

De la «surveillance» à la qualité : les fondements actualisés du droit de la protection des données personnelles dans le gouvernement en ligne

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

Table des matières

Introduction - Un paradigme catastrophiste	1
A- Vers des fondements mieux ciblés	3
1. Une fuite en avant : de la vie privée à la « vie personnelle »	6
2. Les véritables activités de surveillance demeurent.....	8
B- Les garanties de la qualité des informations personnelles	9
1. La maîtrise des données personnelles.....	10
2. Une régulation pour renforcer la confiance.....	11
a) L'impératif de confiance	11
b) Une lecture actualisée des principes de protection des renseignements personnels.....	13
Conclusion - Assurer l'effectivité du droit de la protection des renseignements personnels dans les réseaux	17

Introduction - Un paradigme catastrophiste

Le droit de la protection des données personnelles s'est construit sur les frayeurs suscitées par les technologies de l'information. Rituellement, la plupart des exposés des justifications des règles de droit en cette matière commencent par des considérations sur le potentiel liberticide des technologies de l'information. On escompte que le potentiel d'abus sera nécessairement et

universellement réalisé pour justifier un cadre juridique qui est supposé protéger les personnes contre les périls, voire les apocalypses, que laissent craindre les technologies de l'information pour les libertés.

Lorsqu'elle est appliquée à l'analyse des enjeux des services gouvernementaux en ligne, cette approche des technologies de l'information complique les analyses et réflexions. Elle prive d'une analyse qui donnerait lieu à la mise en place de cadres juridiques plus adéquats pour assurer l'implantation des services publics en ligne en améliorant effectivement la protection de la vie privée.

D'entrée de jeu, il faut disposer des arguments relatifs à la surveillance policière. La plupart des craintes à l'égard de l'usage des technologies de l'information concernent les opérations de surveillance policière. On invoque les risques très réels d'abus policiers pour justifier le renforcement et souvent la bureaucratisation du droit de la protection des données personnelles. Pourtant, les informations que peuvent obtenir et détenir les forces de police et autres forces de sécurité échappent à toutes fins pratiques à la portée des lois sur la protection des renseignements personnels. Dans certains cas, les instances de surveillance compétentes en matière de données personnelles ont le pouvoir d'exercer une surveillance sur les pratiques policières.

Hormis l'accroissement des pouvoirs de police et des dérives qui peuvent en résulter, on ne retrouve que quelques incidents ayant eu pour conséquence de laisser circuler des informations personnelles de façon inappropriée. Mais c'est en vain que l'on cherchera, dans les Administrations, des pratiques généralisées de surveillance des personnes, sauf à étendre le sens du mot surveillance.

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

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

À une époque où se généralise l'usage des technologies de l'information, il faut des fondements plus solides et mieux ciblés. On ne peut se limiter à reconduire indéfiniment les frayeurs d'une époque où l'on confondait l'usage des technologies avec les usages abusifs dont elles peuvent

faire l'objet. Le prix à payer pour des mesures aussi mal ciblées pourrait être un affaiblissement des protections de la vie privée. Par contre, il y a des écueils —réels ceux-là— qui doivent être pris en compte afin de disposer de réseaux assurant une réelle protection des personnes.

A- Vers des fondements mieux ciblés

Les analystes qui ont jeté un regard critique sur l'informatisation ont adhéré, pour la plupart, au paradigme de la surveillance. Pour eux, l'informatique accroît les possibilités de surveillance des personnes. Là résideraient ses effets liberticides. Le mouvement de la protection des renseignements personnels est largement issu de cette mouvance. Plusieurs analyses des enjeux et risques relatifs aux traitements des données personnelles sont essentiellement fondées sur des craintes et des extrapolations. Daniel J. Solove constate le caractère inadéquat des appréhensions à leur égard. Il écrit que :

*Although the problem of databases is understood as one concern over privacy, beyond this, the problem is often not well defined. How much weight should our vague apprehensions be given, especially considering the tremendous utility, profit and efficiency of using databases?*¹

Solove répond à cette question en soutenant que :

