Commissaire à l'information et à la protection de la vie privée/Ontario

La vie privée et l'identification électronique à l'ère de l'informatique

Tom Wright
Commissaire

Novembre 1994

TABLE DES MATIÈRES

Avant-propos

La protection de la vie privée liée à «l'ère de l'informatique» a fait l'objet de plusieurs rapports publiés par le bureau du commissaire à l'information et à la protection de la vie privée — *Health Card Technology : A Privacy Perspective; Privacy and Computer Matching — Report for the Standing Committee on the Legislative Assembly; Des Smart Cards; Les principes de la protection de la vie privée pour les systèmes de courrier électronique; Soyons sur nos gardes : Guide du consommateur pour la protection de la vie privée sur le marché;* et *La protection de la vie privée favorise la saine gestion des affaires.*

Dans chacun de ces rapports, le bureau a attiré l'attention sur les problèmes et les menaces pesant sur la protection des renseignements personnels du fait des pressions, et souvent de l'évolution, des diverses technologies. Dans chacun de ces rapports, le bureau a

également soumis des recommandations et des opinions qui viennent appuyer la protection des renseignements personnels.

Bien qu'il semble exister une certaine tension entre technologie et protection de la vie privée, nous l'estimons superflue. Quant à la technologie et à la protection de la vie privée, le bureau estime toujours qu'un système ou une technologie informatique bien conçus et gérés sont susceptibles d'améliorer la protection des renseignements personnels plutôt que de la diminuer. Il s'agit de considérer la protection de la vie privée comme une priorité à laquelle il faut penser dès l'abord et non pas après coup.

Le présent rapport continue de mettre l'accent sur la protection de la vie privée et l'ère de l'informatique. Il est destiné à informer sur les questions de protection de la vie privée relatives à la manière dont nous, particuliers, nous identifions électroniquement et communiquons avec les grands organismes des secteurs public et privé généralement, mais pas toujours, en contrepartie de prestations, de biens ou de services.

Dans le domaine de l'identification à l'ère de l'informatique, le bureau se préoccupe principalement des conséquences de la dynamique de deux facteurs. Sans garantie appropriée de protection de la vie privée, les deux facteurs suivants porteront ensemble atteinte à la protection des renseignements personnels :

1) la vaste et sans cesse croissante capacité des technologies informatiques (c'est-à-dire, ordinateurs et télécommunications) à recueillir, à stocker, à manipuler et à disséminer l'information;

2) la tendance graduelle mais constante à une identification et à une interaction électronique.

En réponse aux bienfaits perçus que représentent l'opportunité, la convenance et l'efficacité, la technologie ne cesse de nous propulser de plus en plus rapidement vers des systèmes d'identification de plus en plus élaborés qui reposent en général sur un numéro d'identification. Ce numéro d'identification unique peut répondre à divers objectifs — pour peut-être, servir finalement de base à une carte d'identification polyvalente qui deviendra ensuite universelle.

Il se peut que le gouvernement lance un tel système qui s'étendra ensuite à d'autres transactions sur le marché.

L'identificateur commencera à servir les objectifs non prévus. Il suffit de penser à la prolifération du numéro d'assurance sociale pour se rappeler comme il est facile d'avoir recours à un numéro d'identification dans des buts non prévus.

L'autoroute électronique constitue une autre menace potentielle à la protection des renseignements personnels. La convergence de la télévision, des télécommunications et de l'informatique, qui pointe à l'horizon, aura des répercussions permanentes sur notre façon de travailler, de jouer et d'étudier. Mais, dans ce contexte de changements et de promesses remarquables, il faut toujours veiller à garantir la protection des renseignements personnels.

Un facteur important qui peut servir de guide aux secteurs public et privé dans leur garantie de la protection des renseignements personnels est l'influence des consommateurs. Sans l'influence des consommateurs en faveur d'une forte protection de la vie privée, les pratiques commerciales et les projets du gouvernement qui portent atteinte à la protection des renseignements personnels risquent de se poursuivre. Par contre, ce phénomène ne se produira pas si les consommateurs expriment leurs inquiétudes et rejettent les projets et pratiques qui envahissent la vie privée.

