Volume 33, numéro 1, printemps 2014

Ligue des droits et libertés

Droits et libertés

Steve Berthiaume

La surveillance des populations

Révélations Snowden, NSA, CSTC, Google, Facebook… informatique corporelle, informatique et démocratie, profilage, résistances…

La LDL est un organisme à but non lucratif, indépendant et non partisan, issu de la société civile québécoise et affilié à la Fédération internationale des ligues des droits de l'homme (FIDH). Elle milite en faveur de la défense et de la promotion de tous les droits humains reconnus par la Charte internationale des droits de l'homme.

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

Revue de la Ligue des droits et libertés
Volume 33, numéro 1, printemps 2014

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

Ligue des droits et libertés

FONDATION LÉO-CORMIER
pour l'éducation aux droits et libertés

Dans ce numéro

Éditorial:

50 ans de luttes à poursuivre pour les droits humains 3
Nicole Filion et Dominique Peschard

Dossier : Surveillance des populations

Présentation 5
Lysiane Roch

Sécurité ou liberté - un faux dilemme 6
Christian Nadeau

Droit à la vie privée : jurisprudence de la Cour suprême 8
Anne Pineau

Rien à cacher, rien à craindre? 11
David Lyon

Surveillance industrielle 16
Stéphane Leman-Langlois

Informatique corporelle et surveillance 20
Louis Melançon et Jonathan Roberge

Révélations Snowden sur la NSA 23
Roch Tassé

Que savons-nous des activités du CSTC? 27
Anne Dagenais Guertin

Riposte juridique de BCCLA, FIDH et ACLU 29
Dominique Peschard

Surveiller la dissidence: le modèle de Miami au G20 de Toronto 30
Kate Milberry et Andrew Clement

Résistance à la surveillance: le cas de l'UQAM 37
Samuel Ragot et René Delvaux

Dérives sécuritaires et profilages des populations marginalisées 39
Céline Bellot et Marie-Ève Sylvestre

Asujettir l'informatique à la démocratie 41
Pierrot Péladeau

500 écrivain-e-s dénoncent la surveillance numérique 45
Lettre ouverte

La résistance citoyenne s'organise 46
Martine Eloy

Les recommandations de la Commission O'Connor :
Plus pertinentes que jamais 49
Dominique Peschard

Hors Dossier : Le Plan Nord Plus

Rompre avec l'idéologie du « tout à la croissance » 51
Vincent Greason

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

50 ans de luttes à poursuivre pour les droits humains

Nicole Filion, coordonnatrice
Dominique Peschard, président
Ligue des droits et libertés

Le 50e anniversaire de la Ligue des droits et libertés (LDL) aura été l'occasion de rappeler l'importance des luttes qui ont été menées durant les 50 dernières années, en faveur des droits humains, pour une société juste et solidaire, de rappeler également combien l'action de la LDL et les luttes qu'elle a menée s tout au long de son histoire sont intimement liées à la vie sociale et politique du Québec, passée et actuelle. Cet anniversaire aura aussi permis de souligner son rôle de précurseur, son engagement à intervenir inlassablement et ce, même à contre-courant, son rôle de chien de garde pour défendre et préserver les acquis ainsi que son leadership rassembleur autour des questions de droits humains.

Dans le contexte de ce 50e anniversaire, la LDL a également réalisé une série d'activités marquantes qui ont proposé aux organisations de la société civile québécoise une plus grande concertation autour d'un projet de société fondé sur la réalisation de tous les droits humains. Ces activités ont également ouvert la voie vers de nouvelles perspectives de lutte mais aussi mis en lumière les défis auxquels les militant-e-s et les organisations sont confrontés.

C'est ainsi que la LDL a publié la revue sur les *50 ans d'action de la LDL*, mené à terme la réalisation du *Rapport sur l'état des droits humains au Québec et au Canada* (RDH), suivie de la publication de la Revue et la tenue du forum sur les *Perspectives pour les droits humains.*

Lorsque la LDL lance en 2010 le projet de réalisation du RDH, elle propose aux organisations communautaires et syndicales d'y participer collectivement. Tou-te-s prennent alors acte de l'ampleur des reculs subis au cours des dernières années en ce qui concerne l'ensemble des droits humains. Puis, considérant que les droits humains sont interdépendants, on convient collectivement de lier les différentes problématiques auxquelles sont confrontées les organisations afin d'identifier les principaux obstacles à la réalisation de l'ensemble de ces droits. La démarche proposée par la LDL devient en soi un outil de concertation et de mobilisation collective.

L'étape de la cueillette d'information réalisée par chacune des organisations participantes, leur a par la suite offert une réelle possibilité d'ouvrir à l'interne un débat collectif, de faire un bilan des avancées, des reculs sur le terrain des droits humains ainsi qu'un bilan quant aux stratégies de mobilisation auxquelles elles avaient habituellement recours. Chaque organisation l'a fait à sa manière et la richesse des informations recueillies témoigne certainement du sérieux des démarches ainsi réalisées.

Devant l'ensemble des enjeux environnementaux, sociaux et économiques de taille soulevés par les organisations participantes et les obstacles auxquels celles-ci sont confrontées dans leurs luttes, notamment sur le plan de la démocratie et des droits civils et politiques, la LDL conclut à la nécessité d'opérer un changement de fond dans le mode actuel d'organisation économique, social et politique. Plus de 45 organisations de la société civile québécoise adhèrent à cette conclusion qui invite à rompre avec le projet de société qu'on nous impose.

Rencontre à Gatineau sur le Rapport sur l'état des droits humains en 2014.

Les rencontres de formation de formatrices et de formateurs, puis les rencontres régionales qui ont suivi la publication du RDH, auront permis, sur une base intersectorielle, aux organisations en région de partager leur compréhension des conclusions du rapport et d'envisager certaines stratégies de lutte.

Le RDH n'avait pas pour propos d'offrir des perspectives d'intervention ni d'alternative au mode actuel d'organisation sociale, politique et économique. Certes il réfère à certaines perspectives de rupture mais sans plus. Et, bien évidemment, la LDL n'allait pas en rester là. Elle a donc réalisé la revue *Perspectives pour les droits humains*[1] qui propose différentes pistes visant à remettre les droits humains au cœur des décisions politiques, juridiques et économiques à prendre au niveau global tout autant que local.

Le Forum sur les *Perspectives pour les droits humains* qui a eu lieu le 25 avril 2014 a quant à lui convié les organisations et militant-e-s à un moment de réflexion et d'analyse portant sur des pratiques et des luttes qui proposent une rupture avec l'une ou l'autre des trois tendances identifiées dans le rapport sur les droits humains, c'est-à-dire : le tout à la croissance économique, l'extension de la logique de marché à l'ensemble des activités de la société ainsi que les attaques aux droits indispensables à la démocratie. Le forum a permis à la fois de mesurer les défis auxquels nous faisons face et de dégager certaines conclusions quant à des pistes d'action.

Le premier grand défi est que le constat du RDH est encore loin d'être partagé par l'ensemble de la population et que beaucoup de travail reste à faire pour contrer le discours dominant dénoncé dans le rapport. Les trois principaux partis aux dernières élections provinciales, qui défendent tous le modèle de développement que nous contestons, ont recueilli plus de 90% des suffrages votant-e-s. Malgré que le dernier rapport du GIEC ait démontré avec encore plus de force les conséquences catastrophiques de notre mode de développement, environ les deux tiers de la population du Québec demeure favorable à l'exploration et l'exploitation du pétrole au Québec parce que cela serait bon pour l'économie, l'emploi et les finances publiques.

La difficulté à faire émerger une autre vision de l'ordre social et économique est certainement liée au monopole du discours dominant dans l'espace médiatique, comme en témoigne l'omniprésence du débat sur les finances publiques après l'élection du gouvernement libéral. Il y a par ailleurs peu de couverture des luttes populaires et de place dans le débat public pour les visions alternatives.

Dans ce contexte, une responsabilité particulière incombe aux organisations communautaires et syndicales de faire de l'éducation et de la conscientisation une priorité, de refuser l'instrumentalisation des groupes communautaires et de se solidariser avec des mouvements de résistance citoyenne comme celui contre les gaz de schiste. Une lutte qui se présente au départ comme étant un enjeu local, comme celle sur les gaz de schiste, devient l'occasion d'une réflexion, d'une remise en question du mode de développement et une expérience d'organisation et de démocratie citoyenne en dehors des cadres établis.

Il faut sortir du mode défensif qui est démobilisant et se mobiliser sur des alternatives. Face à un ordre mondial qui impose sa domination et aux institutions financières qui dictent leurs politiques aux États sous peine de sanction, nous devons réaffirmer le droit des peuples à l'autodétermination et nos droits de citoyen-ne-s de dire la société que l'on veut. Nous devons développer la solidarité sociale dans un contexte d'insécurité économique pour les populations qui est un terrain fertile pour le repli identitaire et la montée de la xénophobie et des courants de droite. Dans le contexte canadien et québécois, développer la solidarité entre les peuples signifie tout particulièrement réparer l'injustice historique envers les nations autochtones.

Face au caractère supranational de l'adversaire, à des entreprises qui peuvent simplement déménager si les travailleuses et travailleurs font trop de gains dans un pays, ou faire appel à des travailleuses et travailleurs temporaires, la solidarité internationale revêt toute son importance et les luttes se mènent sur plusieurs fronts. Que ce soit dans le cas de l'industrie du textile ou des industries extractives, nous devons tenir responsables les compagnies, notre gouvernement et les instances internationales concernées.

En cette fin d'année de son 50e anniversaire, la Ligue des droits et liberté réaffirme son engagement en tant que composante du mouvement social pour un monde juste et solidaire fondé sur les droits humains.

1. http://liguedesdroits.ca/?p=1825

Dossier
La surveillance des populations

Lysiane Roch, responsable des communications
Ligue des droits et libertés

Dans un contexte où les révélations d'Edward Snowden ont suscité un débat public salutaire sur la mise en place d'un système de surveillance des populations dénoncée depuis plus d'une décennie par des organisations comme la Ligue des droits et libertés, le dossier proposé dans ce numéro de la revue *Droits et libertés* vise à apporter un éclairage supplémentaire sur l'évolution des enjeux de surveillance et de protection de la vie privée et des renseignements personnels, leurs implications en matière de démocratie et de droits humains ainsi que les perspectives en termes de résistance et alternatives.

Alors que la surveillance des populations s'appuie souvent sur l'argument de la sécurité, de façon plus accrue encore depuis 2001, l'article de Christian Nadeau met en évidence la fausse dichotomie entre liberté et sécurité qui permet d'assurer leur hiérarchisation. Comme il le démontre dans son analyse, « vivre libre implique la sécurité et vice versa ». Le dossier se poursuit avec un bref survol de la jurisprudence récente de la Cour suprême sur le droit à la vie privée. Dans son article, Anne Pineau met notamment en évidence la reconnaissance par la Cour du rôle de la protection des renseignements personnels dans l'autonomie des individus et la vie démocratique.

La surveillance des populations a pris des proportions inégalées depuis quelques décennies. L'article de David Lyon analyse le caractère inédit et inquiétant des sociétés de surveillance d'aujourd'hui, notamment en mettant en lumière le développement d'une « culture de la surveillance ». Stéphane Leman-Langlois se penche plus spécifiquement sur le développement de la surveillance industrielle et la marchandisation de l'information personnelle, tandis que Louis Melançon et Jonathan Roberge analysent de leur côté l'évolution récente de l'informatique corporelle et les conséquences des nouvelles pratiques de surveillance qu'elle permet. La surveillance par les États prend elle aussi une ampleur inégalée. Dans son article, Roch Tassé présente un retour historique sur la *National Security Agency* (NSA) et résume les principales informations mises en lumière par les récentes révélations d'Edward Snowden. Le Canada mène lui aussi des activités de surveillance de la population, comme le démontre l'article d'Anne Dagenais Guertin sur les révélations du *Centre de la sécurité des télécommunications Canada* (CSTC).

La surveillance des populations peut être utilisée pour réprimer la contestation sociale. Kate Milberry, dans une analyse de la surveillance survenue lors du G20 à Toronto, démontre les conséquences que ces pratiques peuvent avoir sur l'expression de la dissidence et, plus largement, sur la démocratie. Les pratiques de surveillance et de contrôle s'appuient aussi de plus en plus sur la notion de « risque éventuel », comme l'illustrent Céline Bellot et Marie-Ève Sylvestre. Il en résulte un mécanisme qui favorise le profilage des populations marginalisées, leur judiciarisation et la privation de leurs droits.

L'ampleur et la généralisation des pratiques de surveillance, tout comme leur banalisation, contribuent au développement d'un sentiment d'impuissance. Pourtant, de nombreuses luttes sont menées ici comme ailleurs pour résister à ces pratiques, mais aussi pour se réapproprier des enjeux et les soumettre au débat public. Dominique Peschard présente trois recours menés présentement par des organisations de défense de droits d'Amérique du nord et d'Europe. À l'international, 500 écrivain-e-s ont aussi publié une lettre ouverte et lancé un appel pour dénoncer la surveillance numérique. Plus près d'ici, Samuel Ragot et René Delvaux se penchent sur le mouvement de résistance face à la vidéosurveillance à l'UQAM.

La surveillance des populations n'est pas une fatalité associée au développement des technologies. Pierrot Péladeau, dans son article, démontre que la repolitisation et la démocratisation du développement de l'informatique sont possibles et il suggère plusieurs moyens concrets d'avancer dans cette voie. Martine Eloy, pour sa part, résume les démarches qui ont amené à l'élaboration des « Principes internationaux pour l'application des droits humains à la surveillance des communications » et présente un résumé de ces 13 principes. Enfin, Dominique Peschard rappelle les recommandations importantes que le juge O'Connor avait formulées en 2006 pour la protection des droits et libertés, et qui demeurent plus pertinentes que jamais.

Sécurité ou liberté - un faux dilemme

Christian Nadeau, professeur
Département de philosophie, Université de Montréal

Le rapport conflictuel entre sécurité et liberté exprime un conflit de valeurs typique de notre société contemporaine. Au sein de pays qui se prétendent démocratiques, le principe du droit que nous avons sur nous-mêmes, sur notre personne et sur les éléments de notre vie privée est au fondement des sociétés démocratiques et libérales. En contrepartie, ce respect pour notre personne suppose que celle-ci, tout comme celle d'autrui, soit protégée contre toute forme d'atteinte à son intégrité physique. La question devient alors de savoir si la défense d'une femme ou d'un homme implique d'abord celle de sa personne morale, ou si elle ne correspond pas plutôt à celle de son existence au sens le plus fondamental, c'est-à-dire la protection de son corps et de ses biens. Dans un cas, nous parlons de liberté; dans le second, de sécurité. Le danger consiste à hiérarchiser l'intégrité physique au détriment de toute autre considération. Or, s'il existe encore de nombreux garde-fous pour protéger les libertés individuelles, l'argument le plus courant entendu en faveur d'une primauté de la sécurité est celui qui consiste en gros à nous dire que nous ne pouvons pas vivre libres si nous sommes morts. Une fois cela admis, l'étau se resserre et ce qui nous apparaissait au départ une banale lapalissade s'avère un contrat social liberticide.

D'une fausse dichotomie à un faux dilemme

Personne ne remet en cause l'importance de la sécurité. Le vrai problème est d'évaluer de manière correcte son coût réel. La majorité des gens seront d'accord pour accepter, du moins en principe, des balises pour la conduite automobile. Nous estimerions normal qu'une personne harcelée psychologiquement fasse appel à la police parce qu'elle reçoit chaque jour des appels haineux. Nous avons notre sécurité à cœur et le contraire serait étonnant. Il n'a jamais été question de choisir entre la liberté et la sécurité pour autant. Nous pouvons accepter un certain nombre de contraintes lors de nos déplacements ou dans notre vie sociale, sans pour autant évaluer l'ensemble de nos activités à l'aune d'un principe de sécurité.

