CHAPITRE 5

LES CONDITIONS NÉCESSAIRES AU SUCCÈS

Loin de constituer un projet à caractère technologique, le gouvernement en ligne vise d'abord et avant tout à répondre aux besoins des citoyens et des citoyennes du Québec : la technologie n'est pas une fin en soi, mais bien un moyen pour parvenir à améliorer ces services. Il importe que tout soit fait pour que les citoyens puissent développer le réflexe d'avoir recours aux services en ligne et de se prévaloir des nouvelles possibilités d'expression de leurs droits démocratiques. Si le gouvernement n'entreprend pas des actions concrètes en ce sens ou ne continue pas de le faire, le gouvernement en ligne risque de devenir un instrument coûteux et sous-utilisé. Plusieurs facteurs sont déterminants quant à l'adhésion des citoyens au projet (voir schéma 9, p.111).

En premier lieu, la force de la **volonté politique et la structure de gouvernance** qui découle de cette volonté constituent l'élément fondamental au succès du projet du gouvernement en ligne. C'est d'ailleurs afin de marquer cette importance que cet élément a fait l'objet d'un chapitre distinct dans ce rapport. Les principes de gouvernance proposés, de même que les mécanismes d'imputabilité, doivent ainsi être considérés comme partie prenante des conditions nécessaires au succès.

En deuxième lieu, l'adhésion des citoyens repose essentiellement sur la présence d'un **environnement de confiance** associé au déploiement des prestations électroniques de services. Il s'agit d'une condition *sine qua non* pour que les citoyens et les entreprises aient recours aux services en ligne offerts. Le gouvernement se doit non seulement d'établir cet environnement de confiance, mais doit aussi mettre en œuvre les moyens nécessaires pour le maintenir.

Il est certes difficile de déterminer précisément les facteurs qui influencent cette confiance des citoyens ou des entreprises dans l'utilisation des services en ligne ou des projets liés à la démocratie en ligne, ces facteurs étant multiples. Néanmoins, l''environnement de confiance nécessaire au succès du développement de la prestation électronique des services repose essentiellement sur les deux éléments suivants :

1. la présence de mécanismes de protection des renseignements personnels appropriés, et ce, pour les divers types de services en ligne;
2. la présence de mécanismes sûrs et sécuritaires (l'assurance qu'un tiers ne peut interférer dans le processus).

Ces deux éléments doivent être balisés par un cadre institutionnel procurant l'assurance que l'information dans les systèmes informatiques n'est utilisée et qu'on n'y accède que pour des motifs justifiés. Ainsi, la confiance repose aussi sur des fondements juridiques qui assurent, en autres, la protection des renseignements personnels et du droit à la vie privée (voir schéma 10, p. 112). À cet effet, les lois doivent entre autres tenir compte des nouvelles réalités propres au monde virtuel et à l'État en réseau, afin que le gouvernement puisse offrir aux citoyens et aux entreprises des services améliorés, qui tiennent compte des possibilités maintenant offertes par les TIC.

Ainsi, l'étude menée au Québec, en 2003, par le Centre francophone en informatisation des organisations portant sur l'utilisation des services offerts sur l'Internet laisse entrevoir une population préoccupée par un niveau adéquat de sécurité et par la protection des renseignements personnels et du droit à la vie privée. Ceci constitue un frein majeur au déploiement des prestations des services en ligne. En fait, « les craintes relatives à la vie privée et à la sécurité constituent la principale raison pour laquelle un citoyen, une entreprise, ou un

travailleur autonome n'utiliserait pas les services Internet du gouvernement (ces raisons, regroupées, ont été évoqués par 42 % des citoyens utilisateurs, 27 % des entreprises utilisatrices et 33 % des travailleurs autonomes utilisateurs[31] ». La perception des citoyens et des entreprises à l'égard des moyens mis à leur disposition par le gouvernement est donc critique pour le succès du gouvernement en ligne. Pour dissiper les craintes associées à l'utilisation de ces services, il importe que les systèmes informatiques utilisés pour la prestation électronique de services répondent précisément et concrètement aux attentes des citoyens en matière de sécurité et de protection des renseignements personnels et du droit à la vie privée.

En troisième lieu, le projet de gouvernement en ligne vise une **simplicité de l'accès aux services gouvernementaux**. Dans cette optique, il importe, tel que mentionné précédemment, que ce projet de gouvernement en ligne ne soit pas réservé aux seuls citoyens qui ont accès à l'Internet. C'est pourquoi il est nécessaire de développer, de façon complémentaire au portail unique de services gouvernementaux, des centres multiservices permettant d'accéder à l'ensemble des services offerts par le gouvernement, par téléphone, par courrier et au comptoir. Ces centres multiservices visent à orienter plus aisément le citoyen dans ses démarches auprès de l'État, en tenant compte des citoyens qui n'ont pas accès à Internet. Mentionnons, par ailleurs, que cette prise en compte des citoyens qui n'ont pas accès à Internet ne signifie nullement la capitulation du gouvernement quant à la possibilité que ces citoyens évoluent graduellement vers les services en ligne.

C'est pourquoi le gouvernement se doit de faciliter l'accès à l'Internet. Bien que les récents sondages démontrent que le Québec se positionne en tête de liste du classement de l'OCDE en ce qui trait à l'accessibilité d'Internet , il n'en demeure pas moins que 40 % des québécois n'y ont pas accès[32], que ce soit pour des raisons socio-économiques, démographiques ou géographiques. Il est de la responsabilité du gouvernement de combattre cette fracture numérique, en favorisant une possibilité d'accès gratuit à l'Internet et en soutenant les citoyens peu familiers avec les nouvelles technologies afin qu'ils acquièrent les compétences requises. À cet effet, l'établissement d'un partenariat avec les groupes communautaires constitue une piste à privilégier pour faciliter l'acquisition des compétences par les citoyens. Des réalisations qui méritent d'être signalées démontrent qu'il y a là une voie d'avenir. La généralisation de l'accès Internet à large bande, ou à Internet haute vitesse, constitue également l'un des facteurs à considérer dans le processus de démocratisation de l'accès aux services gouvernementaux. Les clientèles présentant des besoins spéciaux, et en particulier, les personnes souffrant d'un handicap moteur, cognitif ou sensoriel, doivent également être prises en compte dans l'ensemble de la démarche gouvernementale.

L'argent des contribuables risque d'être investi en pure perte si le réflexe de privilégier les services en ligne lors des relations avec l'État ne se développe pas. C'est pourquoi, en quatrième lieu, le gouvernement doit assurer une information adéquate afin que **les citoyens et les entreprises soient informés et sensibilisés** aux nouvelles possibilités qu'offrent les TIC. Le gouvernement doit faire la preuve que le recours à ces nouveaux modes de prestation de services se traduit en gains d'efficacité réels. D'une part, les services en ligne vont permettre aux citoyens et aux entreprises d'économiser du temps, de l'énergie, et en bout de piste, de l'argent. D'autre part, la prestation électronique de services va permettre aux décideurs et aux gestionnaires de programmes publics de prendre de meilleurs décisions, grâce à une collecte d'information de qualité, celle-ci se faisant aussi de façon plus rapide, et les informations étant disponibles « juste à temps ». L'amélioration tangible des services doit guider le gouvernement dans une stratégie de développement du gouvernement en ligne.

---

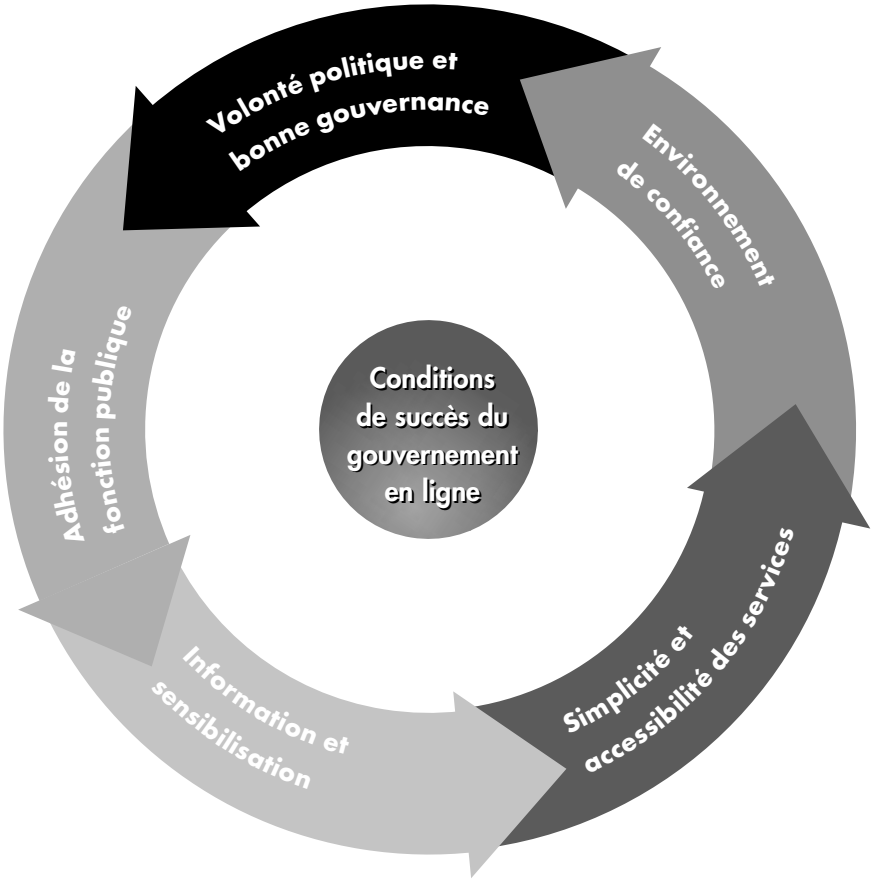
[31] CEFRIO, *NetGouv 2003*, Sondage réalisé auprès des citoyens, des entreprises et des travailleurs autonomes du Québec, 2003, p. 10.

[32] Rappelons que selon les résultats les plus récents du CEFRIO, 60 % des Québécois sont « branchés » (NetTendance 2003).

Lors de l'établissement de l'échéancier de mise en œuvre, celui-ci devra privilégier les projets qui permettent d'évaluer facilement les gains d'efficience. Une vaste campagne de communication doit, à cet effet, être mise en branle dans les plus brefs délais, afin que les citoyens accompagnent le gouvernement dans chacune des étapes de son cheminement vers l'établissement d'un gouvernement en ligne. Les principaux partenaires du gouvernement doivent être partie prenante de cette démarche de sensibilisation, et en particulier ceux, tels le CEFRIO, qui se spécialisent entre autres dans l'appropriation et le transfert des TIC.

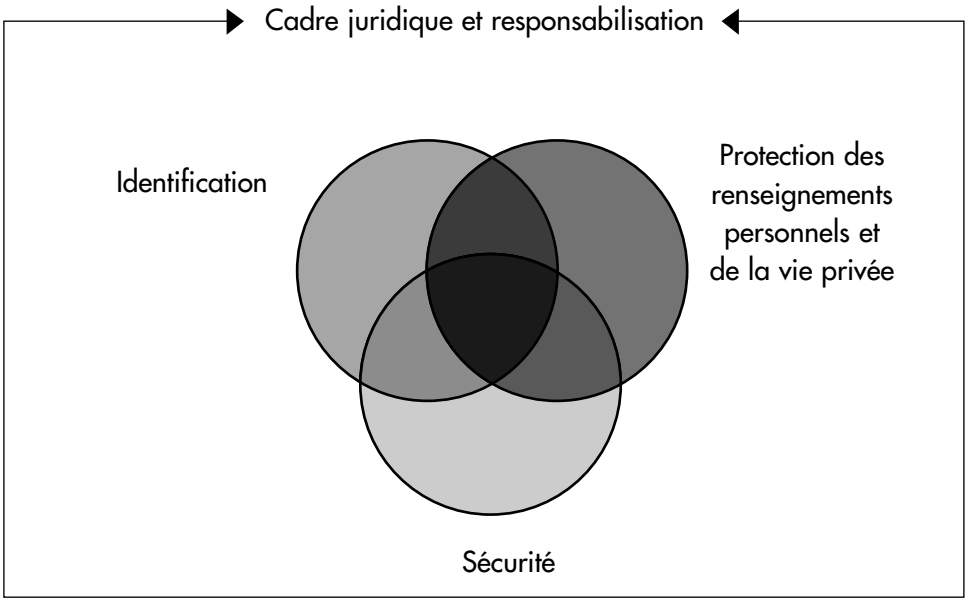
Enfin, d'autres facteurs sont également incontournables pour le succès du gouvernement en ligne, notamment **la sensibilisation et l'adhésion de la fonction publique** au projet. La mise en place du gouvernement en ligne modifiera de façon majeure le travail des employés de la fonction publique, en y apportant, dans bien des cas, des éléments de valeur ajoutée. Il est primordial que les employés de l'État soient partie prenante du projet dès le départ, en le considérant non pas comme une menace, mais bien comme une opportunité.

Schéma 9 : Les conditions de succès du gouvernement en ligne



1. Établir un environnement de confiance

Schéma 10 : Les éléments fondateurs de l'environnement de confiance



1.1 Les fondements juridiques de l'environnement de confiance dans le cadre du gouvernement en ligne

Afin de répondre aux nouvelles réalités amenées par les TIC, le gouvernement adoptait, en 2001, la *Loi concernant le cadre juridique des technologies de l'information*[33].

> « [Cette loi] vient préciser le droit relatif aux documents consignés sur support papier ou sur d'autres supports comme ceux qui reposent sur le recours aux technologies de l'information. Elle apporte des ajustements à plusieurs notions fondamentales du droit civil québécois afin de rendre celui-ci pleinement compatible avec l'usage sécuritaire des technologies de l'information.
>
> La loi est d'application générale : toutes les situations qui ne sont pas l'objet de règles spécifiques dans des lois particulières sont régies par les principes énoncés dans la *Loi concernant le cadre juridique des technologies de l'information*.

[33] L.R.Q. chapitre C-1.1.

> La loi prévoit des règles relativement à l'établissement de documents sur divers supports, au transfert de l'information d'un document d'un support à un autre, aux conditions de l'intégrité des documents tout au long de leur vie, au lien entre une personne et un document, ainsi qu'à la certification. Elle met en place des protections spécifiques pour les renseignements personnels et apporte des précisions sur les conditions de la responsabilité des prestataires de services[34] ».

La loi place le Québec dans une position de tête en matière d'encadrement législatif. En effet, le cadre juridique québécois des technologies de l'information constitue une solution juridique qui répond à plusieurs des préoccupations du groupe de travail de la Commission des Nations Unies pour le droit commercial international (CNUDCI) qui se penche actuellement sur un avant-projet de convention relatif à l'utilisation des technologies de l'information dans le contexte du droit commercial international et, plus particulièrement, des contrats internationaux. Ce groupe s'inquiète particulièrement de la création de régimes juridiques distincts selon que l'on fait appel au support papier ou aux technologies de l'information ainsi que de l'érosion des droits nationaux. La solution québécoise, qui découle de l'application des principes de neutralité et d'équivalence fonctionnelle mis de l'avant par la CNUDCI, offre en outre la liberté de choix et l'interchangeabilité des supports et des technologies que recherchent les intervenants en matière de commerce international, tout en préservant le régime juridique applicable. Cette solution a été présentée par la partie québécoise de la délégation canadienne participant au groupe de travail de la CNUDCI sur le commerce électronique, lors de ses récents travaux de 2004. Celui-ci l'a favorablement accueillie. Il ressort ainsi que la *Loi concernant le cadre juridique des technologies de l'information* fait maintenant figure de texte précurseur en la matière.

En balisant les diverses problématiques et possibilités reliées aux nouvelles technologies de l'information et des communications, la loi constitue un premier pas important en vue de mettre en place un véritable gouvernement en ligne.

Cependant le gouvernement en ligne ne saurait se réaliser sans que l'ensemble du corpus législatif soit adapté, et ce, à deux points de vue :

- d'une part, l'ensemble des lois doit respecter le cadre juridique mis de l'avant par la loi cadre, en particulier en ce qui à trait à la neutralité technologique;
- d'autre part, il importe d'apporter les modifications législatives requises afin de faciliter l'adoption de mesures à caractère transactionnel.

a) Respect du concept de neutralité technologique

La *Loi concernant le cadre juridique des technologies de l'information* introduit le principe de la neutralité technologique, c'est-à-dire que l'expression d'une norme ne doit pas présupposer de support particulier (papier ou électronique). Or, plusieurs éléments dans la législation actuelle ne répondent pas à ces critères de neutralité : ayant été rédigées avant que le recours aux TIC ne soit une réalité, plusieurs lois comprennent des dispositions qui présupposent le recours à un support papier. Par exemple :

---

[34] Conseil du trésor, Autoroute de l'information, http://www.autoroute.gouv.qc.ca/loi_en_ligne/loi/index.html [en ligne], site consulté le 31 mars 2004.

LES CONDITIONS NÉCESSAIRES AU SUCCÈS (suite)

- Certaines dispositions prévoient des plages horaires précises pour la consultation de documents (consultation d'un registre durant les heures « normales » de bureau par exemple). La possibilité de consulter ces documents en ligne rend nécessaire la remise en question de la spécification d'heures de consultation.

- D'autres dispositions législatives ont trait à la présence physique lors d'assemblées (assemblée annuelle ou conseil d'administration, par exemple). Il y a lieu de se demander, pour chacun de ces cas, si la présence physique est réellement nécessaire, ou si le recours aux TIC pourrait permettre de nouvelles formes de présence (que l'on pense à la vidéoconférence, par exemple).

- La référence à des documents annexés ou joints peut impliquer une notion de temps (cela peut être interprété comme exigeant concomitance ou simultanéité de l'envoi). Les nouvelles éventualités reliées à l'envoi de documents sous forme électronique appellent une révision de la notion de documents annexés ou joints. La législation doit permettre une mixité des formats de documents envoyés lors d'une même formalité : des documents en format papier devraient pouvoir être joints à des documents en format électronique, sans que cela pose problème quant à la simultanéité de l'envoi.

