(v97.1) l'antichambre fragments sédiments

Résumé
Sommaire
BIO

Quand *Big Brother* fait du pouce sur l'inforoute

par Martine Gingras

Étudiante au doctorat en communication - Université du Québec à Montréal

Résumé

Ce texte explore la vie privée - des risques d'intrusion aux méthodes de protection - à l'ère des réseaux. Illustrant comment l'informatisation facilite la cueillette, l'emmagasinage, le jumelage et la divulgation des données sur des transactions ou sur des individus, nous soulignons la nécessité de réévaluer les principes et méthodes de protection de la vie privée. Les lignes directrices, codes volontaires, normes internationales et législations nationales ne suffisent pas à protéger efficacement la vie privée sur un réseau mondial; il est nécessaire et impératif de compléter ces méthodes en mettant la technologie elle-même à profit, en utilisant notamment l'encryptage.

Abstract | Resumen

Descripteurs : Internet, interconnexion, vie privée, anonymat, encryptage, citoyens

Sommaire

"Naturellement, il n'y avait pas moyen de savoir si, à un moment donné, on était surveillé. Combien de fois, et suivant quel plan, la Police de la Pensée se branchait-elle sur une ligne individuelle quelconque, personne ne pouvait le savoir. On pouvait même imaginer qu'elle surveillait tout le monde, constamment. Mais de toute façon, elle pouvait mettre une prise sur votre ligne chaque fois qu'elle le désirait. On devait vivre, on vivait, car l'habitude devient instinct, en admettant que tout son émis était entendu et que, sauf dans l'obscurité, tout mouvement était perçu."

George Orwell, 1984.

1. Introduction

Lorsqu'il est question d'inforoutes électroniques, on s'attarde principalement aux constructeurs (compagnies de téléphone, câblodistributeurs, satellites et réseaux informatiques), aux divers matériaux qui seront utilisés pour les paver (câble coaxial, fibre optique, fils de cuivre) et aux véhicules qui y circuleront (télé à la demande, télé-achat, courrier électronique, vote à domicile, etc.).

Nous nous intéressons ici à un thème moins souvent abordé, la vie privée des utilisateurs, qu'on compte déjà au nombre des victimes de ces autoroutes de l'information où les intérêts commerciaux et ceux de l'État ont priorité (1). En effet, la plupart des projets mis en branle prévoient non seulement de permettre la réception de divers services à domicile, mais aussi la transmission d'informations par le citoyen (comme le paiement de factures à domicile). Dans ce contexte, la protection de la vie privée constitue vraisemblablement un des enjeux majeurs des inforoutes.

Nous souhaitons d'abord exposer les risques d'intrusion à l'heure des réseaux, en expliquant comment ceux-ci nous font passer d'une collecte de renseignements nécessaires à un couplage de données établissant le profil des consommateurs et citoyens; un aperçu des brèches que la technologie ouvre dans la vie privée des utilisateurs complétera ce portrait. Dans un deuxième temps, il sera question des solutions éthiques, législatives et technologiques qui peuvent être mises en oeuvre pour contrer les intrusions dans la vie privée.

La vie privée à l'ère de l'informatisation

La vie privée est une valeur universelle, élevée au rang de droit dans les sociétés où les libertés

individuelles sont jugées très importantes. On s'entend généralement pour la définir selon quatre dimensions distinctes, mais néanmoins reliées entre elles: le droit à la solitude, qui consiste à être laissé tranquille lorsqu'on le désire; le droit à l'anonymat donne quant à lui la possibilité de rester inconnu; le droit à l'intimité stipule qu'on n'est pas constamment surveillé; le droit de détermination donne au citoyen le pouvoir de contrôler les données qui circulent à son sujet.

Ces droits implicites ne sont pas pour autant toujours respectés. Tantôt ils se heurtent aux intérêts commerciaux ou gouvernementaux, tantôt ils se retrouvent carrément brimés par les expérimentations plus ou moins philanthropiques d'un pirate qui prône la libre circulation de l'information (hacker). L'informatisation, qui rend de plus en plus aisés et de moins en moins onéreux la collecte, le stockage, le jumelage et la divulgation des données sur des transactions ou sur des individus, a donc de quoi inquiéter les citoyens (2).