L'inquiétude des consommateurs en matière de protection des renseignements personnels doit suivre l'évolution rapide des technologies de gestion de l'information. Si les consommateurs connaissent les dangers qui menacent la protection des renseignements personnels, ils seront mieux à même de choisir le rejet ou l'acceptation de programmes, de politiques et de pratiques dans les secteurs tant public que privé.

Détenir des renseignements sur les questions de protection de la vie privée est le premier pas essentiel — le présent rapport est notre façon d'y contribuer.

Tom Wright

Commissaire

s'en retourner à la table de matières

Vous sentez-vous guetté?

À votre réveil ce matin, le monde n'était pas si différent d'hier matin. Néanmoins, plus le temps passe, et plus les différences dans nos modes de vie, de travail et de jeux deviendront évidentes. De même, notre adaptation à «l'ère de l'informatique» s'est faite graduellement, mais profondément.

L'informatique et les télécommunications nous ont transportés à l'ère de l'informatique. La société actuelle nous décrit en termes de «haute technologie, en ligne et branchés».

De nombreux observateurs ont averti que l'usage envahissant et sans cesse croissant des ordinateurs et de la technologie informatique pour améliorer notre qualité de vie, risque de se faire aux dépens de la protection des renseignements personnels. D'autres considèrent l'atteinte à la protection de la vie privée comme le prix nécessaire à payer. Il est évident que les perspectives varient — l'ère de l'informatique présente des avantages et des inconvénients.

Les pages jaunes de l'annuaire téléphonique de Toronto (consommateurs et ménages) permettent de jeter un regard rapide sur l'ère de l'informatique. Sous la rubrique **Services informatiques**, vous trouverez l'annonce suivante :

> Profitez de notre accès à des milliers de sources de données et d'autres renseignements dans le monde entier. Un coup de fil suffit pour que nous devenions un réseau de renseignements complet et pratique au service de tous vos besoins commerciaux. Pratique. Rentable. Professionnel. Considérez-nous comme votre propre service de recherche intégré[1].

Et ce message plus personnel :

> À chaque appel téléphonique, achat de biens de consommation par carte de crédit, souscription à un magazine ou paiement d'impôts, l'information transmise est enregistrée dans une base de données quelque part. En outre, tous ces dossiers peuvent être joints de façon à ne former en fait qu'un seul dossier sur votre vie — non seulement vos antécédents médicaux et financiers, mais également vos achats, vos destinations de voyage et vos interlocuteurs. Il est pratiquement impossible de connaître toute l'étendue des dossiers que divers organismes conservent à votre sujet, et il est encore plus difficile d'assurer leur exactitude ou de contrôler ceux qui peuvent y avoir accès[2].

Et encore plus personnel :

> Beaucoup de personnes sont au courant des tables d'écoute. Mais peu ont entendu parler du Realtime Residential Power Line Surveillance (RRPLS). Les responsables américains de la mise à exécution des lois ont eu recours pendant des années à une forme primitive de RRPLS, obtenant les dossiers de facturation des compagnies d'électricité en vue de mettre la main sur les utilisateurs de lampes puissantes pour cultiver de la marijuana. Aujourd'hui, les appareils appelés «compteurs à mémoire» relancent la force du recueil de données [...] Ils peuvent enregistrer quels appareils électriques sont utilisés, et quand[3].

Conjugué à d'autres sources de données, le RRPLS pour créer une liste incroyablement détaillée de chaque mouvement que vous effectuez. Imaginez le scénario suivant :

