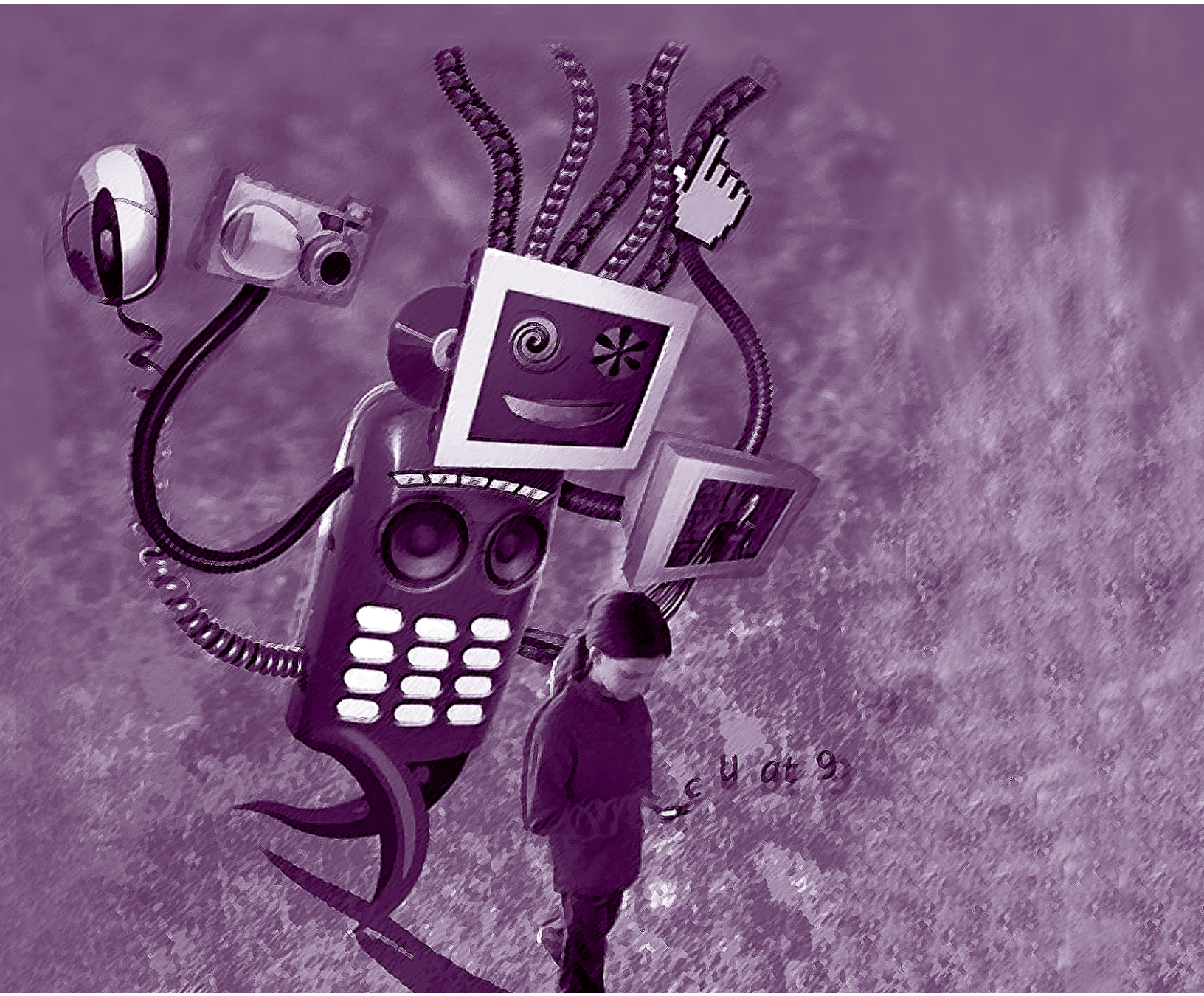
LIGUE DES DROITS ET LIBERTÉS

Bulletin automne 2009



Numéro spécial :

Vie privée et renseignements personnels

La *Ligue des droits et libertés* est membre de la *Fédération internationale des ligues des droits de l'homme* (FIDH) www.fidh.org

Comité éditorial
Martine Eloy
Nicole Filion
Lucie Mercier
Dominique Peschard
Roch Tassé

Conception et Coordination
Martine Eloy
Dominique Peschard

Collaboration à ce numéro
Johanne Doyon
Martine Eloy
Anthony Hémond
Lucie Mercier
Dominique Peschard
Anne Pineau
Patricia Poirier
Jennifer Stoddart
Roch Tassé

Révision linguistique
Lisette Girouard

Correction d'épreuves
Martine Eloy
Dominique Peschard

Graphisme
Sabine Friesinger

Impression
Imprimerie Katasoho

Ce bulletin est une publication de la Ligue des droits et libertés, réalisée collaboration avec la Fondation Léo-Cormier. Il est distribué à leurs membres.

Pour abonnement, avis de changement d'adresse ou commentaires, veuillez communiquer avec nous :
téléphone : 514-849-7717
courriel : info@liguedesdroits.ca

Dépôt légal
Bibliothèque nationale du Québec
Bibliothèque nationale du Canada
ISSN 0828-6892

Dans ce numéro

La Fondation Léo-Cormier

Le respect de la vie privée n'est pas une fioriture de la démocratie

Dominique Peschard, président
Ligue des droits et libertés

Dans son travail cette année, la Ligue des droits et libertés a décidé de porter une attention particulière à la question de la vie privée et des renseignements personnels. Même si cette question a été une préoccupation majeure de la Ligue depuis sa création, nous jugeons que les développements dans ce domaine depuis une décennie sont extrêmement préoccupants et méritent une attention particulière. Comme vous pourrez le constater en lisant ce bulletin, les possibilités offertes par les nouvelles technologies de l'information et des communications, lorsqu'elles sont déployées dans un contexte de capitalisme déréglementé et de phobie « sécuritaire », mènent à des dérives qui menacent les libertés individuelles et sapent les fondements de la démocratie.

Le respect de la vie privée n'est pas une fioriture de la démocratie dont on pourrait se passer dans des temps difficiles. Le respect de la vie privée est une condition essentielle à la dignité et à l'autonomie de chaque être humain. Sans cette autonomie, il ne peut y avoir de liberté, et sans liberté, il ne peut y avoir de vie démocratique.

Aujourd'hui, des pans de plus en plus importants de notre vie sont numérisés et stockés dans des banques de données. Les transactions financières électroniques permettent de répertorier nos habitudes de consommation. Les nouveaux moyens de communications que sont la téléphonie cellulaire et Internet - les deux fonctionnant de plus en plus en symbiose – laissent des traces qui inscrivent nos liens sociaux, nos champs d'intérêts et nos activités dans les mémoires des ordinateurs. Les États possèdent des dizaines de fichiers portant sur les aspects les plus intimes de nos vies, les plus importants étant les dossiers de la SAAQ, de la CSST, de la Régie des rentes, des ministères du revenu, de l'assurance emploi, de l'aide sociale... sans oublier les multiples dossiers dans le domaine de la santé qui sont en voie d'informatisation.

Les États considèrent de moins en moins ces données comme des données sensibles dont ils sont fiduciaires et de plus en plus comme une ressource qu'ils peuvent utiliser pour gérer leurs programmes et exercer un contrôle social sur la population. Pour atteindre ces objectifs, le gouvernement du Québec a affaibli le régime de protection des données personnelles et a augmenté son pouvoir de croiser les données des différents fichiers et de les partager entre ministères, et même avec des gouvernements étrangers. Avec la privatisation des services publics, la gestion de ces données est maintenant souvent confiée à des entreprises privées, ce qui accroît encore les risques de détournement d'usage, surtout quand ces entreprises sont étrangères.

Après les attentats du 11 septembre 2001, les États ont entretenu un climat de peur qui leur a permis de mettre en place des mesures de surveillance et de contrôle des populations qui auraient été inimaginables auparavant. Les services de renseignement, en particulier ceux des États-Unis, se sont mis à bâtir des banques de données sur tous les aspects de la vie des individus. En plus de puiser sans vergogne dans les banques de données de l'entreprise privée, ce que permet le Patriot Act, des agences de renseignement comme la National Security Agency, se sont mises à espionner massivement les communications à l'échelle planétaire. Les compagnies aériennes remettent au Department of Homeland Security toutes les données

sur leurs passagers. Au Canada, le Centre d'analyse des opérations et déclarations financières du Canada (CANAFE) scrute les transactions financières. Sur la base de toutes ces données, les services de renseignements établissent des listes de personnes soupçonnées de représenter un risque pour la sécurité nationale, la plus connue étant celle du Terrorist Screening Center des États-Unis qui contient environ un million de noms. Des personnes se retrouvent ensuite bloquées aux frontières ou empêchées de prendre l'avion sans jamais savoir ce qu'on leur reproche et sans mécanisme leur permettant de corriger la situation.

La lutte au terrorisme sert aussi de prétexte pour étouffer et réprimer les mouvements sociaux. Ceci est particulièrement évident en Amérique latine où les populations et les peuples autochtones qui s'opposent à l'exploitation et à la dépossession de leur territoire par des multinationales sont brutalement réprimés. Plus près d'ici, le gouvernement de Colombie-Britannique a adopté des règlements et des lois pour empêcher toute manifestation qui viendrait ternir l'image des Jeux olympiques. Le dispositif militaro-policier déployé à Vancouver sert à surveiller et harceler les militants qui voudraient manifester pendant les jeux.

Quand on regarde l'évolution des mesures de surveillance et de contrôle des populations au Canada et dans les autres pays, dits démocratiques, on ne peut faire autrement que de méditer sur l'expérience chinoise des dernières décennies. L'idéologie dominante prétend que le capitalisme est par nature porteur de démocratie et que le virage de la Chine vers une économie de marché entraînerait nécessairement un élargissement de l'espace démocratique et un accroissement des libertés. Bien au contraire, l'expérience chinoise démontre, on ne peut mieux, que le capitalisme et l'économie de marché s'accommodent fort bien d'un régime politique totalitaire.

Dans le contexte de la stagnation et des reculs au niveau des droits économiques et sociaux, et de la croissance des inégalités que nous vivons depuis plusieurs années, l'attention des mouvements sociaux s'est naturellement portée, avant tout, sur la défense des conditions de vie. Pourtant les enjeux concernant la liberté et la démocratie sont tout aussi importants. Droits démocratiques et droits économiques et sociaux sont indissociables. Pour défendre nos droits économiques et sociaux, et progresser vers une société plus juste et égalitaire, il faut préserver notre liberté d'action sociale et politique.

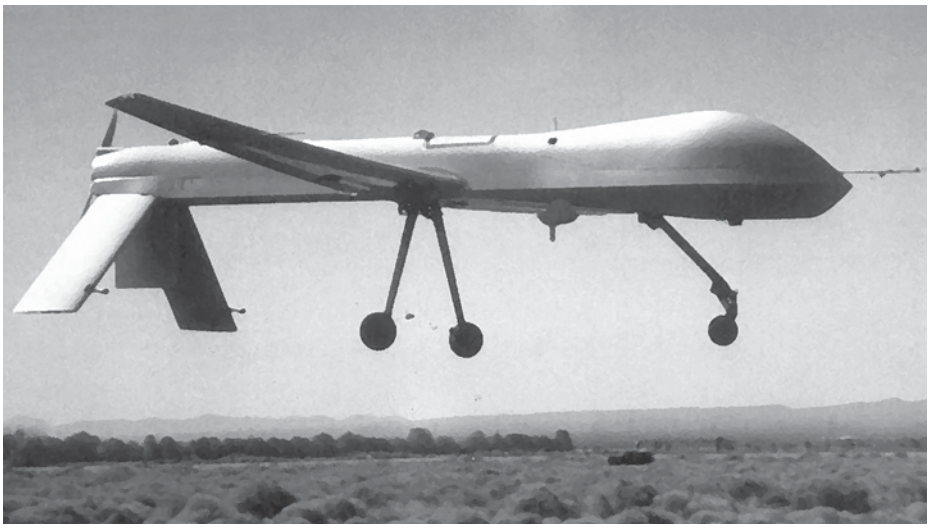
L'évolution vers une société de surveillance n'est pas une fatalité, pas plus que la faim ou la pauvreté ou qu'un monde soumis aux intérêts du capitalisme financier. Cette année, par son intervention sur la question de la protection des renseignements personnels, la Ligue ne vise pas seulement à rendre compte de l'érosion du droit à la vie privée, mais bien plutôt à contribuer, avec d'autres, à trouver les moyens de la stopper.

*****

Un avion sans pilote, bientôt près de chez vous!

Dominique Peschard

Depuis le début de l'année, le gouvernement des États-Unis utilise des avions sans pilote équipés de caméras pour surveiller la frontière entre le Canada et les États-Unis. Les mêmes avions, qui peuvent également être armés, sont couramment utilisés par les États-Unis pour frapper des cibles au Pakistan. L'armée israélienne les utilise pour surveiller les villes des territoires palestiniens et pour perpétrer des assassinats ciblés.



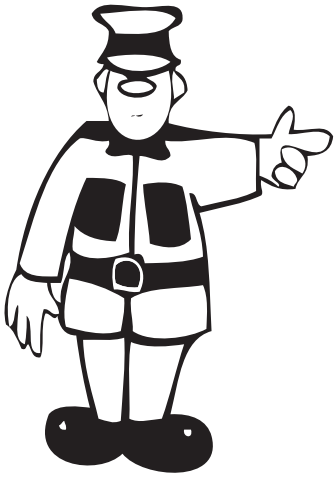
Leurs caméras sont capables de distinguer une personne à partir d'une altitude de 15 000 mètres et de balayer une bande de territoire de 40 km de large. Tout en volant à 15 km à l'intérieur du territoire des États-Unis, ils peuvent donc observer jusqu'à 25 km à l'intérieur du territoire canadien – et tant pis pour la souveraineté du Canada.

Le gouvernement du Royaume Uni étudie maintenant la possibilité d'utiliser ces avions sans pilote pour surveiller le territoire national. Ces avions donneront aux autorités un énorme pouvoir de surveillance. Contrairement aux caméras de surveillance déployées à travers les espaces publics, ces avions peuvent observer tout le territoire, y inclus les espaces privés comme les cours et jardins. Les images sont bien meilleures que celles fournies par des satellites et le problème des nuages qui affecte les satellites peut être contourné en modifiant l'altitude de l'appareil. Le comité de la défense du Parlement britannique prévoit que les avions pourront être déployés lors de catastrophes naturelles, pour soutenir des efforts de recherche en mer, pour effectuer de la surveillance antiterroriste et dans des opérations de contrôle de foule! Bien que le comité reconnaisse que l'utilisation de ces avions soulève des questions de vie privée et de droits humains, sa préoccupation majeure en est une de sécurité aérienne. Un consortium de compagnies privées a été mis sur pied pour élaborer des procédures qui permettront à ces avions de partager l'espace aérien utilisé par l'aviation civile.

Vancouver 2010
Des Jeux sous haute surveillance

Dominique Peschard

Les agences de sécurité canadiennes ont mobilisé avions, blindés, navires et des milliers de soldats et policiers en vue des Jeux olympiques de Vancouver. Les planificateurs de cette opération militaire disent que ce sera la plus importante du genre de l'histoire du Canada, mais qu'ils ont l'intention de la rendre la plus discrète possible. Pour y parvenir, ils comptent utiliser des caméras de surveillance, des senseurs électroniques et des avions sans pilote, à un point tel que David Lyons, sociologue et spécialiste des nouveaux moyens de surveillance à l'université Queen's, a qualifié les Jeux de Vancouver de « jeux de la surveillance ». Pour les autorités, l'expérience de Vancouver servira de modèle à d'autres événements internationaux comme le G8.



Pour la GRC et le SCRS, la menace aux Jeux olympique ne se limite pas à Al Qaida. Les militants altermondialistes, anticapitalistes et des peuples autochtones sont également dans la mire des autorités. D'après un document hautement censuré du Service canadien du renseignement de sécurité (SCRS), obtenu par CANWEST, le SCRS surveille les activités des groupes opposés aux olympiques et s'intéresse en particulier à l'alliance entre militants autochtones et groupes anti-pauvreté.[1]

Les autorités ont également l'intention d'écarter de la place publique toute manifestation d'opposition qui pourrait ternir l'image des Jeux, quitte à bafouer la liberté d'expression. En juin 2010, la ville de Vancouver a adopté un règlement municipal interdisant de distribuer ou d'*exhiber* tout matériel promotionnel non approuvé sur le site des Jeux pendant la durée des olympiques. Le 8 octobre 2009, le gouvernement de la Colombie Britannique a déposé un projet de loi qui permettrait, pendant la durée des Jeux, aux municipalités de Richmond, Whistler et Vancouver de pénétrer dans des résidences et autres propriétés privées, à 24 heures d'avis, afin d'y couvrir ou enlever des affiches. Un autre amendement à la charte de Vancouver permet d'infliger des amendes de 10 000$ et des peines d'emprisonnement de 6 mois pour une infraction aux règlements municipaux et aux règlements concernant l'affichage.[2] Le 29 octobre, le gouvernement de C-B introduisait une autre loi, la *Assistance to Shelter Act*, qui, selon L'Association des libertés civiles de la Colombie-Britannique, pourrait facilement être utilisée pour chasser les sans-abris des endroits publics pendant la tenue des Jeux.

À l'intention de ceux qui oseront quand même manifester, la police de Vancouver a ajouté un LRAD (Long Range Acoustical Device) à son arsenal pour « contrôler » les foules pendant les Jeux de Vancouver. Cette arme, testée en Irak et utilisée également contre les manifestants lors du dernier sommet du G20 à Pittsburgh, envoie des ondes sonores de haute intensité qui provoquent douleur et troubles de vision.

1. Jorge Barrera, service de nouvelles Canwest, 6 mai 2008

2. Communiqué de presse, L'Association des libertés civiles de la Colombie-Britannique, 9 octobre 2009

Adil Charkaoui recouvre la liberté

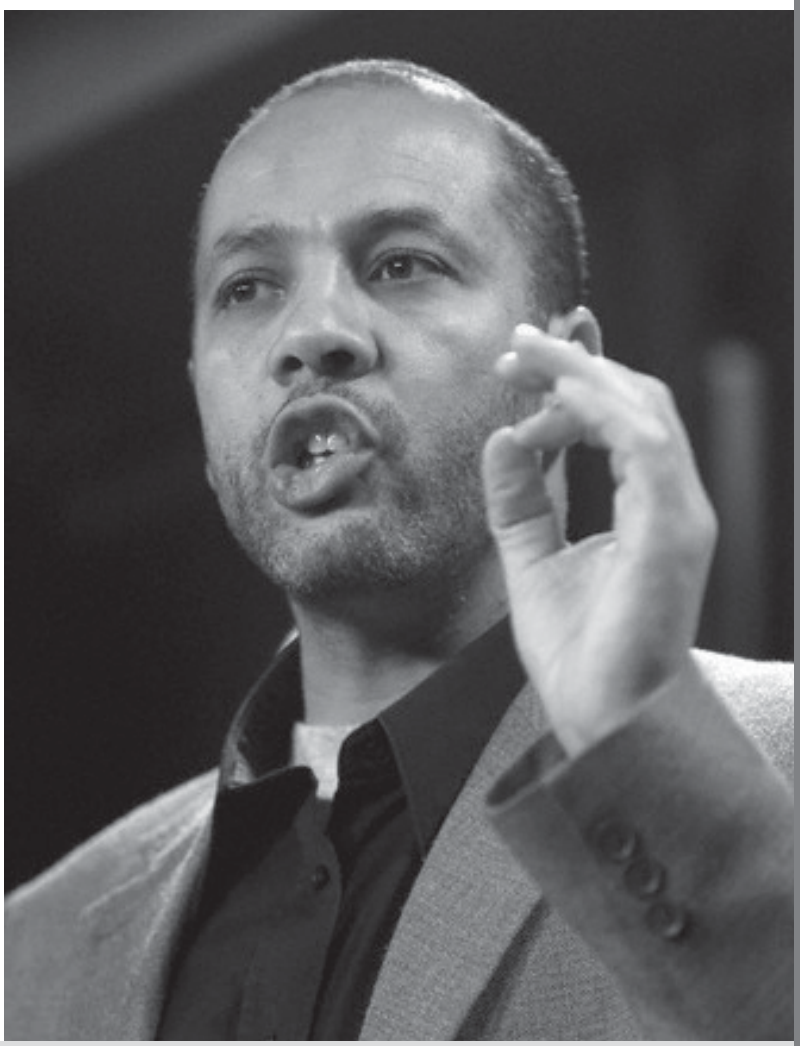
Dominique Peschard

Le 14 octobre 2009, la juge Danièle Tremblay-Lamer de la Cour fédérale mettait fin aux procédures intentées par le gouvernement fédéral pour faire reconnaître la validité du certificat de sécurité émis à l'encontre d'Adil Charkaoui. Elle rejetait dans le même jugement la demande faite par les représentants du gouvernement de référer sa décision sur le dévoilement de la preuve à la Cour d'appel.

En effet, ce jugement fait suite à une décision précédente de la juge Tremblay-Lamer qui intimait au SCRS de rendre publique une partie de la preuve contre Adil Charkaoui parce que la dévoiler ne porterait pas atteinte à la sécurité nationale. Le SCRS a alors préféré retirer cette partie de la preuve du dossier plutôt que de la rendre publique. Une fois cette preuve retirée, la preuve restante n'était plus suffisante pour justifier un certificat de sécurité, de l'avis même du SCRS et de la juge. Mais, plutôt que de retirer la demande de certificat, comme la juge le leur avait suggéré, les représentants du SCRS ont préféré laisser la juge statuer pour pouvoir porter la cause en appel.

La possibilité d'appel dans les procédures de certificats de sécurité est cependant très limitée et n'a rien à voir avec le droit d'appel normalement reconnu. La décision de référer la cause à la Cour d'appel revient au juge de la Cour fédérale et pour que celui-ci accepte de référer la cause, il faut que l'une des parties réussisse à le convaincre que sa décision soulève une « question grave de portée générale ». Cette limite au droit d'appel dans la loi de l'immigration, qui vise normalement à restreindre le droit d'appel des personnes visées par un certificat, s'est retournée contre les représentants du gouvernement quand la juge Tremblay-Lamer a refusé leur requête de référer la question de la preuve à la Cour d'appel.