3. De l'identification au profil

Vous avez vos papiers?

Évidemment, il est nécessaire de divulguer certains renseignements personnels afin d'établir son crédit ... ou sa crédibilité. Le problème consiste à déterminer quelles demandes de renseignements sont nécessaires à quels types de transactions, et lesquelles constituent une atteinte à la vie privée.
Des firmes comme Equifax (3) se spécialisent dans la collecte massive et dans la diffusion d'informations sur les personnes. Les renseignements que ces agences de crédit collectent et transmettent sont d'abord ceux qui servent à l'identification: le nom, l'adresse, le numéro de téléphone, le numéro d'assurance sociale et l'emploi ou l'occupation.

La suite dépend du demandeur. S'il s'agit d'un établissement de crédit, Equifax fournit des renseignements sur la situation financière générale: ouverture de compte, montant de crédit accordé, dates et informations concernant les transactions (on ne sait tout de même pas exactement ce qui a été acheté), mensualités, solde à la date reporté, historique des retards de paiements antérieurs sur une période de six années et cote de crédit. La faillite prend quant à elle sept ans avant d'être effacée du dossier.

Une autre division du bureau de crédit fournit pour sa part l'information aux compagnies d'assurances, qui ont besoin de renseignements plus détaillés qu'un rapport de crédit pour évaluer le risque qu'elles prennent en assurant les personnes. Elles demandent donc au bureau de crédit d'enquêter sur le compte des clients, cherchant à savoir, au-delà de la situation financière, comment se déroule leur vie professionnelle et quelle est leur réputation morale. Cette dernière rubrique englobe la consommation d'alcool ou de stupéfiants, le statut matrimonial et la réputation auprès des collègues et du milieu. Les compagnies d'assurances déboursent généralement entre 20$ et 50$ pour ces enquêtes, réalisées par le biais d'entrevues avec la personne, avec son employeur ou d'autres personnes devant produire des références et parfois même avec ses voisins.

De plus, pour effectuer certaines transactions ou pour recevoir des soins ou services, il est obligatoire de divulguer les renseignements nécessaires, qui diffèrent selon la situation: le numéro d'assurance-maladie pour recevoir des soins médicaux ou pour faire remplir une ordonnance, le numéro d'assurance sociale pour tout ce qui touche à l'emploi, etc.

La constitution d'un double informationnel

Ainsi, nombre d'informations personnelles circulent sans qu'on puisse parler d'intrusion dans la vie

privée, parce qu'elles sont nécessaires pour effectuer certaines transactions, et leur traitement s'effectue dans les balises prescrites par la loi. Toutefois, l'informatisation a fait émerger un nouveau récif pour la vie privée: le couplage de données.

Il arrive en effet que certaines entreprises privées et publiques associent à d'autres renseignements les données qu'elles avaient collectées dans un autre contexte, afin de constituer des dossiers plus complets. En reliant diverses informations sur un individu, il est possible de tracer un portrait de chaque consommateur-citoyen. Ce phénomène inquiète d'ailleurs une majorité de Canadiens: 54 p. cent d'entre eux se sont dits en effet très préoccupés par "le processus relativement mystérieux et caché qu'est la mise en relation de banques de données" (4).

Contrairement à ce que l'on pourrait croire, le monopole de l'indiscrétion n'est pas détenu par les entreprises avides de connaître le profil des consommateurs. Les gouvernements sont également intéressés. (Ainsi, celui du Québec détient plus de 14 000 fichiers de renseignements personnels, dont une soixantaine comporteraient des données sur plus de 100 000 personnes (5).

