

## 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<sup>1</sup> sont les suivants :

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

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

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

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

---

1 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> >.

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.<sup>2</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. 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.

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

---

2 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/cgi-bin/OECDBookShop.storefront/EN/product/932002012P1>>.

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*<sup>3</sup>, que les principes suivants soient pris en considération :

**sensibilisation** : les parties prenantes doivent être sensibilisées au besoin d'assurer la sécurité des systèmes et réseaux d'information et aux actions qu'elles peuvent entreprendre pour renforcer la sécurité;

**responsabilité** : les parties prenantes sont responsables de la sécurité des systèmes et réseaux d'information;

**réaction** : les parties prenantes doivent agir avec promptitude et dans un esprit de coopération pour prévenir, détecter et répondre aux incidents de sécurité;

**éthique** : les parties prenantes doivent respecter les intérêts légitimes des autres parties prenantes;

**démocratie** : la sécurité des systèmes et réseaux d'information doit être compatible avec les valeurs fondamentales d'une société démocratique;

**évaluation des risques** : les parties prenantes doivent procéder à des évaluations des risques;

**conception et mise en œuvre de la sécurité** : les parties prenantes doivent intégrer la sécurité en tant qu'élément essentiel des systèmes et réseaux d'information;

**gestion de la sécurité** : les parties prenantes doivent adopter une approche globale de la gestion de la sécurité;

---

3 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](http://www.oecd.org/dataoecd/58/62/1946930.doc) >.

**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.