Selon la loi, on ne peut obliger quiconque à avoir recours à un support technologique spécifique pour transmettre ou recevoir des documents, à moins que cela ne soit expressément prévu par la loi ou une convention. L'article 29 stipule en effet ce qui suit :

> **« Acquisition d'un support.**
> Nul ne peut exiger de quelqu'un qu'il se procure un support ou une technologie spécifique pour transmettre ou recevoir un document, à moins que cela ne soit expressément prévu par la loi ou par une convention.
>
> **Support de réception.**
> De même, nul n'est tenu d'accepter de recevoir un document sur un autre support que le papier ou au moyen d'une technologie dont il ne dispose pas.
>
> **Choix du support.**
> Lorsque quelqu'un demande d'obtenir un produit, un service ou de l'information au sujet de l'un d'eux et que celui-ci est disponible sur plusieurs supports, le choix du support lui appartient[35]. »

En vertu du principe de neutralité, la loi rend possible l'utilisation des technologies pour l'application de toutes les lois. Le principe de neutralité assure non seulement que les développements à venir tiennent compte du choix des citoyens, mais il est de plus garant d'une sécurité accrue, puisqu'en cas de défaillance des technologies, l'interchangeabilité permettra de recourir aux documents papier, et vice-versa. Certains obstacles se dressent toutefois à l'application de ce principe, par exemple dans les cas où une loi exige l'emploi exclusif d'un support ou d'une technologie spécifique. C'est pourquoi l'ensemble du corpus législatif doit être révisé afin de déterminer si les dispositions législatives qui ne sont pas neutres sur le plan technologique et juridique doivent demeurer, être supprimées ou modifiées.

---

[35] *Loi concernant le cadre juridique des technologies de l'information,* 2001, L.R.Q., chapitre C-1.1, c. 32, a. 29.

C'est pourquoi le législateur doit élaborer une loi d'application de la loi cadre, qui visera à assurer, de façon concrète, la mise en œuvre des principes de neutralité technologique, médiatique et juridique et d'équivalence fonctionnelle, et ce pour l'ensemble de la législation québécoise. Une équipe de juristes du ministère de la Justice travaille déjà à l'ébauche d'un projet de loi qui doit être déposé au printemps 2005. Ce projet de loi fixera les standards, tant technologiques que juridiques, qui devraient trouver application dans l'ensemble des projets de gouvernement en ligne.

Considérant les impacts qu'aura la loi d'application de la loi cadre, il serait opportun que le gouvernement avance la présentation de celle-ci, en y allouant les ressources nécessaires, et s'assure que cette loi cadre tienne compte de la réalité du développement du gouvernement en ligne.

b) Adoption de « lois transactionnelles »

Une loi transactionnelle est une loi qui peut être administrée en ligne, par voie de la prestation électronique de services. Le caractère transactionnel des lois est l'un des éléments majeurs qui permettront de mettre sur pied diverses fonctionnalités qui contribueront à la création d'un véritable gouvernement en ligne au Québec. Cette volonté de rendre les lois transactionnelles nécessite de trouver des solutions à un certain nombre de problèmes.

Ces difficultés ont été relevées lors de l'étude de la *Loi sur les coopératives* du MDER, adoptée en décembre 2003, que l'on voulait pouvoir gérer de façon transactionnelle. Bien que ces difficultés soient spécifiques à la *Loi sur les coopératives*, elles peuvent être généralisées à l'ensemble des lois que le gouvernement voudra adopter en ce sens.

D'ailleurs, dans le cadre des travaux sur la réalisation d'un portail d'entreprise, un groupe de travail chapeauté par le ministère de la Justice a relevé neuf problématiques à résoudre en vue d'offrir aux entrepreneurs la possibilité de transiger en ligne avec le gouvernement (voir l'encadré ci-bas). Ces problématiques s'apparentent à celles soulevées dans le cadre de l'adoption de la *Loi sur les coopératives*. À la suite de son analyse, l'équipe de juristes a ainsi déterminé, pour l'ensemble des ministères, que près de 500 mesures reliées à ces problématiques nécessitent des modifications législatives ou réglementaires pour que les transactions puissent se faire en ligne.

Difficultés liées à l'adoption de « lois transactionnelles »

Plusieurs éléments inscrits dans la législation traditionnelle posent problème dans le monde virtuel :

- les différentes exigences de la signature;
- les modalités de paiement (lorsque le paiement par carte de crédit n'est pas une option);
- la capacité (personne physique, personne morale);
- les documents à fournir;
- le nombre d'exemplaires à transmettre;
- le support, la disposition et la forme de la demande;
- la concordance des exigences;
- l'exigence de l'apposition d'un sceau;
- le mode de transmission de la demande.

C'est pourquoi l'ensemble du corpus législatif doit être revu en fonction des nouvelles réalités propres à un environnement virtuel.

- ***Allègement des processus administratifs***

La mise à niveau des lois et des règlements de manière qu'il soit possible de les appliquer en faisant appel aux TIC vise à simplifier l'action gouvernementale en situant le choix des moyens à employer au niveau administratif plutôt qu'au niveau législatif. Cet assouplissement du corpus législatif ne règle pas pour autant tous les problèmes d'application des lois. De plus, si les processus qui ont été mis en place pour l'administration d'une loi sont lourds et complexes, ils ne seront pas automatiquement changés par l'introduction des technologies. Il faudra les revoir. L'introduction des TIC entraîne quasi nécessairement la révision des processus de gestion, car ceux applicables au papier peuvent être désuets, en plus de ne pas être compatibles avec l'emploi des moyens technologiques. Si une révision du corpus législatif s'impose pour lui permettre d'accueillir complètement les technologies, cela ne peut aller sans une révision des processus administratifs et une gestion intégrée du papier et des technologies de l'information.

Ce travail est d'autant plus important que certaines formalités administratives relativement simples à appliquer dans le monde tangible prennent une dimension beaucoup plus complexe dans la réalité numérique. Par exemple, mentionnons la multiplication des différentes signatures exigées : il est impératif d'évaluer si toutes ces exigences de signature sont nécessaires.

Les implications reliées au fait de rendre les lois transactionnelles nécessitent d'autres réflexions. Par exemple, il faut statuer sur les moyens d'**authentification** des documents qui se présentent sous une forme électronique : ceux-ci doivent être facilement identifiables. Des paramètres clairs doivent être établis à cet égard, par exemple en ce qui a trait à la validité d'un sceau électronique. De même, il faut trouver une façon de s'assurer de l'**intégrité** des documents technologiques, afin d'assurer leur préservation.

RECOMMANDATIONS

5.1 Nous recommandons que la mise à jour de l'ensemble du corpus législatif en vue de s'assurer du respect du principe de neutralité technologique se poursuive à un rythme accéléré.

5.2 Nous recommandons aussi que des dispositions soient prises afin que le projet de loi d'application de la *Loi concernant le cadre juridique des technologies de l'information* soit déposé dans un avenir rapproché.

5.3 Nous recommandons qu'une équipe de juristes revoie les règlements, les directives et les processus de gestion découlant de l'application des lois et des règlements pour qu'ils s'adaptent à une prestation électronique de services.

1.2 Les principes fondateurs de la protection des renseignements personnels et du droit à la vie privée dans le cadre du gouvernement en ligne

La Charte des droits et libertés de la personne reconnaît que « Toute personne a droit à sa vie privée » (article 5). C'est sur cette prémisse que le régime de protection des renseignements personnels et du droit à la vie privée a été établi au Québec.

Néanmoins, le défi posé par l'évolution fulgurante des technologies de l'information et des communications depuis les années soixante-dix, et leurs retombées en matière de protection du droit à la vie privée, est une réalité pressante que l'administration publique doit considérer avec le plus grand sérieux, en examinant de façon continue l'impact de ces nouvelles technologies sur le droit à la vie privée. Ce faisant, il est impératif que l'État québécois continue à se munir de mécanismes institutionnels et légaux clairement définis et qu'il les consolide pour garantir à ses citoyens que les renseignements personnels utilisés lors des prestations électroniques de services sont protégés contre toute atteinte à leur droit à la vie privée. Ces mécanismes doivent par ailleurs être définis de telle sorte qu'ils puissent être adaptables à l'évolution rapide des technologies.

Le gouvernement doit favoriser une approche où les systèmes technologiques et les règles organisationnelles mis en place réduisent au minimum les possibilités de violation du droit à la vie privée. En d'autres termes, plutôt que de tenter de contrôler d'éventuelles violations du droit à la vie privée, le gouvernement doit prendre les mesures qui s'imposent afin que ces éventualités ne puissent simplement pas survenir. Enfin, le gouvernement doit aussi favoriser le déploiement de programmes de sensibilisation et de formation pour permettre aux utilisateurs de bien assimiler les risques liés à la protection des renseignements personnels dans le cadre des systèmes technologiques.

Avant de définir concrètement les étapes que doivent suivre les ministères et les organismes dans le développement et le déploiement des projets de gouvernement en ligne, il y a lieu d'énoncer les principes directeurs applicables à la protection des renseignements personnels. Il importe que les citoyens, tout comme les administrateurs publics, comprennent et assimilent ces principes.

Tout d'abord, une distinction s'impose entre, d'une part, la protection des renseignements personnels et du droit à la vie privée et, d'autre part, la sécurité de ces renseignements dans un ou des systèmes informatiques. Les systèmes informatiques à travers lesquels des renseignements personnels sont traités nécessitent forcément des mesures de sécurité. Cependant, la sécurité seule ne garantit pas nécessairement une protection appropriée des renseignements personnels : un système informatique peut être très sécuritaire sans pour autant protéger le droit à la vie privée.

L'OCDE a établi des lignes directrices régissant la protection de la vie privée et les flux transfrontières de données à caractère personnel[36] . Ces lignes directrices ont été élaborées autour de huit principes, qui sont reproduits ici :

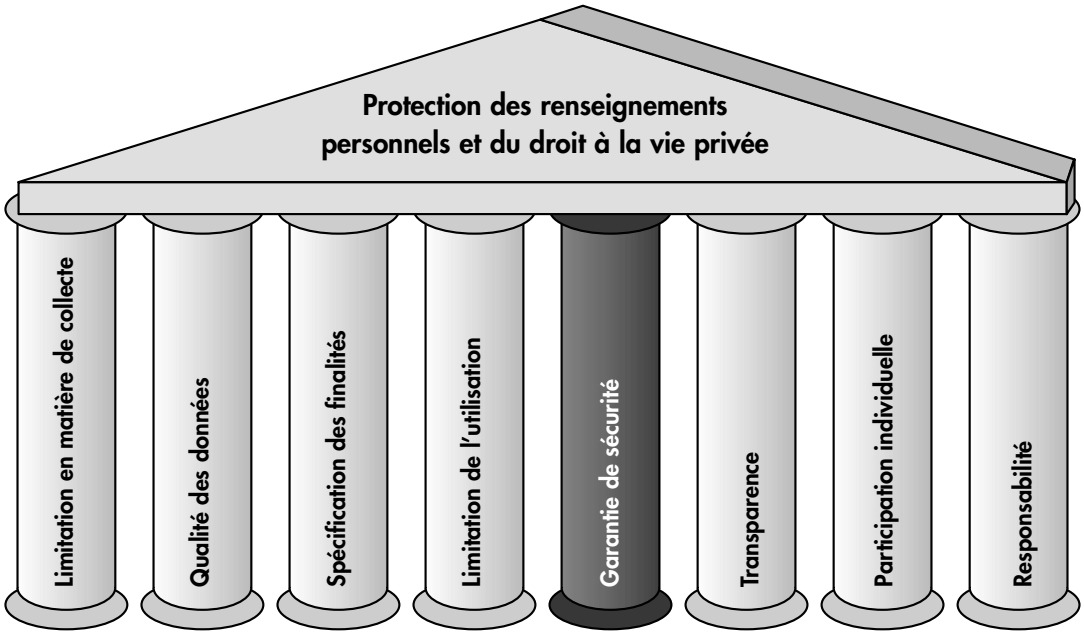
1. **Principe de la limitation en matière de collecte :** il doit y avoir des limites à la collecte de données de caractère personnel et toute donnée de ce type devrait être obtenue par des moyens licites et loyaux et, le cas échéant, après en avoir informé la personne concernée ou avec son consentement.
2. **Principe de la qualité des données :** les données à 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.
3. **Principe de la spécification des finalités :** les finalités en vue desquelles les données de caractère personnel sont collectées devraient être déterminées au plus tard au moment de la collecte des données et lesdites données ne devraient être utilisées par la suite que pour atteindre ces finalités ou d'autres qui ne soient pas incompatibles avec les précédentes et qui seraient déterminées dès lors qu'elles seraient modifiées.
4. **Principe de la limitation de l'utilisation :** les données de caractère personnel ne devraient pas être divulguées, ni fournies, ni utilisées à des fins autres que celles spécifiées conformément au principe

[36] *OCDE, Protection de la vie privée en ligne : Orientations politiques et pratiques de l'OCDE*, 2003, p. 11.

de spécification des finalités précédemment évoqué, si ce n'est a) avec le consentement de la personne concernée ou b) lorsqu'une règle de droit le permet.

5. **Principe de garanties de sécurité :** il conviendrait de protéger les données de caractère personnel, grâce à des garanties de sécurité raisonnables, contre des risques tels que la perte des données ou leur accès, destruction, utilisation, ou divulgation non autorisés.
6. **Principe de la transparence :** il conviendrait d'assurer, d'une façon générale, la transparence des progrès, pratiques et politiques, ayant trait aux données de caractère personnel. Il devrait être possible de se procurer aisément les moyens de déterminer l'existence et la nature des données de caractère personnel, et les finalités principales de leur utilisation, de même que l'identité du maître du fichier et le siège habituel de ses activités.
7. **Principe de la participation individuelle :** toute personne physique devrait avoir le droit : d'obtenir du maître d'un fichier, ou par d'autres voies, confirmation du fait que le maître du fichier détient ou non des données la concernant ; de se faire communiquer les données la concernant; d'être informée des raisons pour lesquelles une demande est rejetée et de pouvoir contester un tel rejet; et de contester les données la concernant et, si la contestation est fondée, de les faire effacer, rectifier, compléter ou corriger.
8. **Principe de la responsabilité :** tout maître de fichier devrait être responsable du respect des mesures donnant effet aux principes énoncés ci-dessus.

Schéma 11 : Les lignes directrices régissant la protection de la vie privée



L'énumération de ces huit principes directeurs nous indique clairement que la sécurité des systèmes informatiques n'est qu'un seul élément parmi d'autres garantissant la protection des renseignements personnels. Comme l'affirme la Commission d'accès à l'information (CAI) : « le concept de la protection des renseignements personnels et du droit à la vie privée dépasse la simple notion de la sécurisation des échanges[37] ». Le principe de sécurité est nécessaire, mais non suffisant.

L'augmentation des attaques de systèmes informatiques et la propagation croissante de virus de plus en plus sophistiqués encouragent la croyance populaire selon laquelle un système sécuritaire garantit, à lui seul, la protection des renseignements personnels. Les systèmes informatiques qui sont alors déployés ressemblent beaucoup plus à des systèmes de contrôle d'accès, où il est facile de compiler des données (journaux) sur toutes les activités des utilisateurs, lesquelles peuvent par le suite être facilement liées à l'identité réelle de ces utilisateurs. **Dans ce contexte, les questions de protection du droit à la vie privée sont, la plupart du temps, largement marginalisées.**

Ainsi, en plus de respecter des principes de sécurité informatique, le gouvernement doit aussi, dans l'élaboration des architectures informatiques, s'assurer que les autres principes garantissant la protection des renseignements personnels et du droit à la vie privée, en plus des obligations légales telles qu'inscrites dans la législation, soient respectés en tout temps. La protection des renseignements personnels doit être la règle, et doit permettre de clairement définir les besoins des architectures et des infrastructures informatiques. Cette perspective permet de résoudre la démarcation conventionnelle entre la sécurité et la protection du droit à la vie privée.

Enfin, le gouvernement doit prendre les mesures nécessaires pour favoriser une meilleure prise en compte de la responsabilisation de l'ensemble des parties prenantes au projet du gouvernement en ligne, y compris les citoyens utilisateurs des services en ligne. Un système informatique ne peut, en effet, offrir l'assurance de la protection des renseignements personnels et de la sécurité que dans la mesure où la gestion des risques est prise en compte à tous les niveaux : cette gestion des risques repose ainsi non seulement sur la responsabilisation des émetteurs de services (les membres de la fonction publique), mais également sur les destinataires de ces services (les citoyens).

a) Contexte juridique québécois lié à la protection des renseignements personnels dans le cadre du gouvernement en ligne

Avant d'aborder les changements potentiellement nécessaires au régime de protection du droit à la vie privée dans le cadre du gouvernement en ligne, il est nécessaire de définir le contexte de protection des renseignements personnels tel qu'établi dans la législation québécoise.

Tout d'abord, il est essentiel d'être clair sur ce qu'est un renseignement personnel. Tel que stipulé par la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (plus loin appelée *Loi sur l'accès*), un renseignement personnel est constitué de n'importe quel type de renseignements nominatifs qui concernent une « personne physique et permettent de l'identifier ». Par exemple, le nom d'une personne physique n'est pas en soi un renseignement personnel, mais peut le devenir lorsqu'il est associé avec un autre renseignement nominatif concernant cette personne, ou qu'il permet d'en révéler un ou plusieurs.

---

[37] Commission d'accès à l'information, *Rapport quinquennal 2002. Une réforme de l'accès à l'information : le choix de la transparence*, novembre 2002, p.85.

De plus, la *Loi sur l'accès* stipule que tous les renseignements personnels recueillis (lorsque cela est nécessaire) et détenus par les M/O en conformité avec la loi doivent être traités de manière confidentielle. Les renseignements personnels détenus par un M/O ne peuvent être communiqués sans l'autorisation de la personne concernée, sauf dans les cas d'exception définis par la loi. Deux exceptions sont ainsi prévues : les communications de renseignements entre les M/O (selon des conditions définies)[38] et l'autorisation de recherche. La CAI explique qu'« échanger des renseignements personnels sans le consentement des personnes, c'est ébranler l'un des piliers du régime de protection des renseignements personnels, d'où la mise en place de dispositifs exceptionnels et contraignants lorsqu'un organisme songe à s'engager dans cette façon de faire[39] ». Finalement, la loi stipule les modalités que les M/O doivent respecter tout au long de la vie utile des renseignements personnels (collecte, communication, conservation et destruction).

b) Adaptation de la législation actuelle au nouveau contexte lié au gouvernement en ligne

Dans le contexte de la mise en place du gouvernement en ligne, il y a lieu de se demander si le cadre juridique actuel assurant la protection de la vie privée doit être reformulé pour encadrer la circulation des informations requises de manière à assurer le bon fonctionnement et l'efficacité de la prestation électronique des services gouvernementaux. En effet, les spécialistes s'entendent à l'effet que l'éventuel développement des services publics intégrés en ligne destinés aux citoyens et aux entreprises, ainsi que leur bon fonctionnement, repose sur l'utilisation et, vraisemblablement, l'échange accru d'informations personnelles entre différents intervenants. Selon ces spécialistes, ces informations et leurs échanges sont vitaux pour le gouvernement, afin qu'il soit en mesure d'optimiser la qualité de ces services. On parle alors d'une personnalisation des services aux citoyens et aux entreprises.