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

Dans les imaginaires intellectuels des années soixante, les problèmes engendrés par le traitement de l'information relative aux personnes se fondent sur la métaphore du *Big Brother* telle qu'elle est utilisée dans le roman *1984* de George Orwell. Une littérature foisonnante justifie la nécessité des lois sur la protection des renseignements personnels en se fondant sur les possibilités que s'instaure une société de surveillance semblable à celle décrite par Orwell dans son célèbre roman. On porte moins attention aux passages du roman, pourtant tout aussi inquiétants, où des armées de copistes réécrivent l'histoire, y effaçant les noms de ceux qui sont disparus et qui donc n'ont jamais existé !

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

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

¹ Daniel J. SOLOVE, « Privacy and Power : Computer Databases and Metaphors for Information Privacy, » [2001] 53 *Stanford L. R.*, 1393, p. 1395.

publiques...), la lutte contre les fraudes, la prévision. Pratiquement toutes les actions administratives passent par un fichage.²

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

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

Le danger provient du caractère inadéquat, équivoque, imprécis, disproportionné de l'information collectée parfois de manière déloyale par rapport à une finalité critiquable qui peut s'abriter derrière un argumentaire la présentant de manière favorable.³

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

La pratique démontre qu'il n'y a pas de données anodines et que la notion de données sensibles (santé, opinion politique ou syndicale, vie privée) définie a priori doit être considérée de manière relative; après tout, les sociétés de vente par correspondance ne demandent pas l'âge de leurs clientes car cela est mal perçu; mais grâce aux tables d'attribution des prénoms de l'INSEE, elles déduisent avec une forte probabilité l'âge des personnes.⁴

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

² André LUCAS, Jean DEVEZE et Jean FRAYSINNET, *Droit de l'informatique et de l'Internet*, Paris PUF coll. Thémis Droit privée, 2001, p. 10.

³ André LUCAS, Jean DEVEZE et Jean FRAYSINNET, *Droit de l'informatique et de l'Internet*, Paris PUF coll. Thémis. n° 18.

⁴ André LUCAS, Jean DEVEZE et Jean FRAYSINNET, *Droit de l'informatique et de l'Internet*, Paris PUF coll. Thémis n° 19.

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

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

Ainsi, les usages abusifs ou incompetents d'information sont invoqués pour justifier un régime juridique qui multiplie les tracasseries bureaucratiques sans pouvoir effectivement protéger la vie privée. Mais si on voulait demeurer cohérent, on viserait à penser un cadre juridique protégeant des usages incompetents de l'information plutôt que multiplier les obstacles à sa circulation.

Les dangers découlant des traitements de données personnelles sont perçus à deux niveaux. Au niveau des représentations globales, on évoque le spectre de la surveillance. Mais comme il est généralement difficile de donner de la substance, de documenter les situations où la surveillance aurait été effectivement faite à partir de banques de données, on évoque en fait les problèmes mettant en cause la qualité des données pour justifier la protection des renseignements personnels. Ce phénomène de glissement met en lumière le caractère inadéquat du paradigme de la surveillance inspiré du roman *1984* de Georges Orwell afin de justifier les mesures de protection des renseignements personnels. Par contre, il révèle un autre paradigme, beaucoup plus pertinent : celui du roman de Kafka *Le Procès*. Ce qui pose problème ce n'est pas tant le risque de surveillance mais bien l'utilisation inadéquate, incompetente, aveugle de données personnelles. Dans le contexte de l'État fournissant des services aux citoyens, c'est le fait que les conclusions soient tirées de données qui ne présentent pas les qualités requises pour y donner ouverture qui est le danger redouté. En somme, c'est la façon dont l'information est utilisée, la question de savoir si elle possède les qualités appropriées aux usages qu'on veut en faire qui pose des difficultés et qui appelle un cadre de gestion et de protection.