De manière ponctuelle, nos dirigeants ou des lobbys puissants tentent de nous faire admettre la nécessité d'accorder une priorité à l'une au détriment de l'autre. Il existe une fausse dichotomie entre la sécurité et la liberté et cette dernière nous a conduits à admettre comme vrai un dilemme sans fondement : en séparant sécurité et liberté et en faisant de cette dernière un luxe par rapport à la première, nous oublions que nous ne voulons pas seulement vivre, nous voulons vivre libres.

La sécurité comme justification de l'autoritarisme

Si ce type de dichotomie existe depuis toujours et fonde la propagande des gouvernements autocratiques, nous avons connu depuis les attentats du 11 septembre 2001 des sommets de la panique sécuritaire, laquelle chaque jour gagne insidieusement du terrain sur nos vies privées.

Bien entendu, il existe encore à l'heure actuelle des balises juridiques propres à notre État de droit. Un tel État implique le respect des normes constitutionnelles par le pouvoir exécutif. Mais est-ce bien le cas? Nous savons avec l'affaire Omar Khadr à quel point la sécurité permet des entorses graves aux droits fondamentaux des individus, même dans notre société, qui n'est pas réputée pour son autoritarisme. La Cour suprême, celle des États-Unis comme la nôtre, n'est pas insensible au chant des sirènes sécuritaires. On fera valoir des arguments typiques du réalisme paternaliste : on ne peut pas être contre la vertu si la vertu est contre elle-même, ce qui est exactement le cas lorsque la défense pour la liberté devient un obstacle à la sécurité en temps de crise. Pour le propre bien des individus, il est de la responsabilité des États de les mettre à l'abri de toute menace, si incertaine soit-elle. À une période exceptionnelle correspondent des mesures exceptionnelles, dont celles qui dépossèderaient temporairement des personnes de leurs libertés fondamentales, à commencer par le droit au respect de leur vie privée. Il apparaitrait dès lors légitime de placer des gens sur une liste d'écoute, d'intercepter leurs courriels, de

2004 - Campagne de la LDL contre les mesures liberticides et l'érosion des libertés civiles.

surveiller leurs déplacements, bref, d'épier les moindre faits et gestes d'une population, toujours soi-disant pour son bien.

Cette défense du réalisme soulève deux questions. D'une part, que voulons-nous défendre au juste lorsque nous jugeons légitime de faire prévaloir la sécurité sur toute autre considération? D'autre part, qu'est-ce qu'une situation de crise? Existe-il quelque chose comme une situation normale, où il ne serait pas possible d'évoquer l'argumentaire de la crise ou de l'urgence et des exceptions qu'elle implique?

L'un des plus importants livres de philosophie politique, le *Léviathan* de Thomas Hobbes (1651) soutient la thèse selon laquelle, sans institutions, nous serions dans un état de guerre de tous contre tous. L'homme est un loup pour l'homme, dit Hobbes, d'où la nécessité pour chaque personne de transférer à une instance tierce son droit de se défendre. L'État existe dès lors d'abord et avant toute chose pour nous protéger les uns des autres. Il est alors normal, dirait Hobbes aujourd'hui, que chaque citoyen et chaque citoyenne d'un État donné acceptent une perte importante de leurs libertés si cela est nécessaire pour assurer la pérennité de l'État, lui-même garant de la paix civile et de la sécurité de toutes et tous. Hobbes adopte une logique assez proche de celle à laquelle nous nous sommes peu à peu habitués depuis 2001. Pour revenir aux deux questions posées plus haut, Hobbes interpréterait la sécurité d'abord et avant tout comme la protection de notre intégrité physique. En outre, nous serions, selon Hobbes toujours, dans une situation exceptionnelle, puisque l'imminence du danger compte somme toute assez peu. La menace la plus grave contre nous, dit-il, est celle contre le droit absolu de l'État. Aucune contrainte, ni constitutionnelle ni de la part de la société civile, ne devrait empêcher l'État de faire ce pour quoi il existe : assurer la protection des individus qu'il gouverne. Sans le pouvoir souverain et donc absolu de l'État, ou d'une institution jouant un rôle analogue, nous ne pourrions espérer jouir de notre vie, ni non plus de nos biens ou de nos libertés.

Ce que valent nos libertés

Nous avons fini par internaliser la nécessité de certains ajustements à nos droits et libertés, sans savoir ni comprendre ce que nous perdons en échange de notre abnégation. Certes, en surface du moins, le paysage politique n'a, à l'heure actuelle, rien de comparable à celui du début des années 2000. Il suffirait toutefois d'une nouvelle attaque d'envergure pour redonner aux pouvoirs coercitifs de l'État ou de compagnies privées spécialisées en sécurité une marge de manœuvre sans limites. Le discours de la peur est le discours terroriste par excellence, précisément parce qu'il terrorise et soumet par la peur des individus qui pourraient s'avérer autrement récalcitrants. En outre, non seulement la peur incite-t-elle à l'obéissance, elle favorise la déférence à l'égard des élites.

La fausse dichotomie entre liberté et sécurité permet d'assurer leur hiérarchisation. Cela suppose un appauvrissement considérable de ces deux valeurs ou de ces deux concepts. La liberté devient secondaire et ne possède plus aucune valeur pour elle-même. Elle ne représente plus un objectif, elle se comprend comme un moyen en vue d'une fin supérieure. Or, cette finalité, celle de la sécurité, ne se trouve guère mieux servie par la dichotomie. Si elle occupe le haut du pavé, elle ne veut plus dire grand-chose. Elle signifie tout au plus la préservation de l'autorité de l'État. Même l'intégrité physique des personnes, comme le pensait Hobbes, n'appartient plus au registre de la sécurité, comme l'ont bien montré les révélations sur la torture, les déportations de prisonniers ou l'assassinat ciblé d'Anouar Al-Aulaki.

Défendre nos droits et libertés ne contredit en rien la sécurité, si nous acceptons de redonner une pleine signification à ces valeurs. Vivre libre implique la sécurité et vice versa. Il n'y a pas d'échanges, pas de négociation possible entre les deux, sans perte majeure pour chacune d'elles. Si nous voulons garantir notre sécurité, nous devons nous assurer de protections contre ceux-là même qui prétendent nous protéger et qui augmentent chaque jour leur pouvoir sur nos choix, nos vies et notre avenir.

Droit à la vie privée : la jurisprudence de la Cour suprême

Anne Pineau, avocate et adjointe au comité exécutif
Confédération des syndicats nationaux (CSN)

> ***« 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 ».***
>
> Juge La Forest dans R.c. Dyment 1988 2 RCS 417

En décembre 2013 Edward Snowden prédisait qu' « un-e enfant qui nait aujourd'hui va grandir sans aucune notion de vie privée ».

La notion même de vie privée serait-elle en voie d'extinction? Pourtant les sondages démontrent régulièrement le fort attachement des canadien-ne-s à ce droit que, ceci dit et curieusement, la Charte canadienne des droits et libertés (CCDL) ne mentionne même pas. C'est en effet par le droit à « la protection contre les fouilles, perquisitions et saisies abusives » (art.8) que la Cour Suprême a pu affirmer l'existence de cet élément essentiel d'une société démocratique.

Le présent texte propose un bref survol de la jurisprudence récente de la Cour sur cette notion. Notons que la plupart des décisions mentionnées ici ont été rendues en matière de droit criminel, la Cour devant déterminer la recevabilité d'un élément de preuve obtenu en violation du droit à la vie privée.

Qu'est-ce que la vie privée?

La vie privée est une « notion protéiforme »; elle inclut le droit à l'image, le droit à l'anonymat, le droit d'être laissé tranquille…

La cour note dans Tessling[1] que « l'article 8 crée pour chacun des zones d'autonomie personnelle » et protège un ensemble de renseignements biographiques d'ordre personnel notamment « des renseignements tendant à révéler des détails intimes sur le mode de vie et les choix personnels »[2].

On a longtemps confondu vie privée et propriété; au moyen-âge c'est à l'intérieur de son domicile uniquement que ce droit s'exerçait[3].

L'évolution des technologies ayant rendu possible la surveillance à distance cette approche s'est heureusement modifiée. On reconnait aujourd'hui que la vie privée n'est pas affaire de propriété; elle « protège les personnes et non la propriété »[4].

Trois aspects sont visés par cette protection : la personne, les lieux et l'information.

La fouille d'une personne et la prise d'échantillons de substance corporelles font partie des atteintes les plus graves[5].

L'expectative de vie privée en ce qui concerne les lieux dépendra de l'endroit où l'on se trouve, la résidence personnelle offrant certes le plus haut niveau de protection. La cour reconnait que les abords de la résidence sont aussi protégés de même que, à des degrés divers, des lieux comme les locaux commerciaux, les véhicules privés, les écoles, les bureaux et même la prison[6].

Finalement l'art.8 assure le droit « des particuliers, des groupes ou des institutions de déterminer eux-mêmes le moment, la manière et la mesure dans lesquels des renseignements les concernant sont communiqués »[7].

Le caractère illicite des activités ou des objets que l'on veut soustraire au regard des agents de l'État ne fait pas échec à la protection contre les fouilles. Le but de l'article 8 étant de prévenir les fouilles abusives « la découverte d'éléments de preuve d'un crime ne saurait justifier après coup une perquisition faite sans mandat dans un lieu privé »[8].

1. R. c. Tessling, [2004] 3 R.C.S. 432, 2004 CSC 67, par.15
2. R. c. Plant, [1993] 3 R.C.S. 281
3. Voir Tessling précité par.16
4. Voir Plant précité note 2
5. r. c. dyment, [1988] 2 R.C.S. 417
6. Voir Tessling précité
7. idem
8. R. c. Patrick, 2009 CSC 17, [2009] 1 R.C.S. 579, par.32

Équilibre de droits

À l'instar de tous les autres droits fondamentaux, le droit à la vie privée n'est pas absolu. La Cour cherchera à « mettre en balance les droits sociétaux à la protection de la dignité, de l'intégrité et de l'autonomie de la personne et l'application efficace de la loi »[9].

Attente raisonnable de vie privée

La Charte condamne les fouilles abusives. Une fouille « raisonnable » est donc permise. Elle devra remplir les conditions suivantes : la fouille est autorisée par la loi; la loi qui l'autorise n'a rien d'abusif; le pouvoir d'effectuer la fouille n'est pas exercé de manière excessive[10].

Mais encore faut-il qu'une attente raisonnable de vie privée existe pour que la protection de l'article 8 entre en jeu. Il n'y a en effet pas de « fouille » s'il n'y a pas d'attente de vie privée. Il faudra donc démontrer qu'une personne raisonnable et bien informée, placée dans la même situation s'attendrait à ce qu'on respecte sa vie privée. L'attente raisonnable dépendra d'un ensemble de circonstances (analyse contextuelle). Autrement dit le contenu de l'attente raisonnable en matière de vie privée dépendra du contexte.

> « *L'examen de facteurs tel la nature des renseignements, celle des relations entre la partie divulguant les renseignements et la partie en réclamant la confidentialité, l'endroit où ils ont été recueillis, les conditions dans lesquelles ils ont été obtenus et la gravité du crime faisant l'objet de l'enquête, permet de pondérer les droits sociétaux à la protection de la dignité, de l'intégrité et de l'autonomie de la personne et l'application efficace de la loi.* » [11]

Par exemple, peut-on entretenir des attentes de vie privée à l'endroit de l'ordinateur fourni par l'employeur? La Cour a récemment reconnu que oui, même si cette attente est moindre que dans le cas de l'ordinateur personnel :

> « *(…) les Canadiens peuvent raisonnablement s'attendre à la protection de leur vie privée à l'égard des renseignements contenus dans leurs propres ordinateurs personnels. À mon avis, le même principe s'applique aux renseignements contenus dans les ordinateurs de travail, du moins lorsque leur utilisation à des fins personnelles est permise ou raisonnablement prévue.* » [12]

En revanche, on a estimé que quelqu'un qui franchit une ligne de piquetage, alors que des affiches l'avisent qu'il est filmé et que sa photo sera utilisée, ne peut invoquer une attente raisonnable de vie privée :

> « *Les personnes franchissant la ligne de piquetage pouvaient raisonnablement s'attendre à être filmées ou photographiées et à ce que leur image soit diffusée par autrui, notamment des journalistes.* » [13]

La Cour a aussi dû se pencher sur l'attente de vie privée en matière…d'ordures ménagères! Loin d'être triviale la question soulève au contraire des enjeux importants.

> « *En effet, les ordures ménagères renferment une énorme quantité de renseignements personnels sur ce qui se passe à l'intérieur de nos maisons, y compris une grande quantité d'ADN sur les papiers mouchoirs, des documents très personnels (par exemple des lettres d'amour, des factures en souffrance, des déclarations de revenus) et sur des vices cachés (contenants de médicaments, seringues, accessoires sexuels, etc. (…)Bon nombre d'entre nous ne souhaitent pas nécessairement que ces renseignements soient révélés au public en général ou à la police en particulier.* »[14]

L'accusé dans cette affaire, de même que des groupes de défense de la vie privée, soutenaient que la mise au chemin des ordures avait une finalité qui devait être respectée, soit la destruction. En conséquence on ne pouvait parler d'abandon ni de renoncement à la vie privée. La Cour rejette cette approche. Si donc existe une expectative de vie privée sur ces « sacs d'information » celle-ci prend fin dès lors qu'on abandonne le sac au bord du chemin…De quoi nous faire mieux comprendre les angoisses de Ti-Mé (Popa) à l'endroit de ses vidanges!

Évolutions technologiques

Les moyens technologiques de surveillance constituent de véritables armes de destruction massive de la vie privée et, du coup, fatalement, de la démocratie. Déjà en 1990 dans l'arrêt Duarte le juge Laforest faisait cette importante mise en garde :

> *« La surveillance électronique est à ce point efficace qu'elle rend possible, en l'absence de réglementation, l'anéantissement de tout espoir que nos communications*

Les moyens technologiques de surveillance constituent de véritables armes de destruction massive de la vie privée et, du coup, fatalement, de la démocratie.

9. Idem, par. 20

10. R. c. Cole, 2012 CSC 53, [2012] 3 R.C.S. 34

11. Voir Plant précité note 2

12. Voir Cole précité note 10, par.1

13. Alberta (Information and Privacy Commissioner) c. Travailleurs et travailleuses unis de l'alimentation et du commerce, section locale 401, 2013 CSC 62, [2013] 3 R.C.S. 733, par.26

14. Voir Patrick précité note 8, par.30

restent privées. Une société nous exposant, au gré de l'État, au risque qu'un enregistrement électronique permanent soit fait de nos propos chaque fois que nous ouvrons la bouche, disposerait peut être d'excellents moyens de combattre le crime, mais serait une société où la notion de vie privée serait vide de sens. Comme le dit le juge Douglas, dissident dans l'affaire United States v. White, précitée, à la p. 756: [TRADUCTION] 'La surveillance électronique est le pire destructeur de la vie privée'.»[15]

Il devient donc crucial que les droits garantis par l'article 8 puissent « progresser au rythme de la technologie »[16].

La Cour a par exemple assimilé à de l'écoute électronique le fait pour la police d'exiger d'un fournisseur internet copie des messages textes échangés par des abonnés :

« *La messagerie texte est, essentiellement, une conversation électronique. La seule distinction entre la messagerie texte et les communications orales traditionnelles réside dans le processus de transmission.*[17]»

On a aussi actualisé le cadre juridique traditionnel selon lequel le mandat de fouille d'un domicile inclut les placards et tiroirs. La Cour a refusé d'étendre ce principe aux ordinateurs trouvés sur place estimant que l'information qu'ils contiennent est sans commune mesure avec un classeur :

« *En effet, les ordinateurs sont susceptibles de donner aux policiers accès à de vastes quantités de données sur lesquelles les utilisateurs n'ont aucune maîtrise, dont ils ne connaissent peut être même pas l'existence ou dont ils peuvent avoir choisi de se départir, et qui d'ailleurs pourraient fort bien ne pas se trouver concrètement dans le lieu fouillé(…) ces facteurs commandent l'obtention d'une autorisation expresse préalable.* »[18]

Une protection théorique?