Ce dernier épisode de la saga judiciaire d'Adil Charkaoui démontre une fois de plus le caractère vicié des certificats de sécurité. Adil Charkaoui est libre, mais le SCRS continue de prétendre qu'il a des preuves contre Adil Charkaoui qu'il ne peut dévoiler. Même si le gouvernement abandonne toute procédure, on ne peut pas dire pour autant que justice a été rendue. Le caractère odieux des preuves secrètes demeure entier et le fait que ces prétendues preuves n'auront jamais été testées dans le cadre d'une procédure judiciaire transparente laissera toujours planer un doute sur la culpabilité d'Adil Charkaoui dans l'opinion publique.



Présentation

Comme le souligne Mme Jennifer Stoddart, « Une démocratie dynamique, ouverte, expressive et innovatrice est menacée lorsqu'on espionne les citoyennes et les citoyens ». Dans « Protéger la vie privée » [p. 7], Mme Stoddart trace un portrait d'ensemble des développements récents qui menacent la protection des renseignements personnels et lance un appel visant à freiner le glissement vers une société de surveillance et à rétablir le droit à la vie privée. L'intervention de la Commissaire auprès de Facebook montre comment il est possible d'interpeller une entreprise pour l'amener à adopter des politiques plus respectueuses des droits des usagers. [D. Peschard, p. 11]

La soif des agences de renseignements d'amasser un maximum d'informations sur l'ensemble des populations trouve son expression la plus monstrueuse dans la National Security Agency des États-Unis. [D. Peschard, p. 12] À cet égard, la Chine est un exemple à méditer sur ce qui pourrait nous attendre si on laisse se poursuivre la dérive de nos sociétés vers la surveillance globale. [D. Peschard, p. 17]

Sur la base des informations recueillies par les agences de renseignement, des individus sont placés sur des listes de personnes soupçonnées de représenter un risque pour la sécurité, comme l'explique Roch Tassé dans « L'arbitraire kafkaesque – les listes antiterroristes ». [p. 19] Une de ces listes est la liste canadienne des personnes interdites de vol. [p. 21] Patricia Poirier explique comment des personnes sont placées sur cette liste sur la base de renseignements secrets; elle montre qu'il n'y a, à toute fin pratique, aucun recours lorsqu'on se retrouve sur une telle liste. Dans « Cela aurait pu vous arriver », Mme Poirier illustre, à partir d'un certain nombre de cas, le cauchemar vécu par des citoyens ordinaires pris dans les mailles de cette liste. [p. 23] Me Johanne Doyon explique pourquoi cette liste viole des droits et libertés reconnus dans la Constitution. [p. 26]

Pour ce qui est du Québec, Lucie Mercier trace un portrait du déploiement fulgurant de l'informatisation dans le secteur de la santé et du développement de banques de données de plus en plus souvent nominatives. [p. 28] À l'instar de la Vérificatrice générale du Canada, Mme Mercier démontre que les violations de confidentialité des renseignements et la faiblesse de la sécurité des systèmes figurent parmi les risques les plus élevés de ces projets. Ces développements sont d'autant plus inquiétants qu'ils se situent dans un contexte où le régime québécois de protection des renseignements personnels a été affaibli. [Anne Pineau, p. 34] De plus, la Loi sur les services de santé et les services sociaux et d'autres dispositions législatives a été amendée de manière à ce que la règle du consentement explicite pour la communication de renseignements contenus dans le dossier de santé de l'usager devienne plutôt l'exception, et l'accès à ces renseignements, la règle générale. [Anthony Hémond, p. 38]

D'autres mesures de surveillance des populations sont en train d'être mises en place. Le gouvernement Harper a déposé deux projets de loi, C-46 et C47, qui élargiraient les pouvoirs de surveillance des communications des Canadiens. [Martine Eloy, p. 40] Au Québec, des caméras de surveillances peuvent être installées dans des lieux publics sans pré-autorisation de la part de la Commission d'accès à l'information qui est chargée de veiller au respect des règles qui protègent la vie privée. [Anne Pineau, p. 42] Enfin, ce dossier ne serait pas complet sans faire état des nouveaux documents d'identité qui permettent de relier les individus à des banques de données. [D. Peschard p. 44]

Dominique Peschard, président
Ligue des droits et libertés

Protéger la vie privée

Jennifer Stoddart
Commissaire à la protection de la vie privée du Canada

Une démocratie dynamique, ouverte, expressive et innovatrice est menacée lorsqu'on espionne les citoyennes et les citoyens. Ces dernières années, trois facteurs clés ont contribué à augmenter de façon draconienne les menaces auxquelles les commissaires à la protection de la vie privée – et nous tous – sommes confrontés : les progrès technologiques, les transformations économiques et les répercussions des événements du 11 septembre 2001.

Progrès technologiques et protection de la vie privée

Au cours des 20 dernières années, les progrès des technologies de l'information et des communications ont fait en sorte qu'il est beaucoup moins cher et plus rapide de recueillir, créer, échanger, traiter et stocker l'information. On qualifie cette prolifération spectaculaire de données d'« exaflood » – la submersion.

La Library of Congress des États-Unis a mis deux siècles à rassembler les quelque 134 millions d'articles qui composent sa collection d'ouvrages imprimés. Grâce à l'explosion de l'information numérique, il suffit maintenant de moins de 15 minutes pour que la planète produise une quantité équivalente d'information. Cette montagne de données renferme beaucoup de renseignements personnels qu'il faut gérer et protéger de façon appropriée.

Le *Washington Post* rapportait, dans un article de mars 2007, qu'une base de données en plein essor menaçait de submerger les personnes chargées de gérer un fonds américain de données sur des présumés terroristes. En quelques années, la taille de cette base de données a plus que quadruplé. Le responsable a affirmé que sa plus grande préoccupation est « le contrôle de qualité à long terme » alors que la base de données continue de se développer.

Chez nous, une vérification effectuée par le Commissariat à la protection de la vie privée en 2007 a démontré que les fichiers inconsultables de la GRC contenaient des dizaines de milliers de dossiers sur la sécurité nationale et de dossiers opérationnels de renseignements sur la criminalité qui ne devraient pas se trouver là. Cette situation était susceptible d'entraîner des risques accrus pour les personnes nommées dans les fichiers.

La puissance des nouvelles technologies a aussi engendré un type de risque complètement nouveau relativement à la protection de la vie privée : la portabilité d'imposants agrégats de renseignements personnels. Il y a 40 ans, il était pratiquement impossible de quitter un édifice gouvernemental en emportant des dossiers contenant les renseignements personnels de millions de citoyens – il aurait fallu un camion pour transporter tout ce papier. Il y a 30 ans, il aurait fallu transporter plusieurs caisses de disquettes. Même il y a 10 ans, il aurait été difficile d'emporter un disque dur en échappant à la vigilance de la sécurité. Mais aujourd'hui, on peut stocker tous ces fichiers dans un ordinateur portatif, sur un DVD ou une clé USB. En Grande-Bretagne, les renseignements personnels de 25 millions de familles ont été compromis suite à la disparition de deux disques informatiques.

La protection de la vie privée dans le contexte d'une économie transformée

L'économie de l'information a complexifié la relation entre les citoyens et l'État, tout comme elle a chamboulé le lien qui unissait les entreprises à leurs clients. La concurrence mondiale a transformé toutes les industries en industries de l'information avides de la plus grande quantité possible de renseignements sur leur clientèle.

Un autre enjeu menace grandement la protection de la vie privée – les changements fondamentaux dans l'approche des gouvernements face à la question de la sécurité nationale. (...) À l'échelle mondiale, tous les gouvernements – les démocraties comme les dictatures – recueillent maintenant plus de renseignements sur les citoyens qu'ils ne l'ont jamais fait auparavant.

À l'instar des matières premières, les données sont désormais transmises par voie électronique partout dans le monde pour être traitées – à quiconque peut les analyser, les retraiter ou les stocker le plus rapidement et à moindre coût. Au fur et à mesure que les coûts de stockage de chaque gigaoctet de données diminuent, les entrepôts de serveurs et de renseignements et le forage de données[1] sont de plus en plus fréquents.

Ces tendances ont de profondes répercussions sur la protection de la vie privée. Le commerce électronique en est l'exemple le plus flagrant. Dans le cadre d'une seule transaction, il est possible de recueillir des renseignements personnels et de les échanger avec des douzaines de parties dans divers pays. Si vous achetez un livre en ligne, vous risquez de créer un sillage international de renseignements personnels de plusieurs milliers de kilomètres.

Les vastes bassins de données personnelles que créent ces transactions sont devenus des cibles alléchantes aux yeux des pirates informatiques. À preuve, les atteintes à la protection des données de grande envergure qui ont été décelées en décembre 2006 chez TJX, le géant américain du commerce de détail, propriétaire des magasins Winners et HomeSense. Plus près de nous, Heartland Payment Systems, une compagnie américaine qui traite les transactions par carte de crédit pour le compte de plus de 250 000 entreprises, était victime d'une énorme atteinte à la sécurité causée par des maliciels présents dans son système de traitement.

Ce type de chaîne d'approvisionnement des données affecte la façon dont le gouvernement fédéral traite les renseignements personnels. Le ministère de la Citoyenneté et de l'Immigration impartit le traitement des données relatives aux demandes de visas à une entreprise privée en Chine; il y avait déjà eu une entente du même genre avec d'autres pays. Cette situation soulève évidemment la question de savoir si les renseignements personnels que détiennent les sociétés privées seront aussi bien protégés que s'ils étaient traités uniquement par des fonctionnaires canadiens.

En raison des dispositions de sécurité en Chine, les autorités du gouvernement chinois peuvent accéder aux données des demandeurs. Pendant ce temps, la compagnie choisie pour traiter les demandes de visas a subi, en ligne, une atteinte à la sécurité, exposant les renseignements personnels de quelque 50 000 Indiens qui avaient fait la demande d'un visa britannique.

Le motif de la sécurité nationale

Un autre enjeu menace grandement la protection de la vie privée – les changements fondamentaux dans l'approche des gouvernements face à la question de la sécurité nationale. Suite à la tragédie du 11 septembre, nous avons vu des « forteresses » de la protection de la vie privée commencer à s'écrouler. À l'échelle mondiale, tous les gouvernements – les démocraties comme les dictatures – recueillent maintenant plus de renseignements sur les citoyens qu'ils ne l'ont jamais fait auparavant.

Certaines initiatives soulèvent d'importantes questions liées aux droits de la personne. Au Canada, les compagnies aériennes sont tenues de communiquer au gouvernement des renseignements sur les passagers. En vertu des lois visant le terrorisme et le blanchiment d'argent, les banques, les bijoutiers-joailliers, les agents immobiliers, les avocats, les courtiers et

1. Pour en savoir plus sur le forage ou l'exploration de données, voir page 15.

les employés de casinos ont l'obligation d'aviser le gouvernement lorsqu'ils jugent suspectes les transactions de leurs clients.

L'an dernier, on lançait un projet pilote à l'aéroport international de Kelowna (Colombie Britannique), qui impliquait l'utilisation volontaire de balayeurs voyant à travers les vêtements pour produire une image détaillée du corps. Cet appareil permet aux agents de détecter les objets potentiellement dangereux qui sont cachés sous les vêtements.

Quant à la liste canadienne des personnes interdites de vol, elle pourrait utiliser secrètement des renseignements personnels d'une manière qui porterait gravement atteinte à la protection de la vie privée et aux droits connexes comme la liberté d'association et d'expression et le droit de se déplacer librement.

Le gouvernement fédéral a déposé en juin deux projets de loi visant à faire en sorte que toutes les entreprises de télécommunications sans fil, les fournisseurs d'accès Internet et autres entreprises de télécommunications puissent surveiller les communications et accéder aux demandes de données sur leurs abonnés émanant des organismes gouvernementaux — et ce, même sans ordonnance judiciaire. Les gardiens de la vie privée de tout le pays ont exhorté le Parlement de faire preuve de prudence dans ces propositions législatives visant à créer un régime de surveillance accrue qui aurait des répercussions importantes sur le droit à la vie privée.

Les commissaires et ombudsmans canadiens ont émis une résolution conjointe priant les parlementaires de s'assurer qu'il existe un besoin clair et démontrable d'étendre les pouvoirs d'enquête existants des organismes d'application de la loi et de sécurité nationale. Les gardiens de la vie privée au Canada recommandent fortement que les parlementaires prennent des mesures pour faire en sorte que tout projet de loi soit le moins envahissant possible et comprenne des mesures de surveillance efficaces — si le Parlement devait déterminer qu'un régime étendu de surveillance soit nécessaire.

Détournement d'usage

Le détournement d'usage est une autre source de préoccupations. Les gouvernements pourraient être tentés d'utiliser tous les renseignements personnels qu'ils recueillent à des fins autres que celles prévues au départ. Généralement, un programme est lancé dans l'intention de s'attaquer à un problème dès qu'il survient. Avec le recul, on s'aperçoit souvent qu'il s'agissait d'événements exceptionnels. Toutefois, la crise passée, la surveillance se continue.

À quoi peut-on s'attendre? Le Royaume-Uni, tout comme les États-Unis qui lui ont rapidement emboîté le pas, pourrait nous donner un aperçu de ce qui nous attend. Plus tôt cette année, les médias britanniques ont rapporté que les conseils municipaux et d'autres organismes publics utilisent les pouvoirs que leur accorde la loi antiterroriste pour enquêter sur des délits mineurs comme la consommation de tabac chez les jeunes, les infractions de stationnement et même l'omission de ramasser les excréments d'un chien.

Nous ne considérons pas que ces renseignements soient du domaine du privé parce que nous avons quelque chose à cacher ou parce que nous avons mal agi. Nous le faisons parce qu'ils sont personnels; parce qu'ils nous appartiennent. Cela ne regarde personne d'autre.

Ce que répondent les gouvernements

Les politiciens et les bureaucrates nous assurent que la protection de la vie privée ne court aucun danger. Mais d'une vérification à l'autre, d'une évaluation à l'autre, d'un rapport à l'autre, le Commissariat à la protection de la vie privée décèle des problèmes, des lacunes dans la sécurité, des atteintes à la protection des données, une piètre tenue des dossiers et de grossières erreurs humaines.

On nous répète souvent que celui qui n'a rien à se reprocher n'a rien à craindre. L'an dernier, lors d'un échange à l'occasion d'une réunion d'un comité parlementaire, un député en faveur de programmes rigoureux de sécurité nationale a dit, tout étonné : « Mais qu'est-ce que ça peut bien faire aux Canadiens que le gouvernement recueille des renseignements

à leur sujet? » David Flaherty, un éminent universitaire qui a été le premier commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique, a répliqué à cette interrogation par une rapide série de questions : « Combien d'argent avez-vous en banque? Avez-vous déjà consulté un psychiatre? Quels médicaments prenez-vous? »

Nous ne considérons pas que ces renseignements soient du domaine du privé parce que nous avons quelque chose à cacher ou parce que nous avons mal agi. Nous le faisons parce qu'ils sont personnels; parce qu'ils nous appartiennent. Cela ne regarde personne d'autre.

Les voies de l'avenir

Dans le monde branché qu'est le nôtre, la protection de la vie privée nécessite une approche globale – il nous faut des défenseurs qui travailleront à instaurer des solutions internationales. Dans plusieurs pays, les lois en matière de protection de la vie privée sont plutôt faibles, sinon inexistantes. Résultat : les données que les gouvernements et les entreprises s'échangent pour une raison précise risquent d'être exploitées et utilisées à une multitude d'autres fins.

La vie privée ne sera pas protégée si nos interventions s'arrêtent à la frontière. Nous avons besoin de réflexions et de solutions de portée mondiale. Sur ce front, je suis très encouragée par les efforts récents de l'OCDE et de l'APEC.

Nous avons également besoin de défenseurs de la protection de la vie privée dans les rues. Chaque Canadienne et chaque Canadien peut apporter son soutien en exprimant ses attentes à l'égard du gouvernement. À mon avis, les Canadiennes et les Canadiens s'attendent à ce que leur gouvernement adopte des mesures de sécurité qui respectent les droits fondamentaux. Ils veulent que le gouvernement garantisse la protection de leurs renseignements personnels. Ils veulent qu'on respecte leur dignité. Le gouvernement doit les écouter.

*****

La protection de la vie privée est un élément fondamental d'une société libre; sans elle, il n'y a pas de réelle liberté. Présentement, le Canada se dirige dangereusement vers une société de surveillance. De plus en plus, nous évaluons les situations quotidiennes en termes de risques; la collecte et l'utilisation de renseignements personnels – qu'on jugeait exceptionnelles jusqu'à tout récemment – deviennent monnaie courante.

L'Histoire démontre que la surveillance des gouvernements fait tache d'huile : la surveillance s'étend alors que les renseignements personnels d'un nombre croissant de personnes sont consignés et examinés à la loupe. Freiner ces tendances ne sera pas facile. À l'instar de plusieurs autres droits et libertés, on ne lutte pas pour la protection de la vie privée en vue d'obtenir une victoire définitive. C'est une bataille qu'il faudra reprendre, encore et encore. L'avenir n'est pas coulé dans le béton – ce n'est pas la politique ou la technologie qui le déterminent, mais bien les personnes elles-mêmes.

L'échec n'est pas une option. Le droit à la vie privée relève d'un intérêt public de premier ordre.

Nous avons également besoin de défenseurs de la protection de la vie privée dans les rues. Chaque Canadienne et chaque Canadien peut apporter son soutien en exprimant ses attentes à l'égard du gouvernement. À mon avis, les Canadiennes et les Canadiens s'attendent à ce que leur gouvernement adopte des mesures de sécurité qui respectent les droits fondamentaux. Ils veulent que le gouvernement garantisse la protection de leurs renseignements personnels. Ils veulent qu'on respecte leur dignité. Le gouvernement doit les écouter.

Facebook contraint à mieux protéger les renseignements personnels des utilisateurs

Dominique Peschard
Ligue des droits et libertés

Le 27 août 2009, la Commissaire à la protection de la vie privée du Canada, Jennifer Stoddart, annonçait une entente avec *Facebook* concernant la protection des renseignements personnels des utilisateurs de ce site de réseautage. *Facebook* compte 12 millions d'utilisateurs au Canada et 200 millions à travers le monde.

Le Commissariat à la protection de la vie privée du Canada (CPVP) a mené un examen des pratiques et politiques de Facebook suite à une plainte déposée par la Clinique d'intérêt public et de politique d'Internet du Canada de l'Université d'Ottawa. Le CPVP a fait une série de recommandations afin que *Facebook* se conforme aux exigences de la loi canadienne sur la protection des renseignements personnels et *Facebook* s'est engagé à modifier ses pratiques à la satisfaction du CPVP.

Le CPVP avait identifié des problèmes majeurs dans le fonctionnent de *Facebook*. Le principal concernait le partage de l'information sur les utilisateurs avec les développeurs d'applications qui sont plus d'un million à travers le monde et le manque de mesure de sécurité pour limiter l'accès de ces développeurs aux renseignements personnels des utilisateurs et de leurs amis.

Facebook a accepté de modifier sa plateforme afin d'empêcher toute application d'avoir accès aux renseignements personnels de l'utilisateur sans le consentement de ce dernier. L'utilisateur pourra de plus contrôler le droit d'accès par catégorie de renseignement. Il pourra également choisir ou non de partager les données de ses amis avec une application.

Avec ce nouveau modèle fondé sur les permissions, les utilisateurs sauront également ce qui ce produit lorsque leurs amis ajoutent une application et pourront choisir de limiter l'accès à leurs données.

Un autre enjeu concernait la conservation par *Facebook* des renseignements personnels d'un utilisateur après que celui-ci ait « désactivé » son compte. Pour que les renseignements personnels soient effacés, l'utilisateur devait plutôt demander la « suppression » de son compte, mais la distinction entre les deux prêtait à confusion dans l'information de *Facebook*. Dorénavant, *Facebook* informera clairement les utilisateurs qu'ils peuvent « désactiver » ou « supprimer » leur compte et ils seront avisés de la possibilité d'effacer leurs données lorsqu'ils désactiveront leur compte.

Facebook laisse le profil de l'utilisateur en ligne après son décès afin que ses amis puissent lui rendre hommage. Les utilisateurs pourront dorénavant donner un consentement valable pour que leur compte soit mis en mode « commémoration » après leur décès.

Facebook devra également informer les utilisateurs qu'ils ont l'obligation d'obtenir le consentement des non-utilisateurs avant de donner les adresses courriel de ces derniers à *Facebook*. *Facebook* s'engage à assurer un suivi des plaintes des non-utilisateurs.

Selon la commissaire adjointe de la CPVP, Elizabeth Benham, ces changements visent à donner le contrôle aux utilisateurs. *Facebook* s'est engagé à mettre en oeuvre toutes les modifications dans un délai d'un an et à fournir des rapports d'étape avant qu'elles soient implantées. Un aspect de l'entente qui mérite particulièrement d'être souligné est son caractère supra-national – tous les utilisateurs de *Facebook* dans le monde bénéficieront de ces changements. À une époque où nous sommes habitués de nous faire imposer des normes internationales qui portent atteinte aux libertés, il est intéressant de constater qu'une action en faveur des libertés dans un pays peut avoir une portée internationale.

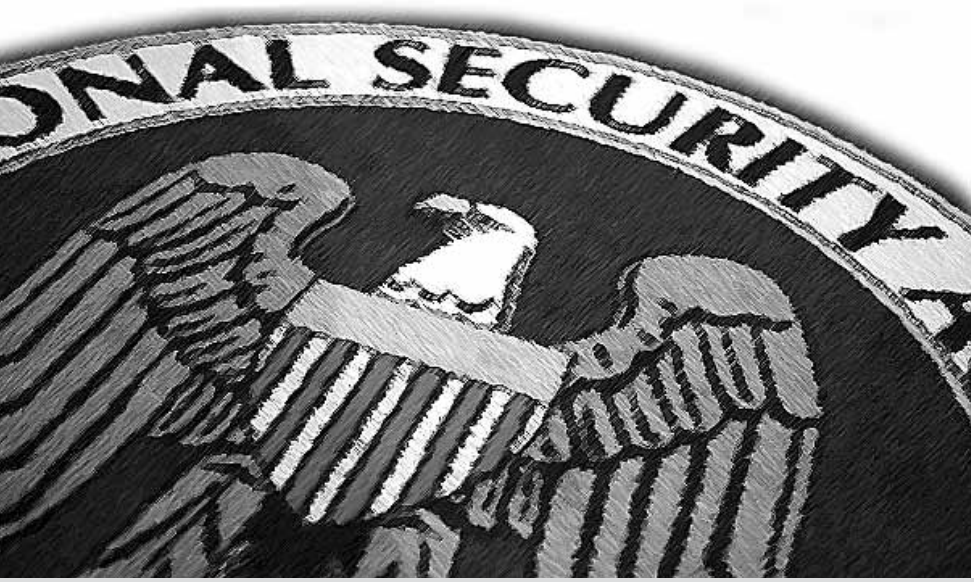
La NSA : à l'écoute du monde

Dominique Peschard
Ligue des droits et libertés

Créée officiellement le 4 novembre 1952, en pleine Guerre froide, la *National Security Agency* (NSA) est la principale agence de sécurité américaine chargée de surveiller les communications électroniques. Avec un budget supérieur à la CIA[1], c'est une des agences les plus secrètes des États-Unis.[2] Elle est responsable, en collaboration avec son pendant canadien, le *Centre de la sécurité des télécommunications* (CST), ainsi qu'avec le *Government Communications Headquarter* de Grande-Bretagne, le *Defence Signals Directorate australien* et le *Government Communications Security Bureau* de Nouvelle-Zélande, du programme *Échelon* qui surveille les communications à l'échelle mondiale.