> Contrairement à la routine d'un ménage, l'un de ses occupants, un homme marié de 43 ans (selon son permis de conduire) se lève tôt un samedi matin, prend une douche, se rase avec son rasoir électrique et repasse quelques vêtements. Il achète de l'essence en ville, et au cours de la soirée paie deux repas et achète deux billets de théâtre (le tout avec sa carte de crédit). A son retour à la maison, il allume la chaîne stéréo (ce qui est rare selon son dossier RRPLS)...
>
> Le lendemain matin, les données indiquent une douche inhabituellement longue, suivie de deux utilisations d'un sèche-cheveux. La seconde est beaucoup plus longue qu'elle ne le devrait pour l'homme, indiquant qu'il a probablement partagé sa douche avec une personne aux longs cheveux.
>
> Au même moment, les dossiers sur les transactions commerciales indiquent que l'épouse de l'occupant se trouve autour du monde en voyage d'affaires payé par son employeur. Les données RRPLS de sa chambre d'hôtel mentionnent également un visiteur nocturne. Quelques jours plus tard, le couple est inondé de publicités envoyées directement par des avocats spécialisés dans le divorce[4].

Des observations de surveillance expérimentées en Australie témoignent de l'existence d'une vaste trame de réseaux informatiques destinés à réglementer de nombreux aspects de la vie et la fusion finale des réseaux informatiques des secteurs public et privé :

> Chaque semaine qui passe, un fil de plus de la trame est achevé. Chaque fil est tissé délicatement, et on nous affirme chaque fois que l'effort fourni est pour notre bien. C'est vrai, chaque fil sert au fisc à soutirer un dollar de plus ou à prendre au piège un autre criminel. Mais chaque fil lie les honnêtes citoyens plus étroitement à l'administration du gouvernement. Lentement, les fils se rapprochent de plus en plus — jusqu'à communiquer, puis se toucher. Vos finances, achats, emplois, intérêts, appels téléphoniques et même vos déplacements géographiques perdent de leur anonymat. Mais tout n'est pas mauvais; la technologie ouvrira des possibilités formidables. Elle sera également la cause du cauchemar de la nudité totale[5].

Le message ci-dessous fait ressortir la subtilité de la surveillance :

> La surveillance s'étend subtilement, souvent à la suite de décisions et processus destinés à atteindre des objectifs tels que l'efficacité ou la productivité. Par ailleurs, son caractère électronique actuel en augmente la subtilité. La plus grande partie de la surveillance se passe littéralement hors de la vue, dans le royaume des signaux numériques; et, comme nous l'avons déjà vu, pas à la manière d'une conspiration clandestine, mais dans les transactions courantes, quand par exemple vous votez, magasinez, téléphonez, conduisez ou travaillez. Autrement dit, les gens savent rarement qu'ils font l'objet de surveillance, ou s'ils le savent, ils ne se doutent pas de l'étendue des renseignements que les autres détiennent sur eux[6].

Les modèles d'interaction sociale sont passés du physique à l'électronique. Aujourd'hui, la plupart des transactions sur le marché, et de plus en plus de transactions gouvernementales, sont menées de façon à permettre le stockage électronique et la recherche d'information.

Au fur et à mesure que nos relations électroniques augmentent, l'emprise de la surveillance en fait de même. Voici des exemples de relations électroniques quotidiennes et de la surveillance qui en résulte :

> La surveillance, au sens que nous lui donnons ici, concerne les choses banales, ordinaires, naturelles de la vie qui consistent à retirer de l'argent des guichets automatiques, à passer un coup de fil, à réclamer des prestations de maladie, à conduire une voiture, à utiliser une carte de crédit, à recevoir de la publicité importune, à aller emprunter des livres à la bibliothèque, ou à traverser une frontière lors de voyages à l'étranger. Dans chacune des activités mentionnées, les ordinateurs enregistrent nos transactions, comparent les détails connus, vérifient que c'est bien nous, et non pas quelqu'un d'autre, qui avons reçu nos factures ou nos versements, stockent des bribes de nos

> biographies, ou évaluent notre état financier, juridique ou national. Chaque fois que nous effectuons l'une de ces transactions, nous laissons ou sommes susceptibles de laisser trace de nos faits et gestes. Les ordinateurs et leurs systèmes de communication connexes sont au coeur de tous ces types de relations; participer à la société moderne signifie être sous surveillance électronique[7].

Vous sentez-vous guetté? Eh bien, vous l'êtes.

s'en retourner à la table de matières

Disposez-vous de quelque identification?