La Cour a bien posé quelques balises intéressantes en matière de vie privée, notamment dans les affaires criminelles, mais force est de constater que ces principes demeurent souvent bien théoriques. Car la Cour peut décider d'admettre un élément de preuve même s'il a été obtenu en violation d'un droit de la Charte. Cela est possible à la condition que l'utilisation de cette preuve ne déconsidère pas l'administration de la justice. C'est le test de l'article 24 de la Charte. Ainsi, dans nombre de dossiers vus précédemment, la Cour a conclu à violation de la vie privée tout en recevant malgré tout l'élément de preuve résultant de cette violation…[19]

Démocratie

Fait important la Cour a reconnu aux lois de protection des renseignements personnels une forme de prépondérance parce qu'elles visent le renforcement de l'autonomie personnelle et, partant, de la vie démocratique :

« *(…) une loi qui vise à protéger un droit de regard sur des renseignements personnels devrait être qualifiée de « quasi constitutionnelle » en raison du rôle fondamental que joue le respect de la vie privée dans le maintien d'une société libre et démocratique.* »[20]

La protection de la vie privée permet en outre l'éclosion d'une pensée non conformiste, caractéristique des sociétés démocratiques :

« *On ne saurait trop insister sur l'importance de protéger la vie privée dans une démocratie dynamique (…) Comme l'affirme Chris D. L. Hunt dans « Conceptualizing Privacy and Elucidating its Importance : Foundational Considerations for the Development of Canada's Fledgling Privacy Tort » (2011), 37 Queen's L.J. 167, p. 217, [TRADUCTION] « [l] a démocratie a besoin de citoyens autonomes qui se réalisent et qui sont libres de formuler et d'exprimer des opinions non conformistes. Si les atteintes à la vie privée gênent l'individualité et entraînent le conformisme, c'est la démocratie elle même qui en souffre.* »[21]

Conclusion

En 1990, dans l'arrêt Wong[22], le juge La Forest prenait à témoin la société totalitaire décrite par Orwell pour illustrer l'importance de la vie privée dans une société démocratique :

« *Dans son roman futuriste classique 1984, George Orwell dresse le portrait sinistre d'une société dont les citoyens ont toutes les raisons de croire que chacun de leurs mouvements est assujetti à la surveillance magnétoscopique électronique. On ne pourrait trouver contraste plus frappant avec nos attentes en matière de vie privée dans une société libre comme la nôtre* ».

Certes nous ne vivons pas, du moins pas encore, dans cette contrée totalitaire d'Océania imaginée par Georges Orwell; mais certaines révélations récentes en matière de surveillance de nos communications par l'État donnent à penser…

Et si la prophétie d'Edward Snowden devait se réaliser ce n'est pas seulement la vie privée qui risquerait alors de disparaître mais, avec elle, la démocratie.

15. R. c. Duarte, [1990] 1 R.C.S. 30

16. R. C. SOCIÉTÉ TELUS COMMUNICATIONS, 2013 CSC 16, [2013] 2 R.C.S. 3

17. Idem par.5

18. R. c. Vu, 2013 CSC 60, [2013] 3 R.C.S. 657, par.24

19. Voir notamment, R. c. Vu, précité note 18, R. c. Plant, précité note 2 et R. c. Cole, précité note 10

20. Voir Alberta précité, note 13 par.19

21. Idem,par.22

22. R. c. Wong, [1990] 3 R.C.S. 36

Rien à cacher, rien à craindre?

David Lyon, professeur
Surveillance Studies Centre. Université Queen's

Steve Berthiaume - www.steveberthiaume.ca

La surveillance comme mode de vie

Lorsque nous allons à l'aéroport, nous nous attendons à une forme de contrôle. Nous nous attendons à ce que nos données soient vérifiées au comptoir de la compagnie aérienne ou par le système de billetterie électronique. Mais peu de gens savent qu'ils sont constamment observés dans leur quotidien. Les formes que prend la surveillance sont multiples. En effet, la majeure partie de la surveillance ne repose pas sur l'observation directe des personnes. On nous observe à travers nos relevés bancaires, nos appels de téléphone portable, les cartes de transport en commun, les cartes d'employé-e-s et de fidélité, les passeports, les cartes de crédit et de services de santé, notre numéro d'assurance sociale et nos activités sur Google, Facebook et Twitter.

Les révélations d'Edward Snowden, depuis juin 2013, démontrent clairement la dépendance de la National Security Agency (NSA) sur les sociétés Internet; elles démontrent aussi que l'utilisation commerciale des données recueillies dans le cadre de transactions quotidiennes et de nos communications nourrit la surveillance de l'État.

Trois questions se posent :

Pourquoi la surveillance prend-elle une place si importante dans la vie quotidienne aujourd'hui?

Pourquoi acceptons-nous si facilement d'être surveillés 24 heures sur 24, 7 jours sur 7?

Pourquoi les gens commencent-ils à exercer eux-mêmes une surveillance?

Un monde sous observation

Ce n'est pas arrivé d'un jour à l'autre. Au cours des cent dernières années, les sociétés de surveillance se sont développées, lentement et progressivement au début, ensuite à un rythme accéléré. Mais les sociétés de surveillance d'aujourd'hui sont quelque chose de nouveau, d'inédit et d'inquiétant à la fois. Évidemment, les gens se sont toujours observés les uns les autres; chose somme toute naturelle. Anciennement, dans un village, chacun savait ce qui se passait dans la vie des autres. Mais la surveillance d'aujourd'hui, bien que semblable sous certains aspects à l'ancienne, s'inscrit dans un nouveau paradigme. Elle répond en partie à une logique économique : les données personnelles n'ont jamais eu autant de valeur. Une logique organisationnelle entre également en jeu en faisant de l'élimination du risque un principe de gestion. À cela, il faut ajouter, bien sûr, une techno-logique : nous avons maintenant les moyens d'amasser et de traiter les données personnelles qui n'étaient pas disponibles auparavant.

S'installe alors une forme de dépendance culturelle à l'observation et à la visibilité. Comment devrions-nous définir la surveillance aujourd'hui? La définir nous aidera à éviter de fonder des espoirs ou des craintes sur les possibilités de la haute technologie ou de privilégier les définitions opératoires relatives à la sécurité nationale qui se concentrent sur « le terrorisme »[1].

La surveillance n'est pas nécessairement sinistre ou effrayante. Mais est-elle « neutre »? Surveiller signifie observer, contrôler le déroulement d'une action, veiller sur quelque chose, sur quelqu'un avec vigilance. Et comme nous l'avons noté, la surveillance peut être virtuelle, par le biais de données numériques réunies (compilées) pour que les gens et les populations puissent être mieux « vus », observés, soumis à la loupe du système de surveillance. L'État nous surveille avec des moyens spécifiques qui aident à maintenir les gens dans le respect des normes étatiques établies, à s'assurer que les impôts soient payés à temps, que les gens détiennent les permis requis pour conduire ou porter des armes à feu, ou que des minorités particulières, comme, par exemple, les nouveaux immigrants, soient traitées selon les normes[2].

Mais la surveillance est également le fait d'agences qui n'ont pas de liens avec une quelconque structure gouvernementale. Prenez, par exemple, Tesco, une importante chaîne de supermarchés britannique. Tesco dirige une base de données appelée le Creuset qui détermine le profil de chaque consommateur au Royaume-Uni : traits de « personnalité », habitudes de voyage, préférences commerciales, niveau de scolarité, appartenance ou non au mouvement écologique, degré de générosité caritative[3]. Le Creuset avance que dans un monde parfait, « nous saurions tout ce dont ont besoin les consommateurs, leurs attitudes, leur comportement et leur style de vie, mais qu'en vérité, nous n'en saurons jamais autant que nous le voudrions ». Tesco utilise un logiciel appelé le Zodiaque qui, avec le concours du Creuset, produit une carte qui permet de savoir comment les individus se situent par rapport au travail et au magasinage et de les classer dans des catégories.

Il existe aussi des courtiers qui disposent de banques d'informations énormes : Experian, Claritas et Equifax, sans compter les multiples sources publiques d'informations comme les listes électorales, le Bureau du cadastre et le Bureau national des statistiques. Toutes ces données permettent aux compagnies de savoir où concentrer leurs énergies et quels clients courtiser.

Au Canada, Canadian Tire a décidé en 2002 d'analyser les résultats des ventes par cartes de crédit. Cette analyse a permis d'associer un profil psychologique au comportement des consommateurs, de prédire quand ils s'inscriront pour un shower de bébé ou pour une liste de mariage, quand leur marge de crédit devra être coupée, et même quand ils auront besoin d'une thérapie de couple[4].

L'utilisation de données personnelles pour toutes sortes d'objectifs, souvent bien au-delà de ce que nous pourrions imaginer, montre qu'il est justifié de parler d'un paradigme de la surveillance. Nos comportements sont « observés » dans le moindre détail et des profils construits non seulement par la police ou les responsables de la sécurité, mais aussi par les entreprises. Nous pouvons ne pas croire que traîner dans un bar fait de nous un mauvais payeur, mais pour Canadian Tire,

1. Pour une présentation en profondeur de cette définition, voir David Lyon, *Surveillance Studies : An Overview*, Cambridge: Polity Press, 2007. Cette définition comporte au moins deux aspects de la surveillance analysés par l'historien français Michel Foucault : la surveillance directe comme dans la prison panoptique et le biopouvoir qui utilise les données statistiques pour gouverner.

2. Voir le livre de James C. Scott, *Seeing like a State*, (New Haven CT: Yale University Press, 1998)

3. Heather Tomlinson and Rob Evans, "Tesco stocks up on inside knowledge of shoppers' lives" *The Guardian,* 20 September 2005.

4. Charles Duhigg, "What does your credit card company know about you? *New York Times*, 12 May 2009.

une telle personne fait partie d'un groupe statistiquement à risque et est considérée comme telle.

La surveillance comme mode de vie : les organisations nous observent

Nous pouvons dire, sans aucune exagération, que la surveillance représente l'aspect le plus important dans la vie organisationnelle d'aujourd'hui[5]. Elle est devenue l'élément-clé d'une gestion réussie, celui qui permet de connaître en détail les consommateurs, les clients, les citoyens, les étudiants, les contrevenants, les voyageurs ou les patients avec qui l'organisation a affaire. Les entreprises ne veulent pas tant connaître leurs clients que tout savoir d'eux. Les organismes gouvernementaux ou les agences frontalières collectent des données personnelles et cherchent les façons ingénieuses de recouper ces données pour créer des groupes significatifs auxquels on peut associer des tendances et des comportements.

En d'autres mots, les organisations s'efforcent de nous rendre de plus en plus visibles. Selon notre point de vue, comme citoyens ordinaires, voyageurs, travailleurs ou consommateurs, nos vies sont de plus en plus transparentes à toutes les pratiques de gestion des agences. La tendance ne montre aucun signe de ralentissement. Nous sommes nus en ce monde. Déjà, dans les années soixante, le sociologue pop américain Vance Packard écrivait *la Société Nue*[6]. Un demi-siècle plus tard, les prédictions de Packard sont devenues réalité. Dans le domaine de la sécurité aérienne, le « passager nu » est maintenant une réalité littérale et pas une fiction ou une conjecture de sociologue. La surveillance Internet a grandi exponentiellement depuis que le World Wide Web est utilisé à grande échelle. La recherche de nouveaux logiciels pour rendre les utilisateurs transparents aux organisations est constante. Depuis 2009, le logiciel « Webwise » permet aux fournisseurs d'accès à Internet de proposer des publicités basés sur les habitudes de navigation en ligne.

Les données Internet sont non seulement ciblées à des fins commerciales, mais représentent des informations sur lesquelles les gouvernements aiment mettre la main. La proposition la plus audacieuse jusqu'à présent vient de la Grande-Bretagne en 2008, pour la création d'une base de données contenant tous les appels téléphoniques, les courriers électroniques et l'utilisation Internet (incluant des services Internet de liaison sonore comme Skype) dont les enregistrements seraient conservés pendant une année[7].

Le Royaume-Uni a soutenu un tel projet depuis les attentats à la bombe de Londres en 2005, mais il semble maintenant être également appuyé par l'Union européenne. En 2009, une directive de l'Union européenne est entrée en vigueur afin de contraindre des fournisseurs d'accès Internet à conserver toutes les informations de courriers électroniques et de visites de sites Web aussi bien que des coups de téléphone et des SMS. Dans ce cas, la surveillance de la population de tout un pays serait mise en œuvre par l'utilisation d'Internet à des fins de sécurité et de maintien de l'ordre.

Maintenant qu'il est clair que des organisations de toutes sortes nous observent, la question qui s'impose est : pourquoi? Comment cela est-il arrivé? Par un certain nombre de courants culturels profonds qui présentent la surveillance comme une solution aux problèmes sociaux et politiques, alors que sur le plan organisationnel on peut identifier deux jalons majeurs. Le premier renvoie à la première expansion moderne de la bureaucratie, pour qui l'efficacité repose sur des règles rationnelles, et le deuxième, à l'utilisation moderne de l'information et des technologies de communication pour ajouter vitesse et flexibilité à la gestion. Laissons la question bureaucratique de côté et concentrons-nous sur l'utilisation des nouvelles technologies.

Au début des années quatre-vingt-dix, le traitement des données personnelles est devenu de plus en plus important. Des préposé-e-s à l'entrée de données, surtout des femmes mal payées, ont commencé à compiler des renseignements personnels disponibles dans le domaine public : maison et automobile, données judiciaires, dossier scolaire, adresse, numéros de téléphone...

Aujourd'hui, les sociétés en savent beaucoup plus. Par exemple, avec les GPS, elles peuvent suivre le positionnement terrestre de leurs clients à tout moment. Au mois d'octobre de l'année 2009, une société américaine de téléphone, Nextel,

5. Voir, par exemple, Kevin Haggerty "'Ten *thousand* times larger…': Anticipating the future of surveillance" in Benjamin J. Goold and Daniel Neyland, éditeurs. *New Directions in Surveillance and Privacy*, Cullompton UK: Willan, 2009.

6. Vance Packard *The Naked Society*, New York: David McKay, 1964.

7. Anil Dawar, "Alarm at plan for central store of telecoms records" *The Guardian*, 20 May 2008.

a transmis plus de huit millions d'emplacements clients aux agences d'application de la loi[8].

Malgré quelques balises légales et techniques, les minces filets d'eau de données personnelles se sont transformés en un torrent tel qu'il est maintenant impossible de suivre tous les conduits et de remonter les ruisseaux à leur source. Les données personnelles sont plus que jamais utilisées. Un peu comme les personnages de Kafka dans son roman le *Procès*, nous ne saurons jamais exactement qui sait quoi et pourquoi… Évidemment les conséquences suivront et cela, malgré que nous soyons conscients que nous sommes sous surveillance.

La surveillance comme mode de vie : nous savons que nous sommes observés

Au-delà de l'appétit des organisations pour nos données personnelles, il faut noter un aspect non moins important de la culture de surveillance, à savoir que les sujets le savent, en sont conscients. La surveillance, de notre temps, peut être discrète dans certaines situations, mais dans beaucoup d'autres, le sujet est en même temps objet de ce contrôle.

Les citoyens conscients des effets de la surveillance peuvent changer de comportement. Mon employé de bureau de pharmacie locale ne manque jamais de me demander si je possède une « Carte Optimum » de fidélité quand je fais un achat. Je réponds, invariablement non et que je n'en veux pas. D'autres magasins veulent des numéros de téléphone et des codes postaux. Certains se conforment simplement à la demande, d'autres refusent poliment, sachant que la connaissance préalable de telles données apparemment innocentes peut donner accès à d'autres données personnelles. Et il faut le dire sans ambages, les résistances à une telle surveillance quotidienne sont une pratique louable.