• *L'échange de renseignements personnels dans le cadre d'une administration électronique de plus en plus intégrée*

Le Centre de recherche en droit public de l'Université de Montréal (CRDP) s'est penché sur l'adaptation du cadre législatif nécessaire aux nouvelles réalités propres à l'émergence des technologies de l'information et aux nouvelles possibilités de prestation électronique de services. Le CRDP énonce ainsi que l'objectif est de mettre en place un « cadre juridique adéquat qui rend possible l'échange balisé des renseignements personnels entre M/O aux fins de permettre les PES accomplies au bénéfice des citoyens qui sont tributaires de renseignements en possession d'une pluralité de M/O ». Les spécialistes du centre affirment en outre que « le renforcement des protections de la vie privée [est possible] par un meilleur ciblage des mécanismes de protection ». En somme, il faut « […] protéger mieux ce qui relève de la vie privée sans pour autant empêcher la

---

[38] La communication de renseignements personnels entre M/O sans le consentement de la personne concernée peut se faire selon les conditions suivantes : communication nécessaire à l'application d'une loi (article 67); communication nécessaire à l'application de conditions de travail (article 67.1); communication nécessaire à l'exercice d'un mandat (article 67.2); communication nécessaire à la mise en œuvre d'un programme (article 68); communication nécessaire pour fins de couplage ou appariement de fichiers (article 68.1). Pour les deux derniers points, une entente écrite doit être conclue et un avis de la CAI doit être établi. Si cet avis est négatif, l'entente peut être soumise au gouvernement pour approbation. Ces documents doivent être déposés à l'Assemblée nationale et publiés dans la Gazette officielle du Québec.

[39] CAI, *Rapport quinquennal 2002. Une réforme de l'accès à l'information : le choix de la transparence*, novembre 2002, p. 79.

circulation des renseignements nécessaires au déroulement des prestations en ligne[40] ». Le gouvernement doit donc, dans cette perspective, établir un cadre juridique innovateur permettant l'échange balisé de renseignements personnels entre une pluralité de M/O, tout en assurant une protection optimale de ces renseignements tout au long de leurs déplacements, de leur utilisation et de leur conservation.

Le régime actuel des ententes pour l'échange de renseignements personnels duplique ou copie les renseignements personnels échangés dans le cadre d'une entente dans les différentes banques de données des M/O concernés. Conséquemment, la duplication de ces renseignements personnels accroît les risques de violation de la vie privée. Ces risques étaient présents même avant la venue des ententes établies avec la CAI. En effet, les renseignements personnels devaient être collectés individuellement par chaque M/O, ce qui diminuait globalement l'efficacité de l'administration publique et de la prestation de services en général. Dans le régime actuel, le changement d'adresse des citoyens, par exemple, est quotidiennement échangé entre les M/O selon l'entente en question et, ce faisant, est dupliqué dans les différentes banques de données.

Le régime actuel pourrait être amélioré grâce à un certain nombre d'actions, par exemple la réduction du nombre d'endroits où sont conservés les renseignements personnels. Les M/O qui ont besoin de ces renseignements dans le cadre de l'application de leurs programmes pourraient y accéder, sans pour autant les conserver. Des ententes pourraient prévoir ces possibilités. Le M/O devenant ainsi détenteur d'un renseignement personnel serait alors responsable de son utilisation et du respect des critères de confidentialité qui y sont associés. Il n'est pas question ici de construire une banque de données centrale où tous les renseignements nominatifs sont conservés, mais au contraire, de minimiser la duplication de renseignements et la collecte excessive de ceux-ci, en donnant des droits d'accès encadrés par un cadre réglementaire ou par des ententes entre les M/O concernés.

Telle qu'établie par la CAI, la règle de cloisonnement limite la circulation et la communication de renseignements personnels à une organisation proprement dite. Toujours selon la CAI, bien qu'elle ne figure pas en toutes lettres dans la *Loi sur l'accès*, cette règle peut être inférée du texte législatif (article 59). À ce sujet, la CAI indique que le principe de cloisonnement des renseignements personnels dans l'administration publique est la meilleure garantie de protection de la vie privée et de la minimisation des possibilités de mettre en place un État surveillant. L'amélioration du régime actuel afin de minimiser la duplication des renseignements personnels, tout en permettant l'accès à ceux-ci dans le cadre de la PES, ne remettrait pas en cause la logique derrière le principe de cloisonnement. En effet, le renseignement personnel serait conservé uniquement là où il doit rester, c'est-à-dire dans une banque de données sous la responsabilité d'un M/O, et non pas dupliqué ou échangé librement entre différents M/O. Le renseignement personnel serait uniquement communiqué ou rendu accessible aux autres M/O lorsque cela est permis par la loi ou lors d'une entente, celle-ci devant être rendue publique. La gestion de l'accès à ces renseignements personnels serait strictement contrôlée à l'intérieur d'un cadre bien défini.

En appui à ces fondements légaux et organisationnels, les technologies modernes améliorant la protection de la vie privée, telles qu'elles seront présentées ultérieurement, pourraient faciliter les échanges des renseignements personnels tout en assurant la protection de ceux-ci. En effet, il appert que la cryptologie moderne peut offrir des outils grâce auxquels des renseignements personnels sont échangés de manière sécuritaire, conformément aux règles de protection des renseignements personnels et de la vie privée. Cette assertion est un constat fondé sur des années de recherche en cryptologie.

---

[40] CRDP, *Les modifications à apporter aux cadres administratifs et juridiques afin de favoriser le développement de l'administration électronique dans le respect de la vie privée* (préparé pour le Secrétariat du Conseil du trésor), Université de Montréal (Faculté de droit), décembre 2003, p. 1.

LES CONDITIONS NÉCESSAIRES AU SUCCÈS (suite)

• *Niveaux de sensibilité variables des renseignements personnels*

Les spécialistes indiquent qu'il est plus qu'important de concevoir un cadre juridique où les renseignements personnels peuvent bénéficier de mesures de protection variables, selon la sensibilité du renseignement. Cette sensibilité, qui tient compte des circonstances, peut être appelée à changer tout au long du cycle vie de la personne concernée. En effet, une information peut devenir plus sensible selon les circonstances en présence. En somme, « même si toutes les informations relatives à une personne ont un statut semblable, elles ne présentent pas toutes les mêmes risques et enjeux[41] ». À ce sujet, le CSRI explique pour sa part que :

> « par exemple, l'adresse d'une personne est déjà souvent diffusée à large échelle dans le bottin téléphonique. Par contre, en certaines circonstances, la diffusion de l'adresse peut comporter des risques pour la sécurité de la personne; il faut alors assurer une protection conséquente[42] ».

Conséquemment, un renseignement personnel peut devenir une information extrêmement sensible pour certaines personnes ou groupes de personnes ce qui, dès lors, nécessite un changement du niveau de protection de ce renseignement. À ce sujet, l'accent doit être mis, lorsque cela est possible, sur le consentement et le choix du citoyen. Dans les autres cas, des mécanismes institutionnels doivent être prévus.

La législation actuelle ne fait pas de distinction ou de jugement de sensibilité concernant les renseignements personnels, mais il est évident que des mesures de protection supplémentaires doivent être prévues dans certains cas. De plus, des dispositions quant à la protection des renseignements personnels dans des lois sectorielles, telle que la *Loi sur les services de santé et les services sociaux* ou la *Loi sur le ministère du Revenu*, établissent des règles beaucoup plus strictes que celles de la *Loi sur l'accès* concernant certains renseignements personnels. Néanmoins, il demeure important que les systèmes informatiques élaborés pour la prestation électronique de services incorporent des fonctionnalités où des niveaux variables de protection sont disponibles, ces niveaux pouvant être modulés en fonction notamment de la sensibilité et de l'utilisation des renseignements en cause. La loi devrait prévoir cette possibilité.

• *Principe de finalité*

Les spécialistes s'entendent pour dire que le principe de finalité doit mieux correspondre aux réalités du gouvernement en ligne. Selon la conception actuelle, un renseignement ne peut être utilisé que pour les fins pour lesquelles il a été collecté et non pour d'autres fins. Or, pour mieux répondre aux nouvelles réalités engendrées par le gouvernement en ligne, et en particulier, pour éviter les pertes de temps liées aux collectes d'information multiples, les M/O doivent pouvoir offrir des services à valeur ajoutée qui ne sont pas initialement prévus par leur loi constituante. Dans de tels cas, le principe de finalité n'est pas respecté, puisque que les renseignements personnels utilisés n'ont pas été collectés aux fins de la prestation de services à valeur ajoutée. Le cadre juridique doit pouvoir encadrer ou permettre ce type de possibilité.

---

[41] Trudel, Pierre, « Améliorer la protection de la vie privée dans l'administration électronique : pistes afin d'ajuster le droit aux réalités de l'État en réseau », CRDP, Faculté de droit, Université de Montréal, p. 41.

[42] Secrétariat du Conseil du trésor, Mémoire du Comité stratégique des ressources informationnelles dans le cadre de la consultation générale à l'égard du document intitulé : *Une réforme à l'accès à l'information : le choix de la transparence*, mémoire présenté à la Commission de la culture, septembre 2003, p.6.

Ce type de service pourrait être effectué dans un contexte où l'on demande, lorsque c'est possible, le consentement libre du citoyen. La *Loi concernant le cadre juridique des technologies de l'information* reconnaît la validité de l'équivalence du geste de signature sur des documents technologiques comme garant d'un élément de consentement (article 39). Dans ce contexte, lorsque le citoyen désire avoir accès en ligne à un service à valeur ajoutée, il suffit de lui demander s'il autorise les M/O à divulguer ses renseignements personnels à un autre M/O, afin que celui-ci puisse lui offrir ce service. Ce consentement peut être direct ou indirect, c'est-à-dire qu'on peut l'induire lorsque le citoyen demande simplement le service, selon la nature de la transaction. La mise en place de tels mécanismes permettrait, d'une part, de respecter les principes fondateurs de la protection des renseignements personnels et, d'autre part, de tirer profit des possibilités offertes par les nouvelles technologies de l'information et des communications afin d'améliorer les services aux citoyens.

RECOMMANDATIONS

5.4 Nous recommandons que le gouvernement poursuive ses réflexions pour établir un cadre juridique qui respecte les principes fondamentaux de la protection des renseignements personnels et facilite le développement du gouvernement en ligne.

5.5 Nous recommandons que le gouvernement prenne tous les moyens appropriés, tels que des programmes de formation et de sensibilisation, pour responsabiliser les membres de la fonction publique et les citoyens quant aux risques liés à l'utilisation des services en ligne.

1.3 Les moyens organisationnels et technologiques permettant le respect des principes fondateurs de la protection des renseignements personnels et du droit à la vie privée

Pour s'assurer que les principes fondateurs et les obligations légales de protection des renseignements personnels sont respectés dans l'élaboration, le déploiement et l'opérationnalisation des systèmes informatiques à travers lesquels ces renseignements sont traités, des mécanismes institutionnels clairement définis et entièrement transparents doivent être renforcés et consolidés. Ces mécanismes ou moyens institutionnels sont de deux ordres, l'un organisationnel et l'autre technologique.

- ***L'organisation***

La CAI a mis à la disposition des ministères et des organismes un *Guide en matière de protection des renseignements personnels dans le développement des systèmes d'information*[43], qui permet d'évaluer les mesures de protection des renseignements personnels adoptées dans les projets technologiques. Ce guide est sans aucun doute un point de départ dans la bonne direction en matière de protection des renseignements personnels dans le contexte du déploiement des nouvelles technologies.

---

[43] Commission d'accès à l'information, *Guide en matière de protection des renseignements personnels dans le développement des systèmes d'information : À l'intention des ministères et organismes publics*, version 1.0, décembre 2002.

Cependant, à la lumière des consultations menées et des développements ayant eu cours dans d'autres États, il est apparu que le contenu de ce Guide devait être développé davantage. Par ailleurs, la Direction du soutien en accès à l'information et en protection des renseignements personnels du MRCI vient de publier le « Modèle de pratiques de protection des renseignements personnels dans le contexte du développement des systèmes d'information par les organismes publics[44] ».

Ce document inclut des règles concrètes et détaillées sur les étapes à suivre pour que l'élaboration, le développement, la modification, le déploiement ou la mise en œuvre des systèmes d'information respectent en tout temps les principes directeurs et les obligations légales de protection des renseignements personnels et du droit à la vie privée. Le modèle porte sur les volets informatique et administratif d'un système d'information. Il vise tous les renseignements personnels versés sur des supports informatiques ou autres supports et inclut les processus administratifs rattachés à ce système. Il ne porte pas sur les phases d'exploitation et d'utilisation.

Le Modèle de pratiques de protection des renseignements personnels dans le contexte du développement des systèmes informatiques par les organismes publics

Le Modèle de pratiques vise à faciliter l'intégration de la protection des renseignements personnels (PRP), tout en améliorant la qualité du processus mis en œuvre d'un projet à un autre. Ce modèle est destiné à servir de référence aux organismes publics pour faciliter le respect des principes et obligations légales de PRP dans les projets de développement, et ce, peu importe la taille et la nature des projets. Il peut également être utilisé dans tout programme et service faisant appel à des renseignements personnels. L'utilisation du Modèle par les parties prenantes permet de partager un vocabulaire commun et de déterminer les activités à réaliser, ainsi que les résultats à atteindre en matière de PRP.

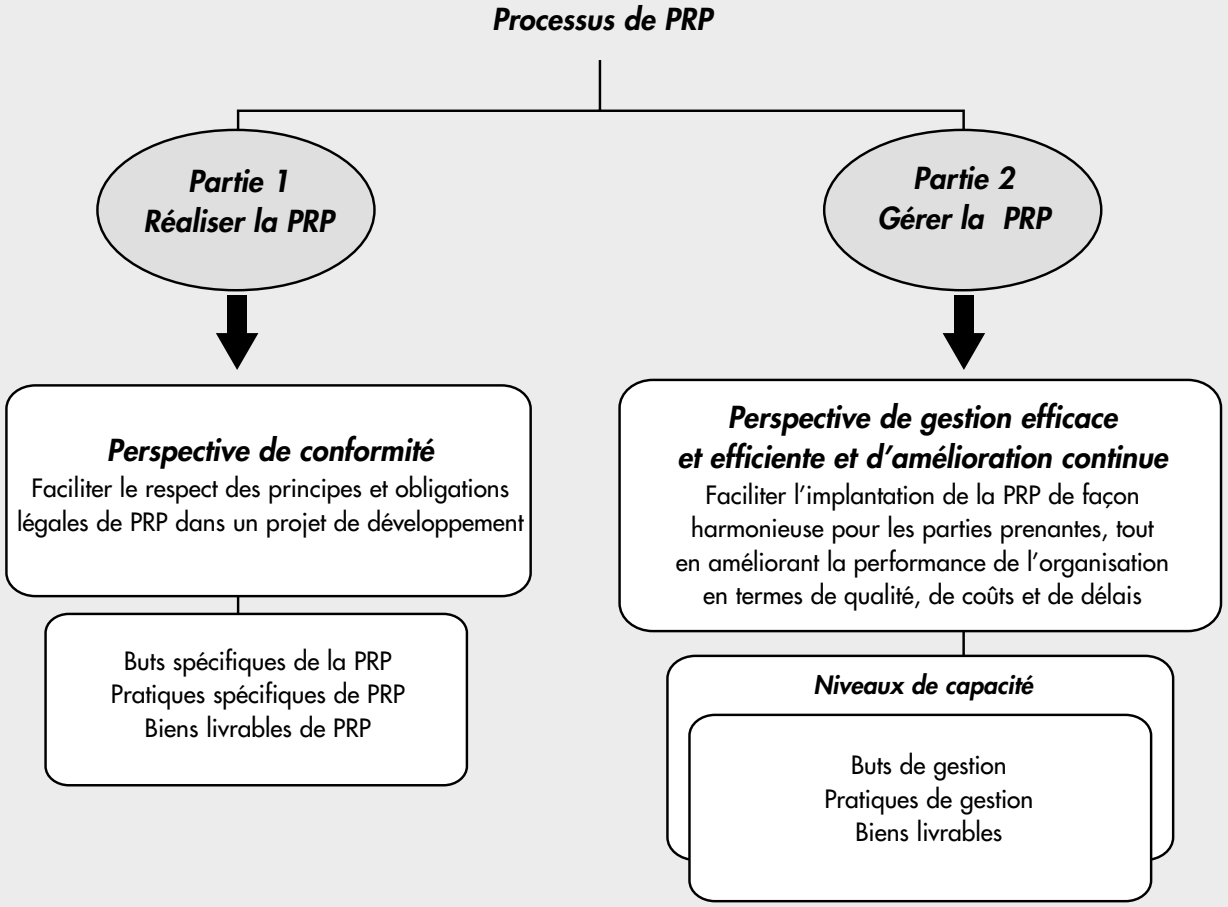
L'approche retenue par le MRCI est de fournir des outils permettant aux organismes publics d'assumer leur responsabilité à l'égard de la mise en application de la *Loi sur l'accès* dans le cadre des projets de développement. L'utilisation du Modèle se fait présentement sur une base volontaire et exige une adaptation à la situation particulière des organismes publics.

La figure de la page suivante illustre le processus de PRP dans les projets de développement, tel que proposé dans le Modèle.

---

[44] Québec, Ministère des Relations avec les citoyens et de l'Immigration, Direction du soutien en accès à l'information et en protection des renseignements personnels, *Modèle de pratiques de protection des renseignements personnels dans le contexte du développement des systèmes d'information par les organismes publics*, version 1.0, Publications du Québec, 2004.

Le Modèle de pratiques de protection des renseignements personnels dans le contexte du développement des systèmes informatiques par les organismes publics (suite)



Ce Modèle de pratiques est nécessaire afin que les projets ne puissent pas, suite à leur implantation, se révéler être à risque quant à la protection des renseignements personnels. En effet, trop souvent encore, ce type de questionnement émerge suite à l'analyse des systèmes informatiques déjà implantés. Il est alors trop tard! Par exemple, au Québec, l'avis de la CAI sur l'infrastructure intérimaire gouvernementale à clés publiques[45] a été donné à la suite de son élaboration. Une évaluation du projet en amont sur les risques liés à protection de la vie privée aurait sans aucun doute évité les critiques soulevées par la CAI dans son avis.