Un peu d'histoire

À la fin de la Deuxième Guerre mondiale, l'ancêtre de la NSA, la *Signal Security Agency* (SSA), avait réussi à obtenir que les quelques entreprises responsables du réseau de communication des É-U – ITT, RCA Communication, Western Union - lui remettent secrètement toutes les communications entrant, sortant ou transitant par les États-Unis. Pour se mettre à l'abri de poursuites criminelles, les dirigeants de ces entreprises avaient exigé des garanties d'immunité de la part du Secrétaire à la défense et du Procureur général des É-U. Ce programme d'espionnage illégal, du nom de code Shamrock, a été poursuivi par la NSA après 1952. Pendant la guerre du Vietnam, la NSA a espionné les conversations téléphoniques et les télégrammes de milliers d'Américains opposés à la guerre, y inclus de personnes comme Joan Baez, Benjamin Spock et Jane Fonda.



L'arrivée des satellites de communications dans les années soixante allait bouleverser non seulement les moyens de communication mais aussi les possibilités de surveillance et d'espionnage. Avec une partie de plus en plus importante des communications se faisant par ondes hertziennes, il suffisait de placer des antennes d'écoute à quelques endroits stratégiques sur la planète pour capter l'ensemble de ces communications. Le programme clandestin *Échelon* était né. Cet espionnage n'était restreint par aucune loi des É-U.

En 1978, le Congrès des États-Unis adoptait la *Foreign Intelligence Surveillance Act* (FISA) après qu'il ait été dévoilé que Richard Nixon utilisait le prétexte de la «sécurité nationale» pour espionner des citoyens américains qu'il considérait être ses «ennemis». En vertu de la FISA, la surveillance électronique de communications par « fils » sur le sol des États-Unis requérait un mandat de la cour spéciale créée par la FISA. Pour obtenir ce mandat, Il suffisait de démontrer à la Cour que la cible de la surveillance avait un lien quelconque avec un gouvernement étranger ou une organisation terroriste et que la surveillance permettrait d'obtenir des renseignements utiles. Avec la FISA, il devenait cependant impossible pour la NSA de pratiquer une surveillance de masse sur le territoire des É-U. Il semble qu'après l'adoption de la FISA, la NSA ait assez bien respecté l'obligation de ne pas espionner sans mandat les citoyens américains et les communications dont au moins un des pôles se trouvait aux É-U.

La situation allait changer radicalement après le 11 septembre 2001. En effet, le 16 décembre 2005, le New York Times dévoilait que Georges Bush avait secrètement donné, dès octobre 2001, l'autorisation à la NSA d'espionner massivement les citoyens américains sans mandat de cour, en violation de la FISA. Le 4 août 2006, malgré la tempête soulevée par cette révélation, arguant qu'en liant les mains de la NSA, le Congrès mettait en danger la vie des soldats américains en Irak, l'administration Bush obtenait l'adoption du *Protect America Act* qui permettait à la NSA de poursuivre ses activités de surveillance sans l'autorisation de la Cour selon les dispositions de la FISA.

La NSA et la guerre cybernétique

La NSA est également le siège de l'unité du Pentagone en charge de mener la guerre cybernétique.[3] L'objectif du centre est de développer la capacité de pénétrer, d'exploiter et d'attaquer les réseaux. La NSA met au point des virus, certains conçus pour pénétrer et soutirer clandestinement l'information d'un réseau et d'autres, pour rester dormant jusqu'au moment où ils reçoivent l'instruction de détruire le contenu de l'ordinateur de l'intérieur. En juillet 2002, Georges Bush signait une directive présidentielle top-secrète ordonnant aux agences de renseignements, en particulier à la NSA, de développer les règles et les politiques qui régiraient une cyber-attaque que les États-Unis mèneraient contre le réseau informatique d'un pays étranger. Cette directive permet également au président des États-Unis de lancer une cyber-attaque préventive contre un autre pays.[4]

La menace n'est pas passée inaperçue pour le président Poutine. En 2008, Vladimir Poutine signait des directives présidentielles ordonnant de découpler les réseaux d'ordinateurs russes ayant des fonctions stratégiques des réseaux internationaux.

Pendant la guerre du Vietnam, la NSA a espionné les conversations téléphoniques et les télégrammes de milliers d'Américains opposés à la guerre, y inclus de personnes comme Joan Baez, Benjamin Spock et Jane Fonda.

La révolution technique des années 90

L'avènement de l'Internet, des téléphones cellulaires et l'invention de la fibre optique allaient bouleverser de nouveau les réseaux de communications. Le volume des communications explosait et il fallait trouver un nouveau moyen de transmettre cette information. La fibre optique était le moyen tout indiqué. En quelques années, le réseau de communication mondial qui reposait sur les satellites et les tours micro-ondes allait être remplacé par un réseau de câbles, composés chacun de plusieurs fibres optiques, traversant les continents et les océans.[5] Les nœuds de ce réseau se trouvent presque tous sur le territoire des États-Unis. Par exemple, cinq des six câbles qui traversent le Pacifique se rejoignent dans un édifice anodin appartenant à AT&T sur la côte californienne. Ces câbles transportent 80% des communications de tous les pays du Pacifique et de l'Extrême Orient.

Le NAP (*National Access Point of the Americas*) situé à Miami, un bâtiment renforcé de 75 000 mètres carrés, est le nœud des communications des pays des Caraïbes, de l'Amérique centrale et de l'Amérique du sud, entre eux et avec le reste du monde.[6] Les signaux de cette grande région sont acheminés au moyen d'un câble qui encercle le continent sud, propriété de Global Crossing. En vertu d'un *Network Security Agreement*, les installations de Global Crossing sont conçues pour que Département de la défense des É-U, dont relève la NSA, ait accès aux communications. Cet accord permettait à la NSA d'intercepter quotidiennement 650 millions de communications en 2002.

3. Le Joint Functional Component Command for Cyberwarfare (JFCC-NW).

4. Il est ironique de constater que des États, comme les États-Unis, se dotent des moyens de commettre des actes de piratage informatique à grande échelle alors qu'ils demandent des pouvoirs de surveillance des internautes pour contrer de tels actes!

5. Entre 1988 et l'an 2000, le volume des communications internationales transitant par câble sous-marin est passé de 2% à 80%.

6. Il est estimé qu'en 2005, 94% du trafic **entre** les pays d'Amérique latine transitait par les États-Unis.

Pour des raisons pratiques d'interconnexion et pour économiser, les entreprises de télécommunications ont concentré leur trafic dans un nombre de lieux restreints appelés *Internet Exchange Point* (IXP). Par exemple, 40% du trafic Internet des États-Unis transite par le MAE (Metropolitan Area Ethernet) West à San Jose, Californie. Cette concentration des communications mondiales sur le sol américain représentait pour la NSA à la fois un défi et une opportunité. Une opportunité, parce que jamais dans l'histoire, une quantité aussi importante des communications mondiales n'avait été concentrée à si peu d'endroits. Un défi légal parce que les transmissions par câble tombaient de nouveau sous la coupe de la FISA et qu'il était impossible d'avoir accès à l'ensemble des communications sans modifier la loi et sans la collaboration des compagnies de communication. Un défi technique, également, parce qu'avec les nouveaux modes de communications, chaque conversation ou message Internet est segmenté en paquets de données numérisées qui peuvent emprunter une myriade de chemins différents. La NSA devait également faire face à un volume des communications qui augmentait exponentiellement année après année.

L'obstacle légal allait rapidement être contourné après le 11 septembre 2001. Le 4 octobre 2001, la NSA recevait de l'administration Bush l'autorisation d'ignorer la FISA et de faire de l'écoute sans mandat.[7] Avec la levée de l'obstacle légal, il ne restait plus à la NSA que de se brancher directement aux IXP pour accéder à toutes les communications transitant par les réseaux. Dès l'automne 2001, la NSA obtenait la collaboration de toutes les grandes compagnies de télécommunication, dont en particulier celle d'AT&T qui, à elle seule, donne accès à la majorité des communications internationales et internes aux É-U.[8]

Pour surmonter les défis techniques, la NSA allait recourir largement à l'entreprise privée. Toute l'information transitant dans un réseau pouvait être extraite au moyen d'un dispositif [9] mis au point par la compagnie AT&T, mais il restait le problème majeur de comment traiter toute cette information. Ce problème allait être résolu par des compagnies comme Narus qui ont développé à l'intention des agences de renseignement des systèmes capable d'extraire l'information recherchée de la masse des communications.[10] D'après Narus, son produit haut de gamme, la « *NarusInsight Intercept Suite* (NIS) [est] le seul système qui permet le ciblage précis en temps réel, la capture et la reconstruction du trafic sur le web. […] Le trafic en provenance de points multiples et répondant à divers protocoles peut être reconstitué et acheminé à une seule station de contrôle ou distribué à de multiples stations. La NIS est capable de traiter un large pourcentage des services courriel offerts, dont Google Gmail, MSN Hotmail, Yahoo! Mail et Gawab Mail (version arabe et anglaise).»[11] Dans sa publicité, Narus prétend être en mesure d'analyser une quantité astronomique de messages : « Narus peut fonctionner dans un environnement de production qui comprend 10 milliards de messages par jour dans des

7. La justification de ces nouveaux pouvoirs reposait sur l'avis d'un conseiller juridique de l'administration Bush, John C. Yoo à l'effet « Qu'il semblait que l'exigence d'un mandat en vertu du quatrième amendement ne s'appliquait pas à de la surveillance et à des saisies faites pour protéger la sécurité nationale face à des menaces externes ». Ce même John C. Yoo est à l'origine des mémos justifiant la torture.

8. En 2003, AT&T acheminait 400 millions d'appels téléphoniques et des milliards de messages Internet quotidiennement. AT&T maintient un registre de toutes ces communications dans une gigantesque base de données de 312 terabytes. Le byte en informatique est l'équivalent du mot en langage ordinaire. Tera veut dire 10^{12} , soit 1 suivi de douze zéro.

9. Ce dispositif, connu sous l'appellation de « splitter » prélève une partie de la lumière voyageant sur le câble sans affecter la transmission de l'information. C'est la version moderne des deux pinces sur la bonne vieille ligne de téléphone.

10. La compagnie Narus a été fondée par cinq Israéliens ayant des liens avec l'armée israélienne et l'équivalent israélien de la NSA.

11. James Bamford, The Shadow factory, Anchor books, page 191

applications globales comme le sans-fil, WiFi, prépayé, large bande, voix et données »[12]

La NSA, Microsoft et Google

Pour combler le manque d'espace pour stocker tous les renseignements qu'elle amasse, la NSA est en train de construire un nouvel « entrepôt » de données à San Antonio (Texas) de 42 000 m^2 - l'équivalent d'environ 10 terrains de football. Ce choix n'est pas innocent. La décision de la NSA suit l'annonce faite par Microsoft, en janvier 2007, du choix de San Antonio comme lieu de son nouveau centre de traitement des données.

Occupant une surface de 47 000 m^2, le centre de Microsoft sera aussi important que celui de la NSA. Microsoft a plus de 280 millions de clients Hotmail et ses serveurs traitent 8 milliards de messages par jour. Microsoft traitera dans son nouveau centre les données sur les courriels et les recherches Internet qui transitent par ses serveurs. Aucune loi étasunienne n'empêche la compagnie de les conserver indéfiniment. Par ailleurs, avec le *Patriot Act*, la loi étasunienne permet à la NSA d'avoir accès à toutes les données de Microsoft, sans mandat de la Cour. Il suffira tout simplement d'installer un câble optique entre les deux installations…

Google est l'autre compagnie qui pourrait s'avérer d'un grand intérêt pour la NSA. Google a non seulement des millions de clients qui utilisent son service courriel quotidiennement, mais la compagnie tient également un registre du billion (1000 milliards) de recherches que des centaines de millions de personnes on fait avec son moteur de recherche.

Mais que faire de toutes ces données?

Le Data mining ou l'exploration de données

Dans les mois suivant les attentats du 11 septembre 2001, le Pentagone, à travers son agence de recherche DARPA, mettait sur pied le projet *Total Information Awareness*. Dirigé par l'amiral à la retraite John Poindexter, le projet visait, ni plus ni moins, à compiler toutes les informations disponibles sur chaque individu : achats, transactions financières, lectures, sites Internet fréquentés, appels téléphoniques, réseau d'amis, activités, voyages, prescriptions médicales, etc. En reliant toutes ces informations, Poindexter prétendait pouvoir identifier le prochain terroriste et l'arrêter avant qu'il ne prenne l'avion. Voilà comment un collègue de Poindexter présentait la chose :

La situation allait changer radicalement après le 11 septembre 2001. En effet, le 16 décembre 2005, le New York Times dévoilait que Georges Bush avait secrètement donné, dès octobre 2001, l'autorisation à la NSA d'espionner massivement les citoyens américains sans mandat de cour, en violation de la FISA.

« On a tous vu ce que veulent dire les concepts de liens et de rapports dans l'année qui vient de s'écouler. Il y a eu de nombreux articles portant sur les événements du 11 septembre, souvent accompagnés de jolis schémas montrant les liens entre les pirates – certains ont partagé une chambre à Hambourg, certains avaient des billets d'avion achetés en même temps avec la même carte de crédit, d'autres ont voyagé à Las Vegas en même temps et les pilotes se sont entraînés ensemble, et plus significatif quant à notre capacité de détecter le complot d'avance, on avait rapporté un comportement suspect et difficile à expliquer lors de leur entraînement. […] Nous avions l'information mais nous n'avons pas relié les différents éléments. »[13]

L'étoile de Poindexter a commencé à pâlir le jour où William Safire, chroniqueur conservateur et ferme défenseur de la vie privée au New York Times, a eu vent du projet TIA. Sa chronique du 14 novembre 2002, « Vous êtes suspect », était un réquisitoire impitoyable contre le TIA. L'année suivante, Poindexter démissionnait et le Congrès coupait

12. Ibid, page 192

13. Ibid, page 103

Dans les mois suivant les attentats du 11 septembre 2001, le Pentagone, à travers son agence de recherche DARPA, mettait sur pied le projet Total Information Awareness. Dirigé par l'amiral à la retraite John Poindexter, le projet visait, ni plus ni moins, à compiler toutes les informations disponibles sur chaque individu : achats, transactions financières, lectures, sites Internet fréquentés, appels téléphoniques, réseau d'amis, activités, voyages, prescriptions médicales, etc. En reliant toutes ces informations, Poindexter prétendait pouvoir identifier le prochain terroriste et l'arrêter avant qu'il ne prenne l'avion.

tous les fonds au programme. Le projet n'était pas mort pour autant – il allait simplement être poursuivi par la bien plus secrète NSA.

Le produit final de cette « exploration de données » est une liste de noms de personnes censées représenter une menace pour les États-Unis. Cette liste contient entre un demi-million et un million de noms et s'enrichit de milliers de noms chaque mois.[14] Elle est la mère de toutes les listes et est à l'origine d'autres listes comme celle des personnes interdites de vol.

Voici comment un responsable du renseignement des États-Unis décrit la manière dont la liste est composée : « le noyau central est composé de 40 000 noms - c'est le noyau dur, identifié. Quand vous élargissez aux deuxième et troisième degrés amis, famille, partenaires d'affaire, on atteint 120 000 noms.[15] Au quatrième degré, on dépasse les 400 000 noms. Au quatrième degré, je pourrais être sur la liste, si, par exemple, je vous connais et vous habitez dans une bâtisse qui abrite un commerce dont le propriétaire est relié à un groupe dans une autre cellule. »[16]

14. Dans son livre, *The Shadow factory*, James Bamford fait référence à une liste de plus de 400 000 noms alors que l'*American Civil Liberties Union* établit la liste à environ un million de noms.

15. Rappelons que c'est sur la base de ce genre de lien que Maher Arar a été qualifié de terroriste lié à Al-Quaeda. M. Arar avait été vu en compagnie de M. Almaki, lui-même suspect, à tort, d'activités terroristes.

16. Bamford, op. cit, page 343

Dans un rapport de 352 pages financé par le *Departement of Homeland Security* et la *National Science Fondation*, le *National Research Council* des États-Unis concluait que cette approche n'était même pas viable pour identifier des terroristes, qu'elle « poursuivait un objectif impossible à réaliser et qu'il n'était pas souhaitable de poursuivre son développement technologique. » Le rapport soulignait que cette technique rendait suspects « des entreprises et des citoyens respectueux des lois ».

La démesure de la NSA

Il est difficile d'imaginer la dimension des banques de données de la NSA et la puissance des ordinateurs utilisés pour les traiter. Au cœur du dispositif de la NSA trône la « veuve noire », un super ordinateur Cray qui est en mesure de faire plusieurs centaine de milliers de milliards de calculs à la seconde. La NSA devrait recevoir en 2010 un ordinateur Cray X-3 capable de franchir la barre du million de milliards de calculs à la seconde.[17] Mais ce n'est pas encore assez. La NSA réclame un ordinateur mille fois plus puissant pour 2018!

La masse de données accumulées par la NSA s'accroît au rythme de 48 petabytes[18] par année, soit l'équivalent de 24 billions de pages de texte ou d'un milliard de classeurs de quatre tiroirs. Dans son livre, James Bamford compare la NSA à la « Librairie de Babel » du roman de Borges, un « endroit où l'information est à la fois infinie et monstrueuse, où toute la connaissance du monde est disponible, mais où aucun mot est compréhensible »[19]

Malheureusement, les centaines de milliers de personnes prises dans les mailles de ce filet monstrueux ne sont pas les personnages d'un roman.

17. La compagnie Cray est maintenue à flots par la NSA qui ne peut se passer de ses services. Les 250 millions requis pour développer le X-3 ont été fournis par le Pentagone.

18. Le byte en informatique est l'équivalent du mot en langage ordinaire. Peta veut dire 10^{15} , soit 1 suivi de quinze zéro.

19. Bamford, op. cit, page 340

La Chine, banc d'essai de la nouvelle société de surveillance globale

Dominique Peschard
Ligue des droits et libertés

À l'occasion des premières audiences sur la National Security Agency (NSA) en 1970, le sénateur Frank Church, premier secrétaire du *Senate Intelligence Committee* (comité sénatorial sur le renseignement) énonçait la mise en garde suivante : « Si un dictateur en venait à prendre le pouvoir dans ce pays [les É.-U.], les moyens technologiques que les services de renseignement mettent à la disposition du gouvernement lui permettraient d'imposer une tyrannie totale, et il n'y aurait pas moyen de riposter, parce que toute tentative d'organiser une riposte, même dans la plus grande discrétion, serait vouée à être connue du gouvernement. Telle est la puissance de cette technologie. »

Alors que la surveillance des populations se développe à un rythme vertigineux dans tous les pays développés, la Chine est sans doute le pays le plus proche de réaliser le type de société contre lequel le sénateur Church formulait cette mise en garde.

Sous la férule du parti unique, la Chine est en voie de créer ce que Naomi Klein appelle un « stalinisme de marché », une société fondée sur la planification centrale, la surveillance constante et la répression impitoyable au service du capitalisme global.[1]

Le passage de la Chine à une économie de marché a engendré la croissance d'inégalités entre ceux qui profitent de la nouvelle richesse et les millions d'exclus. Les expropriations rurales pour permettre le développement de grands projets et les fermetures d'usines liées à la modernisation ont engendré une population de migrants, estimée à 200 millions, qui parcourent le pays à la recherche d'emplois. Cette dernière fournit le bassin de main-d'œuvre bon marché qui assure la compétitivité des entreprises chinoises. D'après les statistiques officielles, le nombre de « conflits sociaux graves », l'euphémisme bureaucratique pour décrire les affrontements violents opposant ouvriers et paysans aux autorités, est passé de 9 000 en 1993 à 87 000 en 2005.[2] Surveillance, contrôle de l'information et répression font partie des moyens privilégiés pour contrôler une situation sociale de plus en plus conflictuelle. Les autorités chinoises ont clairement l'intention de tuer dans l'œuf tout mouvement démocratique comme celui qui s'est manifesté sur la place Tienanmen en 1989.

Une grande partie des composantes des technologies modernes de surveillance utilisées dans le monde, comme les caméras de surveillance, sont fabriquées en Chine. Mais toute cette production n'est pas destinée à l'exportation. Par exemple, le marché interne chinois pour les caméras de surveillance était de 4,1 milliard de dollars en 2006, une augmentation 24% par rapport à 2005.

La ville de Shentzen, une ville phare de la nouvelle économie chinoise avec ces 12,4 millions d'habitants, milliers usines, gratte-ciel, autoroutes et immenses centres d'achats, n'existait tout simplement pas il y a trente ans. C' est aussi un des lieux où les autorité chinoises sont en train de tester leur nouveau système de surveillance globale connu sous le nom de « Golden Shield ». 200 000 caméras ont déjà été installées à Shentzen, beaucoup camouflées en lampadaires ordinaires et ce n'est qu'un début. Les responsables de la sécurité publique de la ville prévoient en installer deux millions, de quoi faire pâlir de jalousie Londres avec son maigre demi-million de caméras. Depuis 2006, tous les cybercafés, restaurants et autres lieux de loisirs doivent installer des caméras reliées directement aux postes de police et une compagnie de Shentzen a développé un programme qui

1. Naomi Klein, China's All-Seeing Eye, http://www.rollingstone.com/politics/story/20797485/chinas_allseeing_eye, consulté le 3 novembre 2009.

2. Voir le dossier de la revue Relations, La Chine : au-delà du miracle, juin 2008

avertit la police lorsqu'une caméra détecte un attroupement inhabituel de personnes.