Cependant, de tels actes cognitifs individuels de résistance, bien qu'importants, ne seront probablement pas très efficaces face au pouvoir des organisations détentrices de systèmes de surveillance. Au moment où nous sommes incités à assurer notre propre protection contre les dérives de la culture de surveillance, la question essentielle, de l'ordre du politique, touche au défi qu'il faut relever contre les organisations afin qu'elles adoptent une politique de gestion des données personnelles récoltées le plus souvent à l'insu des citoyens. La responsabilité des organisations en matière de surveillance est bien plus importante que notre responsabilité personnelle en tant que cibles.

Nous allons maintenant examiner un autre phénomène qui fait partie de la société de surveillance. Plutôt que de fuir la surveillance, certains s'en accommodent.

La surveillance comme mode de vie : nous pouvons aussi surveiller

Nous sommes observés et nous en sommes conscients, mais nous en soucions-nous? Une troisième dimension de la culture de surveillance est que certains pratiquent eux-mêmes la surveillance. Certains utilisent la fonction GPS des téléphones portables pour trouver d'autres utilisateurs, d'autres utilisent les réseaux sociaux comme Facebook pour en apprendre sur des voisins, des collègues ou des amis, d'autres encore installent des « nannycams » pour surveiller la gardienne ou espionner la navigation sur Internet de leurs enfants.

La culture de la surveillance s'installe lorsque les gens ordinaires se mettent à utiliser eux-mêmes la surveillance pour organiser leurs vies, protéger leurs maisons et leurs familles ou vérifier ce que leurs associés ou enfants font[9]. Ou même leurs parents. Des familles aux États-Unis consentent à faire porter à leurs parents âgés, souffrant de la maladie d'Alzheimer ou de perte de mémoire, une puce RFID pour les empêcher de s'égarer et pour les retrouver quand ils sont perdus[10].

La culture de surveillance d'aujourd'hui est sans précédent. Jamais auparavant, autant de temps, d'énergie et d'argent ont été investis dans l'observation des autres avec autant de conséquences. Cette surveillance ne s'exerce pas à sens unique. C'est plus complexe et c'est pour cela que j'utilise la notion de « culture de surveillance ». La surveillance est intégrée dans notre vie quotidienne, parfois presque inconsciemment.

Rien à cacher, rien à craindre

Aussi, quel est exactement le problème? Parce que nous nous sommes habitués graduellement à cette nouvelle réalité, nous n'avons pas posé les questions fondamentales que soulevaient ces changements massifs survenus en très peu d'années. L'idée « d'une société de surveillance » était jadis associée aux États policiers et à la répression et réprouvée

8. Voir http://paranoia.dubfire.net/2009/12/8-million-reasons-for-real-surveillance.html/ , consulté le 1er décembre 2009.

9. Stephanie Rosenbloom, "I spy; doesn't everyone?" *New York Times*, 7 September 2006.

10. Kim Zetter "To tag or not to tag" *Wired*, 05 September 2008 www.wired.com/politics/security/news/2005/08/68271

à cause de son côté abject et hideux. Le roman classique d'Orwell, *1984*, nous a donné un aperçu de « Big Brother » pour décrire un État auquel nous résisterions à tout prix.

Le simple fait d'appartenir à un groupe statistique vous qualifie pour l'inclusion ou l'exclusion, l'accès ou le déni. N'avoir rien à cacher n'est d'aucun secours.

Mais malgré Orwell, la société de surveillance est arrivée, sans les lourdes bottes de la répression brutale, avec les habits neufs de l'efficacité technologique. Elle n'est pas venue d'un État autoritaire, mais de corporations commerciales revendiquant la meilleure connaissance possible de leurs clients afin de leur fournir les marchandises et les services souhaités. Elle n'est pas apparue sur « un écran de télévision », sous la forme du visage effrayant de Big Brother, mais sur un million d'écrans de sites de réseaux sociaux et d'appareils portatifs commercialisés comme des objets commodes, rentables et personnalisés.

Cependant, les sociétés de surveillance d'aujourd'hui sont profondément ambiguës. On ne voit pas généralement l'efficacité, la commodité et la personnalisation comme des ennemis. Non, mais les nouvelles technologies de surveillance qui comportent certains avantages permettent également la mise en place de modes douteux de contrôle et de profilage. Quelles sont les conséquences de ce système? Dans les sociétés où la présomption d'innocence est respectée, vous êtes supposés n'avoir rien à cacher, ni rien à craindre. La loi permet aux autorités d'enquêter seulement sur ceux qui ont quelque chose de grave à cacher. Mais aujourd'hui, la devise « rien à cacher, rien à craindre » est systématiquement sapée par l'ampleur de la nouvelle surveillance.

L'objectif consiste à situer les gens dans des catégories. Rappelons le logiciel « Webwise » qui classifie les gens sur la base de leurs habitudes de navigation. Vous faites partie du monde où vous naviguez. Les décisions d'évaluations automatisées sont faites à partir de tout, de votre solvabilité à votre capacité de détenir un compte bancaire. Et si vous êtes marginal ou désavantagé, le système s'assurera que ces vulnérabilités soient amplifiées par les effets de ce qu'Oscar Gandy appelle « l'inconvénient cumulatif »[11].

Mais ça ne s'arrête pas là. Ces types de classifications sont également utilisés par la police, les services de renseignement et d'autres autorités. Après le onze septembre 2001, le département de la Sécurité intérieure des États-Unis a fait appel à la firme privée « Customer Relationship Management », non pas pour localiser des clients potentiels, mais des terroristes[12].

De telles stratégies ont pour effet d'inscrire des innocents sur des listes d'interdiction de vol, sur des listes de surveillance, de surveiller des maisons ordinaires dans les quartiers chauds de la ville, de traiter des piétons pacifiques comme « suspects » quand ils s'aventurent involontairement sous les caméras de lieux publics. De braves garçons canadiens d'une grande école, comme Alistair Burt, se sont vus refuser la permission de monter à bord d'un avion pour des vacances familiales. Des citoyens « suspects » comme Maher Arar, Ahmad El Maati, Muayyed Nureddin et Abdullah Almalki ont atterri dans les salles de torture syriennes en 2002 et 2003. Même sans motif valable et n'ayant rien à cacher, vous pouvez toujours finir suspect.

Voilà pourquoi, malheureusement, nous autorisons les sociétés de surveillance à se développer sans entrave. Leurs effets positifs peuvent bénéficier à certains groupes de personnes, mais leur impact négatif se fait sentir chez ceux qui, en raison de leur situation économique, leur origine ethnique ou leur sexe, sont déjà défavorisés. D'autre part, comme le prouve l'exemple des listes d'interdiction de vol, n'importe qui peut être touché. Il existe quelques garanties : les lois sur la protection des données et la vie privée. Mais elles ont tendance à être efficaces uniquement dans des cas extrêmes, lorsqu'il y a une violation évidente ou médiatisée de la loi. La plupart du temps, la nouvelle surveillance affecte négativement les personnes, même lorsque ces systèmes fonctionnent correctement, aux fins prévues et dans les limites de la loi. Le « tri social », en particulier, lorsqu'il utilise les bases de données et les moyens de communication en réseau, fonctionne à travers la catégorisation automatique de la population afin que différents groupes puissent être traités différemment. Le simple fait d'appartenir à un groupe statistique vous qualifie pour l'inclusion ou l'exclusion, l'accès ou le déni. N'avoir rien à cacher n'est d'aucun secours.

Vivre à nu est l'oeuvre d'une équipe de recherche multidisciplinaire qui explique comment la surveillance s'accroît dans tous les sphères de notre vie et soulève des questions pressantes en regard de la vie privée et de la justice sociale.

Publié sous la direction de Colin J. Bennett, Kevin D. Haggerty, David Lyon et Valerie Steeves. Disponible gratuitement en ligne. www.aupress.ca/index.php/books/120238/

11. Oscar Gandy, *Coming to Terms with Chance: Engaging Rational Discrimination and Cumulative Disadvantage*, London: Ashgate, 2009.

12. Voir David Lyon, *Surveillance after September 11*, Cambridge: Polity, 2003.

Surveillance industrielle

Stéphane Leman-Langlois, titulaire
Chaire de recherche du Canada en surveillance et construction sociale du risque, Université Laval

Il a beaucoup été question, ces derniers mois, de la surveillance que l'État dirige vers le citoyen, au point qu'on oublie facilement qu'une myriade d'entités privées collectent à chaque seconde des montagnes d'informations sur nous, nos habitudes, nos comportements et nos interactions avec les autres. Pourtant, il arrive régulièrement qu'un jet de lumière nous révèle une portion de ces pratiques, par exemple lorsqu'une publicité particulièrement opportune apparaît sur un site que nous visitons. En général, nous faisons peu de cas de ces étonnantes coïncidences. Une explication est sans doute que pour le consommateur moyen, une publicité ciblée est une publicité avant tout et que la nature et l'intensité du

travail analytique qui l'a produite restent toujours inconnues, voire insoupçonnées. Pourtant, l'ampleur de la surveillance qui est requise se chiffre en milliards de dollars (défrayés par les consommateurs, bien sûr) et la marchandisation de l'information personnelle est le fondement même de l'Internet industriel contemporain.

Surveillance administrative

Plusieurs entités commerciales se doivent d'amasser un minimum d'informations sur leurs clients, tout simplement afin de leur fournir le service qu'ils demandent. Un téléphone portable ne pourrait fonctionner sans continuellement révéler sa position; on devra également conserver, à des fins de facturation, les données sur les appels reçus et effectués à partir du téléphone (les fameuses métadonnées). C'est pour la même raison que les fournisseurs de télévision sur demande conservent des informations sur les choix de leurs clients. Ceci, on peut s'en douter, s'accumule et, à la longue, peut représenter des quantités phénoménales de données; cependant la surveillance purement administrative implique généralement que les entreprises font périodiquement le ménage pour alléger leur fardeau informatique.

La surveillance administrative peut aussi impliquer le filtrage des données, des biens ou des personnes. Par exemple, les fournisseurs d'accès Internet utilisent des dispositifs d'inspection approfondie des paquets (*deep packet inspection*, DPI) afin de moduler la circulation des données pour permettre aux applications qui se déroulent en temps réel (téléphonie, jeux) de passer devant celles qui sont moins urgentes (téléchargements).

Dans cette catégorie, il faut ajouter les systèmes de contrôle d'accès, à des services ou à des lieux physiques par exemple, qui consistent à identifier, filtrer et suivre les individus selon les autorisations qui leur ont été accordées. Ici, nous retrouvons la journalisation (*logging*) des sessions de travail sur les ordinateurs, les cartes d'accès et les systèmes biométriques. La plupart d'entre nous avons acquis une certaine habitude des mots de passe, mais un nombre toujours plus grand de travailleurs sont soumis à des régimes de surveillance microscopique visant à maximiser leur productivité, dont la surveillance de leurs déplacements, de leurs mouvements et de leur utilisation des installations de l'entreprise, des toilettes à l'ordinateur qu'on leur confie.

Surveillance valorisée

Une entreprise peut également réutiliser les renseignements qu'elle accumule à des fins administratives pour ajouter à ses revenus. Le cas de Bell et de la publicité ciblée en est un exemple. Fin 2013, Bell Mobilité et sa subsidiaire écono + Virgin Mobile informaient leurs clients que des publicités ciblées seraient désormais envoyées à leurs téléphones. Pour ce faire, Bell mettrait à profit la banque de données qu'elle possède déjà sur ses clients et qui contient leurs habitudes en matière d'usage d'Internet, de téléphonie (dont leurs déplacements géographiques) et de télévision. Bell/Virgin offrait à ses clients de refuser la publicité ciblée, mais non la collecte et l'analyse d'informations à leur sujet (en quel cas ils recevraient tout de même de la publicité « non ciblée ». Notez que tous les fournisseurs font la même chose). Cette valorisation de renseignements déjà colligés encourage, bien sûr, une collecte et une rétention maximale, qui permettent de « profiler » le client, c'est-à-dire d'identifier et de catégoriser à la fois ses intérêts et la stratégie de marketing qui convient le mieux à son profil psychologique. Ceci est réalisé à l'aide de logiciels algorithmiques sophistiqués qui classeront les clients dans diverses typologies concoctées par des experts en marketing behavioral.

Ce que les métadonnées peuvent révéler à notre sujet est phénoménal. Une expérience en cours à l'Université Stanford, avec 500 volontaires offrant leurs métadonnées, a montré que les chercheurs pouvaient établir le dossier financier, l'état de santé, l'adhésion aux AA, le fait d'avoir eu un avortement ou de posséder des armes, et bien d'autres choses encore.

En plus de la valorisation de métadonnées, il faut également considérer une foule de services de communication comme des moyens de production de données réutilisables. Par exemple, le contenu de courriels envoyés ou reçus à l'aide de Gmail a toujours été utilisé par Google comme une mine d'information sur ses clients (en fait, c'est la raison pour laquelle Google a lancé Gmail). Les robots de la compagnie vont systématiquement à la pêche dans les courriels des utilisateurs pour y trouver des mots-clés pouvant être commercialement utiles. Selon la compagnie, ceci ne viole pas la vie privée des utilisateurs de Gmail puisque ce sont des robots qui font le travail et qu'aucun humain n'a jamais accès aux contenus de conversations privées. Yahoo, MSN et la plupart des autres compagnies de ce type font, bien sûr, exactement la même chose. Facebook fait la saisie, en temps réel, de tout ce que font les utilisateurs sur son site, incluant les mises à jour de statut, commentaires, j'aime et autres clics; dans le cas de FB, il s'agit de tous les mots entrés à l'écran par l'usager, incluant ceux que ce dernier décide ensuite d'effacer sans les publier. En fait, Facebook sait ce que vous faites sur toutes les pages où est inclus un bouton « j'aime ». Voici comment un service gratuit a fait de son fondateur un des hommes les plus riches du monde.

Pour clore cette section, revenons aux dispositifs de DPI mentionnés ci-dessus. Puisqu'on module déjà le trafic Internet à l'aide de cette technologie, autant valoriser cette forme de surveillance également. Les fournisseurs d'accès l'utilisent donc pour favoriser certaines applications et/ou contenus qui participent à leurs revenus.

Surveillance commerciale

Il existe bien sûr une foule d'entités commerciales qui font de la surveillance, dès le départ, uniquement pour constituer une banque de données utilisables à des fins de modification du comportement de l'individu. Un exemple parmi d'autres : fin 2013, il fut démontré que les télévisions « intelligentes » de LG renvoyaient aux serveurs de la compagnie un flux d'informations sur l'usager, incluant son comportement sur Internet, les mots-clés recherchés, les chaînes regardées, les minutes d'utilisation, ainsi que le contenu des supports médias branchés sur sa télé (par exemple, une carte SD ou lecteur USB externe). Que fait LG avec ces informations ? Elle les analyse et les revend à des publicitaires. Sur l'écran d'accueil, le consommateur est ainsi exposé à des publicités taillées sur mesure (produits intéressants, présentés de manière compatible avec la personnalité du consommateur), et constamment ajustées pour obtenir le comportement désiré.

D'autres entités commerciales sont fondées exclusivement sur la surveillance du citoyen. Par exemple, Vigilant Solutions utilise des lecteurs automatisés de plaques d'immatriculation, des statistiques sur le revenu des ménages et d'autres données à des fins de stratégie publicitaire. Les courtiers en données sont des entreprises fondées entièrement sur la collection et la revente de données. Gnip traite près de quatre milliards d'entrées sur les réseaux sociaux et les revend à ses clients C chaque jour. Axciom a pour but de colliger 1 500 points d'information sur chaque citoyen afin de les catégoriser dans son système à 70 types psycho-socio-démographiques. Datalogix, qui collectionne les informations laissées par les clients qui utilisent une carte de fidélisation, détient de l'information sur mille milliards de dollars dépensés par les consommateurs. Assurez-vous de donner le bon code postal la prochaine fois qu'une caissière vous le demandera : de cette manière, on pourra combiner une série de banques de données sur vos habitudes quotidiennes et les relier à votre nom et votre adresse.