En plus de ce Modèle de pratiques, une grille d'évaluation des risques relatifs à la vie privée *(privacy impact assessment)*, doit aussi être développée le plus rapidement possible. Cette évaluation est jugée nécessaire avant de procéder à l'autorisation du gouvernement et au déploiement des systèmes informatiques. La CAI précise d'ailleurs elle-même « [qu'il] est important que le volet de la protection des renseignements personnels de projets technologiques puisse faire l'objet d'une évaluation avant leur déploiement[46] ». À cet effet, plusieurs grilles d'évaluation ont déjà été réalisées, notamment au Canada et en France. Au Québec, des démarches en ce sens ont déjà été entreprises par le MRCI.

Les M/O doivent avoir l'obligation de réaliser ces évaluations, celles-ci devant être rendues publiques. En effet, la perception des risques est une notion sociale, résultant de facteurs culturels, historiques et conjoncturels. C'est pourquoi la transparence de ce processus est centrale à la confiance de la population, qui doit avoir la possibilité d'en débattre, le cas échéant. Il faut démontrer que les systèmes utilisés garantissent le droit à la vie privée. Une évaluation insatisfaisante aurait ainsi pour effet d'obliger les responsables à corriger le projet ou à l'améliorer en conséquence. À l'inverse, une évaluation positive donnerait le feu vert à la poursuite du projet, sous réserve d'une autorisaton gouvernementale, lorsque requis[47]. Les avis émis par la CAI serviraient, dans de tels cas, à éclairer l'autorisation gouvernementale. Pour l'ensemble des projets, l'organisme responsable de la surveillance de la loi (CAI) aurait la latitude d'effectuer une surveillance ou d'émettre des avis et des recommandations afin de s'assurer que les projets développés par les M/O demeurent conformes à la loi, non seulement lors de leur mise en place, mais aussi lors de leur utilisation. Enfin, le ministre responsable de l'application de la loi en matière de protection des renseignements personnels jouerait un rôle de conseil et de soutien pour aider les M/O dans la réalisation des évaluations de risques et la mise en œuvre du Modèle de pratiques de PRP. Il pourrait aussi effectuer une vérification de la conformité du processus de réalisation de chaque évaluation de risque, selon les critères établis. La responsabilité de la vérification et du contrôle des systèmes doit néanmoins revenir aux responsables de l'opérationnalisation des projets dans les M/O (voir schéma 12, p. 127).

Le fait d'avoir des règles claires et d'associer les responsables de la protection des renseignements personnels (RPRP) dans chaque ministère ou organisme dès la conception d'un projet facilite la tâche de ceux-ci, ainsi que la tâche de ceux qui ont à développer les systèmes qui respectent la vie privée.

Afin de solidifier ces mécanismes organisationnels visant une meilleure protection des renseignements personnels, il est donc crucial d'impliquer directement les responsables de la protection des renseignements personnels (RPRP) dans les M/O dès la conception d'un projet. Des voies formelles de communication

---

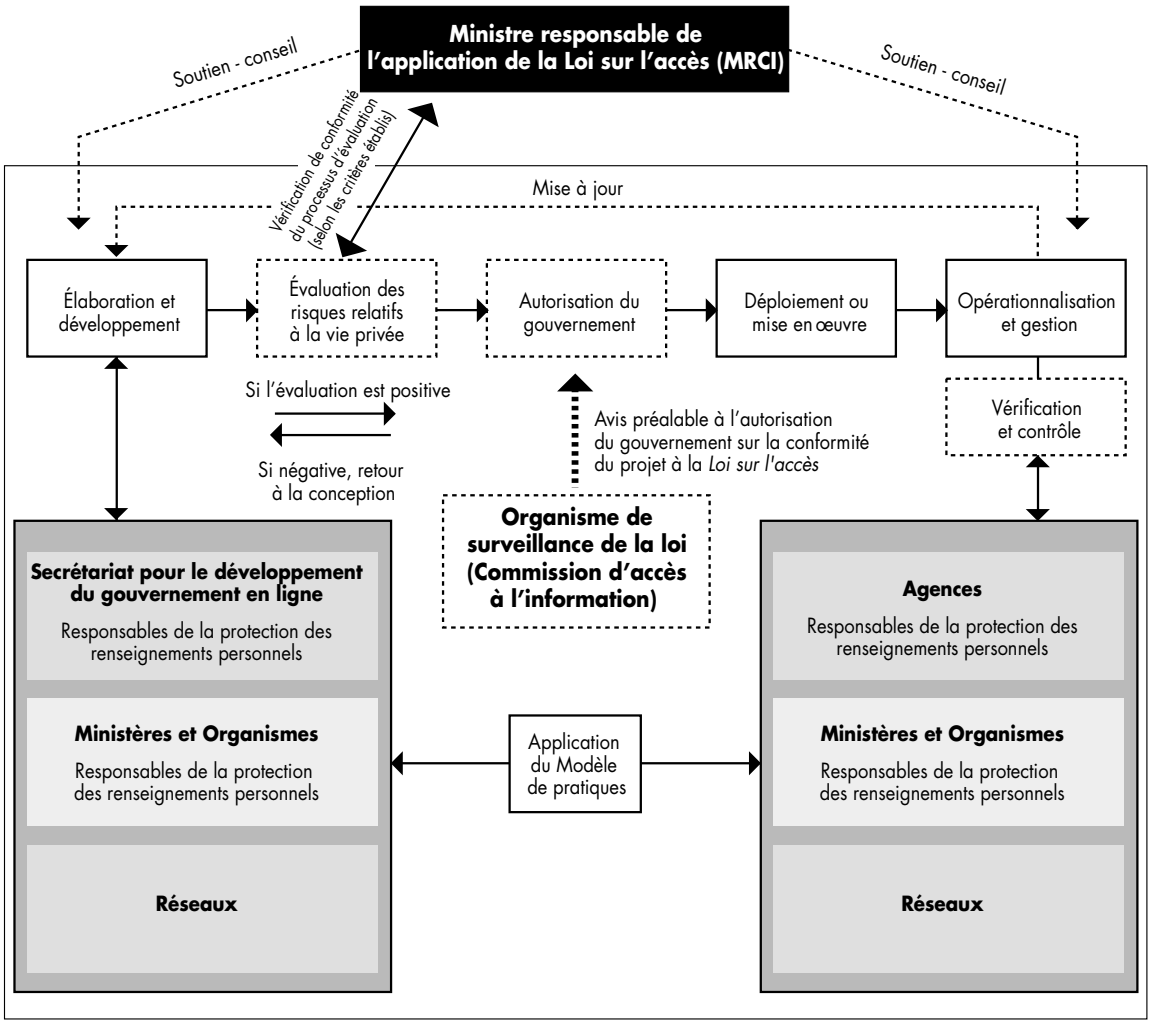
[45] Commission d'accès à l'information, *Avis de pertinence sur la solution intérimaire de l'infrastructure à clés publiques gouvernementale du Secrétariat du conseil du trésor*, dossier 01 11 07, août 2001.

[46] Commission d'accès à l'information, *Rapport quinquennal 2002. Une réforme de l'accès à l'information : le choix de la transparence, Document complémentaire de la Commission d'accès à l'information sur la consultation publique de la Commission parlementaire*, 30 octobre 2003, p. 27.

[47] Les paramètres permettant de déterminer les projets qui devront être soumis à une autorisation gouvernementale devront être établis.

doivent être établies, à la fois pour permettre aux RPRP d'être informés des développements en cours et pour faciliter les échanges entre les parties prenantes des projets au sein des M/O et les RPRP. Les RPRP pourraient, dans leurs tâches, être appuyés en tout temps par le ministre responsable de l'application de la loi en matière de protection des renseignements personnels. Or, pour mener à bien ces tâches et pour que ces échanges portent fruit, il est impératif que le ministre responsable de l'application de la loi en matière de protection des renseignement personnels, les RPRP et l'organisme responsable de la surveillance de la loi (CAI) puissent avoir recours aux conseils et avis des spécialistes et des experts, tels que des informaticiens et des cryptologistes. Le développement rapide des TIC et leur impact sur la protection de la vie privée nécessitera, de façon de plus en plus marquée, le recours à des experts pour se pencher sur les risques éventuels liés à la protection des renseignement personnels et de la vie privée au Québec.

Schéma 12 : Les moyens organisationnels assurant le respect de la protection des renseignements personnels



LES CONDITIONS NÉCESSAIRES AU SUCCÈS (suite)

Même lorsque des mesures technologiques sont mises en place, elles demeurent toujours assujetties à des facteurs humains, ce que l'administration publique ne peut totalement éviter. Il est donc important d'assurer la gestion et les règles administratives qui orientent forcément les comportements et les décisions entourant les systèmes technologiques. Les programmes de sensibilisation et de formation jouent alors un rôle important pour le respect de ces règles organisationnelles. À ce sujet, la CAI constate, dans son Rapport de novembre 2002, que malgré certains efforts d'amélioration, il y a encore beaucoup à faire pour que la protection des renseignements personnels soit clairement inscrite à même les procédures administratives et la culture organisationnelle des ministères et organismes du gouvernement du Québec[48]. Non seulement les règles en la matière doivent-elles être précises, mais des programmes de formation et de sensibilisation à l'intention des fonctionnaires doivent également être mis en place pour que ces règles soient comprises, assimilées et appliquées conformément à l'esprit de la Loi.

RECOMMANDATIONS

5.6 Nous recommandons que le nouveau Modèle de pratiques de protection des renseignement personnels dans le contexte du développement des systèmes d'information par les organismes publics soit mis en œuvre dans tous les organismes publics pour s'assurer du respect des principes directeurs et des obligations légales en matière de protection des renseignements personnels.

5.7 Nous recommandons qu'une grille d'évaluation des risques relatifs à la vie privée *(privacy impact assessment)* soit développée le plus rapidement possible.

5.8 Nous recommandons que les responsables de la protection des renseignements personnels des M/O participent activement au développement des projets en ligne, et qu'ils soient soutenus dans leur travail par le ministre responsable de l'application de la loi en matière de protection des renseignements personnels.

5.9 Nous recommandons que le ministre responsable de l'application de la loi en matière de protection de renseignements personnels, les responsables de la PRP au sein des M/O et l'organisme responsable de la surveillance de la loi puissent avoir recours à des expertises en matière technologique ou à toute autre expertise pouvant les aider dans leur travail.

5.10 Nous recommandons que le ministre responsable de l'application de la loi en matière de protection des renseignements personnels puisse participer activement aux projets du gouvernement en ligne, dans le cadre de son rôle de soutien à la réalisation des évaluations des risques relatifs à la vie privée et à la gestion de ces risques, ainsi qu'à la mise en œuvre des bonnes pratiques de PRP.

5.11 Nous recommandons que les responsables de la protection des renseignements personnels des M/O établissent, avec la participation du ministre responsable de l'application de la loi en matière de protection des renseignement personnels et du DPI, des programmes de sensibilisation et de formation pour les parties prenantes aux projets de développement du gouvernement en ligne pour que les principes directeurs et les obligations légales en matière de protection des renseignements personnels soient compris, assimilés et appliqués correctement pour l'ensemble des organismes publics et privés.

---

[48] Commission d'accès à l'information, *Rapport quinquennal 2002, Une réforme de l'accès à l'information : le choix de la transparence*, novembre 2002, p. 83.

- ***Les technologies***

Le gouvernement doit aussi mettre en place des mécanismes institutionnels, voire juridiques, qui puissent favoriser l'utilisation des technologies spécifiques à la protection des renseignements personnels et du droit à la vie privée. À cet effet, les technologies utilisées doivent non seulement permettre de garantir la protection des renseignements personnels, mais aussi, dans la mesure du possible, favoriser le développement d'un environnement où la protection des renseignements personnels est renforcé.

À cet effet, le ministre néerlandais de la Justice affirmait, en discutant de la Loi néerlandaise sur la protection des la vie privée, que :

> « […] current IT capabilities to abuse personal data necessitate a search for supplementary possibilities to make sure personal data are treated properly and accurately. Consider partial or complete 'anonymising', for instance, by eliminating from personal data their identifying characteristics, or protecting them against use by certain applications/users, or by limiting their use to certain purposes. In this thinking, amendment 22 of the Lower house to Article 13 of the bill added that the prescribed security measures must also focus on the prevention of unnecessary collection and further processing of personal data. This will provide a legal foundation for the application of privacy-enhancing technologies. Such rules respond to the restrictions of the developing information technology[49] ».

La documentation sur les technologies améliorant la vie privée *(Privacy-enhancing technologies - PET)* et les spécialistes en cryptographie font état d'un éventail d'instruments technologiques qui pourraient assurer la protection de la vie privée. Malheureusement, ces instruments sont encore très peu connus et ils n'ont pas encore été développés.

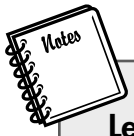
Dans le contexte de la mise en place d'un gouvernement en ligne, les technologies améliorant la protection de la vie privée semblent posséder certaines caractéristiques pouvant non seulement garantir, mais également renforcer la protection des renseignements personnels. Elles permettent en effet une meilleure protection du droit à la vie privée, en réduisant l'utilisation de renseignements personnels aux seules situations où cela s'avère une nécessité, et ce, sans diminuer la performance des systèmes informatiques ni la gestion des prestations électroniques des services. En effet, l'ajout de technologies améliorant la protection de la vie privée dans les systèmes conventionnels n'a pas diminué la performance des systèmes[50]. En fait, l'utilisation de ces technologies peut favoriser de façon significative le respect des principes de protection du droit à la vie privée dans l'administration publique, en garantissant que le traitement des renseignements personnels est effectué correctement. Or, l'ajout de fonctions technologiques améliorant la protection des renseignements personnels dans des systèmes déjà existants peut être complexe et coûteux. À ce sujet, il suffit de rappeler la révision coû-

---

[49] Gouvernement des Pays-Bas, Parliamentary Document 25 892 # 92c, année parlementaire 1999-2000, Memory of Reply to First Chamber regarding the WBP, p.16. Article 13 : « The responsible party shall implement appropriate technical and organizational measures to secure personal data against loss or against any form of unlawful processing. These measures shall guarantee an appropriate level of security, taking into account the state of the art and the costs of implementation, and having regard to the risks associated with the processing and the nature of the data to be protected. These measures shall also aim at preventing unnecessary collection and further processing of personal data. » http://www.cbpweb.nl/

[50] Voir Borking, J. et C. Raab, « Laws, PETs and Other Technologies for Privacy Protection », *The Journal of Information, Law and Technology*, vol 1, 2001.

teuse des milliers, voire des millions, de codes de programmation à la veille du millénaire pour vérifier si les systèmes étaient prêts pour le bogue de l'an 2000. Voilà pourquoi il est important de considérer, dès le départ, l'intégration aux systèmes des technologies qui améliorent la vie privée.



Les technologies améliorant la protection de la vie privée

Une des technologies innovatrices améliorant la protection de la vie privée est le certificat d'attestation électronique. Une attestation électronique peut être considérée comme l'équivalent digital d'un passeport. Elle peut contenir des attributs arbitraires (par exemple: nom, citoyenneté, âge, adresse, clé publique, pseudo-identités etc.) certifiés par un émetteur, et offre donc les mêmes fonctionnalités qu'un certificat d'identité ou d'attributs conventionnel (certificats de type X.509).

Les certificats d'attestation électroniques se distinguent des certificats conventionnels de deux façons :

- Premièrement, la délivrance de l'attestation se fait de manière aveugle (*blind signature*), de telle sorte que l'émetteur du certificat ne reconnaît pas l'attestation une fois celle-ci émise. Ainsi, même si, lors des utilisations subséquentes, l'utilisateur s'identifie à l'émetteur de certificat, ce dernier ne peut être en mesure de tracer l'utilisation du certificat d'attestation. Il est quand même en mesure de vérifier l'authenticité et l'intégrité du certificat d'attestation électronique, tout comme peuvent le faire les entités (M/O) qui délivrent des services, mais sans révéler l'identité de la personne à qui a été émis ledit certificat.

- Deuxièmement, l'utilisateur peut révéler certaines propriétés des attributs de son certificat d'attestation électronique de façon sélective. Il peut choisir de ne révéler que certains attributs (ne montrer que sa citoyenneté en cachant les autres attributs, par exemple), de montrer qu'un attribut respecte un certain critère (que son âge est supérieur à 18 ans, sans le révéler de façon exacte) ou de confirmer qu'un attribut ne possède pas une caractéristique donnée (que son nom ne figure pas sur une liste noire, par exemple, sans le dévoiler). Dans l'ensemble de ces situations, l'utilisateur n'a jamais à s'identifier formellement.

Ces deux propriétés font des certificats d'attestation électronique de très bons outils pour bâtir une infrastructure de contrôle d'accès qui élimine les possibilités de traçabilité, préservant ainsi le droit à la vie privée des utilisateurs.

D'autres technologies modernes peuvent aussi être utilisées pour une meilleure protection de la vie privée, sans diminuer la performance des systèmes informatiques et des réseaux.

- Certains outils de cryptage modernes peuvent être utilisés, tel que le *Zero proof knowledge*, pour comparer ou corroborer des renseignements personnels sans en divulguer le contenu, que l'on veut garder secret. Ces techniques pourraient être utilisées par les fonctionnaires pour s'assurer que les citoyens possèdent les qualités requises pour avoir accès à un programme, sans que les renseignements personnels de ceux-ci soient divulgués.

- La transmission d'un secret partagé est un autre moyen technologique qui répond à des objectifs d'authentification : le citoyen partage une information secrète avec tous les M/O de telle manière que ceux-ci, isolément, ne peuvent connaître ces informations ou les révéler. Cette technique pourrait être utilisée pour la corroboration d'identité, lors d'échanges spécifiques de renseignements personnels entre les M/O, tel que le changement d'adresse.

- Lorsqu'il est nécessaire d'obtenir plusieurs renseignements personnels auprès d'une ou de plusieurs banques de données dans plusieurs M/O afin d'offrir un service intégré ou de valeur ajoutée, des techniques cryptographiques de recherche peuvent être utilisées pour aller puiser, à l'intérieur de ces banques de données, uniquement l'information nécessaire à la prestation de services, sans révéler ou permettre l'accès à l'ensemble des renseignements des personnes concernées dans les différentes banques de données.

- Une technique particulièrement utile pour la démocratie en ligne et l'accès à l'information est celle qui permet de rechercher des informations sur des banques de données, sans que les administrateurs de ces banques ou autre tierce partie puissent connaître la nature de cette recherche. Par exemple, des citoyens ou des groupes d'intérêt pourraient rechercher des informations ou renseignements publics de l'État, sans que d'autres personnes puissent savoir qu'ils le font.