Dans un monde où presque toute l'information est susceptible de circuler en réseau, il devient impossible de s'en remettre à une approche postulant de possibles utilisations fautives des informations. À la limite, aucune information ne pourrait circuler puisque toutes sont susceptibles d'usages abusifs ou inappropriés. Plutôt que persister dans une telle approche restrictive, il faut renforcer les règles afin d'assurer que seule l'information présentant les qualités requises sera utilisée afin de prendre des décisions plutôt que de prétexter le risque d'usages maladroits, incompetents ou malhonnêtes d'informations pour prohiber *a priori* la circulation d'information. En somme, il faut abandonner le paradigme du « Big Brother » et passer au paradigme du « Procès ».

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

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

En soi, un très grand nombre d'usages d'informations personnelles ne sont pas une violation de la vie privée. La notion même de vie privée reconnaît que la vie sociale suppose des interactions faisant usage d'informations sur les personnes⁵. Seules sont sanctionnées les collectes, usages et diffusions fautives de telles informations. Il est en effet difficile de justifier, au nom de la vie privée, les mesures relatives à certaines informations dont la circulation est inhérente à la vie sociale. C'est probablement pour cette raison que certains se sont rabattus sur une notion extrêmement vague et d'une ampleur encore indéterminée : la notion de vie personnelle. Cela paraît découler des difficultés conceptuelles découlant de la fragilité des fondements sur lesquels reposent les mesures de contrôle des informations personnelles ne se rattachant pas à la vie privée.

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

D'où cette revendication pour la reconnaissance d'un « droit à la vie personnelle ». C'est ainsi que Frayssinet fait valoir que « l'atteinte ne concerne pas que la vie privée [...] mais tous les aspects de la vie personnelle »⁶.

Il en résulte une kyrielle de revendications ayant l'apparence d'une quête généralisée d'un droit de veto à l'égard de toutes les informations sur les personnes, y compris celles qui étaient il n'y a pas si longtemps perçues comme relevant des inconvénients normaux de la vie en société. Par

⁵ André BERTRAND, *Droit à la vie privée et droit à l'image*, Paris, Litec, 1999, no. 26.

⁶ Jean FRAYSSINET, « La protection des données personnelles est-elle assurée sur Internet ? », Texte présenté au colloque international *Droit de l'Internet, approches européennes et internationales*, septembre 2001, <http://droit-internet-2001.univ-paris1.fr/pdf/vf/Frayssinet.pdf>. Voir aussi André LUCAS, Jean DEVEZE et Jean FRAYSSINET, *Droit de l'informatique et de l'Internet*, Paris – PUF. coll. Thémis - Droit privé, 2002, n° 50.

exemple, on invoque le droit de ne pas recevoir des dépliants publicitaires, etc. ou de sollicitations par courriel. Ces craintes, en partie justifiées, entraînent des revendications pour mettre en place des contrôles à l'égard de toutes sortes de situations mettant en cause des informations personnelles. La crainte que les informations soient utilisées de manière inadéquate porte à rechercher une protection pour toutes les informations relatives à une personne. Ainsi, l'on commence, au nom d'un droit à la vie personnelle, à demander de censurer les fichiers publics tels ceux des archives des journaux. Le droit à la vie personnelle est en passe de devenir un motif pour réécrire l'histoire : celui qui est gêné à propos des événements publics auxquels il a été mêlé va exiger que l'on purge les archives des traces des événements public auxquels il a été mêlé.

À bien des égards, les revendications pour renforcer la protection des renseignements personnels sont parfois devenues des revendications pour protéger d'inconvénients inhérents à la vie sociale, non pour assurer la protection de la vie privée. C'est une approche incompatible avec les exigences d'une société démocratique car elle nie l'exercice des autres droits fondamentaux comme la liberté d'expression ou les exigences de saine gestion des services publics.