Le rôle des compagnies occidentales

Pour les entreprises occidentales du complexe militaire-sécuritaire-industriel, la Chine représente un marché en pleine expansion, évalué à 33 milliards de dollars en 2011, et un endroit où les technologies les plus sophistiquées en matière de surveillance peuvent être testées. Par exemple, lors d'une compétition organisée par le gouvernement chinois pour sélectionner le meilleur logiciel de reconnaissance faciale, un des concurrents les plus sérieux, la compagnie chinoise Pixel, utilisait sous licence la technologie de la compagnie étasunienne *L-1 Identity Solutions*. Cette compagnie a comme administrateur l'ancien directeur de la CIA, Georges Tenet, et est responsable de la plus grande base de données de reconnaissance faciale du Département d'État des É-U. General Electric a fourni à la ville de Beijing un système qui contrôle des milliers de caméras et qui avertit la police lorsqu'il détecte des objets qui se déplacent rapidement, comme des personnes qui courent. IBM installe son *Smart Surveillance System* à Beijing alors que United Technologies est train d'implanter le réseau de caméras de surveillance de Guangzhou.

En février 2006, plusieurs compagnies ont été mises sur la sellette par un sous-comité du Congrès des États-Unis pour leur implication en Chine : Google pour avoir construit un moteur de recherche qui bloquait certains contenus, Cisco pour avoir fournir de l'équipement pour le GFW, Microsoft pour avoir fermé des blogs qui déplaisaient à Pékin et Yahoo pour avoir remis des informations sur ses clients qui ont permis l'arrestation et l'emprisonnement d'un journaliste chinois.

Cette collaboration n'est pas nouvelle. Déjà en l'an 2000, Greg Walton, dans une recherche faite pour le compte de l'organisme Droits et Démocratie, avait dévoilé l'implication de compagnies comme Nortel et Cisco dans la mise en place d'un système de surveillance globale qui comprenait bases de données, reconnaissance faciale, caméras de surveillance, cartes à puces et surveillance de l'Internet.[3] Le projet Golden Shield, dénoncé par Greg Walton, allait inspirer le programme *Total information Awareness* lancé par les États-Unis après le 11 septembre 2001.[4]

3. Greg Walton, China's Golden Shield, Corporations and the development of surveillance technology in the People's Republic of China, October 2001.

4. Voir l'article La NSA à l'écoute du monde, page 12.

Le contrôle de l'information

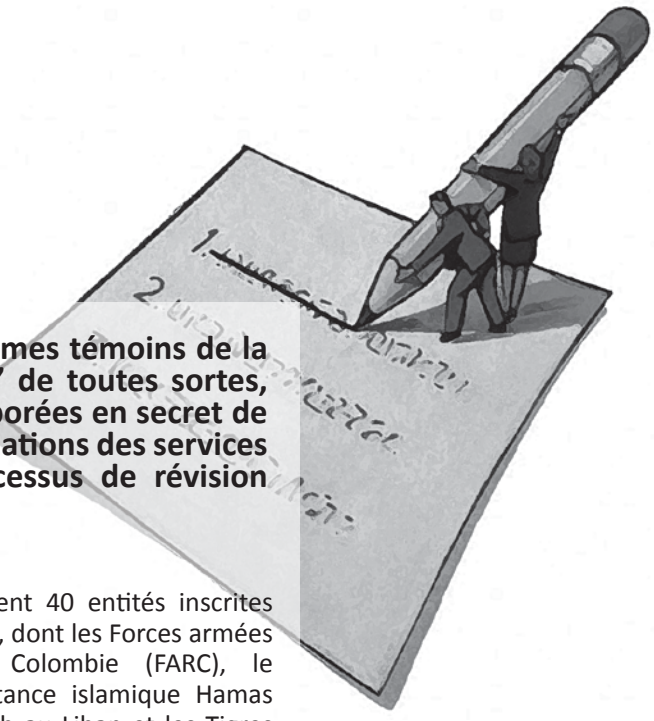
Le dispositif mis en place par les autorités chinoises pour contrôler l'information qui entre et qui sort de la Chine est connu sous le nom de Great Firewall (GFW), en référence à la grande muraille de Chine. Presque toutes les communications Internet entre la Chine et le reste du monde transitent par un nombre restreint de câbles à fibres optiques qui rejoignent le territoire chinois à trois endroits au nord, au centre et au sud de la Chine. Un dispositif similaire à celui que la NSA utilise pour espionner les communications à l'échelle mondiale (voir page 12) envoie un double de toute l'information vers les ordinateurs de surveillance de la Chine afin de déterminer si cette information devrait être bloquée. Dans les secondes qui suivent la requête faite par un utilisateur à son fureteur, cette dernière peut être bloquée de quatre manières :

1. Le GFW donne au DNS (Système de noms de domaine, le bottin d'Internet) l'instruction de renvoyer à l'utilisateur un message d' « adresse introuvable » pour l'adresse IP qu'il souhaite obtenir.
2. Si le DNS a fourni à l'ordinateur la bonne adresse IP, le GFW vérifie la liste des adresses IP interdites et envoie une instruction qui interrompt la communication.
3. Si l'adresse IP n'est pas sur la liste noire, le GFW vérifie si l'adresse URL contient des mots interdits.
4. L'étape finale est la plus sophistiquée. Chaque page est balayée pour vérifier l'acceptabilité du contenu.

Même si le système peut être contourné par des internautes habiles, il suffit pour décourager la plupart des internautes chinois. Par ailleurs, l'existence d'un tel système a un effet dissuasif; un internaute qui tenterait trop souvent d'aller sur des sites bloqués pourrait attirer l'attention des autorités.

L'arbitraire kafkaesque des listes antiterroristes

Roch Tassé, coodonnateur
Coalition pour la surveillance internationale des libertés civiles (CSILC)



Depuis les événements du 11 septembre 2001, nous sommes témoins de la prolifération de listes de surveillance et "antiterroristes" de toutes sortes, mises en place par les gouvernements. Celles-ci sont élaborées en secret de façon arbitraire, le plus souvent sur la base de recommandations des services policiers et des agences de renseignements, sans processus de révision judiciaire et sans mécanisme d'appel véritable.

La Loi antiterroriste canadienne

Au Canada, la Loi antiterroriste adoptée en décembre 2001 confère au Cabinet le pouvoir d'établir une liste sur laquelle il peut inscrire toute entité considérée "terroriste", sur simple recommandation du ministre de la Sécurité publique. Le processus d'inscription commence par des rapports de renseignements de sécurité et de criminalité, faisant état des motifs raisonnables de croire que l'entité s'est sciemment livrée, ou a tenté de se livrer, à une activité terroriste, y a participé ou l'a facilitée; ou que, sciemment, elle agit au nom d'une entité, sous sa direction ou en collaboration avec elle, qui est impliquée dans une activité terroriste. Ces rapports sont soumis à la considération du ministre de la Sécurité publique qui, s'il a des motifs raisonnables de croire que le rapport dit vrai, peut recommander au gouverneur en conseil d'inscrire l'entité sur la liste.

L'inscription d'une entité sur la liste ne signifie pas que celle-ci a commis un crime. Toutefois, une entité inscrite peut voir ses biens saisis, bloqués ou confisqués. En outre, des institutions, par exemple des banques ou des maisons de courtage, ont l'obligation de soumettre des rapports concernant les avoirs d'une entité et d'empêcher l'entité d'accéder à ces avoirs. De plus, tout organisme de charité ou d'aide humanitaire pouvant être associé, directement ou indirectement, à une entité peut voir son statut de charité révoqué et ses avoirs confisqués.

Il y a présentement 40 entités inscrites sur la liste canadienne, dont les Forces armées révolutionnaires de Colombie (FARC), le Mouvement de résistance islamique Hamas en Palestine, Hezbollah au Liban et les Tigres libérateurs de l'Eelam tamoul (TLET) du Sri Lanka. Ainsi, tout citoyen qui envoie de l'argent à des membres de sa famille dans un pays où ces groupes sont actifs, pourrait être accusé de financer le terrorisme. Il en va de même pour les organisations humanitaires qui opèrent dans des zones de conflit et qui, inévitablement, peuvent entrer en contact avec ces entités, comme au Liban par exemple où Hezbollah contrôle une immense partie du territoire et des services sociaux offerts à la population.

Le problème avec une telle liste est que les entités visées sont inscrites sur la base d'une définition vague, imprécise et trop large du *terrorisme* et de l'*activité terroriste* contenue dans la Loi antiterroriste du Canada, et qu'elle n'établit aucune distinction entre les groupes terroristes criminels et les combattants de la liberté ou des mouvements de libération, dont le caractère légitime varie selon les intérêts politiques en place à une période donnée. Avec la définition actuelle, les nobélisés Nelson Mandela et Rigoberta Menchu seraient considérés comme terroristes. Les membres de la Résistance française sous l'Occupation nazie auraient été logés à la même enseigne. De plus, cette définition ne dit rien du terrorisme d'État pratiqué contre leurs propres citoyens par des pays dont certains ont même joint la campagne antiterroriste menée par les États-Unis.

Criminaliser la dissidence

Dans certains pays, les gouvernements utilisent de telles listes pour réprimer la dissidence légitime et la participation démocratique. C'est le cas au Pérou où le gouvernement a invoqué sa loi antiterroriste pour accuser des militants s'opposant à un projet minier, y inclus les dirigeant municipaux ayant organisé un référendum au cours duquel la population s'est prononcée contre un tel projet. Récemment, au Canada, le gouvernement d'Alberta a brandi la menace de porter des accusations en vertu de la Loi antiterroriste contre des militants de Greenpeace ayant occupé des puits de pétrole dans les sables bitumineux.

Les listes étasuniennes

Aux États-Unis, le *Terrorism Screening Centre* maintient une liste de personnes considérées un risque à la sécurité nationale. Cette liste inclut les personnes interdites de vol, les personnes devant être assujetties à des interrogations secondaires chaque fois qu'elles voyagent, les individus interdits de mettre les pieds en territoire étatsunien et autres sous-catégories. À la fin de 2008, il y avait environ 1.1 millions de noms sur cette liste. Quelque 25,000 noms sont ajoutés chaque mois. Pas moins de 16 différentes agences opérant sous l'égide du département du Homeland Security peuvent y inscrire des noms de façon arbitraire, sans procédure judiciaire, selon leurs critères respectifs et sans mécanisme de coordination entre elles. Les individus placés sur la liste n'en sont pas informés, et s'ils le découvrent au moment d'une interdiction de vol par exemple, ils ne peuvent savoir quelle agence les a inscrits, ni les motifs appuyant une telle décision. Bien qu'il y ait un mécanisme d'appel, très peu d'individus ont réussi à ce jour à faire rayer leur nom de la liste. (Voir article sur listes d'interdiction de vol).

La liste des Nations-Unies

Les Nations-Unies aussi maintiennent une liste antiterroriste en vertu de la "résolution 1267 concernant les individus et organisations associés à Al-Qaeda et au Taliban". Tout membre de l'ONU peut soumettre des noms qui doivent être approuvés unanimement par les 15 membres du Conseil de sécurité, encore une fois sans aucune procédure judiciaire. Bien que ces noms soient rendus public, la preuve derrière les allégations demeure secrète. Le Conseil peut aussi rayer des noms de la liste, mais seulement avec le consentement unanime des membres. Selon le site web du comité 1267, il y aurait 400 individus et 111 organisations sur la liste. La résolution 1267 impose une interdiction de vol et un gel des avoirs des individus et organisations inscrites sur la liste.

Abousfian Abdelrazik est le seul citoyen canadien inscrit sur la liste, apparemment à la demande des autorités étatsuniennes. Il a récemment été rapatrié par le gouvernement canadien après un emprisonnement et un exil forcé de six ans au Soudan où il prétend avoir été torturé. Ce n'est qu'après une ordonnance de la Cour fédérale et des moyens de pression exercés par des centaines de citoyens canadiens que le gouvernement a finalement accepté de le rapatrier. Mais en vertu de la loi canadienne, il est interdit à quiconque de lui offrir une aide matérielle, peu importe qu'il s'agisse de salaire, de prêts, de vêtements et même d'assurance-maladie.

À ce jour, le gouvernement canadien refuse toujours de lui venir en aide pour rayer son nom de la liste " 1267 ", lui suggérant plutôt de s'adresser lui-même au comité du Conseil responsable de la liste. Or, comme toute autre question aux Nations-Unies, le processus de révision est extrêmement politisé et personne n'a encore été rayé de la liste sans une intervention de son gouvernement et sans le consentement du pays ayant recommandé l'inscription en premier lieu. Dans le cas Abdelrazik, il faudrait donc non seulement une intervention du gouvernement canadien, mais aussi l'accord des États-Unis. D'ici là, il ne peut blanchir sa réputation et tous ceux qui l'ont appuyé ou qui continuent de lui venir en aide sont susceptibles d'être accusés d'association au terrorisme.

Les listes d'interdiction de vol

Patricia Poirier, coordonnatrice
Projet de recherche action sur les contrôles frontaliers et les listes de surveillance
de la Coalition pour la surveillance internationale des libertés civiles

Une fois par mois, un comité spécial se réunit à Ottawa dans le plus grand secret pour réviser la liste canadienne d'interdiction de vol et ajouter les noms d'individus qui n'auront plus le droit de voyager en avion.

Un haut gradé de la Gendarmerie royale du Canada (GRC) et un cadre du Service canadien du renseignement de sécurité (SCRS) recommandent l'ajout de noms de personnes qu'ils considèrent trop dangereuses pour monter à bord d'un avion, mais trop innocentes pour être arrêtées. Le directeur général du Groupe sécurité et sûreté de Transport Canada préside le comité auquel se joignent parfois d'autres fonctionnaires, mais en fin de compte seuls les représentants officiels de la GRC et du SCRC et le président du comité ont droit de vote. Leur recommandation est alors soumise au ministre des Transports qui approuve toujours leurs suggestions.

Selon Transports Canada, le nom d'une personne sera ajouté à la Liste des personnes désignées (LPD) « si les actions de cette personne portent à croire qu'elle pourrait représenter une menace immédiate pour la sûreté aérienne s'il lui était permis de monter à bord d'un aéronef. » Les critères pour désigner une personne sont vagues et soulèvent bien des interrogations quand on sait que l'ancien directeur de la politique de sécurité à Transports Canada, Brion Brandt a déclaré que le pouvoir du ministre à cet égard est illimité. Il en a remis en disant que les renseignements pour appuyer la désignation des personnes peuvent provenir de toutes sortes de sources, y compris d'agences étrangères.

On estime que cette liste, constituée en vertu du Programme de protection des passagers (PPP) entré en vigueur le 18 juin 2008 compte entre 500 et 3 000 noms. Des demandes d'information en vertu de la *Loi sur l'accès à l'information* n'ont pas permis de savoir combien de personnes sont interdites de vol parce que Transports Canada estime que c'est un secret protégé en vertu de la sécurité nationale. Les personnes dont le nom apparaît sur la liste, ne savent pas qu'elles ont été « désignées » avant d'essayer de prendre l'avion, n'ont pas moyen de connaître les motifs de cette « désignation » et ont encore moins la possibilité de laver leur nom.

Il ne fait pas de doute, comme l'a déjà souligné la Commissaire à la protection de la vie privée Jennifer Stoddart, que le double rôle des agences de sécurité – SCRS et GRC – qui sont en fait juges et parties quand vient le temps de désigner une personne indésirable, est très préoccupant. De plus, il n'est pas impossible que ces agences se servent des renseignements obtenus par l'intermédiaire du PPP, pour cibler des personnes, leur famille et leurs connaissances afin de les surveiller pour des raisons autres que la sûreté aérienne.

Il est aussi possible que cette liste soit partagée avec des gouvernements étrangers. Les conséquences pourraient être très graves si un Syrien ou un Pakistanais se voyait refuser le droit de voyager par avion et que les autorités locales en étaient averties. Quand on sait ce qui est arrivé à Maher Arar qui a été renvoyé en Syrie par les autorités américaines, détenu et torturé pendant 10 mois, il n'est pas difficile d'imaginer ce qui pourrait survenir si la liste canadienne tombait entre les mains de certains services de renseignement étrangers.

D'ailleurs, bien des voyageurs canadiens d'origine arabe ou du Moyen-Orient, ont toujours en mémoire l'épreuve de Maher Arar quand ils voyagent. Non seulement font-ils l'objet d'un profilage religieux et ethnique lors des fouilles et des interrogatoires dans les aéroports, mais en raison de la mauvaise transcription de leurs noms, ils sont plus souvent qu'à leur tour victimes d'erreurs sur la personne.

Les critères pour désigner une personne sont vagues et soulèvent bien des interrogations quand on sait que l'ancien directeur de la politique de sécurité à Transports Canada, Brion Brandt a déclaré que le pouvoir du ministre à cet égard est illimité. Il en a remis en disant que les renseignements pour appuyer la désignation des personnes peuvent provenir de toutes sortes de sources, y compris d'agences étrangères.

Plusieurs voyageurs qui ont accepté de témoigner de leurs expériences, dans le cadre du projet de recherche auquel la Ligue est associé www.surveillancedesvoyageurs.ca, ont déclaré qu'ils voyagent moins souvent en avion qu'avant ou, ont tout simplement renoncé aux voyages à l'étranger, surtout aux États-Unis, depuis l'entrée en vigueur des listes d'interdiction. Non seulement les interrogatoires et les questions supplémentaires sont-ils une source de stress, mais ils craignent de se retrouver coincer à l'étranger.

Lorsque ces personnes ont tenté d'obtenir réparation parce qu'elles avaient été injustement ciblées, plusieurs se sont fait dire de s'adresser aux autorités américaines, de changer leur nom ou encore de se munir d'une carte de fidélité comme Aéroplan d'Air Canada. La plupart des cas rapportés par les voyageurs mentionnent d'ailleurs qu'ils rencontrent toujours des problèmes lorsqu'ils choisissent cette ligne aérienne plutôt qu'une autre. En effet, même si aucune loi ne l'oblige à le faire, Air Canada vérifie toujours si le nom des passagers figure sur la liste américaine, même lorsqu'il s'agit d'un vol intérieur.

On ignore le nombre de noms sur la liste d'interdiction de vol américaine, mais on sait qu'il s'agit d'un sous-ensemble de la liste du *Terrorist Screening Center* (voir article de Roch Tassé, p. 19) qui compte plus de 1,1 million de noms. On retrouve dans cette liste truffée d'erreurs, le même nom épelé de plusieurs manières – ou mal transcrit – ainsi que les noms de personnes décédées, emprisonnées, ou encore d'individus qui ont déjà fait l'objet d'enquêtes mais dont le dossier est fermé depuis des années.

Que l'on soit victime d'une erreur sur la personne ou injustement ciblé, soit par la liste américaine ou la liste canadienne, le résultat est le même : il n'y a pas de recours. Une enquête récente du *U.S. Government Accountability Office* – le Bureau de la reddition des comptes aux États-Unis – a confirmé ce que des centaines de milliers de voyageurs savaient déjà, que ce recours est tout à fait inefficace et que les noms de certains voyageurs qui avaient demandé qu'on corrige leur nom, se sont retrouvés sur une nouvelle liste de personnes indésirables.

Si les listes d'interdictions canadiennes et étatsuniennes sont responsables des retards, de frustrations et des problèmes d'identification d'un grand nombre de voyageurs au pays, l'entrée en vigueur de la dernière étape du programme américain *Secure Flight* pourrait littéralement clouer au sol des milliers de voyageurs au Canada.

Ce programme vise à transférer la responsabilité de vérifier les listes des personnes interdites de vol des compagnies aériennes au TSA (Agence du transport aux États-Unis) et au DHS. Ainsi, lorsque le programme s'appliquera aux vols internationaux d'ici la fin de 2010, ce seront les autorités américaines qui décideront quels voyageurs auront le droit de voler à bord d'un avion au départ, à destination ou survolant les États-Unis.

Comme la plupart des vols au départ du Canada à destination de l'Europe, de l'Amérique latine et des Caraïbes survolent l'espace aérien américain, le programme *Secure Flight* aura in impact immédiat sur la souveraineté du pays et le droit à la vie privée des citoyens. Tous les renseignements personnels des passagers se retrouveront dans les banques de données américaines même si ces voyageurs ne voyagent jamais aux États-Unis, d'autant plus que, comme le PPP, la réglementation ne fait aucune mention des critères ou normes qui seront utilisés pour placer le nom de telle ou telle personne sur la liste d'interdiction étatsunienne.

L'Association du transport aérien du Canada prédit que la mise en œuvre de *Secure Flight* risque de causer le chaos dans les aéroports canadiens.

Cela aurait pu vous arriver …

Patricia Poirier

Le projet de recherche de la Coalition pour la surveillance internationale des libertés civiles (CSILC) et ses partenaires a pour but de recenser les pratiques, les programmes et les systèmes employés pour filtrer les voyageurs dans les aéroports canadiens et aux postes frontaliers afin d'évaluer la portée et la gravité de leur impact concret sur nos droits et d'en informer le public.

Ce projet veut documenter le nombre de personnes qui estiment avoir été ciblées injustement ou par erreur, ainsi que la nature des difficultés qu'elles ont rencontrées.

Les témoignages qui suivent ont été colligés par Patricia Poirier dans le contexte de ce projet. Ces quelques cas, parmis tant d'autres, illustrent bien l'arbitraire de ces listes et les situations cauchemardesques qui en résultent pour les individus pris dans les tentacules de ces listes.

Le cas de John Pass

John Pass, lauréat du Prix du gouverneur général pour la poésie en 2006, a appris qu'il était sur une liste d'interdiction de vol le 27 avril 2008, alors qu'il s'apprêtait à monter à bord d'un avion à destination des Territoires du Nord-Ouest. Ce poète de la Colombie-Britannique avait été invité à lire ses œuvres dans le cadre d'un programme parrainé par les bibliothèques et le Conseil des arts du Canada. Avant de pouvoir obtenir sa carte d'embarquement, il a été interrogé sur son identité par un agent d'Air Canada :

On m'a éventuellement permis de monter à bord, mais on m'a dit que mon nom était sur une liste d'interdiction de vol et que j'aurai à subir les mêmes tracas à chaque fois que j'essaierai de monter à bord d'un avion.

*****

Le cas de Jaspreet Singh

Le jour précédent, un autre auteur primé, Jaspreet Singh, de Montréal, entreprenait une tournée nationale pour faire la promotion de son nouveau livre, *Chef*. Mais, comme John Pass, il n'a pas réussi à imprimer sa carte d'embarquement au kiosque de l'aéroport de Calgary, ni à celui de Montréal.