Pour en savoir plus sur ces technologies, le lecteur peut consulter les références figurant à la fin de ce rapport ou les projets en cours sur les *Privacy-enhancing technologies (PET)* :

- CAFE : http://www.semper.org/sirene/projects/cafe/
- CYBERVOTE : http://www.eucybervote.org/main.html
- PISA : http://www.pet-pisa.nl/pisa_org/pisa/index.html
- SEMPER : http://www.semper.org/
- RAPID : http://www.ra-pid.org
- FIDIS : http://csrc.lse.ac.uk/research/fidis.html
- PAMPAS : http://www.pampas.eu.org

Le sous-développement des technologies améliorant le droit à la vie privée

La documentation sur le sujet et le témoignage des spécialistes de la question évoquent plusieurs causes au sous-développement des technologies améliorant la protection de la vie privée. Premièrement, dans un contexte où le cadre juridique des administrations n'exige ou ne favorise pas la mise en place de technologies améliorant la vie privée, la demande pour ces nouvelles technologies ne se fait pas sentir. Un cadre juridique favorable aux technologies améliorant la protection de la vie privée stimulerait le développement de ces technologies par le secteur privé. Deuxièmement, tout indique que le développement de ces technologies est freiné par différentes forces dans le marché de l'informatique et des télécommunications. Les caractéristiques propres au marché des logiciels, et particulièrement la situation de quasi-monopole que l'on connaît actuellement, seraient en grande partie responsables des dysfonctionnements du marché (*market failures*). En effet, la concentration du secteur

de la programmation fait en sorte que les fournisseurs contrôlent le marché en ce qui concerne les prix et le développement des technologies utilisées. Selon l'avis de plusieurs spécialistes sur le sujet, cette situation ferait en sorte que les logiciels commercialisés sont souvent constitués de simples modifications visant à régler des bogues repérés dans des versions antérieures. En matière d'innovation, le coût de développement d'une nouvelle technologie informatique dépasse souvent les bénéfices qui y sont associés. Ainsi, l'industrie ne semble plus dominée par les *start-ups* et l'innovation, comme cela était le cas au début de l'ère de la nouvelle économie. Dans cette optique, un article de la revue *The Economist* affirme que la recherche et le développement dans l'industrie du logiciel ne relève plus de l'innovation, mais de la simple fabrication. S'appuyant sur les dires de George Gilbert (cofondateur de TechStrategy Group), l'auteur de l'article soutient que la grande part des efforts est désormais concentrée sur la maintenance, l'amélioration (*upgrades)*, et le réglage des bogues informatiques des logiciels (*The Economist, 17 novembre 2003*).

Par exemple, les infrastructures à clé publique, qui sont largement utilisées par les gouvernements et les organisations à travers le monde, et dont la fonction principale est d'assurer la sécurité des transactions entre les utilisateurs dans un environnement d'insécurité (comme c'est le cas sur l'Internet), ne répondent pas nécessairement, dépendamment de leur utilisation, aux besoins de protection de la vie privée dans le contexte du gouvernement en ligne. En effet, un nombre impressionnant de spécialistes* et surtout, des commissaires à la protection de la vie privée dans de nombreux pays (tels la CAI au Québec, le *Information and Privacy Commissioner (IPC)* en Ontario et le *Office of the Federal Privacy Commissioner (OFPC)* en Australie) ont démontré que les ICP, dans leurs architectures conventionnelles, peuvent potentiellement poser des risques élevés pour la protection de la vie privée en permettant, par leur fonctionnement, de nombreuses fonctions pouvant effectuer du profilage, du traçage, de la révélation d'information, etc. La présence de ces risques élevés doit être balisée par des cadres juridiques et réglementaires appropriés. Il faut toutefois garder à l'esprit que l'application de ces mesures s'avère généralement dispendieuse.

Ainsi, le risque de développer et de commercialiser de nouveaux produits répondant spécifiquement à la problématique de la protection de la vie privée semble trop élevé pour les grands de l'industrie. La commercialisation de ces produits informatiques nécessiterait une éducation supplémentaire de la clientèle, notamment en matière de nouvelles technologies de l'information et des communications.

* Par exemple, Clarke, R., *Conventional Public Key Infrastructure : An artefact I11-fitted to the needs of the information socitey, prepared for submission of the 'IS in information Society's Track on the Euro. Conf. In inf. Syst.* (ECIS 2001) in Slovenia, version du 13 novembre 2000 (http://www.anu.edu.au/people/Roger.clark/II/PKIMisFit.html); Brands, S., *Rethinking public key infrastructures and digital certificates; building in privacy*, MIT press, août 2000; Radicchio, *PKI and the protection of data et privacy*, livre blanc WP-LEG-003, version 1.0, 2000 (www.radicchio.org).

RECOMMANDATIONS

5.12 Nous recommandons que le ministre responsable de la loi en matière de protection des renseignements personnels, en collaboration avec le DPI, sensibilise les concepteurs et les responsables des architectures et des infrastructures aux nouvelles technologies protégeant le droit à la vie privée.

5.13 Nous recommandons que le gouvernement encourage et soutienne la recherche et le développement des technologies améliorant la protection de la vie privée.

5.14 Nous recommandons que le gouvernement se penche sur les possibilités d'établir un fondement légal pour assurer que les technologies soient conformes aux impératifs relatifs à la protection de la vie privée (*privacy-compliant technologies* et *privacy-enhancing technologies*).

1.4 Vers une culture de la sécurité

La protection des renseignements personnels est la résultante de nombreuses composantes. La sécurité constitue l'une d'elles. Néanmoins, en elle-même, la sécurité englobe elle aussi plusieurs autres éléments. Dans le cadre de la nouvelle réalité virtuelle en général, et de la mise en place du gouvernement en ligne en particulier, cette composante qu'est la sécurité prend une importance marquée.

L'ère numérique a, en effet, introduit toute une série de risques nouveaux dans la transmission des informations. La multiplication du nombre d'internautes un peu partout dans le monde[51] et la facilité du partage des connaissances qui peuvent servir la cybercriminalité augmentent la vulnérabilité des systèmes informatiques. D'où l'importance accrue de la sécurité de l'information.

> « La sécurité de l'information protège l'information contre des menaces très diverses de façon à assurer la continuité des activités, à minimiser le préjudice causé et à maximiser le rendement du capital investi et les possibilités d'affaires[52] ».

La majorité des intervenants, qu'il s'agisse des entreprises, des particuliers ou du gouvernement lui-même, ne semblent pas toujours pleinement conscients des enjeux reliés à la sécurité de l'informatique, se fiant pour la plupart à l'efficacité des outils communs tels les pare-feux et les logiciels antivirus. Pourtant, les systèmes deviennent de plus en plus complexes et impliquent des architectures et des infrastructures interconnectées. Les risques sont ainsi considérables : pertes d'information, bris de confidentialité et surtout, manque de confiance des citoyens envers les TIC. Enfin, les pertes financières engendrées par les incidents de sécurité informatique peuvent résulter en des coûts non négligeables pour l'économie.

---

[51] Le monde compte 630 millions d'Internautes selon les données recueillies au Sommet mondial sur la société de l'information (2003).

[52] Secrétariat du Conseil du trésor, *Gestion de la sécurité de l'information, Première partie : Code de bonne pratique pour la gestion de la sécurité de l'information*, BS 7799-1, 1999.

LES CONDITIONS NÉCESSAIRES AU SUCCÈS (suite)

À titre d'exemple, le *Canadian Healthcare Technology Magazine* indique que :

> « 15 % des hôpitaux canadiens ont admis avoir subi une atteinte à leur sécurité informatique au cours de la dernière année. De plus, 57 % des établissements sondés ont déclaré que certains de leurs employés contournaient les systèmes de sécurité informatique en place parce que ceux-ci étaient jugés trop encombrants. Par ailleurs, plus du tiers des hôpitaux sondés n'avaient ni plan de secours anti-sinistre, dans le cas de perte d'information, ni plan de continuité qui permettait, en cas de panne informatique, de continuer à fonctionner à l'aide de systèmes de support[53] ».

Pour l'ensemble de ces raisons, la sécurité informatique au Québec est un enjeu majeur pour tous les intervenants et en conséquence, il est impératif que des mesures soient prises pour développer une culture de la sécurité au Québec. Cette culture de sécurité repose d'abord sur la sensibilisation et la responsabilisation de tous les intervenants en présence, à tous les niveaux, comprenant les citoyens utilisateurs des services en ligne. Un système informatique ne peut être sécuritaire que dans la mesure où la gestion des risques est prise en compte à tous les niveaux et que les règles de bonne pratique sont respectées par tous. Les administrateurs de systèmes doivent de plus être crédibles et fiables. Les utilisateurs dans l'administration publique et dans la population en général doivent aussi avoir une idée de ces règles et des risques associés à l'utilisation des systèmes informatiques. Pour ce faire, il est nécessaire que le gouvernement élabore des programmes ou des mécanismes de sensibilisation et de formation à cet effet.

À ce propos, lors de sa 1037e session tenue en juillet 2002, l'OCDE a établi neuf lignes directrices pour la sécurité des systèmes et des réseaux d'information, qu'on peut résumer ainsi[54] :

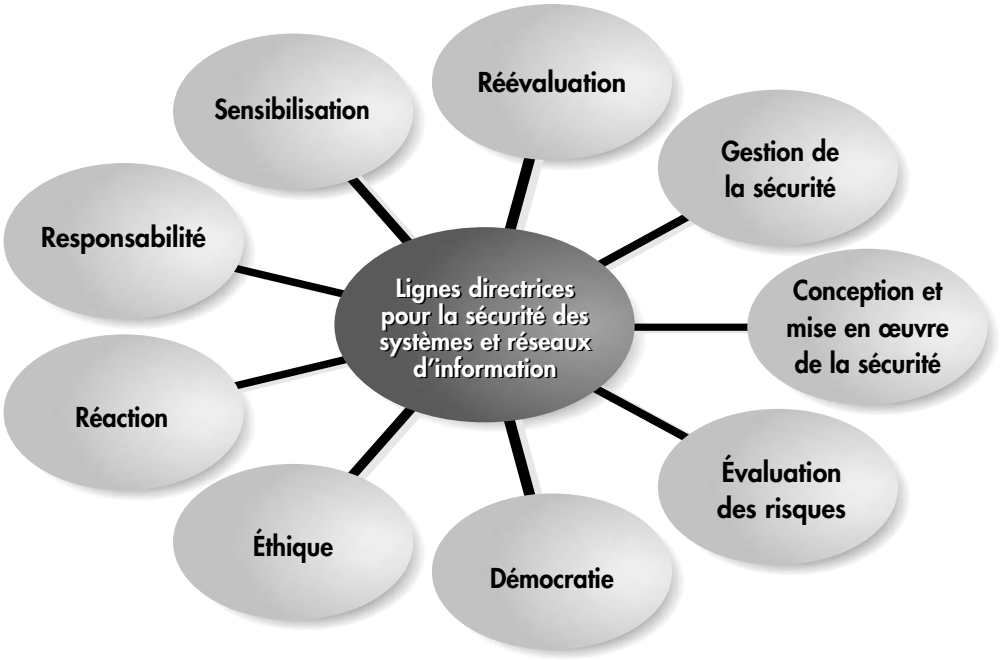
1) **Sensibilisation :** les parties prenantes doivent être sensibilisées au besoin d'assurer la sécurité des systèmes et réseaux d'information et aux actions qu'elles peuvent entreprendre pour renforcer la sécurité.
2) **Responsabilité :** les parties prenantes sont responsables de la sécurité des systèmes et réseaux d'information.
3) **Réaction :** les parties prenantes doivent agir avec promptitude et dans un esprit de coopération pour prévenir et détecter les incidents de sécurité et y répondre.
4) **Éthique :** les parties prenantes doivent respecter les intérêts légitimes des autres parties prenantes.
5) **Démocratie :** la sécurité des systèmes et réseaux d'information doit être compatible avec les valeurs fondamentales d'une société démocratique.
6) **Évaluation des risques :** les parties prenantes doivent procéder à des évaluations de risques.
7) **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.
8) **Gestion de la sécurité :** les parties prenantes doivent adopter une approche globale de la gestion de la sécurité.
9) **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.

---

[53] *Canadian Healthcare Technology Magazine*, 2002.

[54] OCDE, *Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information : vers une culture de la sécurité*, juillet 2002.

Schéma 13 : Les lignes directrices pour la sécurité des systèmes et des réseaux d'information



L'application de ces principes directeurs lors de prestations électroniques de services est plus que satisfaisante pour établir et maintenir la confiance de la population et son adhésion aux nouvelles technologies et, en particulier, à l'utilisation de ces technologies dans la mise en place d'un projet tel celui du gouvernement en ligne.

Ces principes directeurs permettraient aussi de satisfaire les finalités que les spécialistes de la sécurité indiquent comme étant recherchées dans un système informatique :

1. **Disponibilité :** propriété d'une information ou d'un système informatique d'être accessible ou disponible en tout temps ou en temps voulu.

2. **Intégrité :** propriété selon laquelle les données ou les informations ne peuvent être modifiées ou altérées que par les personnes autorisées.

3. **Confidentialité :** propriété des données ou des informations, comme les renseignements personnels, qui ne sont accessibles qu'aux personnes autorisées.

4. **Authentification :** acte permettant d'établir la validité de l'identité d'une personne ou d'un dispositif comme un document électronique ou un site Internet.

5. **Irrévocabilité :** propriété d'une information, d'une action ou d'un document d'être indéniable et clairement attribué à son auteur ou au dispositif qui l'a généré.

LES CONDITIONS NÉCESSAIRES AU SUCCÈS (suite)

En particulier, l'authentification et l'irrévocabilité présentent des défis majeurs dans le cadre du gouvernement en ligne, où les transactions vont de plus en plus se faire dans un espace virtuel dans lequel les contacts physiques sont éliminés. En effet, l'identification des citoyens en ligne présente un enjeu de taille pour la prestation électronique de services. C'est pourquoi le gouvernement doit établir des mécanismes permettant d'assurer que ces finalités soient obtenues, pour un bon fonctionnement de la prestation électronique de services.

Le gouvernement du Québec a amorcé depuis plusieurs années des démarches pour assurer la sécurité dans les systèmes technologiques dans l'administration publique. Ceci a résulté en la création de mécanismes institutionnels, en particulier la « Directive sur la sécurité de l'information numérique et des échanges électroniques dans l'administration gouvernementale », qui est entrée en vigueur en novembre 2000[55]. Cette directive énonce le cadre de gestion de sécurité applicable par les M/O et les responsabilités de ceux-ci en matière de sécurité. Ces démarches sont fructueuses. Cependant, elles doivent faire l'objet d'un meilleur suivi, car elles ne semblent pas être appliquées de façon uniforme dans l'ensemble des M/O. Les programmes doivent aussi être améliorés et renforcés dans cette perspective. De même, il y aurait lieu de revoir cette directive de manière à assurer la sécurité non seulement de l'information numérique, mais aussi de l'ensemble de l'information, que celle-ci soit consignée sur support papier ou sur support numérique.

Le gouvernement du Québec a aussi mis en place des mécanismes de gestion de la sécurité et a développé un ensemble de mesures assurant la protection de l'information numérique et la disponibilité des services publics. Le CERT/AQ, qui a pour rôle de soutenir les M/O en matière de gestion des incidents en sécurité, est l'une de ces mesures. De plus, le CERT/AQ effectue une vigie en sécurité et il permet le ralliement des experts dans ce domaine. Cette démarche doit être encouragée et renforcée. Néanmoins, ces services sont offerts uniquement aux ministères et organismes gouvernementaux : les citoyens, les entreprises et les organismes des réseaux, tant de la santé que de l'éducation, n'y ont pas accès.

• *Un moyen privilégié : l'Institut de la sécurité de l'information du Québec*

Compte tenu de cette lacune et de l'importance de la sécurité dans l'établissement d'un rapport de confiance dans le développement d'un gouvernement en ligne, il semble nécessaire qu'un organisme externe qui a déjà établi sa crédibilité puisse promouvoir et sensibiliser les parties prenantes et la population en général dans le cadre de l'application des principes directeurs sur la sécurité. Cet organisme externe pourrait agir en tant que levier de coopération entre les divers intervenants, tant dans le secteur privé que dans le public, afin que l'échange d'information sur les menaces et la vulnérabilité des systèmes puisse se faire correctement et efficacement. De plus, cet organisme externe serait bien placé pour effectuer l'évaluation des systèmes et mettre en place l'organisation administrative nécessaire pour les certifier et confirmer qu'ils respectent les bonnes pratiques. On pourrait faire l'analogie de la nécessité de la certification avec les processus comptables : chacun est responsable de la tenue de ses livres mais, régulièrement, un comptable certifie l'exactitude des livres et des pratiques comptables.

Afin de répondre à ces préoccupations croissantes en matière de sécurité, le Centre de recherche informatique de Montréal (CRIM) propose la création de l'Institut de la sécurité de l'information du Québec (ISIQ), issue d'un partenariat public-privé.

---

[55] Secrétariat du Conseil du trésor, *Directive sur la sécurité de l'information numérique et des échanges électroniques dans l'administration gouvernementale,* 23 novembre 1999.

Un tel institut se voudrait un catalyseur en matière de services, d'expertise et de meilleures pratiques en sécurité de l'information numérique. Il aurait pour mission de promouvoir et de coordonner les actions visant à assurer la sécurité de l'information numérique dans la société québécoise. Son champ d'action s'articulerait autour de quatre axes principaux, soit la prévention et la sensibilisation, la détection et la réaction en situation d'urgence, la veille et la recherche ainsi que le soutien à l'offre de services. Plus spécifiquement, l'ISIQ pourrait devenir l'organisme qui offrirait au Québec une certification fondée sur des normes internationales basées, entre autres, sur les lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information.

RECOMMANDATIONS

5.15 Nous recommandons de faire de la sécurité informatique une priorité gouvernementale, afin de positionner le Québec comme un leader en matière de sécurité de l'information.

5.16 Nous recommandons au DPI de s'assurer de la généralisation de la mise en œuvre de la « Directive sur la sécurité de l'information numérique et des échanges électroniques ».

5.17 Nous recommandons au gouvernement de soutenir la création d'un Institut de la sécurité de l'information du Québec, tel que proposé par le CRIM (Centre de recherche en informatique de Montréal).

5.18 Nous recommandons que le DPI mette sur pied des programmes de sensibilisation et de formation sur la sécurité informatique auprès de l'ensemble des parties prenantes liées au projet du gouvernement en ligne.