Cette dernière catégorie comprend également ce qu'on pourrait appeler des entreprises de surveillance « indirecte », c'est-à-dire celles qui commercialisent des dispositifs, logiciels, stratégies ou services de surveillance. Il suffit de constater la fréquence d'éclosion de nouveaux systèmes de vidéosurveillance pour se donner une idée de la vitalité de ce marché. Sans compter que derrière ces caméras, des logiciels de traitement de l'image de plus en plus sophistiqués sont offerts, dont ceux qui analysent le comportement et ceux qui reconnaissent les visages.

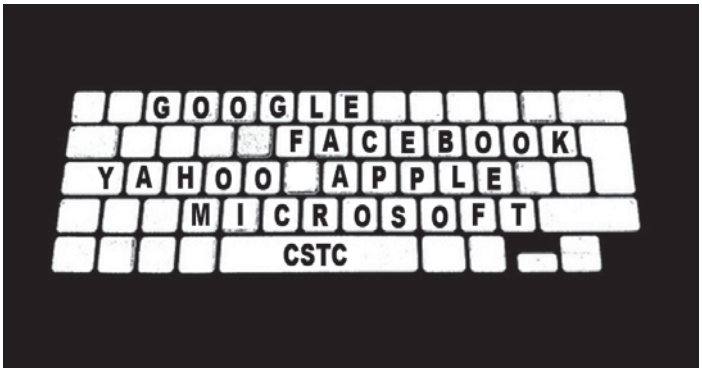
Manifestant dénonçant la surveillance de la NSA.

Retour à l'État

Récemment, les projecteurs ont été braqués sur certains organismes de renseignement gouvernementaux qui sont profondément impliqués dans la collecte généralisée d'informations sur les Canadiens. Il s'agit, en particulier, de la GRC, du Centre de la sécurité des télécommunications Canada (CSTC), du Service canadien du renseignement de sécurité (SCRS) et de la National Security Agency (NSA) des États-Unis. Or, souvent (la fréquence étant impossible à établir puisque ces activités sont clandestines), ces organismes ne font plus de collecte ou d'interception active et se contentent d'exiger des données déjà amassées par les entreprises. Les programmes les plus célèbres révélés par Edward Snowden, Glenn Greenwald et Laura Poitras font état de deux types de collecte. Le premier type, dont les exemples sont « Prism » et « Fairview », consiste à convaincre ou à obliger (à l'aide de certaines dispositions du USA Patriot Act, entre autres) un grand nombre d'entités industrielles et financières de fournir un accès à leurs banques de données et, le cas échéant, aux contenus qui sont confiés à leurs services d'infonuagique (comme Google, Amazon, etc.).

Dans cette catégorie, il y a également les multiples accords, avec presque tous les fournisseurs de services, qui prévoient l'accès aux métadonnées générées par leurs clients, qui alimentent la base de données géante connue sous le nom de « Marina », partagée entre les partenaires des « cinq yeux » (Canada, États-Unis, Royaume-Uni, Australie et Nouvelle-Zélande). Ces accords sont secrets, mais comme il doit forcément y avoir un coût additionnel pour les fournisseurs, il est peu probable qu'ils aient entrepris ces activités sans menace ou compensation. Le second type de collecte « passive » consiste à intercepter le flot d'information entre les serveurs des fournisseurs, avec le programme « Muscular » entre autres. Plusieurs entreprises ont réagi en chiffrant ce trafic C, mais le déchiffrement est l'une des activités principales de la NSA et du CSTC.

Si tout ça nous paraît plutôt éloigné de notre réalité quotidienne et plus proche de l'univers de James Bond ou de George Orwell, cette activité ésotérique a des effets parfaitement tangibles sur nos vies de citoyens ordinaires. Premièrement, la Loi antiterroriste du Canada donne pour mission au CSTC de seconder les activités de la police canadienne lorsque requis et sans que la moindre connexion au terrorisme soit nécessaire, ce qu'il fait approximativement une fois par jour. Deuxièmement, plusieurs lois ayant été introduites récemment font reposer l'activité policière sur les métadonnées industrielles portant sur le citoyen ordinaire. Le défunt projet de Loi sur la protection des enfants contre les cyberprédateurs (C-30), son successeur le projet de Loi sur la protection des Canadiens contre la cybercriminalité (C-13) et le projet de Loi sur la protection des renseignements personnels numériques (S-4) comportent tous des dispositions visant à faciliter les poursuites civiles ou criminelles de citoyens ayant commis des infractions qui sont à la fois généralisées dans le public et de gravité extrêmement faible (par exemple, l'échange de fichiers musicaux). Ce à quoi il faut ajouter les milliards dépensés en programmes qui dépassent de loin l'application de lois pénales, et qui incluent les infoguerres de propagande, la manipulation et la création frauduleuse de médias sociaux, et encore bien d'autres tactiques de la haute police du 21e siècle.



Dès 2003, Donald Rumsfeld, secrétaire de la Défense aux États-Unis signait un document qui lançait le nouveau programme d'opérations militaires en matière de guerre de l'information. On y soulignait déjà à quel point la manipulation de l'information sur Internet est un élément crucial d'un conflit et que celui qui y excelle détient un avantage décisif sur ses opposants. Dans un document récupéré par E. Snowden auprès d'un autre des partenaires des cinq yeux, le Government Communications Headquarters du Royaume-Uni, on découvre qu'une série d'opérations ont pour but explicite d'utiliser les médias sociaux, entre autres, pour manipuler l'opinion publique. Sachant cela, parlerons-nous toujours de « Révolution twitter »? Enfin, encore au niveau du citoyen lambda et plus particulièrement de celui qui se retrouve de temps à autre à traverser la frontière, notons que l'Agence des services frontaliers du Canada (douanes et immigration) a accédé en 2013 plus de 18 000 fois aux données d'usagers de services de téléphonie au Canada ...dont seulement 50 fois à l'aide d'un mandat judiciaire.

Ceci souligne un des aspects fondamentaux de la surveillance industrielle : bien qu'elle soit l'affaire d'entreprises privées qui visent des buts presque uniquement économiques, éventuellement le bassin total des informations collectées et générées est toujours disponible aux États et aux polices. Non pas qu'on doive y voir là le seul inconvénient. Évidemment, puisque la surveillance industrielle se manifeste souvent à nous à travers les offres alléchantes, la convivialité des applications et des contenus et la personnalisation du service, il est difficile d'en entrevoir la portée réelle. Seulement, comme sa capacité à modifier nos comportements se chiffre en milliards de dollars, il serait sans doute sage de s'y attarder d'un peu plus près. Du moins, avant que notre compréhension de la réalité, telle que produite par des systèmes de communication qui seront bientôt entièrement taillés sur mesure, rende cette position critique impossible à adopter, voire à imaginer.

L'infonuagique (Cloud Computing)

L'infonuagique repose sur l'utilisation de la puissance de calcul et de stockage de serveurs en réseau. Ces ordinateurs/serveurs sont loués, à la demande, aux utilisatrices et aux utilisateurs, individus ou entreprises, qui sont ainsi dispensés de posséder, entretenir et moderniser un parc informatique. Le « nuage » leur fournit la puissance informatique dont ils ont besoin. Les grandes compagnies comme Google, Microsoft, IBM et Apple qui sont capables de fournir un tel service à l'échelle planétaire en font la promotion. L'informatique en nuage a comme conséquence que l'usagère ou l'usager ne gère plus lui-même ses données – il ne sait même pas dans bien des cas où sur la planète elles sont stockées. L'avenir de l'infonuagique est compromis par les révélations d'Edward Snowden – les compagnies soucieuses de s'assurer de la protection de leurs données se demandant s'il ne serait pas plus sage de continuer de les traiter elles-mêmes. (NDRL : Dominique Peschard)

Informatique corporelle et surveillance

Les nouveaux enjeux de la médiation technologique auprès de soi

Louis Melançon, chercheur
Chaire de recherche du Canada sur les nouveaux environnements numériques et l'intermédiation culturelle (NENIC), Institut national de la recherche scientifique

Jonathan Roberge, directeur
Chaire de recherche du Canada sur les nouveaux environnements numériques et l'intermédiation culturelle (NENIC), Institut national de la recherche scientifique

« Ok Glass, take a picture ». Sergueï Brin, cofondateur de Google, venait de vivre une véritable épiphanie. Recevant un message texte lors d'un repas, il se rendit compte qu'il n'avait qu'à prononcer ces mots pour prendre un cliché et l'envoyer instantanément à son interlocuteur. Non seulement n'avait-il pas eu à sortir son téléphone de sa poche pour lire le message, il n'en avait pas eu besoin non plus pour y répondre. Constamment à l'affut, la frêle monture posée sur son nez et le petit écran flottant au-dessus de son œil droit l'avaient propulsé dans l'ère instantanée de la communication par les images. Ses lunettes Glass, la proposition la plus poussée de Google dans le domaine en pleine ébullition de l'informatique corporelle, l'avaient prétendument libéré de l'emprise de la technologie[1].

Cette promesse de l'informatique corporelle prend vie dans la mise en marché, en forte accélération ces derniers mois, d'une multitude de nouveaux « ordinateurs vêtements » ou « vêtements connectés » dont les lunettes Glass sont l'un des plus ambitieux précurseurs : dispositifs de géolocalisation, podomètres électroniques, montres intelligentes, etc. Tous sont situés si près du corps qu'ils s'effacent presque, témoins silencieux de nos moindres faits et gestes. Comment en sommes-nous arrivés à un tel engouement technologique? Quelles sont les conséquences de ce nouveau rapport computationnel à la corporéité et à l'expérience quotidienne? Causes et effets s'expliquent ici par une convergence particulière de facteurs techniques, économiques, politiques et sociaux donnant naissance aux nouvelles réalités de l'informatique corporelle, de la quantification de soi et des « données de masse » (big data).

L'industrie des données personnelles, Google en tête, voit dans les avancées technologiques actuelles l'occasion de doter d'une présence physique les algorithmes de traitement de données ayant fait sa grande fortune. À son moteur de recherche original, devenu depuis le principal point d'accès au web tout entier, est rapidement venu se greffer une multitude de services connexes — Gmail, Maps, Youtube — dont les données d'utilisation ont convergé dans l'élaboration de profils d'utilisatrices et d'utilisateurs hautement détaillés. Avec Glass, cette technologie traverse l'écran pour se connecter au corps humain. Dans un soudain renversement de situation, c'est l'appareil qui observe son utilisateur[2]. Avec des capteurs de mouvement, de géolocalisation, de son et d'images au niveau des yeux et des oreilles de ses usagers, Glass réussit à capter bien davantage que les requêtes de recherche. L'appareil gagne accès à l'ensemble de l'expérience de la personne.

Depuis les débuts de l'informatique corporelle dans les années soixante-dix, l'objectif principal de ces dispositifs a toujours été la prise en charge, sinon l'augmentation des sens. La vue et la mémoire en particulier se sont sans cesse vues amplifiées par de nouvelles capacités de captation, d'analyse et de stockage d'information multimédia. Aussi, pour la clientèle grandissante des appareils comme le pisteur d'activité physique Fitbit ou encore le téléphone Galaxy S5 et son capteur de fréquence cardiaque intégré, la quantification de soi représente aujourd'hui un nouvel outil en vue de l'accomplissement personnel. Support technique des aspirations au bonheur et à la santé, « self-help » d'une nouvelle génération de consommateurs, les « ordinateurs vêtements » promettent un idéal autonormé inspiré de la rigueur du calcul mathématique des machines.

L'utilisatrice ou l'utilisateur individuel de ces technologies, connecté en permanence au réseau, en fait désormais partie intégrante. L'environnement numérique devient à la fois mode de vie et cocon, à savoir que les vêtements connectés s'inscrivent dans le dispositif plus large appelé l'internet des objets : chaines stéréo, voitures, réfrigérateurs « intelligents », etc. Google, avec l'acquisition en janvier

1. Nick Bilton. Disruptions : Next Step for Technology Is Becoming the Background. *The New York Times Blogs*, 1er juillet 2012. Accessible au http://bits.blogs.nytimes.com/2012/07/01/google%E2%80%99s-project-glass-lets-technology-slip-into-the-background/

2. « *Wearable computing will free us from peering at life through a four-inch screen. We will no longer have to constantly look at our devices, but instead, these wearable devices will look back at us.* » Nick Bilton, ibid.

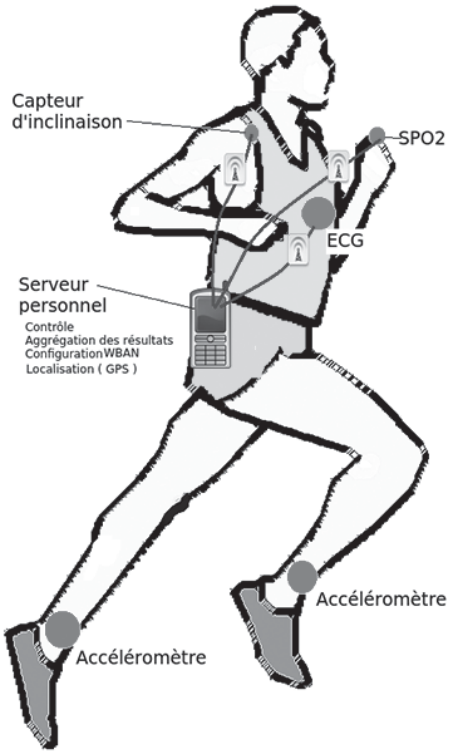
Avec Glass, cette technologie traverse l'écran pour se connecter au corps humain. Dans un soudain renversement de situation, c'est l'appareil qui observe son utilisateur.

dernier de la compagnie spécialisée en domotique Nest Labs pour la somme de 3,2 milliards de dollars, n'est pas en reste dans ce domaine non plus. L'informatique passe dans ce contexte d'une simple activité, confinée à une temporalité et à des objets bien définis, à un environnement complet à l'intérieur duquel on évolue à tout moment.

Cette position de médiation expérientielle dont tire parti Google pour fournir des réponses et afficher des publicités de plus en plus ciblées et personnalisées à ses usagères et usagers est fort convoitée, et pas uniquement pour sa valeur économique. Partout dans le monde, particulièrement chez nous au Canada et aux États-Unis, les agences de renseignement gouvernementales s'affairent à intercepter, analyser et stocker les données qui transitent sur les réseaux. Edward Snowden, ancien consultant pour la National Security Agency américaine, a révélé il y a déjà un an toute l'ampleur du système de surveillance en place, rendu possible entre autres par la sécurité déficiente des protocoles de communication actuels, et par l'étroite collaboration entre agences de renseignement nationales.

Nous en sommes au point où tout ce qui est fait par ordinateur est maintenant sauvegardé, corrélé, étudié et partagé, entre entreprises et entre agences gouvernementales, le plus souvent sans que nous en ayons connaissance ou que l'usagère ou l'usager n'y ait consenti[3]. Les conséquences pour la vie privée sont assurément importantes, et la croissance de l'informatique corporelle et de l'internet des objets, qui ne cessent d'alimenter les réseaux d'une quantité exponentielle de données personnelles, ne peut que contribuer à la détérioration de la situation. En effet, alors que l'activité informatique s'étend de la simple communication à l'ensemble des activités quotidiennes, les profils d'utilisateurs s'en voient considérablement étoffés — profils aussitôt accessibles à une surveillance systématisée alliant contrôle des populations et vigile des corps.