On m'a soumis à un long interrogatoire détaillé lors duquel on m'a questionné à savoir si j'avais le droit de voyager… des employés d'Air Canada m'ont dit que j'étais sur une "liste" mais ont refusé de me donner plus de renseignements, le personnel d'Air Canada m'a fait une suggestion grotesque – ils m'ont suggéré de changer mon nom…

Ce n'est que lorsque l'auteur a annulé sa participation à deux événements médiatisés qui devaient avoir lieu à Toronto que cette histoire est devenue publique. Quelques jours plus tard, Air Canada a fait savoir que son cas avait été examiné et que le problème était désormais corrigé. M. Singh, qui a grandi en Inde, a étudié à l'Université McGill où il a obtenu son doctorat en génie chimique, n'a jamais réussi à savoir pourquoi il avait été ciblé.

*****

Le cas de Glenda Hutton

Madame Hutton rêvait de parcourir le monde lorsqu'elle prendrait finalement sa retraite après avoir travaillé toute sa vie comme secrétaire dans une école de Courtenay en Colombie-Britannique. Mais lorsque son nom s'est retrouvé sur une liste de surveillance, son rêve s'est effondré. En effet, en octobre 2007, lors d'un vol de Comox à Calgary, elle a appris que son nom apparaissait sur une liste de surveillance et qu'elle ne pouvait monter à bord de l'avion.

Après avoir argumenté avec les représentants d'Air Canada, et au terme de longues vérifications, on lui a finalement permis de monter à bord, mais l'incident lui a laissé un goût amer. Glenda et son mari Ken, un ancien militaire qui a 25 années de service, planifiaient un voyage en Thaïlande. Pour en avoir le coeur net, ils ont vérifié auprès de leur agent de voyage s'ils pourraient partir comme prévu. La compagnie Japan Airlines leur a révélé que le nom de Glenda était sur une liste d'interdiction de vol.

Ils ont dit que nous pourrions sans doute quitter le Canada, mais ils ne croyaient pas que c'était une bonne idée d'aller en Thaïlande ou au Japon parce qu'ils ne pouvaient nous promettre que nous n'aurions pas de problèmes avec les autorités étrangères.

Madame Hutton a ensuite entrepris de longues démarches pour tenter de savoir pourquoi elle était ciblée. Tour à tour, elle s'est adressée à son député fédéral, à Passeport Canada, à Transports Canada, à l'Agence des services frontaliers du Canada (ASFC), au ministère des Affaires étrangères et au Département de la Sécurité intérieure (Department of Homeland Security - DHS). Comme d'habitude, les fonctionnaires canadiens lui ont dit de s'adresser aux autorités américaines pour être retirée de la liste. Mais le DHS ne pouvait l'aider :

Parce que les délais (que vous avez connus) ne sont pas reliés aux vols intérieurs ou à destination des États-Unis, le programme DHS TRIP ne peut vous aider.

Finalement, quelqu'un a proposé à Madame Hutton, qu'elle se procure une carte NEXUS même si elle n'avait pas l'intention de visiter les États-Unis. Le programme NEXUS, selon le site de l'ASFC, « *est conçu pour accélérer le passage à la frontière tant canadienne qu'américaine des voyageurs pré-autorisés à faible risque*. »

Elle a décidé de tenter sa chance en pensant que si elle pouvait obtenir la carte, on ne pourrait sûrement pas la considérer comme étant une personne présentant un risque pour la sécurité. En plus des frais d'inscription non remboursables de 50 $ et de tous les documents obligatoires, elle a dû fournir une preuve qu'elle n'avait pas de casier judiciaire, ses empreintes digitales et une lettre de la Commission des libérations conditionnelles, même si elle n'a jamais été accusée de quoique ce soit. Enfin, elle a dû fournir ses données biométriques, des photos de son visage et de l'iris de ses yeux.

Après 19 mois de démarches et après avoir dépensé des milliers de dollars, Glenda et Ken ont finalement pu faire une croisière au canal de Panama. L'histoire de Madame Hutton s'est bien terminée. Toutefois, tous ces ennuis lui ont coûté environ 2 000 $ en frais, sans compter que sa carte NEXUS doit être renouvelée tous les cinq ans. Ceci sans parler du stress et de l'inquiétude de ne pas savoir… si cela risque de se reproduire la prochaine fois qu'elle partira en voyage.

*****

Le cas d'Alistair Butt

Trois jours après l'entrée en vigueur de la liste canadienne d'interdiction de vol en juin 2007, un adolescent d'Ottawa, Alistair Butt, a appris qu'il avait le même nom qu'une personne dont le nom figure sur une liste d'interdiction de vol, alors qu'il tentait de monter à bord d'un vol de Montréal à St-John's (T.N.).

Après de longues discussions avec les employés de la compagnie d'aviation et Transports Canada, il a finalement pu monter à bord. Toutefois, ses parents sont restés inquiets et craignent que leur fils, un étudiant qui a reçu plusieurs prix et qui a fait l'objet d'un documentaire à la télé, soit à nouveau victime de cette liste s'il voyageait à l'étranger.

Pendant plus de deux ans, sa mère Heather Dunbar, qui a le rang de Major au ministère de la Défense nationale, a frappé à toutes les portes. Elle a fait appel à son député fédéral, aux fonctionnaires de Transports Canada et aux représentants de la compagnie aérienne. "*On ne m'a donné aucune aide ou quelque information utile que ce soit; chez Transports*

Canada…un fonctionnaire a seulement recommandé qu'Alistair change son nom. »

Fait étrange, même si son nom semble poser problème lorsqu'il tente de prendre l'avion, Alistair n'a aucun problème lorsqu'il traverse la frontière des États-Unis.

*****

Les frères Kenny

Le sénateur libéral Colin Kenny, qui préside le Comité permanent du Sénat sur la sécurité nationale et la défense, s'est plaint au Sénat le 28 avril 2008, qu'il n'appréciait pas la réponse que lui avait faite le ministre des Transports de l'époque, Lawrence Cannon, au sujet des problèmes rencontrés par ses fils lors de leurs voyages en avion. Son fils aîné, Robert, pourtant procureur de la Couronne à Toronto, se faisait intercepter à chaque fois qu'il voyageait en avion au Canada ou aux États-Unis.

« *Lorsque Robert a commencé à faire l'objet de vérifications, j'ai attribué cela à la malchance. Mais maintenant que mes deux garçons font l'objet de vérifications, cela semble être plus qu'une coïncidence* », a-t-il déclaré.

Dans sa réponse, le ministre a recommandé à « *vos fils qu'ils arrivent plus tôt à l'aéroport et qu'ils apportent des documents additionnels pour faciliter la vérification de leur identité* ». En précisant que les frères Kenny n'étaient pas sur la liste canadienne d'interdiction de vol, il les a invités à communiquer avec le programme DHS-TRIP en leur fournissant l'adresse du site Internet.

Le sénateur Kenny n'a pas apprécié : « *Si le mieux qu'on puisse faire pour les gens dont le nom figure sur une de ces listes est de les renvoyer à un site Internet, je ne crois pas que le gouvernement fait beaucoup pour aider les Canadiens… Est-ce de cette façon que le gouvernement du Canada traite les Canadiens qui sont confrontés à ce problème — et il semble y en avoir des milliers ?* »

Quels recours ?

Le sénateur Kenny a rapidement compris, comme bien d'autres voyageurs depuis l'entrée en vigueur des listes d'interdiction, qu'il n'y a aucun recours pour les victimes d'erreurs sur la personne.

Lorsque John Pass a écrit à Transports Canada pour se plaindre, il a reçu ce courriel après plus de deux mois :

Veuillez prendre note que les fonctionnaires de Transports Canada ont examiné votre lettre et ont conclu que notre ministère n'est pas en mesure de vous aider parce que les problèmes que vous avez rencontrés ne semblent pas liés à notre programme. À la lumière de cette information, il se peut que votre nom apparaisse sur une liste américaine. Donc, nous nous recommandons de communiquer avec le U.S. Department of Homeland Security's Traveler Redress Inquiry Program (DHS TRIP) au http://www.dhs.gov//trip.

Transports Canada renvoie presque toujours la balle au *Department of Homeland Security*, même lorsque les passagers ont rencontré des problèmes lors d'un vol intérieur.

M. Pass a clairement indiqué qu'il n'avait nullement l'intention de communiquer avec les autorités américaines. De nombreux passagers partagent son opinion et ne sont pas prêts à fournir toutes sortes de données personnelles à un gouvernement étranger. Et, de toutes façons, comme Glenda Hutton l'a appris, si les passagers rencontrent des problèmes sur des vols qui ne sont « ni à l'intérieur ni à destination des États-Unis », le programme DHS TRIP n'est d'aucun secours.

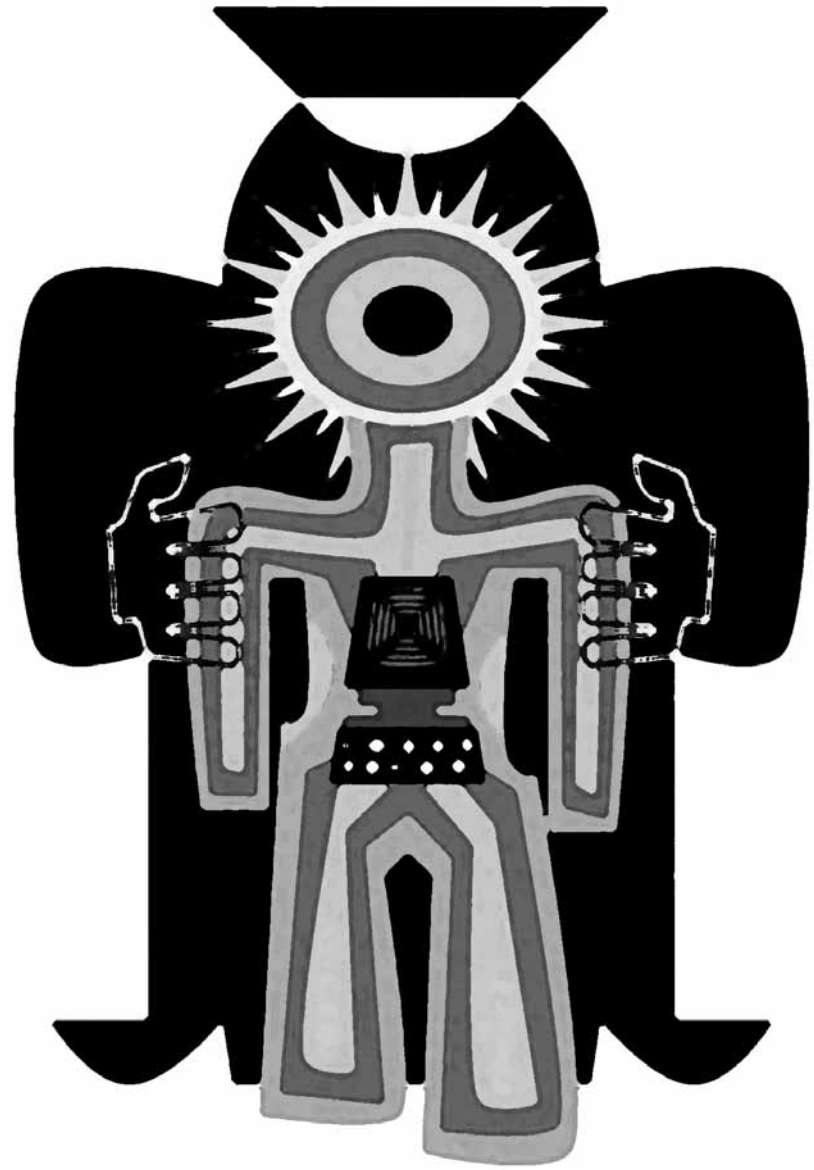
Que l'on soit un étudiant doué, un poète primé, un voyageur ordinaire ou encore un procureur de la Couronne, il n'y a pas de recours pour les passagers victimes d'erreur sur la personne ou injustement ciblés qui se font prendre dans les mailles du filet des listes de surveillance.

surveillancedesvoyageurs.ca

Êtes-vous toujours stoppé, fouillé et interrogé quand vous prenez l'avion ou essayez de traverser la frontière, quoique vous n'ayez jamais été accusé ou trouvé coupable d'un crime ? Pensez-vous être ciblé injustement ou par erreur ? Si vous êtes ciblé de façon systématique ou si vous ne voyagez plus de peur d'être traité différemment, consultez le site http://surveillancedesvoyageurs.ca

La liste des personnes interdites de vol
Chronique d'une mort annoncée

Me Johanne Doyon *
Avocate spécialisée en droit de l'immigration et de la citoyenneté



* Me Doyon conteste la légalité du Programme de protection des passagers devant les tribunaux.

Petit frère du défunt régime des certificats de sécurité[1], le Programme de protection des passagers (ci-après désigné « le programme ») ou le « No Fly List »[2] semble être né du même cerveau :

- Violation, au nom de la sécurité, de droits constitutionnels garantis par la Charte canadienne des droits, tels que notamment la liberté de circulation (article 6), le droit à l'application régulière de la loi face à l'atteinte à la liberté et à la sécurité de la personne (article 7), soit le déni d'audience impartiale et l'usage de preuve /renseignement secret, la violation du droit au respect de la vie privée par la cueillette et l'échange abusifs de renseignements personnels (article 8);
- Absence d'application de mesures moins attentatoires aux droits constitutionnels des personnes suspectées de représenter une menace à la sécurité aérienne (article 1);
- Absence totale de proportionnalité (article 1).

Pourtant, la *Loi sur l'aéronautique* (L.R., 1985, ch. A-2) et le *Règlement canadien sur la sûreté aérienne*, DORS/2000-111, art. 5) prévoient déjà un nombre impressionnant de mesures susceptibles d'assurer la sécurité et la sûreté de l'aviation et des passagers par des pouvoirs de fouille accordés aux agents de contrôle pré-embarquement qui visent les personnes et les biens sous leur garde et sous leur contrôle.

Le règlement exige aussi que toute personne obtempère à la demande d'un agent de se soumettre à une fouille de sa personne ou à une fouille des biens qu'il désire emporter ou de mettre dans l'aéronef. L'agent de contrôle peut également ordonner à une personne

1. Charkaoui c. Canada, 2007 CSC 9

2. Loi sur l'aéronautique (L.R., 1985, ch. A-2) 4.76 à 4.83 Règlement sur le Contrôle de l'identité, [DORS/2007-82] ; règlement modifiant le règlement sur le contrôle de l'identité DORS/2008-250 ; Programme de protection des passagers de Transport Canada ;

de quitter un aéronef si celle-ci est montée à bord sans avoir obtempéré à une demande de fouille. Le règlement fourmille d'interdictions destinées à assurer la sécurité dans les aéronefs et dans les zones règlementées.

Face à l'existence de ces mesures, quelle est donc la véritable raison d'être de *ce programme* ? Le 6 novembre 2007, la Commissaire à la vie privée du Canada affirmait que cette raison d'être n'était pas claire.[3] Vous aurez compris qu'il s'agit moins d'un programme visant la *sécurité* des aéronefs et des passagers que d'un programme de *renseignements*.

Quand on est trop dangereux pour prendre un vol, sans que les autorités se prévalent des mesures de fouille prévues à la loi à son endroit, mais autrement libre comme l'air, le sens commun nous indique que le but de *ce programme* est injustifiable. Tout comme la source de *ce programme* est le renseignement -ce qui est loin d'être rassurant considérant les découvertes faites dans les affaires Arar, Charkaoui, Harkat, Almrei,[4] etc. - son but est aussi le renseignement.

Mais attention, pas le renseignement obtenu de la « personne précisée » volontairement et en conformité des droits constitutionnels garantis à chacun par la constitution canadienne. Non.

Un peu comme son vieux frère, l'ancien régime des certificats de sécurité qui pratiquait la détention pour fins d'enquête, le programme de protection des passagers se trouve à utiliser des méthodes coercitives d'obtention de renseignements, en plaçant la personne précisée dans une situation où elle doit se défendre à l'aveugle, contre des renseignements secrets, pour tenter de récupérer son droit d'embarquement, ce qui l'oblige à renoncer à son droit à la vie privée de même qu'à son droit au silence .

Violation, au nom de la sécurité, de droits constitutionnels garantis par la Charte canadienne des droits, tels que notamment : la liberté de circulation (article 6), le droit à l'application régulière de la loi face à l'atteinte à la liberté et à la sécurité de la personne (article 7), soit le déni d'audience impartiale et l'usage de preuve /renseignement secret, la violation du droit au respect de la vie privée par la cueillette et l'échange abusifs de renseignements personnels (article 8).

Sourds à toutes critiques et même à celles énoncées par les commissaires canadiens à la protection de la vie privée[5] et en marge d'une application constitutionnelle de la Loi sur l'aéronautique, *ce programme* a créé illégalement une « black list », sous la responsabilité principale du Ministre des transports, du SCRS et de la GRC (le groupe consultatif de Transport Canada) en y maintenant continuellement le nom d'une personne, ce qui a pour effet de créer une violation répétée de ses droits constitutionnels, sans véritable recours effectif, jusqu'à décision contraire des autorités précitées.

« *le maintien des droits constitutionnels, qui était considéré à l'époque comme une menace pour la sécurité nationale en période de malaise national, est [TRADUCTION] « l'un des principaux traits » qui distingue une démocratie libérale des [TRADUCTION] « régimes totalitaires* », (p. 4)[6].

Mais c'est bien parce que ces mesures contreviennent à la Charte et représentent une menace à la sécurité nationale, qu'elles sont condamnées à disparaître et avec elles, sans doute quelques autres pouvoirs conférés par d'autres lois, comme la *Loi sur le SCRS*. La sécurité, absolument, mais dans le respect des droits.

3. Mémoire de la Commissaire à la vie privée du Canada à la Commission d'enquête sur les mesures d'investigation prises à la suite de l'attentat à la bombe commis contre le vol 182 d'Air India, 6 novembre 2007;

4. Charkaoui 2008 CSC 38 (destruction de preuve); Re Harkat 2009 FC 553 (défaut de divulgation de preuve disculpatoire) 10-JUN-09 OTT Communication to Mr. Almrei and Honourable Mr. Justice Mosley (défaut de divulgation de preuve disculpatoire); Re Charkaoui : Avis de requête en arrêt des procédures, en jugement déclaratoire et en annulation du certificat 11 août 2009 modifié 18-09-09 et pièces (défaut de divulgation de preuve disculpatoire et autres abus).

5. Résolution des commissaires canadiens à la protection de la vie privée et des responsables de l'application des lois en matière de protection des renseignements personnels du 28 juin 2007;

6. Demande fondée sur l'article 83.28 du Code criminal (Re) 2004 CSC 42 par 113;

L'informatisation dans le réseau de la santé et des services sociaux

Lucie Mercier, conseillère
Fédération interprofessionelle de la santé

Presque inexistante il y a 20 ans, l'informatisation dans le secteur de la santé connaît aujourd'hui des développements fulgurants, généreusement financés par le gouvernement fédéral et les gouvernements provinciaux. Le gouvernement fédéral a d'ailleurs créé à cette fin une agence nommée Inforoute Santé du Canada. Cette informatisation prend plusieurs formes et les projets se multiplient. Parmi les projets en cours actuellement, plusieurs ont trait au dossier médical, comme le Dossier de santé du Québec (DSQ) et le dossier patient électronique (DPE) et ses variantes. L'informatisation, corollaire de la nouvelle gestion publique, passe également par la constitution de banques de données qui ne cessent de se raffiner et contiennent de plus en plus fréquemment des renseignements nominatifs. Les données personnelles en général et les données de santé en particulier sont devenues des ressources naturelles dans nos sociétés en réseaux. Aussi leur circulation est-elle hautement souhaitée. Elle devient même un enjeu de prospérité, comme en fait foi le Partenariat pour la sécurité et la prospérité (PSP). Dans un tel contexte, la vie privée des citoyens-nes est-elle menacée? Comment la protéger?

Dossier de santé du Québec

Pour le gouvernement du Québec, le Dossier de santé du Québec (DSQ) constitue la « pièce maîtresse » de l'informatisation. Il s'agit, à coup sûr, du projet le plus ambitieux et le plus dispendieux. Le DSQ constitue un ensemble de 13 projets dont la valeur était estimée, lors de son lancement officiel en mars 2006, à 563 millions de dollars, financés conjointement par le gouvernement du Québec et par Inforoute Santé du Canada. Au 31 mars 2009, selon le Vérificateur général du Québec (VGQ), le DSQ comprenait 150 contrats d'une valeur de 334 millions de dollars[1].

Pour la mise en œuvre du DSQ, le gouvernement du Québec compte sur toute une série de partenaires comme les agences régionales, les établissements du réseau, la Corporation d'hébergement du Québec, l'Institut national de santé publique du Québec, la Régie de l'assurance maladie du Québec, les Réseaux universitaires intégrés de santé (RUIS) et la SOGIQUE (la division informatique du ministère de la Santé et des Services sociaux), auxquels il faut ajouter de nombreux comités.

L'Agence de la santé et des services sociaux de Montréal est fiduciaire des actifs informationnels du DSQ. Or, l'Agence de Montréal a fait du dossier clinique informatisé (DCI) sa priorité au printemps 2008. Il y a donc un risque identifié par le VGQ relativement à l'absence d'adhésion de cette agence au projet du DSQ. En regard des usagers, leur adhésion a déjà été prévue. D'un consentement explicite prévu au départ, le gouvernement est passé à un consentement implicite. C'est donc dire qu'à moins d'un refus de la part de l'usager, un DSQ sera automatiquement constitué en son nom. Un des motifs invoqués lors de ce changement était la complexité de la gestion des adhésions. L'épargne associée à la valeur de ce changement est estimée à 77 millions de dollars.

Le projet du DSQ suppose aussi un changement de la carte d'assurance maladie du Québec. La carte embossée devrait être remplacée par une carte électronique. Une telle carte ne contient que les données d'identification de l'usager, dont un numéro d'identification unique (NIU) attribué par la RAMQ, un numéro à 12 chiffres qui fait l'objet d'une normalisation internationale. Cette nouvelle carte d'assurance maladie électronique constitue donc dans les faits une carte d'identité informatisée qui donne accès aux banques de données détenues par les différents fiduciaires du DSQ. C'est ainsi que par le DSQ, les Québécois-es seront dotés es

1. Vérificateur général du Québec, Rapport du Vérificateur général du Québec à l'Assemblée nationale pour l'année 2009-2010, Tome 1, chapitre 6 : Vigie relative au projet Dossier de santé du Québec, Québec/Montréal, Le Vérificateur général, 2009, p. 6-20, [En ligne] : http://www.vgq.gouv.qc.ca/fr/publications/rapport-annuel/2009-2010-T1/index.aspx (page consultée le 17 octobre 2009). Il s'agit de la seconde vérification du Vérificateur général. La première a eu lieu en 2008.

d'une carte d'identité électronique en dépit du fait que la Commission de la culture de l'Assemblée nationale l'ait rejetée en 1998.