Vivons-nous pour autant sous le règne du Big Brother décrit par Orwell? Pas encore, car ces dossiers restent distincts. Le danger est d'en venir, sous prétexte d'efficacité de gestion, de réduction des coûts et de nécessité de contrôle, à regrouper tous ces dossiers en un seul, qui contiendrait tous les renseignements sur chaque citoyen.

Outre la constitution d'un fichier monstre qui saurait tout sur chacun de nous, il est possible qu'on en vienne à tenir compte uniquement de quelques données personnelles combinées à des statistiques, des résultats de sondages ou des profils de consommation, pour prendre, souvent à notre insu, des décisions nous concernant directement. Nous serions alors jugés à partir de notre double informationnel, qui constitue un miroir parfois déformant et, surtout, qui prête à interprétation. Ainsi, un individu pourrait se voir refuser un prêt parce qu'ayant acheté tel et tel produits, il entre dans un certain profil de consommation jugé potentiellement "dangereux" par le prêteur. Bref, une situation qui marquerait un recul notable dans une société où le respect des droits individuels a été acquis chèrement.

L'interconnexion des réseaux, qui facilite l'échange de données d'un bout à l'autre de la planète, rend la situation encore plus alarmante. Il y a déjà environ 20 000 circuits à travers lesquels l'information circule entre les divers organismes publics québécois. La mise en place du Réseau intégré de communications informatiques et bureautiques (Ricib), un réseau qui reliera aux centres-serveurs les quelques 27 000 micro-ordinateurs des ministères et organismes publics québécois, rendra encore plus facile la transmission des données.

Par ailleurs, les nouveaux services disponibles ou à venir (vidéo à la demande, magazines thématiques, télé-achat, etc.) permettront la collecte de renseignements encore plus variés et précis sur les intérêts des gens, rendant ainsi plus aisé l'établissement de profils. Déjà, les compagnies de téléphone accumulent des informations sur les habitudes de leurs clients: localisation, fréquence et durée de leurs appels, tout est répertorié. De même, les communications réalisées via l'Internet sont sujettes à ces analyses de trafic, grâce à une technique qui consiste à déduire des informations à partir de la source et de la destination des envois sans pour autant accéder au contenu. En effet, il est facile de cibler les intérêts des gens quand on connaît les conférences auxquelles ils sont abonnés ou les institutions avec lesquelles ils communiquent. De même, la plupart des sites sur le W3 établissent les statistiques d'utilisation de leurs pages, et fournissent ces données aux annonceurs potentiels.

4. Technologie et inquisition

Brèches ouvertes dans la vie privée

Avec l'évolution des technologies, il est de plus en plus facile de jeter un oeil sur la vie privée d'autrui sans même faire le détour par une quelconque banque de données. Le but poursuivi - et la façon de l'atteindre -peut être plus ou moins légitime, selon le cas.

Prenons l'exemple de l'afficheur, un appareil qui peut sembler tout à fait adéquat pour protéger la vie privée, en permettant de connaître le numéro de téléphone - et maintenant le nom - de la personne qui appelle. Cette technologie entraînerait une diminution des appels obscènes et intimidants. Là où le bât blesse, c'est que l'afficheur a été mis sur le marché avant une évaluation complète des impacts, de sorte que de graves problèmes ont surgi: un mari violent pouvait ainsi découvrir que quelqu'un avait appelé chez lui d'une maison d'hébergement pour femmes battues. Depuis, que le Conseil de la radiodiffusion et des télécommunications (CRTC) a obligé les compagnies de téléphone à bloquer gratuitement l'affichage du numéro de téléphone à tout abonné qui le demande, de sorte qu'il est possible de profiter d'une protection pour soi sans menacer celle des autres.

Autre exemple: le travail à domicile. Les entreprises qui y sont favorables cherchent de nouveaux moyens pour contrôler le travail de leurs employés travaillant à la maison:

> [...] supervisors at American Express have retained the ability to monitor employees who have signed up for the Hearth program (working at home) to ensure "tight control" (Sherman, 1993) (6).

Dans cette optique, on peut se demander à partir de quel moment un employé qui travaille à domicile et qui gère lui-même son horaire peut revendiquer qu'on cesse de le surveiller...