3. « *And welcome to a world where all of this, and everything else that you do or is done on a computer, is saved, correlated, studied, passed around from company to company without your knowledge or consent; and where the government accesses it at will without a warrant.* » Bruce Schneier, cryptographe américain et expert en sécurité informatique. https://www.schneier.com/blog/archives/2013/03/our_internet_su.html



http://fr.wikipedia.org

Plusieurs critiques de l'informatique corporelle redoutent que le déluge de données personnelles découlant de la commercialisation massive de dispositifs comme les lunettes Glass mène à de substantiels problèmes de discrimination. Après tout, n'est-ce pas l'objectif fondamental des données de masse que de classifier les individus, c'est-à-dire de les isoler dans des groupes distincts selon la prémisse qu'ils agissent de manière différente? Alors qu'on promet que ce nouveau créneau informatique est fondé sur des critères scientifiques et objectifs, une collecte et une analyse de données qui soit à l'abri des préjugés, plusieurs de ces projets nous indiquent déjà le contraire[4]. L'application mobile Ghetto Tracker (ce n'est pas une blague), renommée Good Part of Town après de virulentes critiques et finalement retirée du web peu longtemps après, se basait sur les évaluations de ses utilisateurs pour cartographier les villes américaines en « bons » et « mauvais » quartiers, question d'assurer la sécurité dans les transports. L'application Cloak, toujours en ligne celle-là, utilise les données de géolocalisation des réseaux sociaux pour permettre d'éviter certaines personnes dans ses déplacements. La reconnaissance faciale quant à elle, fonctionnalité faite sur mesure pour des appareils comme les lunettes Glass, est tout particulièrement appréhendée par les critiques de la nouvelle réalité interconnectée. Combinée à la reconnaissance vocale et aux vastes bases de données de Google par exemple, elle ouvrirait la voie à un accroissement important des capacités de surveillance ainsi qu'à l'accélération de la transformation fondamentale des liens et espaces sociaux déjà en cours.

Certains vont jusqu'à affirmer que notre seul recours contre la surveillance omniprésente et croissante est davantage de surveillance, dirigée cette fois vers les entreprises et gouvernements. Selon l'argumentaire, à la surveillance doit répondre la sousveillance, une surveillance citoyenne par le bas plutôt que par le haut[5]. Une caméra au visage de chaque citoyen comme avec les lunettes Glass, par exemple, permettrait de documenter les abus des plus puissants et d'organiser une résistance collective aux institutions gouvernementales et privées derrière la surveillance. Ainsi, le combat pour la protection de la vie privée se transforme en une lutte morale et politique sur le socle même de l'utilisation de ces technologies — ce qui n'est pas sans soulever plusieurs questions, voire susciter quelques paradoxes entre autres quant à l'abstraction faite des dynamiques de pouvoir et de la propriété des infrastructures technologiques en cause[6]. Pour les tenants de la sousveillance toujours, l'informatique corporelle devient un outil essentiel pour combattre le feu par le feu. Par exemple, empêcher ou même retarder l'adoption de technologies comme la reconnaissance faciale reviendrait à retirer le seul recours pour faire face à la surveillance; la même technologie qui rend possible la discrimination et le profilage systématisés permettrait également de documenter et de dénoncer ses abus.

En somme, l'informatique corporelle, la quantification de soi, l'internet des objets et les données de masse s'amalgament aujourd'hui pour promettre une transformation fondamentale des rapports sociaux qui n'est pas sans poser des défis majeurs pour la protection de la vie privée.

Ces avancées technologiques annoncent une amplification des modes régulatoires et des inclinaisons sociales déjà présentes, pour le meilleur et pour le pire. De manière individuelle, il n'y a pratiquement aucun recours pour répondre à ces problèmes. Les nouvelles technologies mettent en place une surveillance si vaste et omniprésente qu'il est pratiquement impossible de s'en préserver. De surcroit, une forte présence en ligne, sur les réseaux sociaux par exemple, est devenue pour plusieurs individus et institutions absolument essentielle : être absent de la Toile, c'est ne pas exister du tout. Les problématiques de surveillance et de vie privée, plus que jamais à l'ère des Google Glass et de l'internet des objets, doivent être abordées et résolues en tant que phénomènes sociopolitiques, à savoir qu'elles doivent être mieux comprises par le public et discutées davantage au sein des institutions démocratiques.

4. Kate Crawford. Think Again : Big Data. *Foreign Policy*, 9 mai 2013. http://www.foreignpolicy.com/articles/2013/05/09/think_again_big_data?page=full

5. Voir à ce sujet cet article de Steve Mann http://techland.time.com/2012/11/02/eye-am-a-camera-surveillance-and-sousveillance-in-the-glassage/

6. Voir cet article de Richard Stallman ainsi que les commentaires qui y sont liés. http://ieet.org/index.php/IEET/more/stallman20121208

Révélations Snowden sur la NSA

Roch Tassé, coordonnateur
Coalition pour la surveillance internationale des libertés civiles

Les révélations du dénonciateur Edward Snowden sur les activités d'espionnage de la National Security Agency (NSA) aux États-Unis et de ses quatre partenaires internationaux dans le club select des *Five Eyes*, incluant le *Centre de la sécurité des télécommunications du Canada* (CSTC), auront permis de lever le voile sur l'ampleur des méthodes et des pratiques secrètes déployées par ces agences afin de tout savoir sur tou-te-s.

Les documents secrets de la NSA remis par Snowden aux journalistes Glen Greenwald et Laura Poitras ont fait l'objet d'une série d'articles publiés à la pièce depuis juin 2013 par de grands médias, dont The Guardian et le Washington Post. En mars 2014 les deux quotidiens remportaient d'ailleurs le prestigieux prix Pulitzer pour « service rendu au public » en reconnaissance de la qualité de leurs reportages respectifs sur les activités de surveillance démesurées de la NSA et du débat public que cela a suscité à l'échelle mondiale.

Qu'avons-nous appris au fil de ces articles? Les documents analysés par Greenwald et Poitras mettent en lumière un projet élaboré et coordonné, des systèmes et programmes sophistiqués et omniprésents, et des méthodes illégales pour intercepter, conserver et analyser les données de transmission sur l'ensemble des communications du plus grand nombre possible d'individus, qu'ils soient étrangers ou citoyen-nes des États-Unis. On peut raisonnablement présumer que cela inclue les communications de millions de Canadien-ne-s.

Les programmes de la NSA visent, entre autres, les communications téléphoniques de tous genres, le clavardage, les courriels, les recherches internet, les transactions en ligne, ainsi que les photos et images affichées sur les médias sociaux ou circulant en temps réel sur Skype et « chat lines ». Dans certains cas, il est possible aussi d'obtenir simultanément les données de localisation des appareils utilisés. Lorsqu'on ajoute à cela d'autres mesures déjà en place pour assurer la cueillette de données biométriques et le partage des renseignements personnels des voyageuses et voyageurs, des immigrant-e-s et des personnes demandant l'asile, il y a lieu de croire que la NSA poursuit la réalisation du programme orwéllien connu sous le nom de *Total Information Awareness*.

Ce programme de surveillance globale et absolue, prôné et financé par le Pentagon dès 2001, fut aboli et interdit par le Congrès en 2003 parce qu'il constituait « une intrusion massive et injustifiée dans la vie privée des individus ». Le programme avait comme objectif de créer un fichier virtuel sur pratiquement l'ensemble de la population à partir de logiciels et programmes informatisés capables d'accéder à de multiples banques de données afin d'en faire la prospection. En croisant ces données, on peut tout savoir sur une personne, élaborer son profil, et reconstituer à posteriori les moindres détails sa vie. On peut comprendre la tentation pour un état et la police de vouloir se prévaloir de technologies rendant possible la réalisation d'un tel objectif.

Échelon

Échelon est un programme de collecte de renseignements mis en place au début des années 1970 par les Fives Eyes. Le but du programme est d'intercepter les communications mondiales sous toutes leurs formes, allant des conversations téléphoniques aux transmissions par satellites. Le public a pris connaissance de l'existence d'Échelon à la fin des années 1980, quand le programme a été élargi, entre autres pour l'interception des communications dans l'hémisphère sud. Malgré les efforts des États-Unis pour garder le programme secret, le Parlement européen publiait en 2001 un rapport officiel confirmant son existence comme programme global dédié à l'interception des communications privées et commerciales.

Un ex-employé de la NSA a révélé qu'Échelon était utilisé pour espionner des organisations non-gouvernementales comme Amnistie Internationale et Greenpeace.[1] Les lois de chaque pays limitent le pouvoir d'une agence d'espionner ses propres citoyen-ne-s, mais aucune n'empêche les agences des autres pays de le faire. Ainsi, le CSTC peut faire surveiller des canadien-ne-s par la NSA et recevoir ensuite les fruits de cette surveillance. (NDRL : Dominique Peschard)

1. http://digitalcommons.pace.edu/cgi/viewcontent.cgi?article=1202&context=pilr , p. 454

La NSA ... petit retour historique[1]

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, c'est une des agences les plus secrètes des États-Unis. Bien que créée le 4 novembre 1952, en pleine Guerre froide, son existence a seulement été reconnue officiellement en 1957.

1. Pour un historique plus complet, voir : La NSA à l'écoute du monde, bulletin de la LDL, automne 2009.

Five Eyes – les « Cinq yeux »

Les agences de renseignement des États-Unis, du Canada, du Royaume Uni, de l'Australie et de la Nouvelle Zélande forment le club de partage du renseignement le plus select au monde. Ces agences sont la *National Security Agency* NSA des États-Unis, le *Centre de la sécurité des télécommunications Canada* (CSTC), le *Government Communications Headquarter de Grande-Bretagne*, le *Defence Signals Directorate* australien et le *Government Communications Security Bureau* de Nouvelle-Zélande. Ce club est issu de la collaboration étroite entre les agences de renseignement des États-Unis et du Royaume-Uni pendant la Seconde Guerre mondiale, collaboration qui s'est maintenue à travers un accord secret après la guerre. Bien que chacune des agences fonctionne sous la gouverne d'un mandat national, elles interagissent avec une affinité renforcée par leur culture politique anglo-saxonne commune, des intérêts nationaux convergents et un sentiment de confiance réciproque extrêmement développé.

Les responsables des agences se rencontrent au moins une fois par an pour faire le bilan de leur travail et planifier les activités à venir. Les partenaires font de la collecte de renseignement sur des régions particulières du globe en fonction de leurs priorités nationales, mais leur travail de collecte et d'analyse est tellement orchestré qu'elles forment un corps intégré. (NDRL : Dominique Peschard)

À la fin de la Seconde Guerre mondiale, l'ancêtre de la NSA, la *Signal Security Agency*, avait réussi à obtenir que les quelques entreprises responsables du réseau de communication des États-Unis – 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 dirigeant-e-s 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 des personnes comme Joan Baez, Benjamin Spock, Jane Fonda et Martin Luther King, ainsi que des organisations non-gouvernementales comme Amnistie Internationale et Greenpeace.

Puis dans les années 1980 on apprenait l'existence du fameux programme *Échelon* (*voir encadré*) mis en place au début des années 1970 par les *Fives Eyes* (*voir encadré*) dans le but d'intercepter les communications mondiales sous toutes leurs formes, allant des conversations téléphoniques aux transmissions par satellite.

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 citoyen-ne-s américain-ne-s 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 États-Unis. Il semble qu'après l'adoption de la FISA, la NSA ait assez bien respecté l'obligation de ne pas espionner sans mandat les citoyen-ne-s américain-ne-s et les communications dont au moins un des pôles se trouvait aux États-Unis

La situation allait changer après le 11 septembre 2001. Dès octobre 2001, Georges-W Bush autorisait secrètement la NSA à espionner massivement les citoyens américains sans mandat de cour, en violation de la FISA, autorisation dévoilée par le New York Times en décembre 2005. 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 soldat-e-s américain-ne-s 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. Cette autorisation fut confirmée par Barack Obama au cours de son premier mandat.

C'est sur cette toile de fond que se sont déroulées et se poursuivent les activités de la NSA dénoncées dans les reportages du Guardian et du Washington Post au cours de la dernière année.

Ce qu'on a appris ....

Voici une liste partielle de ce qui a été divulgué dans la couverture de presse du Guardian et du Washington Post :

• La NSA peut espionner sur à peu près tout ce qu'un-e internaute fait sur Internet dans le cadre d'un programme nommé *XKeyscore* (*voir encadré*). Le programme permet en outre aux analystes d'accéder à des banques de données qui recueillent et classent en diverses catégories les activités sur Internet. La portée de *XKeyscore* couvre environ 150 points d'accès et plus de 700 serveurs à travers le monde.

• La NSA a eu l'aide de neuf grands fournisseurs de services comme Google, Yahoo, Facebook, YouTube, Apple et Microsoft - largement utilisés par les Canadien-ne-s – en se branchant directement aux serveurs de ces compagnies pour accéder à du contenu comme l'historique des recherches, les courriels, les transferts de fichiers, ou les registres de clavardage dans le cadre d'un programme appelé *PRISM* (*voir*

encadré). La nouvelle a mené à la révélation que l'agence partenaire de la NSA au Canada, le Centre de sécurité des télécommunications Canada, opérait également son propre programme d'écoute électronique, faisant la collecte des lieux et adresses des messages et des appels téléphoniques reliés aux communications étrangères.

• Un autre programme nommé *UPSTREAM* donne à la NSA un accès direct aux câbles de fibre optique à travers lesquels transitent la quasi-totalité des communications téléphoniques et Internet aux États-Unis. Cela inclue les câbles océaniques reliant l'Amérique du Nord au reste du monde. Puisque 98% des communications mondiales par Internet transitent par les États-Unis, ceux –ci sont potentiellement en mesure de cueillir des données sur pratiquement toutes les personnes qui utilisent un appareil de communication.

• Un programme baptisé *MUSCULAR* , mené avec l'homologue britannique de la NSA, le GCHQ, permet à ces deux agences de récupérer des données depuis les fibres optiques utilisées par les géants d'internet. Selon les documents Snowden, quelque 181 millions d'éléments auraient été collectés au cours du seul mois de janvier 2014 -- allant de métadonnées sur des courriels, à des éléments de texte ou des documents audio ou vidéo. Ces interceptions auraient lieu en dehors des États-Unis, grâce à un fournisseur d'accès télécoms dont le nom n'est pas révélé. Les autorités britanniques ont donné leur feu vert en 2007 pour que les données concernant les contacts téléphoniques, les liaisons Internet et les courriers électroniques des Britanniques puissent être archivés et analysés par la NSA. La NSA opère un autre programme à grande échelle qui lui permet de recueillir les métadonnées (*voir encadré*) téléphoniques de tou-te-s les abonnés de la compagnie Verizon, et on présume qu'elle a aussi des ententes avec AT&T et autres. Verizon remettrait quotidiennement à la NSA les relevés de dizaines de millions d'abonné-e-s. La NSA a donc pratiquement accès aux registres d'appels téléphoniques de tou-te-s les abonnés, peu importe le type d'appareil. Elle est aussi en mesure de stocker ces métadonnées indéfiniment et de les croiser avec d'autres banques de données.

XKeystore

XKeystore permet à la NSA d'avoir accès à peu près à tout ce qu'un-e internaute fait sur Internet. Snowden prétend qu'il pouvait, assis à son bureau, « intercepter les communications de quiconque, les vôtres, celles de votre comptable, d'un juge ou même du président, en sachant seulement l'adresse courriel de la personne ». mais les analystes de la NSA peuvent aussi mener leur recherche à partir d'un nom, d'un numéro de téléphone, de l'adresse IP, de mots clés, de la langue ou du moteur de recherche utilisés. XKeystore permet également d'avoir accès aux échanges sur les réseaux sociaux ou d'obtenir les adresses IP de toutes les personnes qui visitent un site Internet.

La masse de communications auxquelles *XKeystone* donne accès est époustouflante. Un document de la NSA datant de 2007 fait état de 850 milliards de « données d'appel » et de 150 milliards de fichiers Internet; la banque s'enrichissant de un à deux milliards de fiches quotidiennement. Plus récemment, William Binney, un ancien mathématicien de la NSA, évaluait le nombre de données de communication que la NSA détenait sur les citoyens des É-U à 20 trillions. Les analystes de la NSA ont accès à ces énormes banques de données sans avoir à obtenir une autorisation judiciaire ou même l'accord d'un supérieur.