1.5 L'identification

Dans le contexte du développement du gouvernement en ligne, à travers lequel le gouvernement est appelé à offrir de plus en plus de services interactionnels, transactionnels et intégrés, l'identification des utilisateurs devient un enjeu majeur. En effet, dans un monde virtuel où les services sont délivrés à distance et où il n'y pas d'interaction physique, un processus d'identification sûr des utilisateurs est essentiel pour s'assurer que celui qui est derrière l'ordinateur possède les qualités et les droits requis pour recevoir une prestation de service électronique. La Commission d'accès à l'information rappelle ainsi, dans son Rapport annuel, que : « l'identité à distance présente un risque plus élevé d'erreurs qu'une vérification d'identité en personne. Ce risque supplémentaire se doit être considéré[56] ».

Afin de s'assurer que le demandeur de services est bien celui qu'il prétend être, le dispensateur de services qui possède déjà des renseignements personnels ou autres informations identifiantes sur le demandeur, par exemple le code d'accès personnel utilisé par le MRQ, n'a qu'à comparer ces informations avec celles fournies par le demandeur. Ce type de procédure correspond au concept reconnu de « secret partagé ». Néanmoins,

[56] Commission d'accès à l'information, *Rapport quinquennal 2002. Une réforme de l'accès à l'information : le choix de la transparence*, novembre 2002, p. 86.

lorsque le dispensateur de services ne possède aucun renseignement personnel ou information identifiante sur le demandeur, des mécanismes doivent être disponibles pour obtenir des garanties raisonnables sur l'identité du demandeur.

La *Loi concernant le cadre juridique des technologies de l'information* précise, à l'article 38, les objectifs de l'identification dans un monde virtuel :

« Le lien entre une personne et un document technologique, ou un lien entre un tel document et une association, une société ou l'État, peut être établi par tout procédé ou par une combinaison de moyens dans la mesure où ceux-ci permettent :

1. de confirmer l'identité de la personne qui effectue la communication ou l'identification de l'association, de la société ou de l'État et, le cas échéant, de sa localisation, ainsi que la confirmation de leur lien avec le document;

2. d'identifier le document et, au besoin, sa provenance et sa destination à un moment déterminé. »

Le degré de certitude quant aux qualités – ou à l'identité - de la personne avec laquelle le dispensateur de services entre en contact est proportionnel à la sensibilité des renseignements échangés : plus les renseignements échangés sont confidentiels, plus le besoin de certitude relativement à l'identité de l'utilisateur du service est élevé, plus les moyens mis en œuvre pour attester de l'identité des auteurs doivent être sécurisés et, par conséquent, plus ils sont coûteux.

Le principal défi dans l'établissement d'un processus d'identification électronique consiste en la mise en place d'un système qui soit le plus simple d'utilisation possible, tout en permettant de minimiser les risques d'usurpation d'identité et de divulgation frauduleuse des renseignements personnels.

Notes

Projet *e-pass* canadien

Le projet e-pass vise à doter chaque citoyen canadien d'un identifiant numérique unique qui lui permette de se prévaloir de services transactionnels qui impliquent l'échange ou le transfert de renseignements personnels et ce, sans porter atteinte au droit à la vie privée. Le e-pass repose sur un processus d'identification de sécurité moyenne, à la suite duquel une clé publique est délivrée au citoyen. C'est à l'aide de cette clé publique et d'un mot de passe (clé privée) que ce dernier peut, par la suite, s'identifier dans chacun des ministères ou organismes auxquels il désire s'adresser. Le gouvernement fédéral entend, au cours des prochaines années, mettre l'infrastructure ainsi développée à la disposition des provinces, afin qu'elles puissent en bénéficier dans leur propre offre de services transactionnels aux citoyens. Tout comme le SQAG, ce système est perfectible sur le plan de la protection de la vie privée.

- ***Situation actuelle***

Le gouvernement du Québec conçoit actuellement un système d'identification qu'il a intitulé le Service québécois d'authentification gouvernementale (SQAG). L'objectif est de déployer un identifiant réutilisable d'un service gouvernemental à l'autre, qui offre un niveau de certitude acceptable et qui peut évoluer vers des niveaux de certitude élevés. Le SQAG a également été conçu pour être compatible avec le système d'authentification développé par le gouvernement du Canada. Cette compatibilité pourrait éventuellement permettre aux citoyens et aux entreprises d'avoir accès aux services en ligne provinciaux et fédéraux, à l'aide d'un même identifiant. La vérification de l'identité se fait par le premier ministère ou organisme auquel le citoyen s'adresse pour se prévaloir d'un service en ligne, en ayant recours à des secrets partagés (échange de renseignements personnels sur le demandeur, renseignements détenus à la fois par celui-ci et par le dispensateur de services). À la demande du ministère ou de l'organisme dispensateur de services, un fournisseur de certificats émet ensuite un identifiant qui ne contient qu'un pseudonyme et qui par conséquent ne révèle pas directement l'identité du détenteur. Les ministères ou organismes peuvent ainsi faire le lien entre un certificat et un citoyen sans avoir accès aux renseignements personnels ayant permis d'établir son identité. Les journaux de transactions associés à l'usage d'un certificat sont conservés par le fournisseur de certificats, lequel n'est pas en mesure de connaître l'identité des détenteurs de certificats, les renseignements sur l'identité étant conservés par une autre entité.

Par ailleurs, le SQAG introduit plusieurs mesures permettant de minimiser les possibilités de traçabilité et de profilage. Un des moyens utilisés offrira aux citoyens le choix d'utiliser plusieurs identifiants.

Le SQAG, toujours en cours de développement, représente donc une voie prometteuse en ce qui concerne la protection de la vie privée; il résoudra en grande partie le défi d'authentification de l'identité en ligne.

- ***Un système perfectible***

Certains analystes qui se sont penchés sur la solution du SQAG et sur d'autres systèmes similaires basés sur l'utilisation de certificats de type X.509 et, entre autres, sur la technologie Entrust (www.entrust.com), sont par ailleurs critiques quant aux risques liés à la protection des renseignements personnels. La mise en place d'un cadre de gestion organisationnel permet, à cet effet, d'assurer une gestion des risques liés à la protection de la vie privée. Cela s'avère d'autant plus important lorsque la technologie n'assure pas en elle-même certains de ces risques, ceux-ci pouvant être élevés. Ces cadres de gestion nécessitent toutefois beaucoup d'investissements, tant au plan financier qu'en matière de ressources humaines.

Par exemple, le Registre des droits personnels et réels mobiliers, dont la structure repose sur une infrastructure à clé publique conventionnelle, comporte des risques pour la vie privée des utilisateurs. Ces risques sont toutefois relativement bien contrôlés par la mise en place d'un cadre de gestion organisationnel approprié.

En effet, lors de l'émission de certificats, le fournisseur de certificats peut, à travers les fonctions classiques de réseau, connaître sans difficulté l'adresse IP de l'utilisateur (voir encadré de la page suivante). Même si le M/O fait office d'intermédiaire entre le fournisseur de certificats et l'utilisateur, l'adresse IP est révélée par la redirection à travers le fureteur de l'utilisateur. Conséquemment, le fournisseur de certificats peut situer géographiquement le récepteur du pseudonyme, ce qui lui permet de connaître son adresse sans difficulté. Il pourrait ensuite utiliser cette information et la jumeler avec le ou les pseudonymes **qu'il connaît** pour créer des profils d'utilisateurs. De plus, le fait que l'utilisateur puisse choisir d'utiliser un seul pseudonyme pour l'ensemble des prestations électroniques de service auxquelles il a recours augmente aussi les risques de profilage.

Qu'est-ce que l'adresse IP ?

Pour faire une analogie, l'adresse IP fonctionne sensiblement comme le code postal utilisé dans l'adresse municipale. En effet, l'adresse IP permet aux ordinateurs de communiquer entre eux. Elle est composée d'un groupe de quatre nombres permettant d'identifier le destinataire d'une connexion Internet. Une adresse IP est représentée sur 32 bits et écrite sous la forme de 4 octets séparés par des points (par exemple : 192.168.10.66).

Les techniques cryptographiques modernes sont une voie prometteuse pour répondre à ces préoccupations, en éliminant ces risques. Comme ces technologies ne sont pas encore mûres et accessibles, il demeure important, pour le gouvernement, d'encourager leur développement le plus rapidement possible afin de pouvoir en tenir compte dans la conception des solutions d'authentification et d'identification en ligne. À titre d'exemple, la signature aveugle et la signature aveugle restrictive empêcheraient, avec un degré de certitude élevé, le fournisseur de certificats d'avoir recours à des fonctions classiques de réseau, comme l'adresse IP, pour établir des profils sur les récepteurs des pseudonymes. En effet, grâce aux techniques cryptographiques modernes, le fournisseur de certificat ne peut, d'aucune façon, connaître le pseudonyme qu'il distribue. Seuls les utilisateurs connaissent les pseudonymes, et seuls les ministères et organismes peuvent effectuer l'appariement entre le pseudonyme et le dossier interne de l'individu. Les M/O n'ont, dans ce cas, qu'à vérifier l'authenticité du certificat (la signature) auprès du fournisseur de certificats.

En sommes, il appert que les risques liés au profilage d'information sur les utilisateurs ne sont pas complètement éliminés avec le SQAG. C'est pourquoi le gouvernement du Québec doit prévoir des mesures additionnelles pour pour améliorer le respect des principes directeurs en matière de protection des renseignements personnels.

RECOMMANDATION

5.19 Nous recommandons de poursuivre le développement du SQAG tout en maintenant les efforts actuels pour, d'une part, diminuer le plus possible les risques relatifs à la protection des renseignements personnels et, d'autre part, s'assurer d'une harmonisation et d'une compatibilité avec les démarches du gouvernement fédéral en matière d'émission de certificats.

2. Simplifier l'accès aux services gouvernementaux

Le gouvernement en ligne vise aussi, de façon générale, à simplifier l'accès aux services gouvernementaux, en mettant l'accent sur les centres multiservices, en favorisant l'accès gratuit au réseau, en étendant le réseau à large bande et en prenant en considération les besoins spécifiques des personnes ayant des limitations motrices, sensorielles ou cognitives (voir schéma 14, p. 149).

2.1 Mettre l'accent sur les centres multiservices d'accès multimodes

Tel que déjà mentionné, le gouvernement en ligne doit prendre en compte les personnes qui ne peuvent pas ou ne veulent pas utiliser l'ordinateur ou l'Internet. Il faut qu'eux aussi puissent avoir accès aux nouveaux services développés. C'est pourquoi il faut développer des centres multiservices, doublés de centres d'appels. Les réseaux que constituent tant les réseaux de Communications-Québec que ceux des Centres locaux d'emploi (CLE) constituent une bonne base pour abriter ces centres multiservices. Il faut au plus vite que des ententes soient prises avec les deux ministères concernés pour en arriver rapidement à l'établissement de ces centres.

• *Le nouveau rôle du fonctionnaire*

La mise sur pied de centres multiservices, accessibles via un comptoir de services ou un numéro de téléphone unique, nécessite la pleine participation des fonctionnaires qui y œuvrent. En effet, le travail des fonctionnaires sera décloisonné de manière à ce qu'il puisse répondre à des questions et des demandes d'ordre général de la part des citoyens, qui dépassent le cadre strict d'un ministère et d'un organisme.

Afin de mener à bien ce projet, le gouvernement du Québec aurait avantage à s'inspirer d'une expérience similaire menée par Service Nouveau-Brunswick. La province a en effet mis sur pied pour ses citoyens des centres multiservices, à l'image de ce qu'il est projeté pour le Québec. Ces centres connaissent un réel succès. Les fonctionnaires en charge de l'accueil et du service aux citoyens ont été parties prenantes du projet dès le départ. De façon générale, ces fonctionnaires considèrent que l'élargissement de leur tâche lié au décloisonnement des services offerts leur permet de mieux répondre aux besoins des citoyens, puisqu'ils sont désormais en mesure de les prendre en charge du début à la fin de leur cheminement auprès des instances gouvernementales. Ces responsabilités élargies procurent aux fonctionnaires un sentiment d'accomplissement et un degré de motivation accru.

2.2 Favoriser l'accès gratuit au réseau

Dans toute société démocratique, l'accès à l'information doit être considéré comme un droit, au même titre que les autres droits fondamentaux. L'Internet est devenu, au fil des ans, l'un des vecteurs principaux de l'information. Pour plusieurs, « […] l'appropriation sociale des technologies doit être vue sous l'angle du droit à l'accès aux technologies, en tant que droit qui s'inscrit dans la foulée des autres droits tels les droits à l'éducation, à la communication, à l'information, etc.[57] »

Certes, l'entreprise privée a développé le marché de l'accès à Internet, et demande aux utilisateurs des droits pour pouvoir se connecter au réseau. Cette situation engendre une concurrence qui s'avère bénéfique pour le citoyen : les coûts d'accès au réseau au Québec seraient parmi les plus bas au monde. Il n'en demeure pas moins qu'un gouvernement responsable se doit d'aider les citoyens qui n'en n'ont pas les moyens ou qui ont d'autres priorités financières à accéder au réseau, en favorisant la multiplication des postes d'accès publics gratuits. La situation économique d'un individu ne devrait pas lui rendre impossible l'accès à Internet.

---

[57] Communautique, *Inforoute Point d'accès* (document de présentation), novembre 2003, p. 6.

LES CONDITIONS NÉCESSAIRES AU SUCCÈS (suite)

C'est ainsi qu'entre 1995 et 1998, le Fonds de l'autoroute de l'information a octroyé 7 millions de dollars à l'installation de plus de 1120 postes dans 831 bibliothèques publiques à travers le Québec. Aujourd'hui, la totalité des bibliothèques publiques autonomes et la plupart des bibliothèques affiliées à un centre régional sont maintenant branchées à Internet. (La plupart de ces connexions sont assurées par un modem téléphonique. La nécessité pour les communautés d'avoir accès à des connexions haute vitesse sera traitée dans les pages qui suivent.) L'accès à l'Internet via le réseau des bibliothèques publiques permet de plus un soutien aux citoyens peu familiers avec les nouvelles technologies de l'information. En effet, les différents intervenants oeuvrant dans les bibliothèques pourraient devenir des personnes-ressources qui feraient office d'agents d'aide auprès des utilisateurs peu familiers avec la navigation Internet et la prestation de services gouvernementaux en ligne.

D'autres initiatives, principalement menées par les groupes d'action communautaire, sont déjà en cours afin de mettre à la disposition des citoyens du Québec des postes publics d'accès à Internet gratuits[58]. À titre d'exemple, citons le groupe Communautique, qui a mis sur pied 98 centres d'accès Internet à travers la province. Ce réseau, en plus d'offrir aux usagers l'accès gratuit à des postes connectés à l'Internet, se donne pour mission de sensibiliser et d'éduquer sa clientèle à l'usage des TIC. Le travail de ces groupes repose sur une stratégie d'implantation dans le milieu qui s'échelonne sur plusieurs années : les responsables doivent connaître leur clientèle potentielle pour gagner la confiance du milieu. Cette implantation dans le milieu doit donc reposer sur un plan stratégique à moyen terme, ce qui n'est possible que dans la mesure où le financement récurrent de ces organismes est assuré pour quelques années.

Dans ce contexte, il est souhaitable que le gouvernement développe un partenariat avec les organismes communautaires pour rendre disponibles aux citoyens dans le besoin la formation et l'accès gratuit à l'Internet, et qu'il le fasse en harmonisation avec le gouvernement fédéral, dans un exercice de renforcement et de rationalisation.

En plus de soutenir les organismes à but non lucratif, le gouvernement du Québec se doit, parallèlement, de contribuer à accroître les possibilités d'accès gratuit au Web. Les centres multiservices gouvernementaux pourraient ainsi être mis à contribution. L'initiative repose donc sur un réseau déjà établi, ce qui s'avère peu coûteux et contribue à faciliter l'initiation aux TIC.

---

[58] L'expérience semble démontrer que les bornes interactives, considérées comme la voie de l'avenir pendant un certain temps, ne constituent pas la solution à privilégier. De l'avis de Bell Canada qui en a fait l'essai, la mise en place de bornes interactives destinées au public semble à la fois impopulaire (les gens ne sont pas familiers avec ce type d'interface et sont réticents à y avoir recours) et très coûteuse (la particularité première des bornes étant de pouvoir être disponibles dans des endroits passants ouverts au grand public, elles sont sujettes à des bris et au vandalisme). Enfin, il semble que les utilisateurs de services Internet soient moins enclins à transmettre de l'information sensible via une borne interactive, faisant davantage confiance à un poste informatique « classique ».

RECOMMANDATIONS

5.20 Nous recommandons de mettre sur pied un programme de partenariat avec les groupes communautaires pour offrir à tous les citoyens un accès réel à l'Internet et de prendre les mesures nécessaires pour que ces groupes partenaires aient accès à du financement récurrent pour assurer leur survie à moyen terme.

5.21 Nous recommandons de mettre sur pied un programme de formation destiné aux personnes-ressources, qui agiront à titre de soutien à l'usager à la fois dans les bibliothèques, dans les centres d'accès communautaires et dans les centres multiservices gouvernementaux.

5.22 Nous recommandons de favoriser les initiatives qui visent à mettre à la disposition des citoyens des postes publics d'accès à Internet gratuits, entre autres par l'entremise des bibliothèques municipales ou des centres de services gouvernementaux.

2.3 Étendre le réseau à large bande

Afin que le plus grand nombre de Québécois possible puisse bénéficier du projet du gouvernement en ligne, le gouvernement a la responsabilité de favoriser l'accès au réseau haute vitesse sur l'ensemble du territoire québécois. En effet, l'accès à des services à large bande s'avère nécessaire pour se prévaloir de toute la potentialité des services offerts par Internet. Selon une récente étude de Statistique Canada, les services à large bande « se prêtent à des applications qui seraient tout simplement impossibles par accès *commuté* à Internet avec une ligne téléphonique et le modem standard »[59]. Il en est ainsi de toutes les applications qui nécessitent de la vidéo (surtout utilisées par les institutions, en matière de télémédecine ou de formation en ligne, par exemple).

Le plan d'action du Parti libéral du Québec, adopté en septembre 2002, souligne d'ailleurs la nécessité de la connexion haute vitesse : « Dans cette ère nouvelle, l'accès à une connexion Internet haute vitesse est aussi essentiel que l'électricité ou le téléphone. […] L'égalité dans l'accès aux technologies doit devenir un principe de base du développement de la société québécoise[60] ». C'est ainsi que, dans son discours inaugural, le premier ministre déclarait, le 4 juin 2003 : « Nous allons brancher les régions. Avant la fin de ce mandat, des connexions Internet haute vitesse seront disponibles dans toutes les régions du Québec ».