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

Au surplus, la notion de « vie personnelle » laisse peu de place aux impératifs de la vie en société, au fait que l'information doit pouvoir circuler et que cette circulation, en pratique, est rarement préjudiciable. Si tout n'est qu'affaire de choix individuels, il reste peu de place pour la circulation de l'information qui répondrait à des impératifs de la collectivité. Enfin, si toutes les activités humaines significatives supposent désormais l'usage des réseaux, il faudra bien convenir qu'il faut un cadre juridique suffisamment nuancé pour assurer les équilibres entre les divers droits mis en cause dans les interactions sociales. C'est sans doute dans ce contexte que la notion de « vie personnelle » paraît une notion trop rudimentaire pour servir de cadre de réflexion. Pire encore, par la négation des autres valeurs inhérentes à la démocratie qu'elle comporte nécessairement, la notion recèle une tendance au totalitarisme de même qu'au recul de l'état de droit.

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

2. Les véritables activités de surveillance demeurent

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

Le phénomène de la surveillance sur les lieux de travail illustre des contradictions de l'approche actuelle en matière de protection des renseignements personnels. Dans une décision, la Cour d'appel du Québec confirmait que les employeurs peuvent, lorsqu'ils ont des motifs sérieux, surveiller leurs employés, même dans leur vie privée⁷. La même contradiction se retrouve dans la jurisprudence de la Commission d'accès à l'information. D'une part, celle-ci a jugé qu'une municipalité ne pouvait recueillir des informations sur support vidéo car l'enregistrement des images captées par des caméras de surveillance n'apporte rien de plus à la protection du public que ce que la simple présence des caméras n'assure déjà⁸. Par contre, la Commission a reconnu qu'un organisme public peut recourir aux services d'un enquêteur et capter des images d'un employé afin de vérifier si celui-ci s'adonne à des activités incompatibles avec son état de santé⁹. Le paradoxe est troublant : la surveillance est *a priori* fautive. Mais elle devient licite lorsque l'on peut faire valoir des motifs, même d'intérêt privé, pour la légitimer après-coup. En somme, il est interdit de surveiller les personnes sauf si cette surveillance permet de recueillir des informations révélant un comportement fautif de la personne surveillée. On conviendra en effet que si une surveillance ne révèle rien de fautif, il y a fort peu d'intérêt à s'y livrer! Alors, c'est peut-être qu'elle n'est pas si illicite que cela!

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

⁷ *Syndicat des travailleurs de Bridgestone-Firestone de Joliette (CSN) c. Me Gilles Trudeau/Firestone Canada inc.*, CA Montréal, 30 août 1999, J.E., 99-1554.

⁸ *Ligue des droits et libertés et ville de Sherbrooke*, Rapport d'enquête du 25 novembre 1992.

⁹ *Eppell. C. Commission de la santé et de la sécurité du travail*, [2000] C.A.I., 194. Voir sur cette contradiction : Raymond DORAY et François CHARETTE, *Accès à l'information, loi annotée, jurisprudence, analyse et commentaires*, Cowansville, Éditions Yvon Blais, p. 64-7.

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

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

B- Les garanties de la qualité des informations personnelles

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

Le droit intervient pour identifier la qualité des informations à utiliser. Par exemple, dans plusieurs situations, le droit exige que l'identification des personnes s'effectue au moyen d'informations présentant certains seuils de précision ou garanties de fiabilité. Pour obtenir un passeport canadien, il faut fournir un document de l'état civil, un formulaire et une déclaration d'un répondant. Toutes ces informations visent à assurer la qualité de l'identification de la personne qui demande un passeport. De la même façon, le droit prescrit des seuils de qualité pour autoriser l'utilisation de certaines informations¹⁰.

Au nombre des exigences de qualité technique de l'information les plus souvent mentionnées, il y a l'intégrité technique de l'information. La valeur juridique d'un document, c'est-à-dire sa capacité de constituer une preuve, dépend de son intégrité. Au Québec, l'article 6 de la *Loi sur le cadre juridique des technologies de l'information*¹¹ vient expliciter les critères d'intégrité d'un document, qui sont les mêmes que ceux reconnus habituellement au support papier. En application du principe d'équivalence fonctionnelle, on a transposé les critères qui sont utilisés afin de déterminer ce qui permet de conclure à l'intégrité à l'égard d'un document sur un support papier.

