responsibilities

A shared area is a virtual space composed of information deposits and communications relays. Every party to an agreement concerning a shared area can be considered the legal holder of the information in the area. As soon as one controls personal data, one is accountable for it.

In this respect, every department and agency is responsible for the confidentiality of information. If there are multiple departments and agencies, their shared area agreement has to stipulate how the responsibility is divided among the parties.

In a shared area, there are those who create information, those who control it and those who use it to make decisions. The responsibilities of the various stakeholders do not depend on their official role but rather on the degree of control that they exercise or are supposed to exercise over information and communication in the networks or parts of networks in question.

Controlling information entails duties. The duties are incumbent on those who produce information and those who process it. However, the duties are different depending on whether one controls the information or simply has knowledge of it.

When a body controls personal data, it has to be able to preserve data integrity, ensure that access is allowed only to those who have the right, and see that changes to the data are in compliance with the law. Naturally, it has to

et considérée comme légitime à la condition que le public ait confiance 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.

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

establish security measures and other precautions to ensure that the information is preserved.

Thus, those who control information are generally accountable for it. Stakeholders that have no control over the information nonetheless have responsibilities that flow from their knowledge of the data. They have to shoulder those responsibilities. However, passive intermediaries, such as those acting as conduits, are in principle not responsible for the actions of others when the documents are simply conveyed or preserved in the normal course of transmission and only for the time required to ensure effectiveness.

Conclusion

A system that relies on redundant measures to protect privacy is vulnerable to being completely defeated by the changes that will inevitably occur in information management. It is therefore crucial to update the means by which privacy and personal information is protected. The means have to be appropriate to the features of network environments. Simply extending the regulatory methods used in a hierarchical model of government is probably the surest way to weaken privacy protection.

In this paper, we have presented a possible approach to personal data protection law based on the imperatives, requirements and risks of network environments.

This approach allows us to conceptualize and situate the processes and principles that have to be established in order to offer online public services that require access to and processing of personal information. By instituting a mechanism that regulates and controls access to personal data by every partner in a network, better protection can be provided for personal information and all stakeholders can be made more accountable.

Networked government requires foundations that are conceptually different from those of paper-based government. In particular, the need for trust plays a considerable role in a world where personal information is available in inter-connected environments. In order to maintain trust between government and individuals, it is important to provide a protection framework in which information about an identifiable person is accessed only for purposes set out in legislation. Since network environments make more frequent interaction possible, it is easier to fulfil the requirement of information quality.

A shared space is a regulated space at the legal level and a space subject to norms at the technological level. This twofold nature forms the basis for the rights and

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

obligations of all partners in e-government. It also allows us to situate the protection that has to be provided for personal data and the respective responsibilities of all those who control them in a network space.

The acceleration of information flows and interactions has consequences on normative frameworks. There is a growing conflict between the speed of network environment activities and the strong desire for stability and conformity in some bureaucratic communities. Privacy protection requires normative frameworks that reflect the speed of operations, not norms that immobilize information on the pretext of protecting it.

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 relative 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.

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 voir 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 que 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.

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.

1. Cette communication reprend des analyses menées dans le cadre de travaux réalisés pour le Secrétariat du Conseil du trésor du Québec de même que le Ministère des relations avec les citoyens et de l'immigration du Québec. Quelques résultats de ces travaux ont été publiés à ce jour. Voir : Pierre

1. This paper reviews analyses conducted for the Québec *Secrétariat du Conseil du trésor* and the Québec *Ministère des*

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 >.

2. Paul M. SCHWARTZ, « Privacy and Democracy in Cyberspace », (1999) 52 *Vanderbilt L.R.*, 1609-1702, pp. 1621-1632.
3. Pierre TRUDEL, « Quel droit et quelle régulation dans le cyberespace ? », *Sociologie et sociétés*, vol. 32, no 2, automne 2000, 189-209. < http://www.erudit.org/erudit/socsoc/v32n02/trudel/trudel.pdf >
4. 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.gfi-nb.com/cgibin/OECDBook Shop.storefront/EN/product/932002012P1 >.
5. 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.
6. 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.
7. Michel DORAIS, « L'évaluation environnementale : les conséquences de l'émergence de la démocratie procédurale, » *Optimum*, hiver 1994-1995, pp. 38-41, p. 38.
8. Christine NOIVILLE, *Du bon gouvernement des risques*, Paris, PUF, « Les voies du droit », 2003, p. 120.

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*, written for the Québec *Ministère des Relations avec les citoyens et de l'immigration*, Montréal, March 2003, online at : < http://www.mrci.gouv.qc.ca/publications/pdf/ViePrivee_AdministrationElectronique_Pierre_Trudel.pdf >.

2. Paul M. SCHWARTZ, " Privacy and Democracy in Cyberspace ", (1999) 52 *Vanderbilt L.R.*, 1609-1702, pp. 1621-1632.
3. Pierre TRUDEL, « Quel droit et quelle régulation dans le cyberespace ? », *Sociologie et sociétés*, vol. 32, no 2, automne 2000, 189-209. < http://www.erudit.org/erudit/socsoc/v32n02/trudel/trudel.pdf >
4. OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, Paris, OECD, 2002, <http://www.oecdpublications. gfi-nb.com/cgibin/OECDBook Shop.storefront/EN/product/ 932002012P1>.
5. OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, Paris, OECD, 2002, <http://www.oecdpublications. gfinb.com/cgibin/ OECDBook Shop.storefront/EN/product/ 932002012P1.
6. ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, *OECD Guidelines for the Security of Information Systems and Networks : Towards a Culture of Security*, 2002, www.oecd.org/dataoecd/16/22/15582260.pdf.
7. Michel DORAIS, " L'évaluation environnementale : les conséquences de l'émergence de la démocratie procédurale ", *Optimum*, Winter 1994–1995, pp. 38–41, p. 38 [our translation].
8. Christine NOIVILLE, *Du bon gouvernement des risques*, Paris, PUF, "Les voies du droit", 2003, p. 120 [our translation].