Le projet du DSQ prévoit la mise en place de registres (intervenants et usagers). Puisqu'il s'agit d'usagers inscrits, autant dire qu'on parle d'un registre de population. L'Index patients maître (IPM) et le Registre des usagers permettent l'identification des usagers, facilitent l'échange d'information et permettent de vérifier en ligne l'admissibilité aux programmes[2]. C'est ainsi qu'il est possible d'affirmer que ce projet facilitera la désassurance des services de santé et leur privatisation.

Selon la Vérificatrice générale du Canada, il semble que le registre des usagers soit prêt mais que « le projet présente des risques élevés, en raison des difficultés importantes que posent la mise en œuvre et l'utilisation du système.»[3] Parmi les risques les plus élevés des projets figurent les violations de confidentialité des renseignements et la sécurité des systèmes[4].

Le DSQ vise-t-il l'amélioration de la qualité des soins? La réponse est non. Le DSQ vise deux objectifs qui n'ont rien à voir avec la qualité des soins. Il vise d'une part l'accroissement de la productivité du travail et, d'autre part, le soutien de l'emploi dans l'industrie de l'informatique. Or, comme pour les autres domaines de l'informatisation, la conservation des données du DSQ se fait par banques de données et, comme dans le cas des autres banques de données, il est prévu que l'entretien du DSQ soit donné en sous-traitance. Se pose alors la question de la protection de la vie privée et de la protection des données personnelles de santé des Québécois-es.

Inforoute Santé du Canada

Inforoute Santé du Canada (ISC) est un organisme indépendant, financé par le gouvernement du Canada. Les 14 sous-ministres de la santé du gouvernement fédéral, des provinces et des territoires composent son conseil d'administration. Sa mission consiste à promouvoir le dossier de santé électronique (DSE) Canada, la version québécoise étant le DSQ. Inforoute a émis des normes visant la compatibilité ou l'interopérabilité des DSE à travers le Canada. Toutefois, elle n'est « pas tenue de veiller à ce que les systèmes respectent les lois sur la protection de la vie privée »[5] La diversité des législations provinciales et territoriales sur la collecte, l'utilisation et la divulgation des renseignements personnels sur la santé entrave le partage des données entre les administrations, aux dires de la Vérificatrice générale du Canada. Un Forum de la confidentialité a été organisé. Des groupes de travail examinent les questions du consentement, de l'utilisation secondaire de l'information et la circulation des données entre les administrations.[6]

Le programme d'investissements d'Inforoute comprend un ensemble de 12 catégories de projets d'une valeur de 2,1 milliards de dollars. Les experts estiment le coût total du projet à 10 milliards de dollars. Inforoute est d'accord avec cette estimation. Au 31 mars 2009, 283 projets étaient complétés ou étaient en cours dans l'ensemble du Canada. Juste pour le DSQ, il était prévu en 2001 que le gouvernement du Québec reçoive un financement d'environ 303 millions de dollars sur les quelques 563 millions que devait coûter initialement le projet, avant la prolongation des échéanciers rendue nécessaire suite aux retards accumulés. Au 31 mars 2009, le gouvernement du Québec n'avait reçu que 92 millions de dollars du gouvernement fédéral et les dépassements de coûts appréhendés n'avaient pas été évalués.

Lors du budget 2009-2010, le gouvernement fédéral a octroyé une nouvelle tranche de 500 millions de dollars sur trois ans à Inforoute Santé du Canada, portant le financement fédéral depuis 2001 à 1,8 milliard de dollars. Un

2. Vérificateur général du Québec, Rapport du Vérificateur général du Québec à l'Assemblée nationale pour l'année 2009-2010, Tome 1, chapitre 6 : Vigie relative au projet Dossier de santé du Québec, Québec/Montréal, Le Vérificateur général, 2009, p. 6-31), [En ligne] : http://www.vgq.gouv.qc.ca/fr/publications/rapport-annuel/2009-2010-T1/index.aspx (page consultée le 17 octobre 2009).

3. Vérificatrice générale du Canada, Rapport d'automne 2009 de la vérificatrice générale du Canada à la Chambre des communes, chapitre 4 : Les dossiers de santé électroniques, Ottawa, Bureau du vérificateur général du Canada, 2009, p. 28.

4. Idem, p. 17.

5. Idem, p. 10.

6. Idem, p. 36.

pourcentage des 500 millions de 2009 devrait servir au développement des DME. Toutefois, l'accord de financement n'avait pas encore été approuvé au 31 mars 2009. Par ailleurs, il ne suffit pas de démarrer un projet pour bénéficier des largesses financières fédérales. En effet, les gouvernements provinciaux et territoriaux reçoivent leur quote-part lors de la livraison des produits et, dans certains cas, lors du déploiement complet du produit. Dans l'intervalle, ils doivent assumer eux-mêmes les coûts.

Dossier patient électronique et variantes

Outre le DSQ, plusieurs projets d'informatisation des dossiers médicaux des patients sont en cours. Chacun affiche sa spécificité. En voici quelques exemples.

Le DME, dossier médical électronique, constitue le dossier médical du patient. Il est prévu qu'il soit tenu par le cabinet du médecin, le Groupe de médecine familiale (GMF), la clinique-réseau. Il remplacerait en fait le dossier patient papier et aurait la même valeur légale. Il est souhaité par la Fédération des médecins omnipraticiens du Québec (FMOQ).

Le DCI, dossier clinique informatisé, connu également sous le nom de DPE, dossier patient électronique, est tenu par l'établissement. Il remplacera également le dossier patient papier. Déjà plusieurs établissements ont commencé l'informatisation des dossiers de leurs patients. Le Vérificateur général du Québec soutient que 16% des établissements sont déjà passés au numérique, surtout en Montérégie et en Estrie. 65% des établissements investissent dans des projets locaux et planifient le déploiement. L'Agence de la santé et des services sociaux de Montréal en a fait sa priorité. Ce dossier est souhaité par la Fédération des médecins spécialistes du Québec (FMSQ).

En 2006, l'Agence de la santé et des services sociaux de Montréal a signé, conjointement avec le ministère de la Santé et des Services sociaux, le Centre hospitalier universitaire de Montréal (CHUM) et le Centre universitaire de santé McGill (CUSM), une entente faisant de l'OACIS (Open Architecture Clinical Information System), développé par TELUS Solutions en santé, son choix comme dossier clinique informatisé (DCI). Au CHUM, afin de rendre l'accès au DCI facile et rapide, les intervenants s'identifient à l'aide de la biométrie.

En avril 2009, l'Agence de Montréal annonçait qu'elle avait choisi d'étendre cette solution, incluant le module de numérisation des dossiers papier existants, à l'ensemble de la région montréalaise. Ce logiciel sera implanté non seulement dans les établissements, mais également dans les Groupes de médecine familiale (GMF), les cliniques-réseaux, les cabinets médicaux, les cliniques médicales associées (CMA) et les centres médicaux spécialisés (CMS) d'ici 2013. L'Agence parle de 511 points de service. Le contrat a une valeur approximative de 140 millions de dollars et s'étale sur une dizaine d'années. Il est assumé à même le budget de l'Agence régionale de Montréal. Il faut encore ajouter à ces sommes, les salaires versés aux 300 ETC (Équivalent temps complet) qui s'occupent de ce projet pour l'Agence de Montréal. Il n'est pas exclu non plus que cette solution soit retenue pour d'autres régions du Québec. La région de Lanaudière s'est montrée intéressée et parle d'un DCI de classe mondiale, rien de moins. Déjà cette solution serait opérationnelle en Ontario, aux États-Unis et en Australie.[7]

Afin d'éviter la multiplication des fournisseurs de DPE, le ministère de la Santé et des Services sociaux a l'intention de qualifier quelques firmes (3 à 5) qui pourraient devenir des fournisseurs de DPE pour les différentes régions du Québec.[8]

7. ASSS-Montréal, *Réunion du Comité d'allocation des ressources et de suivi des ententes de gestion*, 15 avril 2009 et *Extrait du procès-verbal de la cinquième réunion extraordinaire du conseil d'administration de l'Agence de la santé et des services sociaux de Montréal*, 18 mars 2009, [En ligne] : http://www.santemontreal.qc.ca/pdf/ca-20090428/8-OACIS.pdf (page consultée le 17 octobre 2009). Voir également ASSS-Montréal, *Le projet régional d'implantation du dossier clinique informatisé Oacis à Montréal*, par Louis Côté, directeur, Ressources humaines, information et planification, L'Agence de Montréal, 1er juin 2009, [En ligne] : http://www.e-healthconference.com/PDF/1.2.1.pdf (page consultée le 17 octobre 2009); « Emergis signe un contrat pour le déploiement de son système de dossiers de santé électroniques dans la région de Montréal», communiqué de presse, 22 décembre 2006, [En ligne] : http://biz.branchez-vous.com/communiques/detail/communiques_42118.html (page consultée le 17 octobre 2009).

8. Assemblée nationale, Commission de l'administration publique, « Audition portant sur la vigie relative au projet Dossier de santé du Québec », Journal des débats, vol. 41, no 8, 30 septembre 2009, [En ligne] : http://www.assnat.qc.ca/fra/39legislature1/commissions/cap/index.shtml (page consultée le 20 octobre 2009). La région de la Capitale-Nationale utilise Cristal-Net; celle de l'Estrie utilise Ariane.

Le DSI, dossier de santé informatisé, est plutôt un dossier régional et est associé aux Réseaux locaux de services. Ce dossier serait constitué à partir des informations détenues par les membres du réseau local qui donnent des services au patient.

La particularité de ces projets réside dans le fait qu'ils constituent tous des dossiers locaux du patient; ils contiennent l'ensemble des données cliniques locales, le diagnostic et les notes des professionnels, ce que ne contient pas le DSQ. Certaines régions du Québec ont décidé de donner la priorité à ce type de projet plutôt qu'au Dossier de santé du Québec (DSQ) au grand dam du Bureau du DSQ et d'Inforoute Santé du Canada. Qui plus est, aucune stratégie d'arrimage n'a été prévue entre le DPE et le DSQ même si l'objectif est d'intégrer les deux types de dossiers. Ces projets s'autofinancent à partir des budgets des établissements et des agences régionales, bien qu'une subvention ait été annoncée par le ministère de la Santé et des Services sociaux. Leur coût est inconnu selon le Vérificateur général du Québec. Vu la situation, Inforoute Santé du Canada est à revoir sa stratégie d'investissement et pourrait bien contribuer au financement de la mise en place des DPE dans les prochaines années.

Aucune étude sérieuse relativement à la conservation et à la confidentialité des données de santé qui circulent autant dans le secteur privé que dans le secteur public n'a été présentée. Il n'a jamais été question que le patient donne son consentement pour la conservation de l'information le concernant.

Nous ignorons également quelle loi sera applicable au DPE autant qu'au DSQ : la Loi sur la santé et les services sociaux (LSSSS), la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (Loi sur l'accès) ou la Loi sur la protection des renseignements personnels dans le secteur privé?

Qui plus est, l'entretien du DSQ autant que du DPE étant prévu en sous-traitance, les données seront-elles exportées si l'entreprise qui décroche le contrat est une entreprise étrangère?

Banques de données nominatives

La Nouvelle Gestion publique (NGP), rattachée à la remise en question de l'État-providence, prône la modernisation du management dans les administrations publiques. Elle prône l'application des méthodes de gestion du secteur privé au secteur public. L'introduction du marché ou de quasi-marchés en découle. La NGP a inspiré nombre de réformes dont notamment, la réforme de la santé en Grande-Bretagne sous Tony Blair. Elle a également inspiré la réforme de la santé entreprise sous le gouvernement Charest en 2003. Sa mise en œuvre passe par la poursuite d'objectifs de performance, déclinés en dizaines ou en centaines d'indicateurs de gestion spécifiques que les technologies de l'information rendent possible.[9]

Le ministère de la Santé et des Services sociaux dispose déjà d'une quarantaine de banques de données dont plus du tiers contiennent des données nominatives. De plus, il est à mettre en place de nouvelles banques de données nominatives sur l'utilisation des services dans les établissements publics. Le MSSS a d'ailleurs publié un règlement à cet effet[10]. En vertu de ce dernier, les établissements sont tenus de transmettre une quantité invraisemblable d'informations nominatives relatives à l'utilisation des services par les usagers-ères. Les établissements visés sont les CLSC, les CHSLD, les CH et les urgences. Cette transmission d'information est rendue possible grâce à l'implantation de systèmes d'information clientèle dans les établissements. Non seulement le consentement de l'usager n'est pas requis, mais ce dernier ne peut pas s'opposer ni se soustraire à cette transmission d'informations le concernant.

Parmi les 30 systèmes d'information clientèle en opération, figure le SIC-SRD (Système d'information clientèle pour les services de réadaptation dépendances) qui a fait l'objet d'un boycott par les professionnels-les du Centre de réadaptation Dollard-Cormier.

9. Florence Faucher-King et Patrick Galès, Tony Blair 1997-2007. Le bilan des réformes, Paris, Presses de Sciences politiques, 2007, (Coll. Nouveaux Débats), p. 75.

10. Règlement sur les renseignements devant être transmis par les établissements au ministre de la Santé et des Services sociaux, (2009) 141 G.O. II, 346, (Décret 103-2009).

En effet, les travailleurs-euses ont refusé pendant près d'un an de transmettre les données nominatives de leurs patients-es au ministère de la Santé et des Services sociaux. Sous la menace de la mise en tutelle, ils-elles se sont finalement exécutés-es.

Ces banques de données devraient servir à mesurer la performance du système de santé. Quel autre usage pourra en être fait? On appréhende déjà qu'elles puissent être utilisées à d'autres fins, comme la désassurance de services ou l'exploration de données. En Grande Bretagne, différents fichiers de données ont été utilisés pour effectuer des :

> ***« croisements systématiques de données [sont faits] par les compagnies d'assurance, les banques, la police et sans doute le National Health Service […]. L'enthousiasme du New Labour pour les nouvelles technologies a rendu accessibles de nombreuses données très privées. Dans le contexte des lois antiterroristes, tout un ensemble d'atteintes à la vie privée a été légalisée, sans qu'il soit besoin de demander d'autorisations. »*** [11]

En sera-t-il de même au Québec?

Réseau intégré de télécommunication multimédia

En 2006, le gouvernement du Québec a décidé de fusionner le Réseau de télécommunication multimédia (RETEM) (dédié aux transmissions de données et aux communications de l'administration publique) et le Réseau de télécommunication sociosanitaire (RTSS) (dédié aux transmissions de données du réseau de la santé et des services sociaux). Un contrat, d'une durée de cinq ans et d'une valeur de 900 millions de dollars, a été accordé à TELUS en février 2009 afin qu'il mette « en place un pipeline » pour la transmission d'informations. Parmi les applications, signalons le DSQ, les PACS (Picture Archiving and Communication System ou imagerie médicale) et l'OACIS. Le système desservira 350 établissements de santé et de services sociaux et 160 ministères et organismes; il comptera 3 500 points de service. L'échéancier pour la migration des systèmes est fixé au 31 décembre 2010. Les données de santé seront hébergées chez TELUS[12], alors qu'actuellement l'hébergement est fait par le RTSS. Qu'en est-il des données des autres ministères? Il est fort plausible qu'elles prennent le même chemin. On parle de rien de moins que de l'ensemble des informations que le gouvernement du Québec détient sur tous les Québécois-es!

Des questions se posent : TELUS est-elle en mesure de réaliser un tel mandat alors qu'elle n'arrive même pas à livrer les services de téléphonie filaire à la Ville de Montréal[13]? En matière de protection de la vie privée, les données de santé continueront-elles d'être soumises à la protection de la Loi sur les services de santé et les services sociaux une fois hébergées chez un fournisseur privé? Seront-elles plutôt soumises à la Loi sur l'accès ou encore relèveront-elle de la Loi sur la protection des renseignements personnels dans le secteur privé?

Partenariat nord-américain pour la sécurité et la prospérité et circulation de l'information

En 2005, les trois chefs d'État du Canada, des États-Unis et du Mexique établissaient le Partenariat nord-américain pour la sécurité et la prospérité (PSP). Afin d'assurer la prospérité des trois pays, diverses initiatives ont été entreprises, dont l'initiative sur le commerce électronique et les technologies de l'information et des communications (TIC).

Dans ce cadre, un Comité trilatéral sur la circulation transfrontalière des données a été mis sur pied afin de promouvoir les buts visés par la « Déclaration sur la libre circulation de l'information et du commerce en Amérique du Nord ». La Déclaration, signée en 2008, s'appuie elle-même sur un cadre de principes communs (adopté en 2005) parmi lesquels figure la protection de la vie privée. Or, dans ce cadre, la protection de la vie privée repose sur les principes suivants : la mise en place

11. Florence Faucher-King et Patrick Galès, op. cit., p. 167.

12. AQESSS, Le Réseau intégré de télécommunication multimédia (RITM) pour la santé, Colloque Informatique-Santé 2009, p. 31.

13. Denis Lessard, « Une panne téléphonique majeure menace la ville», Cyberpresse, 4 novembre 2009.

de mécanismes d'autoréglementation par la secteur privé ; l'encouragement du secteur privé à créer et mettre en œuvre des pratiques de protection de la vie privée ; la mise en place de mécanismes visant à assurer la protection de la vie privée en l'absence de solutions du secteur privé.

Dans un tel contexte, il apparaît donc de plus en plus évident que les données personnelles et, notamment les données de santé, constituent une ressource naturelle dans les sociétés post-industrielles. À ce chapitre, le Canada exporte des données vers les États-Unis et en perd le contrôle :

> *« L'État n'a plus de contrôle sur ces informations et doit compter sur la coopération d'un État étranger (ou de ses nationaux) afin d'y avoir accès pour être en mesure d'élaborer ses stratégies économiques et budgétaires.»*[14]

À titre comparatif, l'OCDE et la Communauté européenne ont émis des normes internationales afin de régir la circulation de données à caractère personnel. Le Conseil de l'Europe a même adopté des recommandations visant à protéger les renseignements personnels dans des domaines comme la santé[15]. De son côté, le gouvernement du Québec a plutôt opté pour l'assouplissement de ses législations. Ainsi, en 2006, il a amendé la Loi sur l'accès à l'information afin de faciliter la communication d'informations personnelles d'organismes gouvernementaux vers l'entreprise privée et vers un organisme d'un autre gouvernement et ce, sans consentement. Il a suivi la même orientation pour les informations personnelles en santé.

Le gouvernement du Québec n'a donc pas jugé bon suivre la voie tracée par l'OCDE et par la Communauté européenne en matière de protection de la vie privée de telle sorte qu'il a imprimé un recul à la protection des renseignements personnels en général et aux renseignements de santé en particulier. Il faut maintenant corriger le tir et exiger une protection adéquate des renseignements personnels dans le cadre de la libre circulation de l'information. Il revient à l'État d'assumer ce rôle; l'entreprise privée a trop bien démontré jusqu'à maintenant son incapacité à s'autoréglementer.

****

En conclusion, nous pouvons nous demander quel est l'intérêt que poursuivent nos gouvernements dans le développement de l'informatisation du réseau sociosanitaire québécois.

Comme l'a très bien exprimé un proche du ministère de la Santé et des Services sociaux récemment, l'un des objectifs consiste à créer de l'emploi dans l'industrie informatique québécoise. Il ne s'agit donc aucunement de poursuivre des objectifs cliniques, ni des objectifs d'amélioration de la qualité des soins de santé à la population.

Ensuite, il appert que l'informatisation permet d'accroître la productivité du personnel soignant. De plus, il semble que l'informatisation facilite la privatisation. En effet, comme nous l'avons vu plus haut, le projet Index patients maître et le Registre des usagers permettent la vérification en ligne de l'admissibilité aux programmes. Depuis une quinzaine d'années, les gouvernements successifs se sont efforcés de soustraire des soins et des services de la couverture d'assurance publique. Un tel instrument ne peut que soutenir les initiatives de privatisation en cours. Enfin, le développement informatique permettra d'introduire une carte d'assurance maladie qui aura la particularité d'être aussi une carte d'identité électronique

Dans ce contexte, il nous faut continuer de rechercher la meilleure protection possible des renseignements personnels et notamment des renseignements personnels de santé.

14. Karim Kenyekhlef, « Libre-échange, information, souveraineté, libéralisme et leurs incohérences », dans C. Debloc, C. Emeri, J.C. Gautron et A. Macleod (dir.), *Du libre-échange à l'union politique*, Paris, L'Harmattan, 1996, p. 423-426, [En ligne] : https://papyrus.bib.umontreal.ca/jspui/handle/1866/47 (page consultée le 15 octobre 2009).

15. Karim Benyelhlef, « Les normes internationales de protection des données personnelles et l'autoroute de l'information», dans Les Journées Maximilien-Caron, Le respect de la vie privée dans l'entreprise, Montréal, Éd. Thémis, 1996, p. 70, [En ligne] : https://papyrus.bib.umontreal.ca/jspui/handle/1866/43 (page consultée le 15 octobre 2009).

L'érosion du régime de protection des renseignements personnels au Québec

Anne Pineau, avocate
Centrale des syndicats nationaux

En 1988, dans la cause R c. Dyment, la Cour suprême du Canada décidait qu'un échantillon de sang, prélevé à des fins médicales, ne pouvait ensuite être remis à un agent de police sans mandat. La Cour reconnaissait, de ce fait, qu'un renseignement personnel obtenu à une fin particulière ne peut ensuite être utilisé à une autre fin ou être transmis à un tiers sans le consentement de l'individu concerné. Pour la Cour, une telle saisie violait tous les aspects de la vie privée – spatiaux, physiques et informationnels.

La vie privée comporte, en effet, de multiples facettes. Quoique la première image qui vienne à l'esprit a trait à l'inviolabilité du domicile, il reste que le droit à la vie privée ne concerne pas tant les lieux que la personne : ce droit suit l'individu partout où il va (aspect spatial).

Ce droit concerne aussi l'inviolabilité du corps et le « droit à une sphère irréductible d'autonomie personnelle où les individus peuvent prendre des décisions intrinsèquement privées sans intervention de l'État »[1].

