

# **Renforcer la protection de la vie privée dans l'État en réseau :**

## **l'aire de partage de données personnelles**

**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**

---

### **Résumé**

L'administration électronique suppose la circulation accrue d'informations sur les personnes. 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'utilisateur; 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.

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.

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.

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. L'aire de partage est établie par une entente à la suite d'un processus public au cours duquel les enjeux et risques sont ouvertement débattus. Elle comporte des garanties conséquentes et situe les responsabilités des entités étatiques participantes.

## Introduction

La migration dans les réseaux de plusieurs activités et services publics requiert de revoir les notions permettant d'assurer la protection des informations relevant de la vie privée<sup>1</sup>. La question du cadre juridique appliqué aux espaces d'interactions résultant de la virtualisation est un enjeu central du développement du e-gouvernement. Il faut concevoir des règles pour faire en sorte que les informations personnelles soient protégées où qu'elles se trouvent au sein d'un réseau voué aux interactions État-citoyen. La protection de la vie privée doit désormais se fonder sur des repères organisationnels et spatiaux capables de rendre compte du fonctionnement des espaces de réseaux. Il faut des règles capables d'assurer l'encadrement des conduites dans des lieux virtuels insensibles aux frontières ou organigrammes et non plus au sein d'organismes publics considérés isolément les uns des autres.

Dès lors que la circulation de données personnelles entre les organismes publics cesse d'avoir un caractère exceptionnel, il vaut mieux disposer d'un cadre juridique résolument axé sur les conditions à respecter lors du déploiement de prestations de services en ligne. Il faut aussi des garanties lors de la mise en place des espaces de circulation des données personnelles. Au plan juridique, les espaces-réseaux dans lesquels circulent des données personnelles doivent être encadrés par des règles précisant les responsabilités de l'ensemble des entités concernées. En somme, il s'agit de mettre en place les règles désignant celui qui répond des informations ainsi partagées en réseau. Pour ce faire, il importe de revoir les prémisses sur lesquelles reposent la plupart des lois sur la protection des données personnelles. Ces textes ont, pour la plupart, été adoptés à l'époque où l'information était centralisée. On visait alors à contenir les velléités de surveillance 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<sup>2</sup>. 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. Il est donc nécessaire de penser la protection des données personnelles suivant un modèle conséquent.

---

<sup>1</sup> Ce texte 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 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](http://www.mrci.gouv.qc.ca/publications/pdf/ViePrivee_AdministrationElectronique_Pierre_Trudel.pdf) >.

<sup>2</sup> On ne traite pas ici du droit des forces de police d'accéder aux données. Selon les lois actuelles, les forces de police peuvent pratiquement obtenir la plupart des renseignements qui sont nécessaires à la lutte contre le crime. L'approche présentée ici n'accroît pas les pouvoirs policiers.

## A. E-gouvernement et nouvelles circulations de l'information

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'utilisateur; il facilite la collaboration et le travail coopératif entre une pluralité d'acteurs de statut différent. Il facilite la spécialisation flexible se fondant sur l'échange entre des pôles interagissants.

Le cadre juridique actuel postule le caractère exceptionnel des transferts de données personnelles sans le consentement des personnes visées. En dépit de ce caractère exceptionnel, force est de constater que les transferts de renseignements personnels sont considérables entre certains organismes publics. Dans la plupart des pays, le partage de renseignements est autorisé mais généralement de façon à augmenter la duplication de données d'un organisme vers l'autre. Cette approche encourage la duplication et, compte tenu de la persistance de l'information, accroît la quantité de renseignements personnels détenus par les Administrations.

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. 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'attendent 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. 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. 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 devant être informés du changement.

L'État tendra à adopter un fonctionnement qui visera à prendre avantage des environnements en réseaux<sup>3</sup>. Une structure arborescente et collaborative tendant à se substituer à la structure hiérarchique caractérisant les organisations bureaucratiques. 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.

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. Pour l'information qui

---

<sup>3</sup> Voir par exemple pour la France, le *Plan stratégique de l'administration électronique 2004-2007*, du Ministère de la Fonction publique, de la réforme de l'État et de l'Aménagement du territoire, <[http://www.adae.gouv.fr/article.php?id\\_article=315](http://www.adae.gouv.fr/article.php?id_article=315)>.

est 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 de savoir si une donnée 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 chaque situation spécifique.

## 1. L'impératif de confiance

Tout au long du cycle de traitement de l'information, il faut garantir un environnement dans lequel l'utilisateur/citoyen est en confiance. Les traitements doivent se faire en pleine transparence. En informant l'utilisateur de ce qu'il advient de l'information qu'il confie à l'État, on tisse un lien de confiance. Plus les informations sont sensibles, plus il faut multiplier les précautions afin de garantir le niveau de confiance conséquent. Lorsque des garanties sont données, il faut impérativement que des mesures appropriées en assurent le respect.

La mise en en place de l'environnement en réseau doit découler 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 données personnelles, il importe que tous les enjeux, toutes les appréhensions soient pris en considération. Les questions que se posent les citoyens doivent recevoir des réponses.

Christine Noiville écrit 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.<sup>4</sup>*

Ce qui préoccupe 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 veut être rassuré à l'égard des précautions, des analyses d'impacts et des mesures de contrôle qui préviendront les possibles dérives.

Pourtant, 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

---

<sup>4</sup> Christine NOIVILLE, *Du bon gouvernement des risques*, Paris, PUF, « Les voies du droit », 2003, p. 120.

publique. Il permet un débat éclairé sur les choix à faire et un regard critique sur les choix qui ont été faits.