XKeystore collecte tellement d'information que celle-ci peut seulement être conservée pour une période de temps limité, soit 3 ou 4 jours – 30 jours pour les métadonnées. Un autre programme de la NSA, PRISM, permet de palier à ce problème. (NDRL : Dominique Peschard)

PRISM

Avec *PRISM*, la NSA et le FBI ont accès aux données de Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube et Apple. Ce programme permettrait de se connecter directement aux serveurs de ces compagnies, sans leur consentement, et d'avoir accès en temps réel aux courriels, photos, fichiers, contenu des communications, informations sur les réseaux sociaux et connexions à certains sites. Étant donné que les géants de l'Internet conservent l'historique des activités de leurs utilisateurs, PRISM permet également de scruter les activités passées d'une personne. (NDRL : Dominique Peschard)

• La NSA intercepte les données de localisation de centaines de millions de téléphones portables dans le monde. Les documents Snowden indiquent que l'agence est capable de suivre des personnes à la trace grâce à leur portable, même quand celui-ci n'est pas utilisé. L'agence stocke des informations sur au moins des centaines de millions d'appareils et enregistre près de 5 milliards de données de localisation par jour. L'agence peut ainsi suivre des individus, où qu'ils se déplacent dans le monde – y inclus les lieux de résidence –,et peux même retracer leurs voyages précédents.

• Les services de renseignement britanniques et américains ont décodé avec succès une grande partie du cryptage en ligne utilisé par des centaines de millions de personnes dans le but de protéger la confidentialité de leurs données personnelles, de leurs transactions en ligne et de leurs courriels. Grâce à des partenariats secrets avec des sociétés de technologie et des fournisseurs de services internet, les agences ont inséré des vulnérabilités secrètes - connues sous le nom de portes arrières ou de trappes - dans des logiciels de cryptage commerciaux. Des experts en sécurité ont accusé les agences d'attaquer l'internet lui-même et la vie privée de toutes les personnes qui s'en servent. Avec son expertise, le CSTC au

Canada aurait joué un rôle primordial dans le développement de ces vulnérabilités.

• La NSA a les moyens techniques d'enregistrer l'ensemble des appels téléphoniques passés depuis un pays et de décrypter ces conversations 30 jours après qu'elles aient eu lieu. Le programme, surnommé MYSTIC, a été lancé en 2009 et a atteint sa pleine capacité en 2011. L'un des outils du programme permet de « récupérer des enregistrements qui ne paraissaient pas dignes d'intérêt au moment de l'appel original », selon des documents officiels.

• La NSA se livre au « mapping » de réseaux sociaux en procédant à la collecte de centaines de millions de listes de contacts par l'intermédiaire de courriels ou de messageries instantanées, dont certaines pourraient appartenir à des citoyen-ne-s américain-ne-s. En une seule journée en 2012, la NSA a intercepté 444 743 listes de contacts provenant de comptes Yahoo!, 105 068 de comptes Hotmail, 82 857 de comptes Facebook, 33 697 de comptes G-mail, et 22 881 d'autres fournisseurs d'accès, selon les informations contenues dans une présentation PowerPoint de l'agence. Extrapolés sur une année, ces chiffres correspondraient à la collecte de 250 millions de listes de contacts courriels par an. Des dizaines de millions d'Américain-ne-s sont concernés par cette collecte, et sans doute aussi un grand nombre de Canadien-ne-s.

• Un mémo interne de la NSA, rédigé en 2005, révèle que l'agence avait l'intention d'espionner unilatéralement les Canadien-ne-s sans le consentement du CSTC. L'opération aurait ciblé les citoyen-ne-s et les systèmes de communication du Canada et de l'Australie. Le memo stipulait que la NSA pouvait espionner ses partenaires du « Five Eyes » même quand un gouvernement ami leur interdisait explicitement de le faire. Le mémo est également clair au sujet de ne pas informer les pays partenaires de ces activités.

G20 à Toronto

• Le Canada a donné son feu vert à une vaste opération américaine de surveillance des communications lors du sommet du G20 à Toronto, en 2010. L'ambassade américaine à Ottawa est devenue pendant une semaine le centre de contrôle d'une opération d'espionnage menée par les États-Unis, mais cautionnée par le Canada et étroitement coordonnée avec le CSTC.

Espionnage politique et industriel

• La NSA a espionné les communications du Secrétaire Général des Nations-Unies et d'une trentaine de chefs d'État, y inclus les présidentes de l'Allemagne et du Brésil ainsi que plusieurs partenaires européens.

Métadonnées

Les métadonnées sont, littéralement, les données sur les données. En matière de communication électronique ce sont toutes les données sur le message, à l'exclusion du contenu du message. Cela comprend les données sur l'expéditeur et le récipiendaire, l'heure à laquelle le message a été envoyé et la durée de la communication, y inclus les transactions électroniques, les consultations de sites internet, les communications téléphoniques.

Les gouvernements et les agences de renseignement tentent de minimiser le caractère privé de ces informations en arguant que seul le contenu du message mérite d'être protégé. Pourtant, à une époque où tout ce que nous faisons laisse une trace électronique, ces données sont une mine d'or pour les agences de renseignement. Les métadonnées dévoilent nos champs d'intérêt, nos réseaux sociaux, nos habitudes de consommation, de voyage... C'est en passant au crible les métadonnées de populations entières que les agences déterminent quelles sont les personnes qui doivent être surveillées plus étroitement avec des outils plus pointus comme XKeyscore et PRISM. (NDRL : Dominique Peschard)

Conclusion

Si certains croient exagéré de conclure que les programmes et activités exposés dans les documents divulgués par Edward Snowden constituent la preuve que le projet de Total Information Awareness est encore bien vivant, les révélations confirment pourtant la portée apparemment sans limite, l'ampleur massive et la légalité douteuse des opérations d'espionnage de la NSA et de ses partenaires. Il faut aussi reconnaître que chacune des activités et des programmes révélés constitue une pièce maîtresse et indispensable de l'architecture globale de TIF. Big Brother est déchaîné. Il est grand temps de le mettre sous surveillance.

Que savons-nous des activités du CSTC?

Anne Dagenais Guertin, coordonnatrice, recherche et communications
Coalition pour la surveillance internationale des libertés civiles

Le Centre de la sécurité des télécommunications Canada (CSTC)

Le CSTC est l'agence civile de cryptologie du Canada, chargée à la fois du renseignement et de la protection de l'information pour le gouvernement canadien. C'est la contre partie canadienne de la *National Security Agency* des États-Unis.

L'agence d'espionnage a été créée en 1946 par un décret en Conseil en amalgamant deux agences de renseignement issues de la Seconde Guerre mondiale, l'une civile, la Sous-section de l'examen et l'autre, militaire, la *Joint Discrimination Unit*, pour former la Direction des télécommunications du Conseil national de recherches (DTCNR).

En 1975, la DTCNR devenait le CSTC dont le mandat était transféré au Ministère de la Défense nationale. Le CSTC est mentionné pour la première fois dans une loi du Canada dans le cadre d'un amendement apporté à la Loi sur la défense nationale lors de l'adoption de la Loi anti-terroriste de 2001.

Le budget du CSTC est passé d'environ 100 millions de dollars en 1999 à 461 millions de dollars en 2013. Les dépenses liées au renseignement continuent d'augmenter alors que la menace terroriste semble diminuer.[1] Les prévisions déposées au Parlement indiquent que le budget du CSTC doublera presque en 2014-2015 pour atteindre 829 millions $. Le CSTC emploie plus de 2000 personnes, dont presque la moitié est impliquée dans l'interception de conversations téléphoniques et l'infiltration de systèmes informatiques.

Les révélations sur le CSTC

10 juin 2013 Un article du Globe and Mail révèle que le CSTC a recueilli les métadonnées des Canadien-nes après que le ministre de la Défense, Peter MacKay, ait signé une directive ministérielle en novembre 2011 autorisant le redémarrage d'un « programme d'écoute électronique secret qui parcourt les enregistrements téléphoniques mondiaux et les données Internet - y compris ceux des Canadien-nes - à la recherche d'activités suspectes. »

11 septembre 2013 On apprend que le CSTC est responsable de la création, en 2006, d'une norme ou clé de cryptage utilisée à l'échelle mondiale par les banques, les entreprises privées, les particuliers et les gouvernements pour protéger

Bill Clennett

Le nouveau quartier général du CSTC, situé en banlieue d'Ottawa, coûtera près de 1.2 milliards de dollars. Il s'agirait de l'édifice gouvernemental le plus coûteux au Canada.

les données sensibles stockées sur le Web, mais que le CSTC a permis à la NSA de « prendre le contrôle » du processus et de créer une « porte arrière » pour accéder aux données qui devaient être protégées par le cryptage. À la lumière des récentes révélations sur la faille de sécurité Heartbleed, affectant le logiciel de cryptage OpenSSL – et qui aurait été exploitée par la NSA depuis deux ans afin d'amasser des données – nous sommes en droit de nous demander si cette faille n'est pas liée à cette « porte arrière », ou même le produit de sa création par la NSA et si le CSTC a également exploité cette faille pour espionner les Canadien-nes[2].

5 octobre 2013 La chaîne de télévision brésilienne Globo révèle que le CSTC a espionné des ordinateurs et téléphones intelligents associés au ministère des Mines et de l'Énergie du Brésil, en 2012, dans l'espoir de recueillir des renseignements économiques.

29 octobre 2013 Une nouvelle fuite suggère que le Canada utilise, de concert avec les États-Unis, une vingtaine de ses ambassades à l'étranger pour des opérations d'écoute électronique clandestines. Un document obtenu par Snowden révèle que le nom de code du programme est « Stateroom », mais n'indique pas les emplacements des postes d'écoute présumés[3]. Thomas Drake, un ancien dirigeant de la NSA devenu dénonciateur, dit ne pas être surpris par cette révélation : « Il suffit de penser à certains accords ou relations étrangères que le Canada entretient, mais dont les États-Unis ne font pas partie, et sous le couvert de ces relations, devinez ce que vous pouvez faire? Ce type d'efforts de surveillance ou de collecte secrète. » Drake dit avoir travaillé avec le CSTC sur

1. http://www.theglobeandmail.com/news/politics/how-csec-became-an-electronic-spying-giant/article15699694/?page=all

2. http://www.bloomberg.com/news/2014-04-11/nsa-said-to-have-used-heartbleed-bug-exposing-consumers.html

3. http://www.theglobeandmail.com/news/world/canada-involved-in-us-spying-efforts-abroad-leaked-document-says/article15133508/

divers projets, alors qu'il était à la NSA, et que les Canadiens étaient « extraordinairement capables[4]. »

25 novembre 2013 La Cour fédérale réprimande le Service canadien du renseignement de sécurité (SCRS) pour l'utilisation du réseau Five Eyes dans la surveillance des communications de Canadiens soupçonnés de « terrorisme » au cours de voyages à l'étranger. Dans un résumé de la décision classifiée, le juge Richard Mosley affirme que le SCRS a « manqué à son devoir de franchise » à la cour en omettant de divulguer cette pratique. En janvier 2009, la Cour fédérale avait émis un mandat autorisant le SCRS à exploiter les capacités d'écoute du CSTC pour espionner deux Canadiens pendant qu'ils étaient à l'étranger, mais n'avait pas été informée que d'autres membres des Five Eyes allaient participer à l'interception de leurs communications[5].

27 novembre 2013 On apprend que le CSTC a autorisé la NSA à espionner les leaders mondiaux en sol canadien lors du sommet du G20 à Toronto en juin 2010 afin de procurer un avantage dans les négociations aux États-Unis et d'appuyer leurs objectifs politiques. De plus, la partie du document consacrée aux détails de sécurité du sommet met l'accent, non pas sur la menace terroriste, mais sur la possibilité d'actes de vandalisme commis par des « extrémistes d'origine intérieure militant pour des causes précises ». Suite aux arrestations massives et sans précédent survenues lors du sommet, les services de police ont été accusés de violations graves des droits civils[6].

30 novembre 2013 Des documents obtenus par le Globe and Mail révèlent que le 15 mars 2004 – trois jours après que le programme de surveillance globale de la NSA fut freiné par le Président George W. Bush suite à la menace de démission de hauts responsables des services de police après qu'ils aient appris l'existence de ce programme – Ottawa signait une « autorisation ministérielle » pour un programme canadien de collecte de métadonnées. Le Globe a pris connaissance de l'existence de ce programme dans un document lourdement censuré obtenu en vertu de la Loi sur l'accès à l'information. Près d'une décennie plus tard, personne ne veut parler du programme. « Même si je me souvenais des détails, je ne pourrais pas en parler », a déclaré David Pratt, l'ancien ministre libéral de la Défense qui a signé le document.

L'expérience de tracking dans un aéroport

Le 30 janvier 2014, la CBC publie un document top secret obtenu par Edward Snowden, datant de mai 2012, qui démontre que le CSTC a recueilli pendant deux semaines des informations dans un grand aéroport canadien, grâce à l'accès internet gratuit (le Wi-Fi), afin de suivre à la trace les appareils mobiles de milliers de passagers ordinaires pour une semaine ou plus après qu'ils aient quitté l'aéroport. Le document montre que l'agence pouvait suivre les voyageurs lorsqu'ils – et leurs appareils mobiles – apparaissaient à d'autres points publics d'accès Internet gratuit à travers le Canada, y compris hôtels, cafés, restaurants, bibliothèques, stations de transport public, etc., et même dans les aéroports américains. Le CSTC avait tellement d'information qu'il pouvait même retracer les mouvements des voyageurs pour plusieurs jours *avant* leur arrivée à l'aéroport. Ronald Deibert, un éminent expert canadien en cybersécurité, a affirmé à la CBC qu'il ne voyait « aucune circonstance dans laquelle ceci ne serait pas illégal, en vertu de la loi canadienne, de notre Charte, et des mandats du CSTC. »

Le CSTC a affirmé dans une déclaration écrite à la CBC qu'il est « légalement autorisé à recueillir et analyser des métadonnées », et « qu'aucune communication canadienne n'a été (ou n'est) ciblée, recueillie ou utilisée. » En résumé, le CSTC affirme que, puisqu'il n'a recueilli que les métadonnées des passagers de l'aéroport, il n'a donc pas espionné les communications de ces individus (ce qui est illégal).

Le document indique aussi que l'opération de suivi des passagers avait pour but de mettre à l'essai un nouveau et puissant logiciel que le CSTC aurait développé avec l'aide de son homologue américain, la NSA. Dans le document, le CSTC affirme que la nouvelle technologie pourrait être utilisée afin de suivre « toute cible faisant des incursions occasionnelles dans d'autres villes/régions. » Des sources ont dit à la CBC que les technologies testées sur les Canadiens en 2012 sont depuis devenues entièrement opérationnelles.

Le document ne dit pas exactement comment le service d'espionnage canadien a réussi à mettre la main sur deux semaines de données sans fil du système Wi-Fi de l'aéroport, mais il y a des indications qu'elles auraient été fournies volontairement par une « source particulière ». Le document n'explique pas non plus comment le CSTC a réussi à pénétrer autant de systèmes d'accès Internet sans fil pour voir qui les utilisait, en particulier, comment il savait que quelqu'un ciblé à l'aéroport apparaissait sur un autre point d'Internet sans fil ailleurs. Deibert et d'autres experts s'entendent pour dire que le CSTC doit avoir obtenu un accès direct à au moins certains des principaux câbles de téléphone et d'Internet du pays, permettant ainsi la surveillance de masse des courriels et des appels téléphoniques canadiens.

Le document indique clairement que le CSTC visait à partager à la fois les technologies et l'information générée par celles-ci avec ses partenaires du réseau Five Eyes.