L'identification au sens de «vous êtes ce que vous déclarez être» et «vous êtes admissible» a toujours constitué un énorme défi pour les fournisseurs de biens et de services, en particulier le gouvernement.

L'identification à l'ère de l'informatique signifie NIP (numéro d'identification personnel), cartes d'accès et mots de passe. Notre identification individuelle s'insère dans une pile de cartes en plastique. Sans ces cartes, il serait beaucoup plus difficile d'accéder à la plupart des services des secteurs privés et à certains des secteurs publics.

Comme votre porte-monnaie le prouvera, les cartes en plastique sont très variées. Sur quelques-unes, les renseignements figurent à la surface, d'autres présentent des lettres gravées en relief ou une bande magnétique. La prochaine vague de cartes faisant leur apparition sont les «cartes à mémoire». Une carte à mémoire consiste en un dispositif de la taille d'une carte de crédit, contenant une ou plusieurs puces de circuit intégré, qui agit comme un microprocesseur, une mémoire et une interface d'entrée/sortie[8]. C'est pratiquement un ordinateur dans une carte.

Il est connu que les cartes à mémoire peuvent être bénéfiques, en termes d'amélioration du service de la clientèle, d'efficacité opérationnelle et de sécurité, tant pour le secteur public que privé. Cependant, les cartes à mémoire risquent également de devenir une technologie de surveillance et de contrôle[9].

La même technologie qui facilite le péage pour des milliers de voitures par heure, peut servir à suivre les mouvements d'un véhicule et de son conducteur. La même technologie qui permet à un consommateur de débiter directement son compte en banque, permet au commerçant d'enregistrer les préférences d'achat de ce même consommateur à des fins de marketing direct. La même technologie qui permet au gouvernement de faciliter la prestation de programmes et de services, peut servir à surveiller et contrôler ses citoyens[10].

Les cartes à mémoire ne portent pas en soi atteinte à la vie privée. Néanmoins, elles permettent de mener une surveillance efficace, ouvertement et secrètement. M. Roland Moreno, qu'on nomme souvent l'inventeur des cartes à mémoire, a fait remarquer que celles-ci peuvent facilement se transformer en «petit assistant électronique du Big Brother»[11].

En fin de compte, le facteur essentiel est la manière dont les bases de données vous reconnaissent ou vous distinguent, vous et vos dossiers électroniques, parmi des millions d'autres. Généralement, une quelconque transaction électronique au moment du service, qui attribue notamment un code qui vous est unique, le permet. Sans cette «clef», la gestion électronique de l'information ne pourrait avoir lieu. Mais, cette clef ouvre toute grande la porte de la surveillance électronique.

Quel que soit le mécanisme original de dispense de l'information, celle-ci est presque toujours stockée électroniquement dans une base de données. Une fois stockée, presque tout est possible — fusion, rapprochement, sommaire, tri, sélection, compilation et partage de données avec des tiers, à votre insu ou contre votre gré.

La capacité apparemment sans limite des technologies informatiques à fusionner, à rapprocher, à résumer, à trier, à sélectionner, à compiler et à envoyer de l'information partout dans le monde aboutit souvent à divers avantages. Une amélioration de la qualité de la vie constitue indiscutablement un côté de la médaille que représente l'ère de l'informatique.

Le revers de la médaille est plus complexe. Il s'agit de la contrepartie — surveillance ou précisément, surveillance de données.

L'expert australien des systèmes informatiques, M. Roger Clarke, a défini la surveillance de données comme suit : «le recours systémique à des systèmes de données personnelles pour enquêter sur les actions ou communications d'une ou de plusieurs personnes, ou les surveiller[12].» (Un système de données personnelles repose sur le recueil des dossiers électroniques d'une personne.)

Traditionnellement, l'inquiétude résultant du risque de surveillance par un Big Brother se fonde sur l'idée qu'un seul ordinateur peut stocker d'énormes quantités d'informations sur les individus. Quand à la protection des renseignements personnels, on soutenait traditionnellement que le stockage décentralisé d'informations valait mieux qu'un stockage centralisé.