Finalement, la vie privée comporte un volet informationnel qui s'intéresse, lui, au contrôle de l'individu sur les renseignements qui le concernent :

> « (…) Dans la société contemporaine tout spécialement, la conservation de renseignements à notre sujet revêt une importance accrue. Il peut arriver, pour une raison ou pour une autre, que nous voulions divulguer ces renseignements ou que nous soyons forcés de le faire, mais les cas abondent où l'on se doit de protéger les attentes raisonnables de l'individu que ces renseignements seront gardés confidentiellement par ceux à qui ils sont divulgués, et qu'ils ne seront utilisés que pour les fins pour lesquelles ils ont été divulgués. Tous les paliers de gouvernement ont, ces dernières années, reconnu cela et ont conçu des règles et des règlements en vue de restreindre l'utilisation des données qu'ils recueillent à celle pour laquelle ils le font; voir, par exemple, la *Loi sur la protection des renseignements personnels*, »[2]

C'est à cette facette du droit à la vie privée que s'attachent les lois de protection des renseignements personnels.

La loi québécoise de protection des renseignements personnels

En 1982, lorsqu'il adopte la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels dans le secteur public* (L.R.Q., c. A-2.1) (ci-après LAI), l'État québécois fait figure de pionnier.

Les principes au fondement de cette loi sont clairs : la cueillette de renseignements doit s'effectuer auprès de la personne concernée. Celle-ci doit donner un consentement éclairé à la divulgation d'information, ce qui suppose qu'elle sera informée du pourquoi de la cueillette.

L'information ne peut être utilisée à d'autres fins que celle pour laquelle elle a été recueillie : c'est le respect de la finalité, une des pierres d'assise de la Loi.

En outre, l'administration publique ne peut amasser que les renseignements « nécessaires » ; la nécessité d'une information s'évalue par rapport à la finalité :

1. Godbout c. Longueuil (Ville), [1997] 3 R.C.S. 844

2. Opus cité note 1, par. 22.

> « Il ne s'agit pas de déterminer ce qu'est la nécessité en soi, mais plutôt de chercher, dans le contexte de la protection des renseignements personnels, et pour chaque situation, ce qui est nécessaire à l'accomplissement de chaque fin particulière pour laquelle un organisme public plaide la nécessité. »[3]

Autre balise : il ne saurait y avoir transfert de l'information recueillie à un tiers sans le consentement de l'individu, à moins que la Loi ne le permette spécifiquement.

Le Rapport Paré[4], qui est à l'origine de la LAI, tablait sur une information gouvernementale en silo. Le principe d'étanchéité, au coeur de la Loi, devait assurer que chaque organisme ou ministère soit traité comme une entité distincte afin de faire échec à la libre circulation des renseignements dans l'appareil gouvernemental :

> ***« Il convient d'établir des normes sévères quant aux transferts de données personnelles entre les organismes. La principale inquiétude a trait à la possibilité de regrouper, par ces transferts, l'ensemble des données recueillies sur une personne. L'informatique permet facilement le repérage et la réunion des données. D'une façon générale, la loi devra interdire les transferts de données personnelles entre fichiers. »***[5]

Bref, il fallait éviter la création de vastes banques de données où l'administration pourrait s'abreuver sans égard à la fin pour laquelle une personne avait consenti à fournir un renseignement.

La Loi devait spécifier les transferts autorisés entre organismes et ceux-ci devaient s'effectuer dans la cadre d'ententes écrites soumises préalablement à la Commission d'accès à l'information (ci-après CAI) pour avis

3. X c. STL, 2003 CAI 667, par. 33.

4. Commission d'étude sur l'accès du citoyen à l'information gouvernementale et sur la protection des renseignements personnels, Information et liberté, Québec, 1981.

5. Id. p. 17.

Nous sommes donc passés, au fil des ans, d'un régime de cueillette et d'utilisation strictement lié à une finalité, où le consentement devait être obtenu sauf exception prévue à la loi, et où les transferts de renseignements faisaient l'objet d'un contrôle a priori de la CAI ; à un régime où l'utilisation à une fin autre est admise ; où une communication sans consentement est permise quoiqu'elle ne soit pas expressément prévue par la loi ; où une telle communication n'a pas à faire l'objet d'une entente soumise à la CAI, une simple mention à un registre suffisant (sauf pour la comparaison de fichiers).

et approbation par le gouvernement, c'est ce qu'on a appelé le contrôle « a priori ».

Sous prétexte qu'un tel système était trop lourd, on glisse en 1985 vers un système de « contrôle a posteriori » des échanges. Certains transferts seront même possibles sans entente[6] ; il suffit de les mentionner à un registre.

En 1992 et en 1997, la CAI demande le retour du contrôle « a priori ». La Commission de la culture de l'Assemblée nationale, dans son rapport sur l'exercice quinquennal de la CAI, fait sienne cette proposition en soulignant :

> « La Commission de la culture est d'accord avec les propositions formulées par la CAI à l'effet que le régime général de transferts de renseignements personnels entre organismes publics doit inclure un contrôle a priori d'opportunité confié à la CAI. Cette précaution, un peu plus lourde que la règle actuelle, est de nature à mieux sauvegarder l'équilibre entre efficacité administrative et protection de la vie privée recherché par les citoyens et leurs représentants.[7]

Malgré tout, cette recommandation restera lettre morte.

En fait, de 1990 à 2005, il n'y aura aucune modification de fond à la LAI, et ce, malgré le dépôt de trois (3) rapports quinquennaux de la CAI et la tenue de quatre (4) consultations publiques en vue d'améliorer la loi[8].

La loi 86

En 2006, le projet de loi no 86 tombe[9]. Loin de resserrer les règles de protection des renseignements personnels, la Loi 86 ouvre au contraire une brèche fondamentale; elle rompt avec le principe primordial du respect des finalités. On permet l'utilisation d'un renseignement à une fin autre que celle pour laquelle il a été requis : il suffit que la fin soit « compatible » avec la finalité initiale (article 65.1).

Pourtant la CAI, dans ses rapports de 1997 et de 2002, mettait en garde contre l'utilisation à des fins secondaires :

> « Il y a un risque sérieux d'un glissement vers une utilisation des données personnelles à une autre fin que celle pour laquelle elles ont été recueillies. Ne risquons-nous pas d'ériger un système d'utilisation de données à des fins secondaires et conserver ultimement des renseignements personnels pour une durée plus longue même si la fin principale a été accomplie. »[10]

En plus d'altérer le principe de finalité, la Loi 86 facilite la communication d'un renseignement pour l'application d'une loi. L'article 67 est modifié : pour être « nécessaire » à l'application d'une loi, une communication n'a plus à être expressément prévue par la loi :

> « Le législateur n'aura pas à autoriser toutes les communications de renseignements personnels avec des détails inhérents à cette activité qui changent ou évoluent rapidement, ce qui, autrement, aurait pu s'avérer lourd et rigide pour l'Administration. Il suffira, par exemple,

6. Notamment lorsque l'échange entre organismes est nécessaire à l'application d'une loi et n'implique pas de couplage de fichiers.

7. Assemblée nationale, Québec, Commission de la culture, Étude du rapport quinquennal de la CAI. Rapport final. Avril 1998, point 2.3.

8. Voir Me Yves D. DUSSAULT, Modifications au régime de protection des renseignements personnels. Texte présenté lors du Colloque du Barreau du Québec : Vie privée et protection des renseignements personnels, 23 novembre 2006, Québec.

9. Chapitre 22 des Lois du Québec de 2006.

10. CAI. Une réforme de l'accès à l'information : le droit de la transparence. Rapport quinquennal, Novembre 2002, p. 97.

que la loi ait prévu une collaboration ou une entente entre deux organismes concernant un programme relatif aux ressources humaines pour que l'on puisse comprendre une autorisation législative de communiquer des renseignements personnels.

La CAI avait donné, lors de l'exercice de son rôle-conseil, une interprétation très stricte de l'expression « nécessaire à l'application de la loi » présente à l'article 67 de la Loi sur l'accès. Selon la CAI, il était essentiel qu'une loi mentionne expressément qu'un organisme public doit communiquer des renseignements personnels à une personne ou à un organisme public ou privé pour que l'on puisse appliquer l'article 67. Plusieurs lois ont dû être modifiées, par le passé, afin de répondre à cette exigence. »[11]

On s'écarte donc résolument du modèle de départ préconisé dans le Rapport Paré où tout transfert sans consentement devait être prévu à la loi, de sorte à garantir la publicité et le débat démocratique :

« Toutes les exceptions devront être inscrites dans des lois, faisant ainsi l'objet d'un débat à l'Assemblée nationale. Ce débat permettra aux citoyens de connaître les pratiques actuelles en matière de transferts et aux parlementaires de juger de leur pertinence et leur nécessité. »

Nous sommes donc passés, au fil des ans, d'un régime de cueillette et d'utilisation strictement lié à une finalité, où le consentement devait être obtenu sauf exception prévue à la loi, et où les transferts de renseignements faisaient l'objet d'un contrôle a priori de la CAI ; à un régime où l'utilisation à une fin autre est admise ; où une communication sans consentement est permise quoiqu'elle ne soit pas expressément prévue par la loi ; où une telle communication n'a pas à faire l'objet d'une entente soumise à la CAI, une simple mention à un registre suffisant (sauf pour la comparaison de fichiers).

En outre, de nombreuses lois ont été amendées au fil du temps pour permettre un régime dérogatoire de transfert d'informations entre organismes malgré les dispositions de la LAI, notamment en faveur du ministère du Revenu.

Cette lente érosion des mécanismes de protection des renseignements personnels est d'autant plus inquiétante que s'y ajoutent d'autres phénomènes de contrôle, notamment l'utilisation, devenue banale, des caméras et de la filature par l'administration publique (Ville, corps policiers, CSST, etc.).

Alors que des systèmes informatiques et technologiques de plus en plus envahissants devraient justifier le renforcement du régime initial mis en place en 1982, on assiste au contraire à une dilution des protections d'origine.

Dans une société de l'information, le contrôle des individus sur les renseignements qui les concernent, voire qui les définissent, se situe au coeur du droit à la vie privée. Or, plus que jamais assiste-t-on à ce qui semble une démission autour de cette question. Comme si la vie privée était en passe de devenir un vague élément de folklore, un héritage encombrant qui entraverait les exigences « d'efficacité » de « bonne gouvernance » et de sécurité de nos sociétés modernes. Pourtant, ce fameux droit à la vie privée est indissociable d'un régime démocratique aux dires même de la Cour suprême :

« Fondée sur l'autonomie morale et physique de la personne, la notion de vie privée est essentielle à son bien-être. Ne serait-ce que pour cette raison, elle mériterait une protection constitutionnelle, mais elle revêt aussi une importance capitale sur le plan de l'ordre public. L'interdiction qui est faite au gouvernement de s'intéresser de trop près à la vie des citoyens touche à l'essence même de l'État démocratique. »[12]

Mais attendez … à moins que ce ne soit l'État démocratique lui-même qui soit en voie de folklorisation ?

Alors que des systèmes informatiques et technologiques de plus en plus envahissants devraient justifier le renforcement du régime initial mis en place en 1982, on assiste au contraire à une dilution des protections d'origine.

11. Opus cité, note 9, Colloque du Barreau, p. 16.

12. R. c. Dyment, op. cité, p. 427-428.

Quelques réflexions sur le Projet de Loi 83

Anthony Hémond, avocat
Analyste en télécommunications, radiodiffusion et vie privée

Le projet de Loi 83, intitulé « Loi modifiant la Loi sur les services de santé et les services sociaux et d'autres dispositions législatives » (dont certaines dispositions sont entrées en vigueur le 30 novembre 2005) avait notamment pour objectif d'accroître la circulation, entre certains intervenants du milieu de la santé, de l'information clinique contenue dans le dossier santé de l'usager, et ce, même sans son consentement. Certaines des modifications proposées et adoptées sont majeures et ont indubitablement des incidences sur le droit à la vie privée des personnes. Dans ce cadre, le consentement que l'usager doit donner pour la mise en place de son dossier de santé revêt une importance primordiale.

Le consentement au dossier de santé:

L'article 19 de la Loi sur les services de santé et les services sociaux (LSSS), modifié par le projet de Loi 83, précise explicitement que «le dossier (de santé) d'un usager est confidentiel et nul ne peut y avoir accès, si ce n'est avec le consentement de l'usager ou de la personne pouvant donner un consentement en son nom.» Cependant, la suite de l'article énumère nombre de situations où un renseignement contenu dans ce dossier peut être communiqué sans le consentement de l'usager.[1] À la lecture du nombre d'exceptions, il appert que la règle du consentement explicite pour la communication de renseignements contenus dans le dossier de santé de l'usager devient plutôt l'exception, et l'accès à ces renseignements, la règle générale. Cela peut être extrêmement préjudiciable pour l'usager. En effet, les renseignements personnels de santé peuvent donner de l'information sur les différentes maladies qu'il a pu contracter, sur sa santé mentale, son orientation sexuelle, etc. Cette information touche à l'intimité de la personne. Il faut donc veiller à assurer un niveau certain de confidentialité, et ce n'est certainement pas en généralisant l'accès que l'on y parviendra.

Il reste encore de nombreux articles du projet de Loi 83 qui n'ont pas été adoptés et qui méritent d'être mentionnés, dont ceux qui introduisent à la LSSS les articles 520.14, 520.9 et 520.20. Ainsi, pour consentir à l'établissement d'un dossier de santé, encore faut-il que l'usager puisse consentir de façon éclairée, c'est-à-dire en pleine connaissance de cause. L'administration est assujettie à une obligation d'information de l'usager ; ainsi les usagers, selon l'article 520.14, «doivent préalablement être informés des objectifs et des finalités poursuivis et des modalités de fonctionnement concernant l'accès, l'utilisation, la communication, la conservation et la destruction des renseignements conservés (...).». S'ensuivent alors plusieurs alinéas qui énoncent les différentes catégories d'accès possibles au dossier de santé. Cet article nous amène à nous interroger sur la façon dont les usagers vont être informés de la portée du consentement qu'ils vont accorder. La question devient alors : comment l'administration va-t-elle se conformer à cette nouvelle exigence d'information de l'usager?

1. À titre d'exemple, mentionnons l'exception qui nous renvoie à l'article 27.1.de la LSSS : « *Un établissement peut communiquer un renseignement contenu au dossier d'un usager* ***à toute personne ou organisme****, si la communication de ce renseignement est nécessaire à l'exercice d'un mandat ou à l'exécution d'un contrat de service, à durée déterminée, confié par l'établissement à cette personne ou à cet organisme, à l'exception, sous réserve de l'article 108, de tout mandat ou de tout contrat de service lié à la prestation de certains services de santé ou de services sociaux ». L'article 108 prévoit : « (…) un établissement peut communiquer un renseignement contenu au dossier d'un usager seulement si la communication de ce renseignement est nécessaire afin d'assurer, selon le cas, la dispensation, par* ***cet autre établissement, organisme ou autre personne****, de certains services de santé ou services sociaux à l'usager concerné ou la préparation centralisée de certains médicaments(…)*» C'est nous qui soulignons.

Renseignements contenus dans le Dossier de santé:

L'article 520.9 précise l'information à laquelle auront accès les établissements de santé : ce sont entre autres les données d'identification de la personne, les coordonnées des contacts professionnels, les allergies et intolérances, les résultats d'examens de laboratoire et d'imagerie médicale, les médicaments, les données immunologiques et les données d'urgence. La catégorie des données d'urgence est suffisamment étendue et imprécise pour que toutes sortes de renseignements puissent y être inscrits.

L'accès à l'information contenue dans le dossier de santé:

L'article 520.20 détaille de façon précise les personnes habilitées à avoir accès au dossier de santé ; outre les professionnels de la santé, le personnel administratif qui agit sous la direction de ces professionnels de la santé aura accès au dossier.

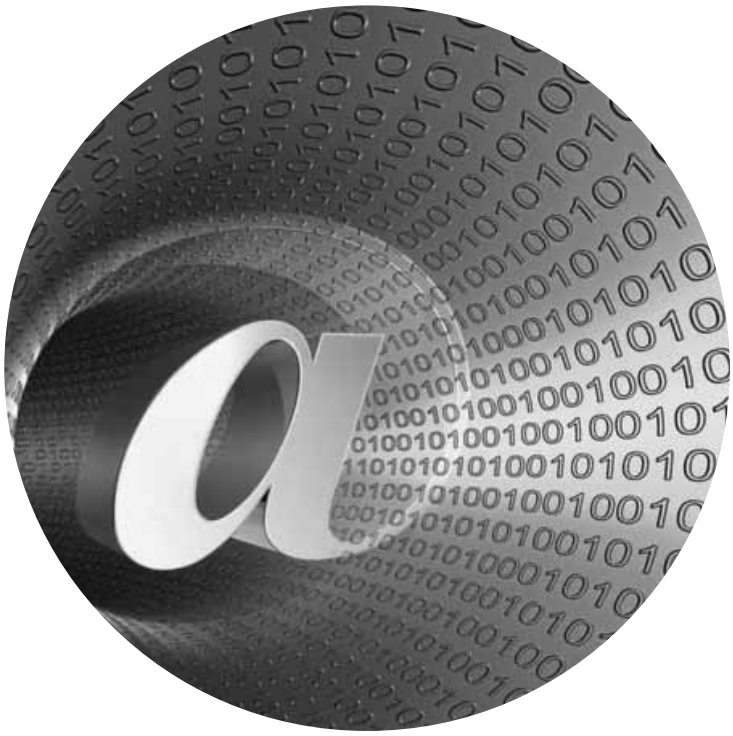
La liste de personnes pouvant avoir accès au dossier de santé est si longue qu'elle ne peut qu'inquiéter. En effet, une perte de l'information ou même des accès sans but légitime pourraient avoir lieu sans que l'usager en ait connaissance.

En vertu du projet de Loi 83, l'usager pourra surveiller a *posteriori* les renseignements collectés sur lui. Les établissements de santé auront, pour leur part, l'obligation de surveiller les accès aux renseignements des usagers afin de détecter les accès non autorisés, mais aucune obligation d'informer l'usager des accès non autorisés n'est imposée aux établissements. On ne peut que regretter cette absence.

Il demeure qu'avec le projet de Loi 83 de nombreuses zones d'ombre mériteraient d'être clarifiées pour rassurer les usagers sur ce projet ambitieux. Au contraire, ce projet tend à devenir une véritable usine à gaz[2]...

2. Comparaison faite avec une usine de fabrication du gaz, d'aspect monstrueux, compliqué et incompréhensible pour le non initié.

En effet, les renseignements personnels de santé peuvent donner de l'information sur les différentes maladies que l'usager a pu contracter, sur sa santé mentale, son orientation sexuelle, etc. Cette information touche à l'intimité de la personne. Il faut donc veiller à assurer un niveau certain de confidentialité, et ce n'est certainement pas en généralisant l'accès que l'on y parviendra.



La surveillance de nos communications n'avons-nous rien à craindre ? *

Martine Eloy, membre du conseil d'administration
Ligue des droits et libertés

Le gouvernement fédéral a présenté, en juin dernier, deux projets de loi, C-46 et C 47, qui donnent aux autorités de nouveaux pouvoirs de surveillance des communications des Canadien-nes.

La *Convention sur la cybercriminalité* est à l'origine des projets de loi C-46 et C-47. Cette Convention a été élaborée par le Conseil de l'Europe avec la participation active du Canada, des États-Unis, du Japon et de l'Afrique du Sud. Jusqu'à l'été 2001, les négociations sur la Convention semblaient vouées à l'impasse. Toutefois, les attentats du 11 septembre 2001 fournissant le prétexte pour justifier une surveillance accrue des télécommunications, le texte définitif a été adopté en novembre 2001 et signé par le Canada en août 2002. En signant la Convention, les pays s'engageaient à se doter de législations facilitant la surveillance électronique des communications.

En 2002 le gouvernement a tenu une consultation « quasi secrète » sur un projet intitulé Accès légal, par la suite renommé Accès licite. Les réponses des représentants du gouvernement aux questions que suscitait le projet étaient on ne peut plus vagues et la réaction des participants à la consultation a été plutôt négative.

Par la suite, à l'automne 2005, la ministre de la Sécurité publique, Anne McLellan, soumettait le projet de loi C-74 – *Loi sur la modernisation des techniques d'enquête*. Toutefois, le projet de loi est mort au feuilleton lors du déclenchement des élections en 2006.

Le 18 juin 2009, le gouvernement Harper est revenu à la charge avec les projets de loi C-46 – *Loi sur les pouvoirs d'enquête au 21e siècle* et C-47 – *Loi sur l'assistance au contrôle d'application des lois au 21e siècle*. Ces projets de loi viennent d'être adoptés en deuxième lecture et sont présentement à l'étude devant des comités de la Chambre.

Une intrusion sans précédent dans la vie privée

Le gouvernement présente ces projets de loi comme une adaptation nécessaire des pouvoirs d'enquête traditionnels pour l'écoute téléphonique aux nouvelles technologies des communications. Or, à une époque où les nouvelles technologies de l'information et des communications envahissent notre vie quotidienne, des pans de plus en plus importants de notre vie sont numérisés. Ainsi, il n'y a pas de commune mesure entre l'information transmise lors d'une conversation téléphonique et celle qui circule électroniquement. De plus, contrairement à la conversation téléphonique, dont les paroles s'envolent – à moins d'avoir été enregistrées --, les communications modernes laissent dans les mémoires des ordinateurs des traces qui peuvent être suivies longtemps après les faits.

Les milliers de faits et gestes qui constituent la vie de chacun pourraient devenir l'objet d'examens policiers : en premier lieu, les sites électroniques visités par chacun, le courrier électronique reçu ou envoyé, l'utilisation de la carte de crédit, les achats de toute nature (vêtements, livres, équipements divers), les sorties, les déplacements à l'étranger, mais aussi au pays (par les achats d'essence, etc.), ainsi que toutes les informations qui circulent dans un système informatique et, à ce titre, les transactions bancaires faites par Internet ou au guichet et les informations médicales. Et la liste pourrait évidemment s'allonger.

* Cet article est tiré du fascicule « La surveillance de nos communications; n'avons-nous vraiment rien à craindre? »

Il faut souligner le caractère très étendu des données soumises à ces nouveaux pouvoirs d'enquête. En effet, la définition de *données informatiques* dans les projets de loi comprend toute donnée qui est sous une *forme qui en permet le traitement par un ordinateur*, ce qui représente en fait toute donnée numérisée. Les projets de loi couvrent donc également les objets et les biens, qui transmettent des informations sous forme numérique pouvant être reliées à un individu. Dans un monde d'objets dotés de GPS et de puces d'identification par radiofréquence (RFID), les possibilités de surveillance sont quasi illimitées.

Des protections réduites ou inexistantes contre les saisies abusives

- **Sans mandat judiciaire**, les autorités pourront obtenir vos données d'abonné, alors que la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE) reconnaît que ces renseignements sont de nature privée.