La téléphonie mobile, qui se propose de donner à chacun un numéro de téléphone unique, promet d'amplifier le phénomène: on qualifie parfois cette technologie de "laisse électronique". Elle pose doublement la question de la protection de la vie privée, car il est en plus relativement facile d'écouter les conversations téléphoniques effectuées via un téléphone cellulaire.

La vie privée et l'Internet

Constatant les nombreux écueils qui menacent déjà la vie privée, on peut s'inquiéter de ceux qui joncheront les inforoutes électroniques, en facilitant l'accès et la transmission de données diverses sur les individus.

Il est possible d'en avoir un premier aperçu en étudiant le cas de l'Internet, le réseau informatique le plus développé au monde. Du point de vue de la vie privée, on pourrait qualifier ses utilisateurs de *crash test dummies* (7) des inforoutes en construction...

Sur l'Internet, la frontière entre la nécessaire identification et la sphère privée est encore floue; on cherche encore le juste milieu entre une protection adéquate des droits entourant la vie privée des citoyens et une identification suffisante pour repérer facilement les fauteurs de troubles.

Pour l'instant, c'est l'adresse électronique qui détermine principalement l'identité des utilisateurs. Celle-ci donne un certain nombre de renseignements (par exemple, aux États-Unis, les adresses des établissements d'enseignement se terminent par edu, ceux des commerces par com, etc.), mais laisse aux utilisateurs le soin de spécifier ou d'omettre ce que bon leur semble. En effet, toutes les adresses ne comportent pas nécessairement le nom de l'utilisateur, ni même son statut dans la hiérarchie d'une

institution. De plus, il est possible d'avoir différentes adresses de courrier électronique, les adresses étant par ailleurs sujettes à changement, suivant la situation dans l'institution, les paramètres techniques, etc. L'identité électronique reste donc extrêmement floue.

Aucune technique ne permet de s'assurer que l'identification donnée par une personne est bien la sienne. Il est en effet très facile pour quelqu'un qui connaît le mot de passe d'une autre personne d'expédier du courrier de son adresse. Il est aussi relativement facile pour les pirates avertis de changer la source inscrite dans l'en-tête d'un message électronique. Il est aussi possible pour les usagers possédant une bonne connaissance de l'informatique de savoir qui est connecté à un ordinateur central au même moment qu'eux. La plupart des sites permettent en outre à leurs usagers de vérifier quels autres usagers sont connectés à l'ordinateur serveur en même temps qu'eux, et ce qu'ils font sur le réseau. Ces possibilités vont clairement à l'encontre du droit à l'intimité.

De plus, le fonctionnement actuel de l'Internet oblige les usagers à avoir une confiance aveugle en leur administrateur de réseau. La plupart des systèmes qui gèrent les sites conservent en effet de manière exhaustive l'historique des endroits où leurs usagers se connectent, la liste des commandes qu'ils tapent et le moment où ces actions sont posées. Ces informations ne sont pas systématiquement consultées, sinon lorsqu'un usage douteux du système survient: les connexions ratées, les tentatives d'accès aux dossiers de mots de passe, etc.

Le courrier électronique reçu et envoyé n'est pas non plus à l'abri des yeux indiscrets des responsables de systèmes. Par exemple, les messages en instance d'être envoyés ou qui viennent juste d'être reçus transitent par un dossier intermédiaire (spool file) avant d'arriver à destination finale. Le hic, c'est que les opérateurs de systèmes y ont accès, et on peut supposer que les moins scrupuleux lisent parfois les envois.

En somme, la vie privée sur le réseau, qui consiste à avoir un usage exclusif de son compte, de même qu'un accès unique aux données qui y sont conservées et à celles qui y parviennent, n'est aucunement assurée à l'heure actuelle. Des mesures doivent être prises pour colmater les trous déjà nombreux par lesquels les entreprises privées, le gouvernement et les pirates informatiques peuvent s'immiscer. Les méthodes de protection ne font toutefois pas l'unanimité, comme nous allons le voir dans la prochaine partie.