Selon cette même étude, Statistique Canada rapporte que « près de la moitié (49 %) de l'ensemble des ménages [canadiens] où l'on se sert régulièrement d'Internet avaient une connexion à Internet haute vitesse en 2001 », ce qui classe les Canadiens parmi les plus importants utilisateurs des services à large bande au monde (la Corée se classe au premier rang, le Canada au deuxième et la Suède en troisième en ce qui a trait à la proportion des utilisateurs branchés haute vitesse sur l'ensemble de la population). En comparaison avec le reste du pays, le Québec affiche du retard, 42 % des ménages branchés à l'Internet ayant une liaison à haute vitesse. Cette même étude révèle qu'en 2002, « 58 % des entreprises branchées à Internet avaient recours aux technologies à large bande».

---

[59] Statistique Canada, *À grande vitesse sur l'autoroute de l'information : les services à large bande au Canada,* Série sur la connectivité, septembre 2003.

[60] http://www.plq.org/tousdocuments/planaction.pdf, p.33.

LES CONDITIONS NÉCESSAIRES AU SUCCÈS (suite)

Plusieurs technologies permettent d'avoir une connexion dite à large bande ou haute vitesse[61], les principales étant le modem de câblodistribution, la ligne numérique d'accès à Internet (offerte par les fournisseurs de services téléphoniques) et le satellite. Alors que ce dernier est encore très dispendieux et non disponible sur la totalité du territoire québécois[62], l'accessibilité par voie de câblodistribution, tout comme celle par ligne numérique, nécessitent que les fournisseurs de câblodistribution et de téléphonie mettent à niveau l'infrastructure de base existante. Or, cette mise à niveau implique des investissements qui ne se rentabilisent qu'à partir d'un nombre d'abonnés donné. C'est pourquoi les entreprises de téléphonie et de câblodistribution ne sont pas en mesure de fournir l'accès à Internet haute vitesse sur l'ensemble du territoire québécois, et ce même si leur infrastructure de base couvre l'ensemble du territoire (particulièrement en ce qui concerne la téléphonie). Ainsi, en 2001, seules 27 % des petites localités[63] ayant accès au câble avaient aussi accès à Internet par câble.

Les entreprises de services de télécommunication consultées estiment que plus de 90 % de la population du Québec a la possibilité d'accéder à l'Internet haute vitesse. Bien que cette proportion soit encourageante, il n'en demeure pas moins que le gouvernement a une responsabilité envers la portion restante de la population qui n'a pas accès à ces services, d'autant plus que c'est souvent cette population plus éloignée qui pourrait tirer le plus d'avantages de ces services (que l'on pense à la formation à distance ou à la prestation de services gouvernementaux en ligne par exemple).

Afin d'élargir l'accès à l'Internet haute vitesse à l'ensemble des régions éloignées, le Groupe de travail national sur la large bande propose, d'une part, « l'appui de l'infrastructure pour encourager les fournisseurs de services à large bande à accroître la desserte, et [le] regroupement communautaire pour agréger la demande de divers groupes qui pourraient profiter de tels services[64] » . Quelques programmes répondant à ces objectifs ont déjà été mis en place au pays. À titre d'exemple, en Alberta, via le programme *SuperNet* qui mise sur un partenariat entre le public et le privé, 422 communautés éloignées ont été branchées à Internet, pour un investissement de 193 M$. Le gouvernement fédéral compte quant à lui investir 105 M$ en trois ans dans le cadre du Programme pilote rural et nordique de développement de services à large bande [65]. Ce programme vise à étendre le réseau à large bande aux communautés éloignées, en finançant jusqu'à 50 % des coûts d'infrastructure nécessaires, la portion restante étant financée par les entreprises fournisseurs de services et par les communautés elles-mêmes.

---

[61] Le *Groupe de travail national sur la large bande* établit que pour être qualifiée de haute vitesse, une connexion doit avoir une vitesse de transmission bidirectionnelle minimale de 1,5 Mb/s (Source : Statistique Canada).

[62] Le satellite Hugues Aircraft, commercialisé par plusieurs entreprises au Canada, est positionné au-dessus du territoire américain. Cela a pour conséquence que plus on s'éloigne vers le nord, plus il devient difficile d'avoir accès au signal, cela devenant quasi impossible à la latitude du Lac-St-Jean. Un second type de lien satellite est possible (celui utilisé par les compagnies de téléphone et les télédiffuseurs), mais son coût est trop élevé pour constituer une solution envisageable, mis à part pour les sites très isolés (Source : Conseil du trésor).

[63] Par petites localités, Statistique Canada entend les divisions de recensement en dehors des régions métropolitaine de recensement et des agglomérations de recensement (lesquelles sont d'au moins 10 000 habitants).

[64] Statistique Canada, *À grande vitesse sur l'autoroute de l'information : les services à large bande au Canada*, Série sur la connectivité, septembre 2003, p. 21.

[65] Jusqu'à maintenant, le Québec a soumis 33 projets au programme, dont trois ont été acceptés pour une subvention totale de 4,8 M$.

Au Québec, le programme Villages branchés du Québec prévoit un partenariat entre les commissions scolaires, les municipalités, les entreprises privées et l'État, afin d'étendre l'accès à Internet haute vitesse aux régions éloignées. En connectant les établissements scolaires et les bâtiments municipaux au réseau à large bande, le programme constitue un levier qui accélère le déploiement des infrastructures du secteur privé. Il répond ainsi à l'un des impératifs soulevés par le groupe CANARIE[66] quant au développement de solutions qui permettent l'accessibilité à l'Internet haute vitesse. Le groupe favorise ainsi les initiatives qui font en sorte que les citoyens ou les municipalités prennent en charge leur connexion Internet, en voyant eux-mêmes à l'installation d'infrastructures qui leur permettent de se connecter sur un réseau déjà existant.

Programme Villages branchés du Québec

Le programme Villages branchés du Québec connecte entre eux les établissements scolaires et municipaux, les connexions externes continuant à se faire via les réseaux de services qui desservent actuellement le gouvernement, tels le Réseau d'information scientifique du Québec (RISQ), le Réseau de télécommunication multimédias de l'administration publique (RETEM) et le Réseau de télécommunication sociosanitaire (RTSS). L'usage de la fibre optique est explicitement favorisé par le programme. Par analogie avec ce que l'on trouve dans le secteur de l'habitation, le modèle de financement des projets est celui des *condominiums*, où chaque partenaire contribue à la mise en place des infrastructures. Le programme assume aux deux tiers les dépenses admissibles, la portion restante de un tiers devant être fournie par les organismes admissibles. Ce sont les ministères de l'Éducation et des Affaires municipales, du Sport et du Loisir qui engagent les montants initiaux, les projets approuvés en vertu du programme étant par la suite remboursés à ces ministères. Une étude préliminaire de chaque projet est préalable à toute demande faite au programme Villages branchés. Ces études peuvent être subventionnées par le Fonds de l'autoroute de l'information jusqu'à hauteur de 25 000 $.

À la fin de l'année 2003, 14 projets avaient déjà été réalisés, pour un investissement total de 71 M$. De ce montant, 39 M$ étaient fournis via le programme Villages branchés, et 32 M$ étaient directement investis par les promoteurs et partenaires privés. À cette même date, 46 projets étaient toujours en cours d'analyse, totalisant des investissements potentiels de 107 M$ de la part de l'État, et de 80 M$ de la part des promoteurs et partenaires privés. Le gouvernement vient de consentir 150 M$ au programme afin de mettre en œuvre les projets soumis. À terme, la réalisation de ces projets permettra de connecter quelque 800 municipalités à travers la province.

En facilitant le déploiement d'une infrastructure de base entre les établissements visés, le programme minimise d'autant les investissements des promoteurs privés nécessaires pour connecter au réseau à large bande les entreprises et les ménages des particuliers. « Les télécommunicateurs qui s'associent aux projets financés par le programme […] en profitent pour ajouter eux-mêmes des capacités de transmission qu'ils pourront mettre à profit pour desservir entreprises et ménages des régions concernées. […] Ces investissements privés ne seraient pas réalisés sans le partage des coûts entre le secteur public et le secteur privé que permet le programme ».

Source : Secrétariat du Conseil du trésor, document interne, 2004.

---

[66] CANARIE inc. est un organisme sans but lucratif soutenu par ses membres, par ses partenaires de projet et par le gouvernement fédéral. La mission de l'organisme est d'accélérer l'aménagement et l'utilisation de l'Internet évolué au Canada en encourageant l'adoption généralisée de réseaux plus rapides et plus efficaces et en habilitant la prochaine génération de produits, d'applications et de services évolués. (Tiré du site Internet de l'organisme. Pour plus d'information, voir http://www.canarie.ca).

RECOMMANDATIONS

5.23 Nous recommandons au gouvernement de faire en sorte, en partenariat avec les réseaux de télécommunication présents au Québec, que l'accès à haute vitesse soit une réalité à la fin de 2007 pour la presque totalité des citoyens du Québec.

5.24 Nous recommandons, afin de refléter la priorité gouvernementale, que l'état d'avancement du déploiement de la large bande sur le territoire québécois soit communiqué de façon régulière à l'ensemble des citoyens.

2.4 Tenir compte des personnes ayant des limitations motrices, sensorielles ou cognitives

Le projet du gouvernement en ligne vise à améliorer les services auxquels ont droit tous les citoyens, citoyennes et entreprises du Québec. Les personnes ayant des limitations motrices, sensorielles ou cognitives ne doivent surtout pas être mises à l'écart du projet, d'autant plus que l'Internet peut constituer, pour cette clientèle particulière, une source d'information des plus riches, de même qu'un moyen de communiquer avec des personnes qui vivent des situations semblables. En ce sens, l'accès à l'Internet constitue souvent, pour ces clientèles, non seulement une façon plus pratique d'accéder aux services de l'État, mais bien l'ouverture à des possibilités jusque-là inconcevables : « For people without disabilities, technology makes things convenient, for people with disabilities, it makes things possible[67] ». Or, l'accès à l'Internet pour ces clientèles particulières n'est possible que dans la mesure où des éléments techniques et des orientations précises en ce sens sont considérés et concrétisés en des règles formelles.

Dans le cadre du projet de loi 155 sur l'exercice des droits des personnes handicapées, le Comité d'adaptation de la main-d'œuvre (CAMO) soulignait ainsi, dans son mémoire, « [qu'il] est clair que sans un engagement formel sur la question [de l'accès aux technologies de l'information], de la part du gouvernement du Québec, la fracture numérique à laquelle sont confrontées les personnes handicapées continuera de s'étendre et prendra bientôt les allures d'un véritable gouffre[68] ».

---

[67] Treviranus, J., *Expanding the Digital Media in More Human Directions*, 2000, cité dans Comité d'adaptation de la main-d'œuvre (CAMO) pour personnes handicapées, *Projet de loi 155. Loi modifiant la Loi assurant l'exercice des droits des personnes handicapées et d'autres dispositions législatives, Mémoire du comité d'adaptation de la main-d'œuvre pour personnes handicapées*, 2003, disponible à l'adresse www.camo.qc.ca/proloi155.htm (février 2004) p.9.

[68] Comité d'adaptation de la main-d'œuvre (CAMO) pour personnes handicapées, *Projet de loi 155, Loi modifiant la Loi assurant l'exercice des droits des personnes handicapées et d'autres dispositions législatives, Mémoire du comité d'adaptation de la main-d'œuvre pour personnes handicapées*, 2003, disponible à l'adresse www.camo.qc.ca/camo/proloi155.htm (février 2004).

a) Des efforts déjà amorcés dans la bonne direction

Le gouvernement fédéral a inclus des critères spécifiques d'accessibilité dans son document « Normes et directives sur la normalisation des sites Internet[69] », par exemple en prévoyant le sous-titrage, un service d'aide téléphonique en ligne, etc. Les ministères sont tenus de souscrire à ces normes. La *Loi de 2001 sur les personnes handicapées* de l'Ontario[70] comprend quant à elle des dispositions qui concernent l'accessibilité des sites Web.

Au Québec, le ministère des Relations avec les citoyens et de l'Immigration a publié le « Cadre de diffusion de l'information gouvernementale sur Internet[71] », qui propose quelques consignes minimales en matière d'accessibilité. Il semble toutefois que cette règle ne soit pas systématiquement appliquée.

En effet, selon une récente étude[72] ayant analysé, entre autres, cinquante sites du gouvernement du Québec, la très grande majorité (94 %) d'entre eux présentent un degré d'accessibilité allant de « nul » à « faible ». Le Cadre de diffusion aurait ainsi avantage à être bonifié, afin d'inclure des consignes complètes en ce qui a trait aux normes et techniques d'accessibilité.

Notes

Les éléments techniques de programmation liés à l'accessibilité des sites Web

L'accessibilité des sites Internet aux personnes ayant des déficits moteurs et sensoriels est étroitement liée à des éléments de programmation, qui pourraient être facilement pris en compte lors de la programmation initiale des sites. Ainsi, les erreurs les plus fréquentes sont les suivantes :

- erreur de codage html ou CSS;
- manque d'équivalents textuels pour les images;
- utilisation de caractères trop petits ou contraste insuffisant entre la couleur des textes et celle du fond de l'écran;
- en-têtes absents ou mal utilisés;
- utilisation de java script (partiellement supporté par les technologies d'adaptation);
- script inaccessible au clavier;
- ouverture de fenêtre sans avertissement;
- changement de langue non identifié;
- étiquettes des formulaires mal associées ou manquantes.

---

[69] Secrétariat du Conseil du trésor du Canada, *Normalisation des sites Internet*, disponible à l'adresse www.cio-dpi.gc.ca/clf-upe/back-cont_f.asp (février 2004).

[70] Gouvernement de l'Ontario, *Loi de 2001 sur les personnes handicapées de l'Ontario*, chapitre 32, Lois de l'Ontario de 2001.

[71] Ministère des Relations avec les citoyens et de l'Immigration, *Cadre de diffusion de l'information gouvernementale sur Internet*, disponible à www.webmaestro.gouv.qc.ca/ress/Cadre/cadre.htm.

[72] Jean-Marie D'Amour, *Rapport synthèse sur l'évaluation de l'accessibilité des sites Web québécois et canadiens francophones*, 2003, disponible à www.accessibiliteweb.org, [en ligne], site consulté le 20 février 2004.

LES CONDITIONS NÉCESSAIRES AU SUCCÈS (suite)

b) Utilisation du langage simplifié

L'accessibilité à l'information disponible sur l'Internet passe également par la vulgarisation et l'allègement des textes, afin qu'ils puissent être compris par le plus grand nombre possible, y compris par les personnes ayant des limites cognitives. À cet effet, il importe de rappeler que les statistiques sur l'analphabétisme au Québec sont préoccupantes. Dans ce contexte, la convivialité des pages Web est essentielle à l'adhésion des utilisateurs (recours aux sigles et aux images pour expliciter des démarches, par exemple). De même, le langage utilisé doit être compréhensible par le plus grand nombre. Celui-ci doit aussi respecter la nécessité d'une communication rapide, voire instantanée, propre aux démarches menées sur Internet. Si de grands efforts ont déjà été entrepris au cours des dernières années à l'égard de ces deux points (convivialité et niveau de langage), force est de constater qu'il y a encore place à l'amélioration, par exemple en ce qui concerne la longueur et la lourdeur des clauses contractuelles que l'on trouve sur plusieurs sites lors de transactions en ligne.

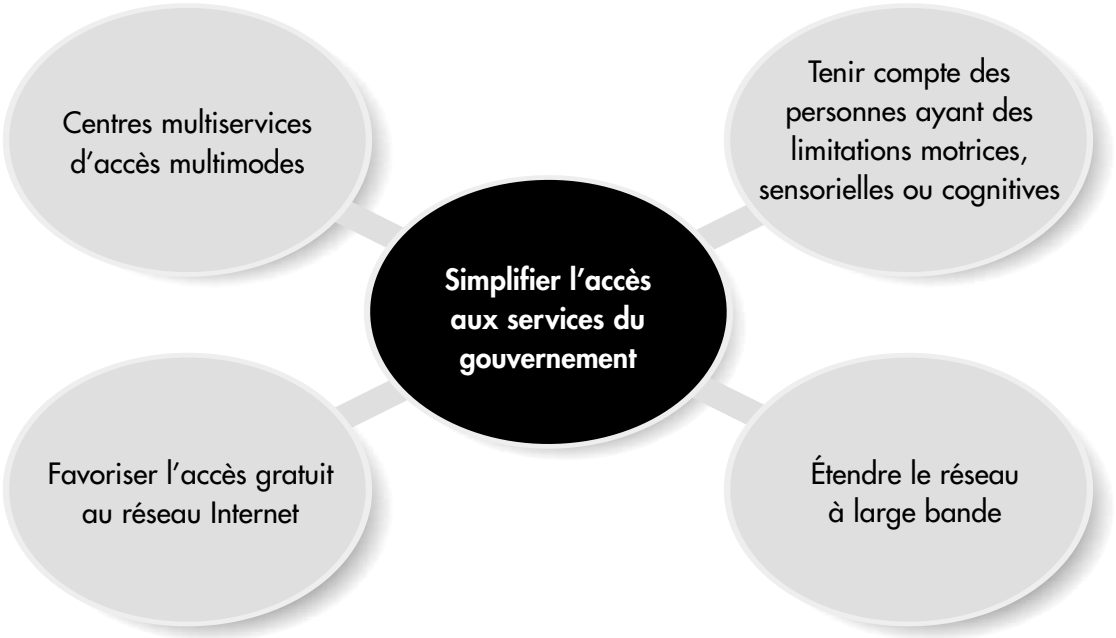
RECOMMANDATIONS

5.25 Nous recommandons d'élaborer et d'adopter une politique en matière d'accès à l'Internet des personnes ayant un handicap, et de modifier en conséquence la *Loi assurant l'exercice des droits des personnes handicapées*.

5.26 Nous recommandons d'adopter une politique sur les règles d'allègement des textes des sites Internet ministériels.

5.27 Nous recommandons de faire en sorte que le C*adre de diffusion de l'information gouvernementale sur Internet* soit bonifié afin d'inclure des consignes complètes en ce qui a trait aux normes et techniques d'accessibilité, et que des mesures soient prises pour qu'il soit appliqué de façon systématique par les webmestres du gouvernement.

Schéma 14 : Comment simplifier l'accès aux services du gouvernement?