## 2. Une lecture actualisée des principes de protection des données personnelles

Dans l'État en réseau, les informations sont essentiellement circulantes, disponibles au moment où elles doivent l'être pour accomplir une prestation de service. Cette circulation nécessite des précautions car les potentialités d'accumulation et de couplage des informations peuvent s'accroître. Une protection située au niveau des accès par les Administrations procure une protection de beaucoup supérieure à celle que l'on peut espérer des régimes actuels.

La détention dans un environnement d'information accessible à une pluralité d'organismes publics, afin de leur permettre d'assurer seuls ou en partenariat un ensemble de services aux citoyens n'est envisageable que si de fortes garanties assurent la protection de la vie privée. La formulation d'un tel cadre juridique suppose une lecture actualisée des principes fondamentaux de la protection des renseignements personnels s'avère nécessaire. Les principes énoncés par l'OCDE<sup>5</sup> prescrivent la limitation en matière de collecte, la spécification des finalités, la transparence dans le traitement, la participation individuelle, l'assumption de la responsabilité résultant du traitement, la limitation de l'utilisation, des garanties de qualité des données de même que des garanties de sécurité.

La **limitation en matière de collecte** suppose la mise en place de processus décisionnels qui feront usage du minimum d'informations personnelles nécessaires afin d'assurer les prestations ou la prise de décision. Il faut être en mesure de justifier le pourquoi de la collecte de chaque renseignement personnel.

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

La règle empêchant la circulation et la réutilisation des informations pour le motif que celles-ci pourraient être détournées de leur finalité, doit être relue dans le contexte de dialogue accru que permet le réseau. Plus que jamais, l'Administration est en mesure d'indiquer à chaque administré quelles sont les informations qu'il possède sur son compte,

---

<sup>5</sup> 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/cgi-bin/OECDBookShop.storefront/EN/product/932002012P1>.

lesquelles il entend utiliser afin de prendre une décision. Le citoyen est désormais en mesure d'interagir et d'exiger le retrait et l'ajout d'informations.

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

Le principe de finalité pose que l'on ne peut recueillir et utiliser les renseignements personnels que pour des fins compatibles avec celles de la collecte initiale. Le principe de finalité est lié au maintien de la qualité de l'information. Dans les principes de l'OCDE, cette exigence est 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.<sup>6</sup>*

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

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

Il faut que l'information sur les **finalités** des informations détenues soit constamment disponible et portée à la connaissance de l'utilisateur lors de chaque collecte. Pour respecter le principe de la limitation de l'utilisation, les environnements d'information devraient desservir des familles délimitées de prestations : ce qui assure que les renseignements

---

<sup>6</sup> 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/OECDBookShop.storefront/EN/product/932002012P1>>.

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'utilisateur 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.

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

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

À cet égard, le principe de la **participation individuelle** de la personne concernée dans les décisions relatives au traitement des renseignements personnels acquiert dans les réseaux une portée renouvelée. Dans les réseaux, il est possible de présenter l'information que l'on 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.

S'agissant de la **responsabilité**, chaque organisme public susceptible d'accéder à des données personnelles au sein d'un réseau peut être considéré comme en étant le détenteur juridique. À ce titre, chaque organisme est responsable de la confidentialité des renseignements et l'ensemble des organismes en répondent solidairement. Comme il y a pluralité d'organismes, ces derniers auront à déterminer comment se répartiront les responsabilités de l'un et l'autre des participants.

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

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

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

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

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

## **B. Le concept d'aire de partage**

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

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

Au plan juridique, l'aire de partage est un espace régulé. Au plan technique, c'est un espace normé. Elle 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 se trouvent à en avoir la maîtrise au sein d'un espace en réseau.

## **1. Le processus de création**

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 de services envisagées.

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.

Les échanges d'informations relatives aux personnes emportent des appréciations diversifiées des risques qui pourraient résulter de la mise en place des aires de partage. Les espaces de circulation seront délimités en fonction des risques et enjeux jugés acceptables à la suite d'un processus de consultation publique. 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. 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.

## **2. Le régime juridique**

Le régime juridique doit nécessairement respecter les principes fondamentaux en matière de protection des données personnelles. 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 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, 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.

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

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

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

- les finalités auxquelles peuvent servir les informations incluses dans l'aire;
- les catégories de personnes qui peuvent avoir accès aux informations de même que la nature de leur droit d'accès;
- les conditions d'utilisation des informations;
- les moyens par lesquels les informations personnelles sont validées auprès des personnes concernées lors d'une décision;
- 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.

Il faut aussi prévoir un régime de gestion des conditions moyennant lesquelles un organisme et les individus qui y oeuvrent peuvent accéder aux données. 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'utilisateur.

L'acte 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 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.

Dans une aire de partage, les responsabilités découlent du degré de maîtrise exercé sur l'information. 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

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.

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.

## **Conclusion**

L'état en réseau a des fondements qui se conçoivent de façon différente de ceux 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.

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. Une véritable protection de la vie privée nécessite un cadre juridique évitant la duplication des renseignements personnels. Dans le contexte où les services de l'État fonctionnent en réseau la loi devrait autoriser l'accès conditionnel et balisé aux données détenues en quelque point du réseau à la condition que cet accès soit autorisé par la loi et que cela n'emporte pas de copie persistante de l'information.

Les aires de partage sont un modèle possible d'évolution du droit de la protection des données personnelles reflétant les exigences et risques caractérisant les environnements en réseaux. Ce modèle permet de penser et de situer les principes et les processus à mettre en place lorsque vient le temps d'assurer en ligne des services publics nécessitant le traitement de données personnelles. En instituant un mécanisme qui régule et contrôle les accès aux données personnelles par toute entité partenaire dans un réseau, on accroît l'effectivité de la protection de la vie privée tout en favorisant une meilleure responsabilisation de l'ensemble des acteurs.