5. Levée de boucliers plus ou moins efficaces

Lignes directrices, codes volontaires et normes

À la fin des années 1970, l'Organisation de coopération et de développement économiques (OCDE) a établi des lignes directrices pour assurer la saine gestion des renseignements personnels et la protection de la vie privée à l'échelle mondiale. Ces lignes directrices couvraient huit grands principes: limitation en matière de collecte, qualité des données, précision des finalités, limitation de l'utilisation, garanties de sécurité, transparence, participation et responsabilité individuelles (8).

En 1984, le Canada a signé les lignes directrices de l'OCDE et le ministère de la Justice a incité l'industrie à s'y conformer. De plus, c'est en s'inspirant des lignes directrices de l'OCDE que l'Association canadienne de normalisation (CSA) a élaboré son propre code de protection de la vie privée. Son projet est maintenant d'élaborer, conjointement avec les gouvernements, milieux d'affaires et organismes de protection des consommateurs, une norme canadienne sur la vie privée, qui dépasserait le cadre des codes volontaires sans pour autant légiférer sur la question. Ceci permettrait d'établir des lignes directrices plus claires que celles des codes volontaires élaborés par les entreprises .

Les normes de l'Association canadienne de normalisation, annoncées pour le début de 1996, n'étaient pas encore disponibles au moment de la publication de ce document.

La méthode la plus valorisée par les gens d'affaires demeure donc encore celle de l'autoréglementation, qui peut prendre la forme de codes directifs, normatifs ou volontaires. Les codes volontaires ne sont pas nécessairement moins stricts que les lois en ce qui a trait à la protection de la vie privée et des renseignements personnels. Néanmoins, lorsqu'on observe la situation sous l'angle du citoyen, ils présentent de nombreuses lacunes. Ainsi, le manque d'uniformité - et parfois l'absence - de procédures pour connaître l'existence d'un dossier, y accéder ou y faire des corrections rend le processus nébuleux et peu fiable. En cas d'abus, la marche à suivre pour porter plainte n'est pas clairement établie, de sorte que les consommateurs peuvent avoir du mal à faire respecter leurs droits.

Notons que même pour les entreprises, il est de moins en moins avantageux que les renseignements personnels soient insuffisamment protégés dans leur pays. En effet, la Communauté économique européenne (CEE) a émis en 1990 une directive qui exige des garanties assurant aux données à caractère personnel transmises d'un pays à un autre une protection au moins équivalente dans le pays destinataire. L'échange et la manipulation de renseignements personnels se trouvent ainsi encadrés de façon stricte tant à l'intérieur qu'à l'extérieur des pays membres. Une entreprise privée canadienne ayant une filiale en Angleterre pourrait donc se voir refuser la consultation des dossiers de ses employés outre-mer, puisque ce pays possède une loi protégeant les renseignements personnels, alors que le Canada n'en a pas.

Au nom de la loi

Pour l'instant, les lois fédérales canadiennes protègent les renseignements personnels des citoyens uniquement dans le secteur public, avec la Loi sur la protection des renseignements personnels adoptée en 1982 (9). Le Commissaire à la protection de la vie privée du Canada (10) est chargé de faire respecter cette loi. En cas de litige dans le secteur privé, il faut se référer à la Charte des droits et libertés, qui ne protège pas la vie privée de manière explicite. Néanmoins, des jugements récents sur l'article 8 de la Charte (concernant le droit à la protection contre les fouilles, les perquisitions ou les saisies abusives), ont reconnu que les citoyens sont en droit de s'attendre à ce qu'on respecte leur vie privée dans une mesure raisonnable, ce qui demeure somme toute bien peu précis en cas de nécessité de recours. Tout de même, la Loi sur les télécommunications adoptée en 1993 donne au CRTC le mandat et le pouvoir de protéger la vie privée dans les télécommunications.