Dans la plupart des situations, la qualité de l'information s'apprécie en fonction du contexte. Une information peut répondre convenablement à un besoin alors qu'elle sera nettement insuffisante,

¹⁰ Pierre TRUDEL, « Law in pursuit of information quality », dans Urs GASSER (ed.) *Information Quality Regulation : Foundations, Perspectives and Applications*, Baden-Baden, Nomos Verlagsgesellschaft, Schulthess, 2004, pp. 91-106.

¹¹ L.Q. 2001, c. 32, en ligne avec annotations à < http://www.autoroute.gouv.qc.ca/loi_en_ligne > .

voire contre-indiquée, dans un autre contexte. Dans le contexte des interactions entre l'État et le citoyen au sein des réseaux, il devient possible d'évaluer, de concert avec la personne concernée, si l'information répond aux exigences qualitatives requises pour la décision qui doit être prise.

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 est renforcée lorsque les processus de décision imposent qu'à chaque fois que l'on entend prendre une décision au sujet d'une personne, on lui présente — en ligne ou autrement — l'information sur laquelle on entend se fonder. Le citoyen se trouve à même de réviser et, le cas échéant, de rectifier les informations personnelles.

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

1. La maîtrise des données personnelles

La protection de la vie privée et des informations personnelles suppose de reconnaître à la personne concernée un droit d'exercer un certain contrôle sur ce qu'il advient des renseignements la concernant. Mais ce droit de contrôle n'a jamais été et ne saurait être absolu. Lucas, Devèze et Frayssinet rappellent qu'« il n'y a pas de vie sociale sans échanges de données personnelles ». Ces auteurs ajoutent qu'« une personne est non seulement un être physique et psychique mais aussi un être informationnel [...] ». Il faut donc poser le principe en convenant de ses limites. Le rapport Truche rappelle que « le principe de maîtrise des données personnelles ne saurait être posé en absolu »¹². La CNIL exprime aussi des réserves au sujet d'un droit de maîtrise des données personnelles en rappelant que ce qui est essentiel, c'est que les données soient de qualité. Dans son 22^e rapport d'activité, la CNIL écrit que :

*Mais ne peut-on soutenir que si le droit d'accès est peu exercé, en pratique, c'est qu'au fond l'essentiel pour nos concitoyens n'est pas tant de vérifier la teneur des données qu'ils ont le plus souvent communiquées eux-mêmes à l'administration concernée, que d'avoir la garantie que ces données ne seront pas détournées de la finalité initiale, communiquées à des tiers qui n'ont pas à en connaître ou leur serait opposables de nombreuses années après.*¹³

Le droit de contrôle des données peut être conçu comme un droit s'exerçant *a priori*. Il peut aussi s'exercer *a posteriori*, lorsqu'un usage inadéquat a été fait d'une information et qu'il convient de

¹² Pierre TRUCHE, Jean-Paul FAUGERE et Patrice FLICHY, *Administration électronique et protection des données personnelles livre blanc*, Rapport au ministre de la fonction publique et de la réforme de l'État, Paris, La documentation française, 2002, p. 77.

< <http://www.ladocumentationfrancaise.fr/brp/notices/024000100.shtml> >

¹³ COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, *22^e rapport d'activités 2001*, Paris, La documentation française, 2002, p. 108,

< <http://www.ladocumentationfrancaise.fr/BRP/024000377/0000.pdf> >.

le rectifier. Ainsi un droit de contrôle *a priori* peut être exercé par la personne concernée à l'égard de toutes les informations personnelles circulant au sein d'un domaine de confiance. Il devrait être possible d'exercer un droit d'accès et de vérification des informations circulant dans un domaine de confiance et d'éventuellement demander des correctifs. Il devrait également être possible, en tout temps, de s'assurer de la qualité des informations utilisées pour prendre une décision à son sujet.

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

2. Une régulation pour renforcer la confiance

La clé du succès de l'administration électronique réside dans sa capacité d'inspirer confiance. Des moyens de protection conséquents doivent être mis en place. Pour exiger légitimement des citoyens qu'ils laissent circuler des informations qui les concernent dans des réseaux, l'État doit être hautement crédible. Il faut donc organiser des espaces virtuels de confiance au sein desquels les informations pourront circuler moyennant des garanties strictes de qualité et des balises en limitant la collecte et les usages¹⁴.