La centralisation d'informations est problématique à cause de la facilité avec laquelle on peut accéder, manipuler et ensuite utiliser l'information à des fins qui n'ont pas été prévues au départ. Par contre, des bribes d'information à votre sujet recuellies au cours de toute votre vie sont en fait fondamentalement sauvegardées, parce que beaucoup plus difficiles à localiser et manipuler quand elles sont réparties dans plusieurs bases de données. Néanmoins, cette théorie reste vraie tant qu'il n'existe pas de lien commun. Un seul emplacement relié informatiquement à plusieurs emplacements augmente la possibilité d'accès à l'information contenue dans la base de données et à sa manipulation par des personnes autorisées et non autorisées.

Dans les années 60, aux États-Unis, on a tenu des audiences sur la création d'un centre national de données. Selon un témoignage apporté, les garanties à la protection de la vie privée étaient inhérentes à la fragmentation de l'information. Dans ses commentaires sur ce témoignage, M. Clarke a soutenu que des bases de données d'information nationales et centralisées ne sont plus nécessaires à l'établissement d'une «société de dossiers» tant que les conditions suivantes existent:

1) une gamme de systèmes de données personnelles doit exister, chacun traitant des données à des fins précises,

2) certains systèmes de données personnelles, et de préférence tous les systèmes, doivent être reliés par l'intermédiaire d'un ou de plusieurs réseaux de télécommunications,

3) **les données doivent être identifiées uniformément**[13]. [mise en relief ajoutée]

M. Clarke estime que les deux premières conditions existent déjà et que «la troisième n'a pas encore été réalisée, en raison de la difficulté à identifier de façon fiable les objets de surveillance, en associant les données stockées aux individus, et en rapprochant les nouvelles données des anciennes[14].»

«Les données doivent être identifiées uniformément.» Il ressort de l'examen de l'analyse de M. Clarke que le dernier obstacle à une surveillance absolue de données peut bien consister en un système d'identification uniforme — un seul numéro appliqué uniformément à chaque transaction. Si un tel numéro existait, chaque transaction effectuée pourrait facilement être reliée à des centaines de bases de données.

Ne serait-il pas plus pratique d'avoir un numéro ou une carte? Une carte qui vous identifie et vous légitimise pour des programmes ou services ne serait-elle pas plus efficace et ne réduirait-elle pas la fraude? Il suffirait d'un code immuable ou unique pour vous identifier, par exemple, dans chacune de vos transactions avec le gouvernement du Canada ou de l'Ontario.

Pour les Canadiens, l'expérience vécue avec le numéro d'assurance sociale est devenu l'exemple classique des conséquences néfastes de la commodité d'un seul numéro, en d'autres mots «la fonction tentaculaire». Avec la fonction tentaculaire, les systèmes conçus pour un objectif servent à long terme d'autres objectifs qui n'ont pas été prévus à l'origine.

Avec le numéro d'assurance sociale, bien que destiné à des objectifs explicites en matière d'assurance-chômage et de régime de retraite, un usage non autorisé s'est infiltré dans tous les domaines de transactions — de l'émission d'un chèque, à la location d'un

vidéo ou à l'abonnement à des services de téléphone interurbains.

Trente ans après l'introduction du numéro d'assurance sociale, beaucoup de gouvernements s'intéressent de plus en plus à la mise au point de nouvelles méthodes d'identification de leurs citoyens.

Les avantages perçus de l'efficacité administrative, d'un meilleur service à la clientèle, et de la réduction de la fraude et du gaspillage — convenance, commodité et efficacité — témoignent de cet intérêt. Les solutions technologiques font souvent partie intégrante des discussions concernant ces domaines de politique publique ou de leurs solutions — des empreintes digitales sur cartes aux photos numérisées.

Il se peut que nous trouvions une foule d'exemples de mesures du gouvernement fédéral et des gouvernements provinciaux tournant autour de nouveaux systèmes perfectionnés d'identification. Les titres de la presse écrite illustrent les réactions aux soi-disant systèmes fiables et antifraude. Voici un instantané sur cinq mois de titres choisis :

«Ottawa eyes 'hand' print ID for travellers,» *Toronto Star,* le 5 juin 1994.