Jusqu'à tout récemment, alors que les quelque 3 700 organismes publics québécois étaient assujettis à la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels depuis 1982, rien ne réglementait de façon précise l'usage des renseignements personnels dans le secteur privé. Encore une fois, le citoyen lésé devait avoir recours à des protections plus larges : la Charte québécoise des droits et libertés de la personne, la Loi de protection du consommateur et les recours généraux en matière de responsabilité civile.

Le 1er janvier 1994, le Québec devenait la première province canadienne à réglementer la protection des renseignements personnels dans l'entreprise privée. La Loi sur la protection des renseignements personnels dans le secteur privé (la loi 68) établit des règles strictes de collecte, d'utilisation et de diffusion de ces informations. Il est donc plus facile pour les citoyens d'exercer un certain contrôle sur les données personnelles détenues à leur sujet par les quelque 200 000 entreprises privées québécoises.

Ainsi, en constituant un dossier sur une personne, toute entreprise doit désormais inscrire l'objet, c'est-à-dire la raison d'être du dossier, et ne peut recueillir que les renseignements personnels nécessaires à cet objet. Par exemple, si l'objet du dossier est la location de cassettes vidéo, l'entreprise

ne peut exiger le numéro de permis de conduire, à moins d'arriver à démontrer qu'il existe bel et bien un lien entre la conduite automobile et la location de vidéocassettes... Une entreprise privée qui détient des renseignements personnels est aussi tenue de prendre des mesures de sécurité afin d'assurer leur caractère confidentiel. Elle doit donc déterminer qui, dans le cadre de ses fonctions, doit avoir accès aux dossiers contenant des renseignements personnels. En outre, le consentement "manifeste, libre, éclairé et donné à des fins spécifiques" de la personne est requis pour que les renseignements personnels qui lui sont demandés soient ensuite communiqués à des tiers, ce qui diminue les risques qu'il y ait couplage de données à l'insu des individus. Enfin, toute personne a droit d'accéder à son dossier et d'y faire apporter des rectifications. En cas de litige, c'est la Commission d'accès à l'information, le même organisme qui régit déjà le secteur public, qui tranche.

Comme toute loi peut être transgressée, les citoyens doivent tout de même rester vigilants. Même si la loi 68 oblige les entreprises à obtenir l'assentiment du consommateur avant de pouvoir consulter son dossier, certaines tenteront sans doute de passer outre. Sachant qu'une firme comme Equifax reçoit 10 000 demandes par jour, il est évident que la vérification ne se fait pas cas par cas auprès des consommateurs concernés. Par contre, toute demande de consultation est inscrite au dossier de ces derniers, de sorte qu'ils peuvent toujours se plaindre après coup s'ils constatent qu'une entreprise a consulté leur dossier sans leur consentement. La loi permet aussi aux citoyens d'ajouter des précisions dans leurs dossiers si certaines informations contenues semblent incomplètes ou erronées.

La technologie au service de la vie privée

Une dernière façon de protéger la vie privée consiste à "combattre le feu par le feu": trouver des solutions technologiques pour contrer les problèmes d'intrusion amenés par l'informatisation. Sur l'Internet, on conseille de changer périodiquement de mot de passe et de ne pas le divulguer, de toujours taper la commande logout (déconnexion) avant d'éteindre son modem et de ne jamais laisser sa machine sans surveillance lorsqu'elle est connectée au réseau. De plus, des techniques de signature digitale se développent afin d'empêcher les "emprunts" d'identité.

Pour permettre l'envoi anonyme de courrier électronique, des réexpéditeurs (remailers) ont vu le jour. Il s'agit de destinataires intermédiaires qui enlèvent les informations de l'en-tête des envois électroniques avant de les expédier au destinataire.

Une autre technique de protection consiste à utiliser un code de cryptage des données, aussi appelé chiffrement à clé révélée. Ceci empêche qu'une personne qui intercepte une conversation téléphonique, un message ou une transaction électronique puisse prendre connaissance de son contenu, qui ne peut être décodé qu'à destination.