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

a) 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'utilisateur, il faut tenir parole et fournir des garanties solides quant à l'usage possible des informations.

La confiance est un élément essentiel de tout cadre de gestion des informations portant sur les personnes. Tout au long du cycle de traitement de l'information, il faut garantir un environnement dans lequel l'utilisateur/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'utilisateur à l'égard de ce qu'il advient de l'information qu'il confie à l'État, on tisse un climat de confiance. Plus les informations demandées sont susceptibles d'être

¹⁴ Pierre TRUDEL, « Renforcer la protection de la vie privée dans l'État en réseau : l'aire de partage de données personnelles », [2004] 110 *Revue française d'administration publique*, pp. 257-266.

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 quelque 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.¹⁵

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.¹⁶

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.

¹⁵ Michel DORAIS, « L'évaluation environnementale : les conséquences de l'émergence de la démocratie procédurale, » *Optimum*, hiver 1994-1995, pp. 38-41, p. 38.

¹⁶ Christine NOIVILLE, *Du bon gouvernement des risques*, Paris, PUF, « Les voies du droit », 2003, p. 120.

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.

b) 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'OCDE¹⁷ sont les suivants :

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

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

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

¹⁷ 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/OECDBookShop.storefront/EN/product/932002012P1> .

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

Plus que jamais, l'État est en position d'indiquer à chaque administré quelles sont les informations qu'il possède sur son compte, lesquelles il entend utiliser afin de prendre une décision. Le citoyen, ou l'administré, est désormais en mesure d'interagir et d'exiger le retrait et l'ajout d'informations. Par conséquent, la règle empêchant la circulation et la réutilisation des informations pour le motif que celles-ci pourraient être détournées de leur finalité, doit être relue dans le contexte de dialogue accru que permet le réseau.

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

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

*Les données de caractère personnel devraient être pertinentes par rapport aux finalités en vue desquelles elles doivent être utilisées et, dans la mesure où ces finalités l'exigent, elles devraient être exactes, complètes et tenues à jour.*¹⁸

Dans le contexte d'un environnement en réseau, la question des finalités se pose en tenant compte que les informations peuvent être 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'utilisateur.

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

Le respect de la **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. Cette information doit être rappelée lors de chaque collecte. Pour respecter le principe de la limitation de l'utilisation, les environnements d'information devraient desservir des familles délimitées de prestations : ce qui assure que les renseignements personnels 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.

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. De plus en plus, il paraît possible de fonder la protection des personnes sur un droit du citoyen à un dialogue avec les décideurs chargés de déterminer ses droits et obligations.

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

La **qualité des données** s'apprécie à l'égard des prestations et décisions à être accomplies avec les renseignements : il faut garantir que les renseignements utilisés pour rendre le service ou effectuer la prestation sont exacts, précis, autorisés par les lois et ne présentent pas d'équivoque. La légitimité de pareilles circulations d'informations personnelles serait renforcée lorsque les processus de décision imposent qu'à chaque fois que l'on entend prendre une décision au sujet d'une personne, on lui présente — en ligne ou autrement — l'information sur laquelle on entend se fonder. Le citoyen se trouve à même de réviser et, le cas échéant, de rectifier les informations personnelles. Le droit de rectification prend ainsi tout son sens.

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

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

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

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

La **sécurité** tant physique que logique est évidemment une exigence essentielle pour tout environnement de services fonctionnant en réseau. C'est une obligation de l'ensemble des détenteurs de renseignements personnels. Le cadre juridique doit donc fonctionner de manière à inciter les responsables à prendre les mesures afin de garantir la sécurité des informations sur les personnes. Afin de développer une « culture de la sécurité », il importe, comme cela est exprimé dans les *Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information. Vers une culture de la sécurité*¹⁹, 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;

¹⁹ 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.

- **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.

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