«OHIP photo-ID» — éditorial, *Toronto Star,* le 7 mai 1994.

«Regular uses of medicare by ineligible people biggest problem,» *Globe and Mail,* le 5 mai 1994.

«Ontarians to get photo OHIP cards,» *Toronto Sun*, le 4 mai 1994.

«Super-ID: keeping an eye on everybody,» *Globe and Mail*, le 17 mars 1994.

«Fraud cases spur new ID cards for status Indians,» *Ottawa Citizen*, le 27 février 1994.

«Mennonites concerned about universal ID cards,» *Kitchener-Waterloo Record*, le 25 février 1994.

«ID blues — The better to know you,» *Windsor Star,* le 24 février 1994.

«Immigrants to get special ID card,» *Globe and Mail*, le 22 février 1994.

«A national identification card,» *Sault Star,* le 21 février 1994.

«Universal ID card will reduce fraud,» *Kitchener-Waterloo Record*, le 21 février 1994.

«Too much identification — Too little privacy,» *Hamilton Spectator,* le 21 février 1994.

«It's 19-Ninety-4, and Big Brother is still trying to put the finger on us,» *Ottawa Citizen*, le 19 février 1994.

«Your identity card, please,» *Globe and Mail*, le 18 février 1994.

«SIN heralded concerns over identification,» *Globe and Mail*, le 18 février 1994.

«Fingerprinting: for all, or for none,» *London Free Press*, le 18 février 1994.

«Fingerprinting ID called invasion of human rights,» *Hamilton Spectator*, le 18 février 1994.

«Ontario considers universal ID; Driver's Licence, health card would be replaced to reduce fraud,» *Globe and Mail*, le 17 février 1994.

«Ontario ponders ID card,» *Windsor Star*, le 17 février 1994.

«An appalling intrusion,» *St. Catharines Standard*, le 14 février 1994.

Historiquement, le débat sur l'identification et les cartes d'identité a été passionné, faisant souvent ressortir l'aspect inhumain et dégradant de la réduction d'une personne à un numéro. Dans quelques territoires, l'intensité du débat dépend de la conjoncture économique et de la politique du jour.

Néanmoins, dans les années 80, le gouvernement australien a proposé d'établir une carte nationale d'identité, expérience qui s'est révélée particulièrement convaincante. Au départ, l'opinion publique a été favorable au projet, mais une fois mise au courant des problèmes de protection de la vie privée, l'engouement a diminué. Le projet sur la carte de l'Australie a finalement avorté.

Les pouvoirs qui envisagent d'établir des cartes d'identification polyvalentes ou universelles pour résoudre divers problèmes administratifs risquent de trouver l'expérience australienne instructive.

Mis au point en 1986 par le gouvernement fédéral australien, le système de la carte d'identité était considéré comme nécessaire «pour créer une société juste.»[15] Le système est né du problème de l'évasion fiscale et des échappatoires auxquels le gouvernement était confronté au début des années 80. Comme le fait remarquer le défenseur de la protection de la vie privée, M. Simon Davis : «Inquiets de l'étendue de la fraude au système de la sécurité sociale, certains ont fait valoir qu'une carte d'identité ou qu'un système national d'inscription faciliterait l'administration publique. Les craintes au sujet de l'étendue de l'immigration illégale a apporté de l'eau au moulin en faveur de ces suggestions.»[16]

Le comité de la protection de la vie privée de la Nouvelle-Galles du sud a recommandé au comité mixte sur la carte australienne le rejet du programme sur la carte australienne. Au nombre des points soulevés par le comité de la protection de la vie privée, on peut citer les suivants :

(i) en effet, les cartes d'identité s'avèreront nécessaires dans diverses circonstances indépendantes des objectifs originaux de la carte. En conséquence, les personnes incapables ou réticentes à présenter une carte feront l'objet d'un traitement défavorable;

(ii) la proposition d'un registre central de la population ouvre de nouvelles possibilités de surveillance informatique largement répandue. Le registre lui-même servira de clé à l'information conservée dans les ministères sur les particuliers;

(iii) l'accès au registre sera largement ouvert. En d'autres mots, il est très probable que des personnes non autorisées aient accès à l'information personnelle en se servant du numéro d'identité ou de la clé;

(iv) l'établissement du système aboutira lui-même à une augmentation de la demande d'accès de la part des agences (fédérales, des États et privées)[17].