Le cryptage des données soulève cependant une polémique: si cette technique permet de préserver la confidentialité des informations et l'anonymat des citoyens, elle en fait autant pour les fauteurs de trouble. Pour cette raison, la plupart des agences gouvernementales sont opposées au droit inconditionnel de la vie privée et au développement de techniques qui favorisent ce droit, puisque les activités illicites sont, du même coup, difficiles à surprendre. C'est pour cette raison que le Federal Bureau of Investigation (FBI) a souhaité imposer aux États-Unis un code national de chiffrement, le Clipper Chip, dont il aurait un double des clés, au cas où il s'avérerait nécessaire de mettre un criminel sur écoute électronique. Suite aux remous causés par ce projet, le gouvernement américain a finalement concédé que si le Clipper Chip pouvait s'appliquer à la téléphonie, cette technologie n'avait pas d'avenir dans les transactions électroniques.

Si la proposition du FBI a fait autant de remous aux États-Unis, c'est parce que le projet de loi rend coupable d'une infraction civile toute personne - autre que le FBI - qui développerait des technologies

de cryptage de données que le Gouvernement américain ne pourrait décoder. Un peu comme si on n'avait pas le droit d'acheter une serrure à toute épreuve pour protéger sa demeure, sous prétexte que les criminels peuvent aussi protéger leur repaire de cette manière. En conséquence, Philip Zimmermann a risqué la prison pour avoir répandu gratuitement sur l'Internet son logiciel Pretty Good Privacy, un code de cryptage que la police américaine n'a pu percer. Après trois années d'enquête sur Zimmermann, le gouvernement américain a finalement abandonné les charges d'"activités criminelles" qui pesaient contre lui.

D'autre part, la technologie du Clipper Chip, quoiqu'en dise le FBI, n'est pas à toute épreuve. Il est d'ailleurs cocasse que des pirates informatiques aient réussi à violer la sécurité de l'ordinateur de Mykotronx Inc., le fabriquant du code du Clipper Chip, et d'en répandre le contenu sur l'Internet. Les solutions technologiques, si elles permettent d'assurer une protection accrue de la vie privée, demeurent peu fiables et doivent donc absolument être accompagnées de lois qui donneront un recours précis aux personnes lésées.

6. Conclusion

Il reste encore beaucoup de chemin à parcourir pour que la protection des renseignements personnels des citoyens soit assurée sur l'inforoute électronique. Il faut à la fois développer des technologies qui assureront la confidentialité des données conservées et transmises, de même que des procédures claires de recours en cas d'abus.

La question de la vie privée sur l'inforoute électronique inquiète les Canadiens. Il y a donc fort à parier que ceux-ci ne s'y engageront pas massivement tant que la protection des quatre facettes de leur vie privée ne sera pas garantie.

Il faudra donc d'abord s'assurer que ces inforoutes ne seront pas en fait une bretelle d'accès commerciale par laquelle les solliciteurs viendraient brimer le droit à la solitude des citoyens. Il sera ensuite nécessaire de préserver le droit à l'anonymat des utilisateurs, qui ne souhaitent pas particulièrement que tout ce qu'ils tapent sur leur télécommande soit comptabilisé dans une gigantesque banque de données pour établir leur profil de citoyens ou de consommateurs. Aussi, ils devront être en mesure de rouler sur l'inforoute sans être suivis, c'est-à-dire en étant assurés que leur itinéraire reste connu d'eux seuls. Finalement, aucune donnée disponible à leur sujet ne devra circuler à leur insu, ce qui consacrera leur droit à la détermination.

Dans ces conditions, il est impératif que les constructeurs d'inforoutes, entreprises, institutions et gouvernements intéressés par leur développement prennent des mesures pour assurer la sécurité des nombreux renseignements personnels qui y circulent déjà. Un contrôle doit être exercé sur la collecte, le stockage, l'exactitude, l'utilisation et la diffusion des données personnelles. Normes, lois ou technologies: les moyens de protéger les renseignements sont multiples. Il faut toutefois que des mécanismes précis soient mis en place rapidement pour éviter que les projets d'inforoutes n'amplifient une situation déjà problématique.