3. Informer et sensibiliser la population aux nouveaux modes de relations avec l'État

La réussite du projet de gouvernement en ligne repose avant tout sur la satisfaction des besoins des citoyens. Le gouvernement doit s'assurer de leur adhésion au projet, en leur faisant connaître les services offerts et en les convainquant des avantages à avoir recours aux TIC dans leurs relations avec l'État (voir schéma 15, p. 152). Une telle stratégie de mise en valeur des initiatives gouvernementales passe par une vaste campagne de communication. Les partenaires du gouvernement doivent être partie intégrante de cette sensibilisation.

Une fois les principaux projets mis en place (portail gouvernemental unique de services, page citoyen « Mes info gouv » et initiatives de démocratie en ligne), il serait utile d'entamer une vaste tournée de sensibilisation à travers toutes les régions du Québec. Un plan de communication détaillé devra être rédigé et mis en place afin de cibler tous les publics nécessaires et d'identifier les moyens de mise en valeur des avantages reliés au gouvernement en ligne.

Faire connaître les services en ligne aux citoyens

Un plan de communication devra être élaboré afin de faire en sorte que le projet du gouvernement en ligne et les principales applications qui en découlent soient connus et compris par l'ensemble de la population québécoise. Les citoyens et les entreprises doivent tenir compte des possibilités offertes par les nouvelles technologies et développer le réflexe d'y avoir recours, sans quoi le projet risque de ne demeurer qu'une initiative aux retombées technologiques.

Les technologies de l'information et des communications présentent plusieurs avantages et pourraient être mises au bénéfice des citoyens dans cet effort de sensibilisation au projet du gouvernement en ligne. Par exemple, si l'analyse des coûts et des bénéfices démontre que cela est avantageux, il serait possible de remettre à chaque foyer québécois un CD-ROM interactif d'accompagnement du citoyen lors de sa première utilisation des services en ligne de type transactionnel. Ce CD-ROM pourrait être disponible via les centres multiservices gouvernementaux. De même, il est possible d'offrir aux citoyens de la formation en ligne.

RECOMMANDATIONS

5.28 Nous recommandons de mettre en œuvre une vaste campagne de communication à travers toutes les régions du Québec, comprenant une tournée de sensibilisation en région.

5.29 Nous recommandons d'avoir recours aux outils issus des nouvelles technologies pour accompagner les citoyens lors de leurs premières démarches transactionnelles offertes sur les sites de services gouvernementaux.

3.1 Favoriser le virage technologique de la population du Québec en faisant d'Internet une source d'information à valeur ajoutée

L'Internet ne peut et ne doit pas être considéré uniquement comme un réseau permettant de relier entre eux des millions d'utilisateurs. La *tuyauterie* est certes importante, mais le contenu l'est encore davantage. Les citoyens et citoyennes du Québec doivent développer le réflexe de faire de l'Internet leur première référence, que ce soit pour se prévaloir d'un service gouvernemental ou pour obtenir de l'information sur une gamme élargie de sujets. Ce n'est qu'une fois ce réflexe bien ancré que les possibilités offertes par le gouvernement en ligne seront utilisées à leur pleine potentialité. Le gouvernement doit ainsi non seulement encourager les citoyens à avoir recours au Web dans leur recherche d'information, mais aussi contribuer à faciliter la mise en ligne de contenus utiles aux Québécoises et aux Québécois.

Des initiatives qui visent à mettre du contenu sur l'Internet

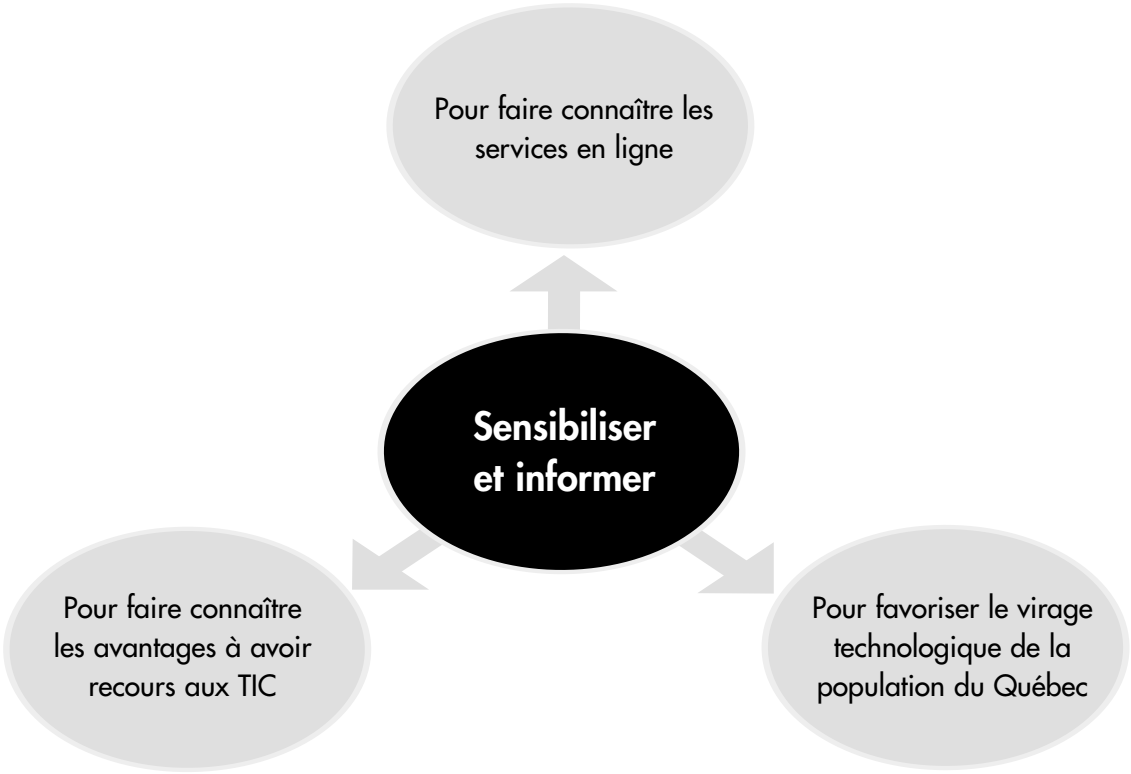
Plusieurs initiatives québécoises visant à mettre du contenu en ligne méritent d'être soulignées. Parmi celles-ci, citons le site de l'Encyclopédie de l'Agora (www.agora.qc.ca), « première encyclopédie virtuelle, évolutive et participative en langue française ». Cette encyclopédie, qui permet aux utilisateurs de faire une recherche sur plus de 6 000 documents, est aussi la première qui a été conçue entièrement en fonction d'Internet. Toute personne peut soumettre un texte à l'encyclopédie afin d'en bonifier le contenu : « chaque élément qui s'ajoute au noyau original de l'œuvre fait l'objet d'un jugement personnel respectant les principes exposés dans la Charte de L'Encyclopédie ». Le site propose ainsi des textes originaux, tout en regroupant des liens qui mènent à d'autres sites Internet reliés au sujet. C'est ainsi que des collections entières de livres peuvent être téléchargées à l'écran! « Cette année, 6 000 000 personnes, dont 1 200 000 Canadiens francophones et 4 500 000 Européens, auront consulté l'encyclopédie et ses documents, répartis en 12 catégories. Cette fréquentation continue de doubler d'une année à l'autre. Un vieux rêve se réalise ainsi : la diffusion de la pensée québécoise dans l'ensemble de la francophonie en synergie avec une technologie moderne. À titre d'exemple, 48 500 personnes ont lu les écrits du politologue Marc Chevrier au cours des 24 derniers mois, chose impensable avec le simple support papier. »

Le portail du Carrefour mondial de l'Internet citoyen (www.globalcn.org) est un espace de convergence, de débats et de coopération pour et par les membres des réseaux citoyens, les organismes, les institutions et les individus impliqués dans l'utilisation des TIC à des fins citoyennes et de promotion et de défense des droits et libertés. Le portail collaboratif trilingue (français, anglais et espagnol), propose des textes sur des sujets aussi variés que les droits de l'Internet, les logiciels libres, la société de l'information et les projets d'applications concrètes des TIC menés par des praticiens de la société civile, tout en privilégiant la pluralité et la diversité culturelle. Un répertoire d'organismes ainsi que des liens vers des ressources externes complètent l'information offerte par le portail.

RECOMMANDATION

5.30 Nous recommandons que le gouvernement se dote de moyens d'action pour favoriser l'émergence de services à contenu québécois sur Internet.

Schéma 15 : Pourquoi sensibiliser et informer la population?



4. Adhésion de la fonction publique et des intervenants des réseaux

La mise en place d'un réel gouvernement en ligne nécessite non seulement un changement dans la façon de présenter les services aux citoyens (ce qu'on appelle les services de première ligne), mais également une transformation de la prestation de services en soi (ce qu'on appelle l'arrière-boutique). Cette transformation implique une révision des façons de faire et de fait, une révision de l'organisation du travail des fonctionnaires, autant ceux des ministères et organismes que ceux des établissements du réseau public et parapublic. En effet, l'automatisation de plusieurs fonctions gouvernementales rend obsolètes certains travaux de bureau. La mise en œuvre d'un gouvernement en ligne crée une occasion unique de valoriser davantage le rôle de plusieurs membres de la fonction publique, en accroissant leur degré d'autonomie et en introduisant dans leurs tâches de nouvelles opérations qui exigent plus de connaissance et d'habileté. Ceci est fondamental à la prestation électronique des services de type horizontal (voir schéma 16, p. 155).

Pour une valorisation du rôle des fonctionnaires

Dans le contexte de la mise en place de centres multiservices (via les services au comptoir ou les centres d'appels), les fonctionnaires verront leur tâche décloisonnée, car elle inclura le traitement de demandes relatives aux services de plusieurs ministères et organismes. Par exemple, une personne dont les fonctions sont liées au service à la clientèle étant, à l'origine, à l'emploi du MRCI, devra aussi, dans ce nouveau contexte, être en mesure de répondre aux demandes des citoyens concernant l'emploi, l'obtention de permis, les questions relatives aux revenus, etc. Ces fonctionnaires deviendront ainsi des personnes-ressources capables de prendre en charge l'ensemble des besoins des citoyens et des entreprises.

De même, une personne qui remplissait une fonction de soutien téléphonique pourra voir son rôle transformé en celui de formateur, par exemple pour guider les citoyens lors de leur première utilisation des services en ligne, que cet apprentissage se fasse au téléphone ou en personne, via les services au comptoir.

Dans tous les cas, il sera impératif que les fonctionnaires prennent une part active dans ce processus de transformation de leur rôle. Individuellement, ils doivent aussi avoir le loisir de choisir vers quelle transformation ils souhaitent se diriger.

Les membres de la fonction publique doivent envisager la transformation des services due à la mise en place du gouvernement en ligne comme une opportunité plutôt que comme une contrainte. Or, comme l'expérience l'a maintes fois démontré, les changements mal préparés entraînent généralement des craintes et de la réticence chez les personnes visées. La mise en place du gouvernement en ligne doit se faire en associant les fonctionnaires aux changements qui en découleront.

Le Secrétariat du Conseil du trésor a développé, en 2001, un « Modèle d'accompagnement des changements technologiques pour la fonction publique québécoise ». Les responsables de la mise en œuvre du projet de gouvernement en ligne devront s'inspirer de ce modèle pour l'adapter au contexte propre au projet actuel.

Modèle d'accompagnement des changements technologiques pour la fonction publique québécoise

Le but de ce modèle est de « cerner les éléments de l'environnement propres à la fonction publique québécoise qui interviennent dans les processus de changements technologiques; déterminer les forces et les faiblesses types des changements technologiques de la fonction publique; comprendre la dynamique et l'influence de la relation qui s'établit dans le cadre de ce processus entre les différents acteurs; déterminer des indicateurs de l'efficience de ce processus de changement; déterminer, à l'aide de l'étalonnage avec d'autres administrations publiques, les meilleures pratiques au regard de la gestion des changements technologiques ».

Source *: Fiche synthèse de projet du centre d'expertise en gestion des ressources humaines,* www.tresor.gouv.qc.ca/resource/acrobat/projets/develop.pdf.

- ***La formation***

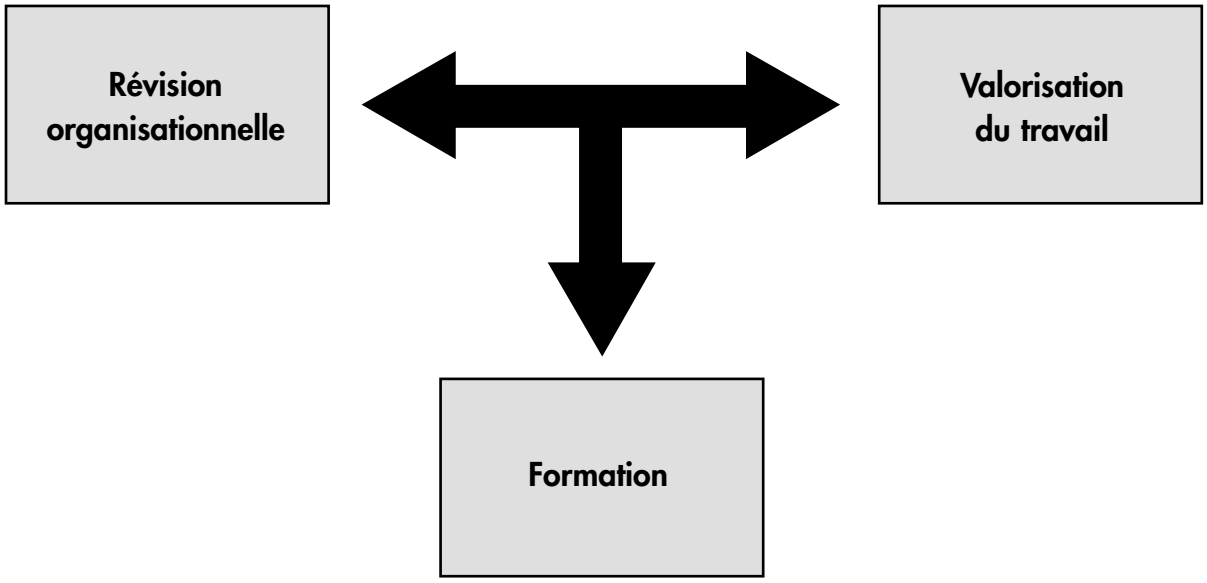
La mise en place du gouvernement en ligne entraînera inévitablement des besoins en matière de formation des membres de la fonction publique. Les fonctionnaires verront leur tâche se transformer, entre autres en raison du décloisonnement de leurs fonctions. La mise en ligne de services nécessitera, pour les fonctionnaires, l'intégration de nouveaux outils techniques à leur tâche. Des formations d'appoint seront ainsi nécessaires afin que les fonctionnaires s'approprient ces outils.

Enfin, ce nouveau contexte lié à la mise en ligne de services aura des implications sur le travail des fonctionnaires, entre autres, en ce qui a trait à la protection des renseignements personnels et du droit à la vie privée et à la sécurité de l'information et des systèmes informatiques. La prestation électronique de services implique que certains fonctionnaires aient accès aux banques de données contenant des renseignements personnels. C'est pourquoi il y aura lieu de sensibiliser les fonctionnaires et d'adapter en conséquence les codes de déontologies auxquels ils doivent se soumettre, afin de mieux baliser les droits d'accès de ceux-ci aux systèmes d'information. Cela s'avère particulièrement nécessaire pour les fonctionnaires de première ligne, qui ont un contact direct avec les citoyens. Une classification des renseignements personnels liée à différents droits d'accès en fonction des niveaux hiérarchiques est également à mettre sur pied. Une telle démarche permettra « d'éviter les risques d'utilisations indues, d'effacement ou de perte des renseignements personnels[73] ».

[73] Centre de recherche en droit public, *Les modifications à apporter aux cadres administratifs et juridiques afin de favoriser le développement de l'administration électronique dans le respect de la vie privée,* Faculté de droit, Université de Montréal, préparé pour le Secrétariat du Conseil du trésor, 18 décembre 2003, p.60.

Afin de s'acquitter de ces formations, le gouvernement entend avoir recours aux possibilités offertes grâce à l'introduction des nouvelles technologies, entre autres des outils de *e-learning*. Ces programmes novateurs permettent aujourd'hui d'assouplir les contraintes généralement reliées aux formations traditionnelles, tout en diminuant les ressources nécessaires à leur mise sur pied.

Schéma 16 : L'adhésion de la fonction publique et des intervenants des réseaux



Les avantages de l'apprentissage en ligne

L'apprentissage en ligne, ou le *e-learning*, présente plusieurs avantages, particulièrement dans le contexte de la formation du personnel.

- Mise en jour instantanée des formations, puisque le contenu est hébergé sur Internet. À cet effet, le gouvernement du Québec entend demeurer ouvert aux possibilités émergentes reposant sur les TIC. À titre d'exemple, le recours à des CD-ROM de type *hybride*, sur lesquels est gravée une partie du contenu de la formation, le reste étant téléchargé à partir de l'Internet de façon tout à fait transparente pour l'utilisateur, constitue une solution prometteuse pour les années à venir en matière d'actualisation de contenu.

- Heure, date et lieu de la formation choisis par l'utilisateur (la formation peut en effet se faire à partir de la maison, dans la mesure où l'employé a accès à l'Internet. Les logiciels de navigation habituels sont suffisants pour permettre le fonctionnement des applications de *e-learning*).

- Intégration de nouvelles approches d'apprentissage (par exemple, évaluation immédiate des acquis, processus non linéaire ou adaptation de la formation aux connaissances préalables de l'utilisateur).

- Diminution des coûts reliés aux formateurs, puisque des économies d'échelle substantielles peuvent être générées.

- Uniformité du message (aucune distorsion possible par les formateurs).

- Possibilité d'échange entre les utilisateurs sur les formations et les apprentissages, grâce à des applications Web complémentaires, par exemple à l'aide de forums de discussion.

RECOMMANDATIONS

5.31 Nous recommandons d'associer les membres de la fonction publique concernés aux transformations découlant de la mise en place d'un gouvernement en ligne.

5.32 Nous recommandons au Conseil du trésor d'adapter le « Modèle d'accompagnement des changements technologiques pour la fonction publique québécoise » afin d'y intégrer les réalités propres au gouvernement en ligne.

5.33 Nous recommandons que soient instaurés des programmes de formation qui pourront utiliser les technologies modernes, pour permettre aux fonctionnaires concernés de s'adapter aux changements liés à la mise en ligne des services et à la création de centres multiservices.