L'expérience australienne sert de point de repère important aux gouvernements en quête de solutions aux divers problèmes administratifs et fiscaux — que ce soit le gaspillage, la fraude, l'évasion fiscale, les échappatoires ou l'immigration. A part les questions tels l'efficacité et le coût, les problèmes les plus importants soulevés par les cartes d'identité sont le potentiel de surveillance généralisée et la modification fondamentale des relations entre l'état et ses citoyens.

L'idée qu'une carte nationale d'identité (ou une carte polyvalente) constitue la panacée des maux des gouvernements reste une solution

capable de résoudre les problèmes à long terme.

s'en retourner à la table de matières

Quand on veut, on peut … est-ce toujours vrai?

Les menaces à la protection de la vie privée inhérentes aux systèmes d'identification qui font appel à un numéro d'identité unique appliqué à chaque transaction peuvent avoir une grande portée. Sans protection suffisante de la vie privée, l'ombre d'une surveillance totale des données pèse invisiblement sur tous les aspects de la vie quotidienne.

Mais d'un point de vue plus optimiste, certaines applications de technologie peuvent également permettre la préservation de la protection électronique des renseignements personnels. Ces nouvelles applications technologiques sous forme de systèmes codés, méritent notre attention. En voici un exemple.

Des cryptographes du centre de mathématiques et d'informatique (CWI) d'Amsterdam ont mis au point une nouvelle méthode qui permet la réalisation de transactions tout en «empêchant toute possibilité de fraude et en conservant la protection de la vie privée de ses utilisateurs»[18]. Cette technologie de la protection de la vie privée, intitulée «signature numérique invisible» repose sur un important système public de chiffrement.

M. David Chaum, directeur du groupe de cryptographie du CWI, décrit la méthode de son groupe, fondée sur des développements fondamentaux théoriques et pratiques en cryptographie:

> Dans notre système, les individus attribueraient en fait un pseudonyme différent (mais tout à fait vérifiable) à chaque organisme avec lequel ils traitent, ce qui rend impossible la tenue de dossiers. Ils pourraient payer leurs achats en espèces électroniques non retraçables ou présenter des pièces d'identité numériques servant de mot de passe bancaire, de permis de conduire ou de carte de vote sans révéler leur identité. En même temps, les organismes bénéficieraient d'une augmentation de la sécurité et d'une baisse des coûts d'entretien des dossiers[19].

Le recours à la technologie pour améliorer plutôt que pour porter atteinte à la protection des renseignements personnels est clairement possible, pourvu que se manifeste la volonté de trouver la solution.

Au fur et à mesure que les consommateurs expriment de plus en plus leurs besoins d'une meilleure protection de leurs renseignements personnels, les gouvernements et les entreprises devront s'intéresser à d'autres méthodes telle la signature numérique invisible.

Les pouvoirs publics ne cessent de lutter pour réduire la fraude et le gaspillage, tout en essayant de jongler avec des intérêts tels que la protection de la vie privée. La signature numérique invisible pourrait représenter une importante application technologique dans la recherche du bon équilibre. En effet, l'application d'une telle signature est bénéfique tant aux fournisseurs de services qu'aux consommateurs pour plusieurs raisons : elle accroît la sécurité des transactions; elle permet une protection totale de la vie privée; elle empêche la collecte et la conservation centrale d'informations identifiables; et elle élimine la poursuite électronique d'informations identifiables. Les programmes et prestations gouvernementaux concernant les services de santé, l'immigration et l'assurance sociale, par exemple, pourraient constituer des données de prédilection pour un système protégé d'informations utilisant des signatures numériques invisibles.