Notes

(1) À titre d'exemple, soulignons qu'aucune des recommandations du Rapport du comité consultatif sur

l'autoroute de l'information ne mentionne les problèmes relatifs à la vie privée. Le rapport, déposé en juillet 1995, est disponible à l'adresse suivante: http://www.sai.gouv.qc.ca/doc_sai/rapport.html

(2) Selon un sondage réalisé en avril 1994 par la firme Gallup pour le compte de Andersen Consulting Canada, 85% des Canadiens seraient d'ailleurs inquiets de ce qu'il adviendra de leur vie privée sur une éventuelle autoroute de l'information (*Public word about privacy*, sondage Gallup,1994). Plus précis, le rapport *La vie exposée* réalisé par la firme Ekos en 1993 établit un lien entre le niveau de connaissances et la précision des inquiétudes face à la technologie: "Plus les membres d'une société sont instruits et sont au fait de la technologie, moins ils éprouvent de craintes vagues et plus ils sont attentifs à des menaces précises (par ex., l'établissement de liens entre banques de données)" (Frank Graves et Nancy Porteous, *La vie privée exposée, Le sondage canadien sur le respect de la vie privée*, Les associés de recherche Ekos Inc., Ottawa, 1993, p. 15.

(3) Equifax est une agence de collecte de renseignements personnels dont le siège social se trouve à Atlanta, autrefois nommée le Bureau de crédit de Montréal.

(4) Frank Graves et Nancy Porteous, *La vie privée exposée, Le sondage canadien sur le respect de la vie privée*, Les associés de recherche Ekos Inc., Ottawa, 1993, p. 14.

(5) Michel Venne,"L'autoroute des renseignements personnels, Québec se dote d'un réseau électronique reliant tous les ministères", *Le* Devoir, 8 février 1993, A1.

(6) Michael J. Paul, "Telecommunications, isolation, and the erosion of privacy", *Interpersonal* computing *and* technology, vol. 2, n°3, p. 82-98.

(7) Poupées qui servent à tester la sécurité des véhicules automobiles.

(8) Pour en savoir plus sur les mesures prônées par l'OCDE, voir le document *Lignes* directrices régissant *la* protection *de* la *vie* privée *et* les *flux* transfrontières *de* données *de* caractère *personnel*, disponible à l'adresse: http://www.oecd.org/dsti/iccp/legal/priv-fr.html

(9) Voir le document de travail d'Industrie Canada intitulé *La* protection *de* la *vie* privée *et* l'autoroute *canadienne* de *l'information*, à l'adresse: http://info.ic.gc.ca/info-highway/reports/privacy/priv_f.asc

(10) Le site du Commissaire à la protection de la vie privée du Canada est accessible à l'adresse: http://infoweb.magi.com/~privcan/f_index.html

Quelques liens pour en savoir plus...

L'Electronic Frontier Foundation, un organisme sans but lucratif qui défend activement la vie privée et la liberté d'expression sur l'Internet:
http://www.eff.org/

L'Electronic Privacy Information Center (EPIC), recelant de ressources sur la question de la vie privée sur le réseau:
http://www.epic.org/

L'Internet Privacy Coalition, maître d'oeuvre de la campagne de la clé d'or, prônant le recours aux méthodes d'encryptage pour protéger la vie privée dans l'Internet:

http://www.privacy.org/ipc/

Le site Encryption Policy Resource Page, également sur l'encryptage:
http://www.crypto.com/

L'Electronic Frontier Canada, organisme canadien qui s'assure que le développement et l'utilisation des nouvelles technologies respectent les principes de la Charte canadienne des droits et libertés:
http://insight.mcmaster.ca/org/efc/

Les pages du Commissaire à la protection de la vie privée du Canada:
http://infoweb.magi.com/~privcan/f_index.html/