- **Sans mandat judiciaire et sur la base du soupçon**, un agent pourra demander à un fournisseur de services de conserver le contenu de toutes vos communications. C'est comme si on demandait au service des postes de photocopier toutes vos lettres… au cas où!

- **Avec un mandat obtenu sur la base du simple soupçon**, un agent pourra facilement obtenir que le fournisseur de services soit tenu de remettre la liste de toutes les personnes avec qui vous avez communiqué et de tous les sites Internet que vous avez visités.

- **Avec un mandat sur la base du motif raisonnable de croire, mais moins exigeant que celui nécessaire pour l'écoute téléphonique**, le contenu de vos communications pourra être intercepté.

Vers une société de surveillance?

Les projets de loi C-46 et C-47 accordent aux autorités canadiennes des moyens et des pouvoirs sans précédent leur permettant de fouiller dans la vie intime des citoyen-nes et de les surveiller. Or, on reconnait habituellement que, dans une démocratie, la vie des individus est privée, alors que le travail du gouvernement est public. Dans une société de surveillance, c'est nos vies qui deviennent transparentes, alors que les travaux du gouvernement demeurent secrets.

Compte tenu que gouvernement n'a pas démontré que les pouvoirs d'enquête existants étaient insuffisants, la *Ligue des droits et libertés* demande le retrait des projets de loi C 46 et C 47.

Pour en savoir plus sur les nouveaux pouvoirs de surveillance introduits par ces projets de loi, nous vous invitons à lire le dernier fascicule de la Ligue intitulé, « *La surveillance de nos communications; avons-nous vraiment rien à craindre?* » Vous pouvez vous le procurer en quantité en communiquant avec les bureaux de la Ligue.

La Commission d'accès à l'information et la vidéosurveillance

Anne Pineau, avocate
Centrale des syndicats nationaux

Autrefois associée au régime carcéral, la caméra de surveillance semble en voie de devenir un élément standard du décor urbain. Encore un peu et on la prendrait presque pour une amie tant elle est censée nous protéger tous et toutes. De quoi ? De qui ? Des terroristes qui arpentent les rues, des dealers impudents, des voleurs à la petite semaine, des graffiteurs impénitents, des citoyens ordinaires ?

Dans un avis rendu en 2002 au sujet de la surveillance vidéo, l'ancien juge de la Cour suprême, Gérald Laforest notait avec pertinence :

> ***« À Kelowna et ailleurs, certains citoyens ont dit qu'ils n'ont rien à cacher et qu'ils sont rassurés à la pensée que la surveillance vidéo permettra à la police de surveiller les agissements des malfaiteurs. Mais c'est se tromper grossièrement sur la nature d'une société libre. Les violations de la liberté ne nuisent pas seulement aux criminels. À moins de justification contraignante, nous devrions tous être libres de nous déplacer sans craindre l'observation systématique des agents de l'État. » [1]***

La Commission d'accès à l'information (CAI) a mené une consultation importante sur la surveillance des lieux publics en 2003. Le bilan dressé par le commissaire Michel Laporte, dans son rapport d'avril 2004, l'amenait au constat suivant : « Je retiens que

- L'utilisation de la vidéosurveillance doit être soumise à un processus d'approbation devant être à la fois simple, souple et efficace;
- L'adoption de règles uniformes, obligatoires et contraignantes est préconisée aux fins de rendre publiques et transparentes les actions des organismes en matière de vidéosurveillance;
- La forte majorité des organismes est favorable à la mise en place d'un mécanisme d'autorisation émanant de la Commission. »[2]

Dans un communiqué du 9 juin 2004[3], la CAI demandait au gouvernement de considérer une intervention législative lui permettant d'assumer un tel rôle.

> « Par ailleurs, des intervenants lors de la consultation souhaitaient qu'un organisme indépendant, telle la CAI, ait le mandat d'évaluer au préalable la nécessité pour les organismes publics d'avoir recours à la vidéosurveillance avec enregistrement dans les lieux publics et de disposer des ressources nécessaires à cette fin. La CAI demande au gouvernement de considérer une intervention législative lui permettant d'exercer un tel rôle. »

Certains groupes réclament, en effet, depuis des années, qu'un mécanisme de pré-autorisation soit rendu obligatoire pour procéder à une surveillance vidéo.

1. Gérald LAFOREST, Avis juridique sur la surveillance vidéo adressé au commissaire à la protection de la vie privée du Canada, 5 avril 2002, disponible à www.priv.gc.ca – section communiqués.

2. CAI : Consultation publique : L'utilisation des caméras de surveillance par des organismes publics dans les lieux publics, BILAN, Avril 2004. Voir : www.cai.gouv.qc.ca – section Communiqués et discours.

3. Décision en matière de vidéosurveillance avec enregistrement dans les lieux publics. Voir www.cai.gouv.qc.ca

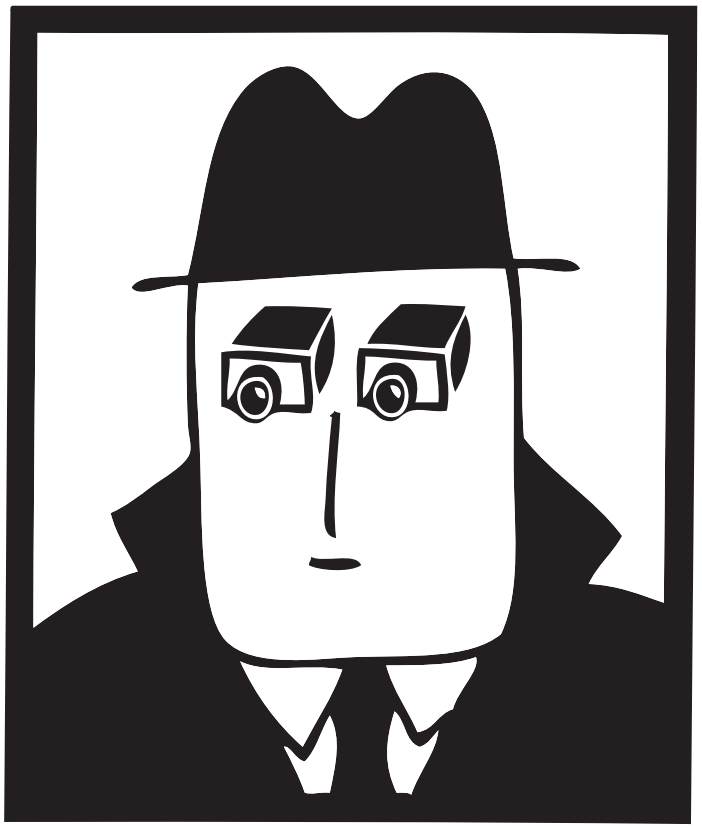
Il s'agit d'assurer que les 20 règles minimales d'utilisation des caméras établies par la CAI[4] soient respectées, et ce, avant même que n'intervienne la surveillance. Ces règles assurent que :

- La surveillance est nécessaire à une fin déterminée;
- L'objectif est sérieux et important;
- Une étude des risques et dangers réels a été faite;
- Des solutions moins préjudiciables ont été envisagées ou mises à l'essai;
- L'impact de la surveillance est mesuré;
- Il ne doit pas y avoir détournement de finalité;
- La finalité doit être explicite;
- La vidéosurveillance doit être utilisée uniquement lors d'événements critiques ou pour des périodes limitées;
- Seuls les enregistrements nécessaires doivent être effectués;
- Le public doit être informé de la surveillance;
- L'utilisation des enregistrements doit être limitée;
- Il doit y avoir réévaluation périodique de la décision de recourir à la vidéosurveillance.

Malheureusement, le gouvernement n'a pas donné suite à la demande pour un mécanisme de pré-autorisation. Or, il est illusoire de croire au respect des 20 Règles si aucun contrôle n'est mis en place pour en imposer l'application avant que ne débute la surveillance. Une vérification post-surveillance est inappropriée, car, si tant est qu'elle ait lieu, elle n'interviendra qu'après violation éventuelle du droit à la vie privée. Le cas de la rue Saint-Denis en offre un exemple éloquent.

On se souviendra qu'en avril 2004, le Service de police de Montréal (SPVM) annonçait publiquement son intention d'implanter un projet-pilote de surveillance caméra (Robotcam) sur la rue Saint-Denis pour l'été 2004 (mai à août). La CAI mènera une enquête afin de vérifier la conformité du projet avec les règles édictées.

4. CAI : Les règles d'utilisation de la vidéosurveillance avec enregistrement dans les lieux publics par les organismes publics, Juin 2004. Voir : www.cai.gouv.qc.ca



Un rapport d'enquête étoffé sera remis, en février 2005, soit quelques six mois après la fin du projet-pilote. La conclusion de l'enquêteur : les balises de la CAI n'ont pas été respectées…[5]

Si la vie privée doit être protégée, on ne peut se contenter qu'elle ne le soit qu'après coup. Une procédure de pré-autorisation existe d'ailleurs en France où l'installation de caméras dans des lieux publics nécessite une autorisation préfectorale. La Commission Nationale de l'informatique et des libertés (CNIL) – équivalent en France de la CAI québécoise – réclame d'ailleurs que ce pouvoir d'autorisation lui soit maintenant dévolu.[6]

5. Rapport final d'enquête concernant l'installation de caméras de surveillance par le Service de police de la Ville de Montréal, 23 février 2005, Laurent Bilodeau. Voir : www.cai.gouv.qc.ca

6. Commission nationale de l'informatique et des libertés. Vidéosurveillance : La CNIL demande un contrôle indépendant, 8 avril 2008. Voir : www.cnil.fr.

Documents d'identité et biométrie

Dominique Peschard
Ligue des droits et libertés

La capacité d'identifier les individus est au cœur de tout dispositif de surveillance. En effet, à quoi serviraient banques de données, surveillance des communications et listes de personnes réputées dangereuses si toutes ces informations ne pouvaient être reliées à l'individu qui traverse une frontière ou prend l'avion? La capacité d'identifier les individus, de les relier à des banques de données et de partager ces données requiert des systèmes d'identification standardisés, exploitables par des machines.

Soulignons pour commencer, que le simple fait d'être obligé de s'identifier constitue un virage majeur pour une société comme la nôtre. Dans les sociétés qui adhèrent à une tradition de liberté anglo-saxonne, comme le Canada, le citoyen n'est pas obligé de porter sur lui une pièce d'identité et il n'a pas l'obligation de décliner son identité à un agent de l'État, à moins d'être en état d'arrestation. L'idée que le citoyen doit être en mesure de s'identifier en tout temps remet en question le droit à l'anonymat qui est un des principes de notre démocratie. Effectivement, dans des États où la carte d'identité est inscrite dans les mœurs, les citoyens doivent porter leur carte et la présenter sur demande. Cela accrédite l'idée que le citoyen doit rendre des comptes à l'État dans ses activités quotidiennes. Cependant, avec les nouveaux systèmes de surveillance qui sont mis en place, l'ordre « citoyen, vos papiers! », associé aux régimes totalitaires, est appelé à disparaître. Dans un proche avenir, les personnes pourront être identifiées le plus souvent par des dispositifs automatiques et même à leur insu.

Les deux plus importantes technologies qui sont en train de révolutionner les documents d'identité et multiplier les moyens qui permettent d'identifier une personne sont les puces d'identification par radiofréquence (RFID) et la biométrie. Les RFID sont des circuits électroniques miniatures qui ont

comme caractéristique de transmettre de l'information lorsqu'ils se trouvent à proximité d'un transpondeur conçu pour les interroger.[1] Initialement, les puces RFID ont été inventées par l'industrie pour remplacer les code-barres sur les marchandises. Elles sont très bon marché et peuvent être insérées dans n'importe quel objet ou document d'identité. Certains modèles sont même conçus pour être insérés sous la peau.

La biométrie est la reconnaissance des individus à partir de leurs caractères biologiques spécifiques. Les progrès techniques permettent d'exploiter à des fins biométriques de plus en plus de caractéristiques physiologiques, biologiques et comportementales d'un individu : **physiologiques** - empreintes digitales, iris, rétine, faciès, forme de la main; **biologiques** – ADN, odeur, salive, urine; **comportementales** - écriture, démarche. Certaines de ces techniques, comme la reconnaissance du visage ou de la démarche, peuvent être utilisées à distance et donc à l'insu de la personne. Plusieurs, comme la reconnaissance des empreintes digitales, de la forme de la main, de l'iris et du visage, sont déjà opérationnelles et utilisées.

De plus, l'incorporation d'un microprocesseur dans un document d'identité offre la possibilité d'incorporer une quantité phénoménale d'information concernant le porteur tels que le dossier criminel, le dossier de conduite automobile, un dossier médical, etc. Les limites dans ce domaine sont bien plus politiques que techniques. Elles sont fixées par ce que les gouvernements sont prêts à faire et par ce que les populations sont prêtes à accepter.

Les nouveaux documents d'identité

En mars 1997, le Secrétariat de l'autoroute de l'information (SAI) du gouvernement du Québec publiait un document de référence, *L'identification des citoyens et l'inforoute*, dans lequel il proposait la carte à microprocesseur comme moyen d'identification des citoyens. Le SAI préconisait une carte ayant une architecture permettant une évolution ultérieure, par exemple l'ajout de nouvelles fonctions et informations.[2] Le SAI évaluait que la RAMQ et le MSSS seraient probablement les premiers organismes gouvernementaux à émettre des cartes à microprocesseur pour les professionnels et les bénéficiaires du régime d'assurance maladie et qu'il serait envisageable de vendre de l'espace mémoire dans la carte à des organisations ayant de larges clientèles, y compris à l'entreprise privée.[3] Le 19 décembre 2001, le gouvernement du Québec présentait un avant-projet de loi intitulé *Loi sur la carte santé du Québec*. Ce projet de loi a suscité beaucoup d'opposition et est mort au feuilleton.[4] La nouvelle carte qui sera introduite avec le Dossier de santé du Québec (DSQ) contiendra un numéro d'identification

Dans les sociétés qui adhèrent à une tradition de liberté anglo-saxonne, comme le Canada, le citoyen n'est pas obligé de porter sur lui une pièce d'identité et il n'a pas l'obligation de décliner son identité à un agent de l'État, à moins d'être en état d'arrestation. L'idée que le citoyen doit être en mesure de s'identifier en tout temps remet en question le droit à l'anonymat qui est un des principes de notre démocratie. Effectivement, dans des États où la carte d'identité est inscrite dans les mœurs, les citoyens doivent porter leur carte et la présenter sur demande. Cela accrédite l'idée que le citoyen doit rendre des comptes à l'État dans ses activités quotidiennes.

1. La distance peut varier de quelques cm à une dizaine de mètres pour les RFID les plus courants, dits passifs, c'est à dire ne possédant pas de pile électrique. Les RFID actifs possèdent une source d'énergie leur permettant de communiquer à de plus grandes distances.

2. Secrétariat de l'autoroute de l'information, L'identification des citoyens et l'inforoute – ISBN 2-550-31399-2, page 38.

3. Idem, pages 36 et 37.

4. Le projet du DSQ suppose que la carte d'assurance maladie sera remplacée par une carte électronique qui pourrait servir, de facto, de carte d'identité québécoise. Voir article : L'informatisation dans le réseau de la santé et des services sociaux, page 28.

correspondant à une norme internationale et deviendra, de facto, la nouvelle carte d'identité électronique des Québécois-es.[5]

Depuis le 11 septembre 2001, les tentatives d'imposer des documents d'identité à des fins de « sécurité » se sont multipliées aux niveaux national, régional et mondial. Le 12 décembre 2001, le Canada et les États Unis signaient l'*Accord sur la frontière intelligente*. Le 9 septembre 2002, dans le cadre de cette entente[6], Jean Chrétien et George Bush se sont entendus sur l'identification biométrique : « *Le Canada et les États-Unis se sont entendus pour fixer des normes communes et pour adopter une technologie compatible et interopérable afin de lire ces données. En ce qui a trait à l'intérêt d'avoir des cartes pouvant être utilisées pour divers modes de voyage, nous nous sommes mis d'accord sur des cartes qui peuvent emmagasiner des données biométriques multiples.* »[7]

Pour donner suite à cette entente, le ministre de l'Immigration et de la citoyenneté, Denis Coderre, lançait à l'automne de la même année l'idée d'une carte d'identité, également appelée carte de citoyenneté, qui faciliterait le passage des Canadiens à la frontière américaine. Le projet rencontra une forte opposition et fut mis sur la glace.

Les nouveaux permis de conduire « plus », introduits au Canada cette année, sont une manière détournée d'introduire la carte d'identité nationale rejetée par la population en 2003. Les nouveaux permis de conduire ont été élaborés par les provinces en collaboration avec le Ministère de la sécurité publique du gouvernement fédéral et les autorités des États-Unis. Les puces d'identification à radiofréquence qui sont incorporées dans le permis et qui transmettront votre numéro d'identification personnel aux agents frontaliers ne contiennent aucune mesure de protection, ne peuvent être éteintes et peuvent être lues à une distance de dix mètres avec un lecteur commercial peu dispendieux.[8]

Les systèmes biométriques à plus grande échelle sont ceux déployés au niveau international sur la base de décisions prises par des instances sur lesquelles les citoyens n'ont aucune prise. Ainsi, l'Organisation de l'aviation civile internationale (OACI) a décidé au printemps 2004 d'adopter le passeport biométrique avec puce d'identification radio-fréquence comme nouvelle norme de passeport. La nouvelle génération de passeports canadiens se conformera à cette norme.

5. Idem.

6. Ministère des affaires étrangères et du Commerce International, Plan d'action pour une frontière intelligente, Rapport d'étape, le 6 décembre 2002, http://www.dfait-maeci.gc.ca .

7. Ministère des Affaires étrangères et du Commerce International, Rapport d'étape Chrétien-Bush concernant le plan d'action sur la frontière intelligente, 9 septembre 2002, http://www.dfait-maeci.gc.ca/can-am/main/border/chr%C3%A9tien_bush_status-fr.asp

8. Voir Un monde sous surveillance, Bulletin de la Ligue des droits et libertés, printemps 2009

La Ligue publie une série de fascicules dans le but de porter à l'attention de la population différentes mesures qui portent atteinte aux droits et libertés.

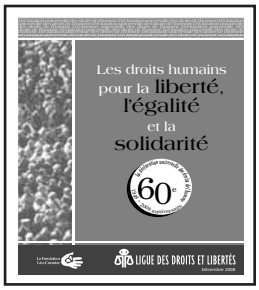
La liste noire de passagers aériens

La Loi antiterroriste

Les certificats de sécurité

Les poursuites-bâillons

Le *« Taser »*



Le 60e de la Déclaration universelle des droits de l'homme

La surveillance de nos communications

La Ligue des droits et libertés:

Présidence :
Dominique Peschard

LIGUE DES DROITS ET LIBERTÉS

Permanence :
Nicole Filion
Coordonnatrice

Marie-Josée Béliveau
Chargée des communications

Afifa Maaninou
Adjointe à la direction

Bannière gracieuseté de Christian Bourget.

Faire un don en ligne, c'est si facile!
Il suffit de taper www.liguedesdroits.ca

OUI! J'APPUIE LA LIGUE DES DROITS ET LIBERTÉS!

Nom : Prénom :

Adresse : Ville : Prov. : Code postal :

Courriel : Tél. maison : Tél. travail :

COTISATION

- ☐ Membre * 30$
- ☐ Étudiant ou personne à faible revenu 10$
- ☐ Organisme communautaire 65$
- ☐ Syndicat et institution 200$

DONS

J'aimerais faire un don

- ☐ 50 $
- ☐ 100 $
- ☐ 200 $
- ☐ 500 $
- ☐ Autre : _____

☐ Je désire recevoir les publications de la Ligue par courriel plutôt que par la poste.

*** La Ligue accepte les adhésions individuelles, quelle que soit la somme versée.**

En devenant membre de la Ligue, vous recevrez ses publications ainsi que l'envoi hebdomadaire (courriel). Faites parvenir votre coupon dûment rempli à LDL, 65 ouest rue De Castelnau, Bureau 301, Montréal, Qc H2R 2W3 ou au bureau de votre section régionale. Les renseignements nominatifs que vous fournissez demeurent confidentiels.

Colloque

sur la protection des renseignements personnels à l'ère des technologies de l'information et des communications

les 29 et 30 janvier 2010

On nous fiche, ne nous en fichons pas!

Le Dossier santé Québec, la liste noire des passagers aériens, le Permis de conduire Plus, ainsi que les projets d'imagerie visuelle du corps complet dans les aéroports canadiens, de Système national intégré d'information interorganismes… tous, parmi tant d'autres, sont des menaces à notre vie privée ainsi qu'à nos droits et libertés.
De plus en plus, nous sommes fichés.

Programme préliminaire

Vendredi soir le 29 janvier 2010 à 19h00

Jennifer Stoddart,
Commissaire à la protection de la vie privée du Canada.
Salle Marie-Gérin-Lajoie, UQÀM
(Pavillon Judith-Jasmin, 405, rue Ste-Catherine E.)

Samedi 30 janvier 2010 à l'UQAM

David Lyons,
professeur à Queen's University et directeur du Surveillance Project

Paul-André Comeau,
ex-président de la Commission d'accès à l'information du Québec et professeur invité à l'ÉNAP (École nationale d'administration publique)

Pour inscription et information :

Ligue des droits et libertés 514-849-7717 poste : 421
info@liguedesdroits.ca

LDL – SIÈGE SOCIAL
65, rue de Castelnau ouest, bureau 301
Montréal, Québec, H2R 2W3
Téléphone : 514-849-7717
Télécopieur : 514-849-6717
Courriel : info@liguedesdroits.ca
Site internet : www.liguedesdroits.ca

SECTIONS RÉGIONALES
LDL – Section Estrie
187, rue Laurier, bureau 313
Sherbrooke, Québec, J1H 4Z4
Téléphone : 819-346-7373
Télécopieur : 819-566-2664
Courriel : liguedesdroitsetlibertes@hotmail.com

LDL – Section Saguenay-Lac-St-Jean
3791, rue de la Fabrique, bureau 707.10
C.P. 2291, Succursale Kénogami
Jonquière, Québec, G7X 7X8
Téléphone : 418-542-2777
Télécopieur : 418-542-8187
Courriel : ldl-saglac@bellnet.ca
Site internet : www.ldl-saglac.com

LDL – Section Québec
405, 3e avenue, Bureau 202
Québec (QC) G1L 2W2
Téléphone : 418-522-4506
Télécopieur : 418-522-4413
Courriel : info@liguedesdroitsqc.org
Site internet : www.liguedesdroitsqc.org

LIGUE DES DROITS ET LIBERTÉS

La Fondation Léo-Cormier