De nouvelles applications innovatrices de la technologie de l'information arrivent presque tous les jours. Le recours à ces technologies, telle la signature numérique invisible, pour préserver la protection des renseignements personnels vous est désormais ouvert. Cependant, l'engagement des gouvernements est indispensable au recours à d'autres mesures de protection de la vie privée. Les signatures numériques invisibles pour des transactions allant d'opérations bancaires à la collecte de prestations de sécurité sociale, peuvent non seulement être efficaces, mais également efficientes et privées — sans nécessiter de sacrifices ou de compromis.

Considérons les conséquences de deux possibilités:

> Chaque fois qu'un gouvernement ou qu'une entreprise décide d'automatiser une autre série de transactions, il a fait le choix entre conserver l'information entre les mains des particuliers ou d'organismes. Dans un cas, cela signifie examens minutieux et contrôles sans précédent des vies privées; dans l'autre, cela rétablit la parité entre les particuliers et les organismes. La configuration de la société du siècle prochain dépend peut-être de la méthode qui aura la primauté[20].

s'en retourner à la table de matières

Conclusion

L'ère de l'informatique offre des possibilités d'énormes avantages et d'amélioration de la qualité de vie. Mais l'atteinte à la protection des renseignements personnels résultant de l'application de technologies violant la vie privée, modère ces avantages.

Il n'y a pas qu'une seule manière de protéger les renseignements personnels. Il faut s'attaquer à autant de fronts que possible.

Une augmentation de l'intérêt des consommateurs conjuguée à des mesures prises pour protéger les renseignements personnels déterminera assez bien à quel point nous avançons dans la surveillance de données. Un système d'identification uniforme et continue ouvre la porte à une «société de dossiers» — la surveillance totale de données. Invisible et subtil, l'impact sur la protection de la vie privée sera foudroyant et irréparable.

Les applications technologiques, telle «la signature numérique invisible», peuvent satisfaire la sécurité organisationnelle et la protection des renseignements personnels dans les secteurs public et privé. Le recours à la technologie pour améliorer la protection des renseignements personnels exige des organismes qu'ils incluent la protection de la vie privée dans la conception des programmes et la mise en oeuvre des systèmes informatiques.

La pression des consommateurs et la demande de programmes, de politiques, et de pratiques qui cherchent sérieusement à protéger les renseignements personnels peuvent motiver cette «volonté».

s'en retourner à la table de matières

Notes

1. Consumer and Household Yellow Pages, Tele-Direct Publications Inc., juin 1994-1995, p. 619.
2. David Chaum, «Achieving Electronic Privacy», *Scientific American* (août 1992), p. 96.
3. Rick Crawford, «Techno Prisoners», *Adbusters* (Quarterly Summer, 1994), p. 21.
4. *Ibid.*, p. 21-22.
5. Simon Davies, *Big Brother: Australia's Growing Web of Surveillance*, East Roseville, NSW: Simon & Schuster Australia, 1992, p. v-vi.
6. David Lyon, *Electronic Eye*, Minneapolis, University of Minnesota Press, 1994, p. 5.
7. *Ibid.*, p. 4.
8. Commissaire à l'information et à la protection de la vie privée, *Smart Cards*, avril 1993, p. 4.
9. *Ibid.*, p. 28.
10. *Ibid.*
11. *Ibid.*, p. 29.
12. Roger A. Clarke, «Information Technology and Dataveillance», *Communications of the ACM*, vol. 31 (no 5, mai 1988), p. 499.
13. *Ibid.*, p. 500.

14. *Ibid.*, p. 501.
15. Davies, *Big Brother*, p. 40.
16. *Ibid.*, p. 30 et 31.
17. Privacy Committee of New South Wales, *Privacy Issues and the Proposed National Identification Scheme — A Special Report*, mars 1986, p. ix.
18. David Chaum, «Achieving Electronic Privacy», *Scientific American*, (août 1992), p. 96
19. *Ibid.*
20. *Ibid.*, p. 101.

s'en retourner à la table de matières