La Commissaire à la vie privée de l'Ontario, Ann Cavoukian, a dit être « renversée » par les révélations. « Il est vraiment incroyable que le CSTC soit engagé dans ce genre de surveillance des Canadiens. [...] Cela ressemble aux activités d'un État totalitaire, pas d'une société libre et ouverte. »[7]

4. http://www.cbc.ca/news/politics/snowden-document-shows-canada-set-up-spy-posts-for-nsa-1.2456886

5. http://www.thestar.com/business/2014/01/03/csis_should_be_subject_of_independent_investigation_geist.html

6. http://www.cbc.ca/news/politics/new-snowden-docs-show-u-s-spied-during-g20-in-toronto-1.2442448

7. http://www.cbc.ca/news/politics/csec-used-airport-wi-fi-to-track-canadian-travellers-edward-snowden-documents-1.2517881

Riposte juridique de BCCLA, FIDH, ACLU

Les autorités accusées d'agir illégalement

Dominique Peschard, président
Ligue des droits et libertés

Campagne de la BCCLA

Au Canada : La *British Columbia Civil liberties Association* (BCCLA) poursuit le CSTC pour espionnage illégal

Le 22 octobre 2013, la *British Columbia Civil liberties Association* (BCCLA) a intenté une poursuite contre le Centre de la sécurité des télécommunications Canada (CSTC). La poursuite conteste la constitutionnalité de la surveillance secrète et sans balises des canadien-ne-s de la part du CSTC. Cette poursuite est une première au Canada.

La Loi sur la défense nationale, amendée par la Loi antiterroriste de 2001, permet d'intercepter le contenu des communications de canadien-ne-s avec une personne à l'étranger, sur simple autorisation ministérielle, sans contrôle judiciaire. Ces autorisations sont vagues, valables pour douze mois et peuvent être renouvelées indéfiniment. De plus, une directive ministérielle de 2005, renouvelée en 2011, permet au CSTC de collecter les métadonnées sur les communications des canadiens. Comment le CSTC partage cette information avec ses partenaires du *Five Eyes* est également secret.

Cette poursuite a pour but de forcer le gouvernement à dévoiler qui sont les cibles de cet espionnage, quelle information est récoltée et quelle utilisation est faite de cette information. Elle vise à ce que soient mis en place les mécanismes nécessaires pour protéger la vie privée des canadiens.

En France : Plainte de la Fédération internationale des droits de l'homme (FIDH) et de la Ligue de droits de l'homme (LDH) de France

Le 1er juillet 2013, la FIDH et la LDH ont porté plainte auprès de Monsieur le Procureur de la République près le Tribunal de grande instance de Paris pour les gestes illégaux posés par les agences de renseignement des États-Unis à l'égard de citoyen-ne-s français et des associations requérantes.

Selon la FIDH et la LDH les éléments factuels révélés par Edward Snowden sont constitutifs de plusieurs infractions imputables d'une part à la NSA et au FBI comme auteurs principaux et, d'autre part, aux sociétés Microsoft, Yahoo, Google, Paltalk, Facebook, Youtube, Skype, AOL et Apple comme d'éventuels complices. En vertu du droit français, les infractions pénales commises sont :

- Infraction relative à l'accès et au maintien frauduleux dans tout ou partie d'un système de traitement automatisé de données;
- Infraction relative à la collecte frauduleuse de données personnelles;
- Infraction relative à l'atteinte à l'intimité de la vie privée d'autrui;
- Infraction relative à l'utilisation et la conservation d'enregistrements et de documents obtenus par le moyen d'une atteinte à l'intimité de la vie privée d'autrui;
- Infraction relative à l'atteinte au secret des correspondances électroniques.

La FIDH et la LDH considèrent indispensable et nécessaire qu'une information judiciaire, ou à tout le moins une enquête préliminaire soit diligentée, afin de caractériser les infractions dénoncées.

Aux États-Unis : L'*American Civil Liberties Union* (ACLU) conteste la constitutionnalité de la collecte de métadonnées par la NSA

En janvier 2014, l'ACLU a déposé une poursuite en cour contestant la constitutionnalité de la collecte des métadonnées sur les appels téléphoniques des américain-ne-s. L'ACLU considère que la collecte massive de ces informations viole le droit à la vie privée protégé par le 4è amendement ainsi que la liberté d'expression et le droit d'association protégés par le 1er amendement de la Constitution des États-Unis. La plainte soutient que le programme de collecte de données excède les pouvoirs accordés par le Congrès des États-Unis dans le *Patriot Act*. La poursuite vise à mettre fin à l'espionnage domestique de masse et à faire détruire les informations colligées.

L'ACLU n'en est pas à sa première action judiciaire. Une poursuite précédente initiée en 2008 a été rejetée en février 2013 par la Cour suprême des États-Unis à 5 juges contre 4. Les juges ont invoqué le fait que les plaignant-e-s ne pouvaient pas démontrer qu'ils avaient été espionnés. Cette fois les documents révélés par Snowden montrent que la compagnie de téléphone Verizon, dont l'ACLU est un client, remet toutes les données d'appel de ses client-e-s.

Surveiller la dissidence : le modèle de Miami au G20 de Toronto

Kate Milberry, PhD
Faculté de l'Éducation permanente, Université de l'Alberta

Andrew Clement, professeur
Faculté des sciences de l'information, Université de Toronto

Traduction : **Christine Renaud**

Introduction

La surveillance, ce n'est rien de nouveau : c'est une caractéristique essentielle de la transition vers la modernité qui augmente en importance et en sophistication avec l'évolution de la gouvernance bureaucratique (Foucault, 2004)[1] . La montée de la « société de la surveillance » a précédé l'ère numérique et elle parvient à son apogée avec l'intégration de l'internet dans la vie quotidienne. La collecte, le stockage et l'extraction de renseignements personnels, pratiqués par les gouvernements par le piratage d'ordinateurs et les logiciels d'espionnage, ont des implications troublantes. Cette nouvelle réalité de l'omniprésence de la surveillance en ligne soulève des questions urgentes autour du pouvoir politique, du contrôle social, des libertés et de la démocratie. Les dissident-e-s politiques, notamment, font l'objet d'une surveillance et d'une répression accrues de la part de l'État. Avec la naissance des mouvements sociaux reliés via l'internet, tels que le mouvement pour la justice mondiale et, plus récemment, le printemps arabe, le mouvement Occupy et le printemps érable, les militant-e-s découvrent l'internet comme un espace et un outil de libération mais aussi comme un terrain surveillé. Cet article examine l'évolution du modèle de Miami, à travers son application au contrôle des méga-manifestations, en explorant les différents modes de surveillance déployés par les gouvernements afin d'ébranler et de contenir les mouvements sociaux et les dissident-e-s politiques, ainsi que la résistance à la surveillance permanente de l'État.

L'émergence des mouvements sociaux reliés via l'internet

Historiquement, l'activité principale des « agents de contrôle » des mouvements sociaux consistait à recueillir des renseignements à l'aide de techniques incluant la subversion, l'espionnage, le harcèlement et le contre-espionnage (Marx, 1979). Les progrès technologiques – notamment l'informatisation et la numérisation – ont rendu ces techniques de plus en plus sophistiquées. Avec l'éruption du mouvement pour la justice mondiale lors des manifestations de masse contre la réunion de l'Organisation mondiale du commerce à Seattle en 1999, on a assisté à un changement majeur dans le jeu de surveillance du chat et de la souris. Les organismes d'application de la loi se sont mobilisés pour faire face aux nouveaux mouvements sociaux « reliés via l'internet » et leur nouveau mode d'organisation, largement facilité par l'internet et la téléphonie mobile.

Les experts en sécurité nationale ont scruté de près le mouvement pour la justice mondiale, notamment ses relations avec l'internet et son utilisation. Le Service canadien du renseignement de sécurité (SCRS) a identifié l'internet comme essentiel pour la réussite du mouvement et comme « une source principale de planification et d'encouragement à protester » et a recommandé « de surveiller les communications des protestataires » (SCRS 2000). Il ne fait aucun doute que l'internet a renforcé le « répertoire de la contestation » militante, en lui fournissant de nouveaux modes de communication, de collaboration, d'éducation et d'agitation. Mais il a aussi ouvert de nouvelles avenues pour la collecte de renseignements, telles que la surveillance en ligne des sites Web militants et des comptes sur les médias sociaux ainsi que le repérage des militants en ligne via des techniques telles que l'analyse de trafic sur les réseaux.

Répression étatique des mouvements de justice sociale après le 11 septembre

Les attaques terroristes du 11 septembre 2001 à New York ont eu un effet dévastateur sur les libertés civiles et le militantisme pour la justice sociale. Le *Patriot Act* des États-Unis a facilité la surveillance des activités sur l'internet par les organismes d'application de la loi tandis que le *Homeland Security Act* a réduit les restrictions qui entouraient la communication de renseignements sur leurs clients par les fournisseurs d'accès à l'internet.

1. Les références complètes sont disponibles dans la version en ligne sur notre site à l'adresse suivante : http://liguedesdroits.ca/?p=2078.

Avec le coût personnel croissant du fait de manifester, incluant les blessures corporelles, les arrestations, les procès et les peines d'emprisonnement, ces facteurs ont contribué au recul et à l'effondrement apparent du mouvement pour la justice sociale. Ce n'était pas une coïncidence mais en partie le résultat d'une méthode émergente de contrôle des manifestations, appelée le modèle de Miami.

La définition du terrorisme s'est trouvée élargie par l'usage d'un langage « si vague que la désobéissance civile répond aux critères » (Potter 2009, 37). Les agences de sécurité ont réorienté leurs efforts de la scène internationale vers la scène intérieure, délaissant les criminel-le-s conventionnels pour les personnes soupçonnées de terrorisme. Ce recentrage a mené à un recodage des « identités terroristes », du terrorisme de style 11 septembre vers un « extrémisme » à motivation idéologique qui englobe une vaste gamme de mouvements sociaux, incluant l'antimondialisation, la protection de l'environnement, les autochtones, la paix et la justice sociale (Monaghan et Walby 2012). Parallèlement à cette redéfinition du terrorisme intérieur, les forces de l'ordre sont devenues plus agressives dans les grandes manifestations. Avec le coût personnel croissant du fait de manifester, incluant les blessures corporelles, les arrestations, les procès et les peines d'emprisonnement, ces facteurs ont contribué au recul et à l'effondrement apparent du mouvement pour la justice sociale. Ce n'était pas une coïncidence mais en partie le résultat d'une méthode émergente de contrôle des manifestations, appelée le modèle de Miami.

Le contrôle policier des méga-manifestations et le modèle de Miami

Le modèle de Miami a été une réponse aux mouvements sociaux reliés via l'internet et à leur nouveau mode d'organisation – virtuel, mobile et insensible aux anciens obstacles du temps, de l'espace et du coût. Le maintien de l'ordre lors de méga-événements fournit l'occasion de présenter de nouvelles technologies de surveillance et de développer de nouvelles techniques connexes de contrôle social.

Les « méga-manifestations » caractérisent le mouvement pour la justice sociale depuis ses débuts. Elles ont lieu souvent pendant des méga-événements, notamment lors de sommets économiques mondiaux organisés par des instances supranationales comme l'OMC, le Fonds monétaire international et le Groupe des 8/Groupe des 20 (G8/G20). Ces sommets attirent des milliers de manifestant-e-s unis dans leur opposition aux programmes d'austérité économique. Ces méga-manifestations impliquent des défilés de masse dans les rues, de l'action directe et parfois du vandalisme de biens corporatifs – style Black Block. Les techniques de contrôle des grandes manifestations diffèrent de l'intervention policière traditionnelle et se retrouvent toutes dans le modèle de Miami.

Ce modèle, identifié pour la première fois au Sommet de la zone de libre-échange des Amériques, à Miami en 2003, comporte un style de commandement et de contrôle des forces policières qui « utilise des niveaux élevés de confrontation et de force pour des infractions même mineures »… (Vitale 2005, 287). Les principaux objectifs du modèle de Miami sont la perturbation de l'activité du mouvement social et le contrôle policier de l'espace public. Les fondements et la caractéristique distinctive de ce mode de contrôle policier, c'est la surveillance. Ses autres attributs incluent un appareil de sécurité massif, une militarisation de la ville et des alliances temporaires entre les organismes de maintien de l'ordre. La

Affiche de mobilisation contre le G-20 à Toronto.
Les agences de sécurité ont réorienté leurs efforts de la scène internationale vers la scène intérieure, délaissant les criminel-le-s conventionnels pour (…) une vaste gamme de mouvements sociaux, incluant l'antimondialisation, la protection de l'environnement, les autochtones, la paix et la justice sociale.

Photo : J_P_D - https://creativecommons.org

Un aspect important du modèle de Miami réside aussi dans son rôle pédagogique public; il utilise l'intimidation pour inculquer que la dissidence est dangereuse.

combinaison visuellement dramatique de ces divers éléments tend à créer un cirque de la sécurité - un déploiement public palliatif de puissance militaire et de prouesse technique, destiné davantage à donner un « sentiment de sécurité plutôt que la réalité [de la sécurité] » (Schneier 2003, 38). Un aspect important du modèle de Miami réside aussi dans son rôle pédagogique public; il utilise l'intimidation pour inculquer que la dissidence est dangereuse.

Le quatrième Sommet du G20 : Sécuriser la forteresse Toronto

Au Canada, les organismes de maintien de l'ordre avaient acquis de l'expérience dans le contrôle policier des méga-manifestations lors des mobilisations massives contre l'Organisation des États américains à Windsor, Ontario, en 2000; la Zone de libre-échange des Amériques à Québec, en 2001 et la réunion du G8 à Kananaskis, Alberta, en 2002. Les Jeux olympiques de Vancouver ont fourni la première occasion de déployer toutes les composantes du modèle de Miami. La principale évolution par rapport au contrôle des méga-événements antérieurs a été l'intégration sans précédent des organismes d'application de la loi, avec la création du Groupe intégré de la sécurité (GIS). Le GIS de Vancouver était une initiative fédérale, dirigée par la Gendarmerie Royale du Canada (GRC), impliquant le SCRS, les Forces canadiennes, plus d'une centaine de corps policiers municipaux et au moins une dizaine de ministères fédéraux (Molnar et Snider 2011).

Le GIS a pu bénéficier des enseignements tirés et du personnel formé dans le cadre des Jeux olympiques, pour préparer le Sommet du G20 à Toronto (Levitz 2009). Décrite comme la « forteresse Toronto », la ville-hôte du quatrième Sommet du G20 a fourni l'occasion de démontrer et de perfectionner le contrôle policier des méga-manifestations. Toronto est devenue le site de la plus grande opération de sécurité dans l'histoire du Canada. Le dispositif de sécurité comprenait de nouvelles caméras de vidéosurveillance; 10 km de clôtures de sécurité et 20 000 policières et policiers, militaires et agent-e-s de sécurité privés (Bureau du vérificateur général du Canada, 2011) L'opération de sécurité, dirigée par le GIS du G20, a impliqué 26 services de police.

Comme lors des Jeux olympiques de Vancouver, il n'y a eu aucune atteinte grave à la sécurité lors du G20 de Toronto. Néanmoins, « des niveaux élevés de confrontation et de force » - une caractéristique du modèle de Miami – ont été appliqués durant toute la fin de semaine du sommet qui a été marquée par des niveaux de brutalité policière sans précédent. La violence qui a éclaté dans les rues du centre-ville de Toronto a été largement provoquée par les membres du Service de police de Toronto. Parmi les exemples les plus flagrants d'agression et de brutalité policière figurent l'attaque surprise des manifestant-e-s regroupés pacifiquement dans la zone désignée pour les manifestations à Queen's Park; l'encerclement de manifestant-e-s pacifistes dans divers endroits de la ville; l'arrestation violente de plusieurs manifestant-e-s qui a causé des blessures physiques graves. Il y a eu des arrestations préventives de militant-e-s bien connus et des arrestations massives de militant-e-s logés par le syndicat des étudiant-e-s diplômés de l'Université de Toronto et au centre de rassemblement des militant-e-s. Au total, plus de 1 100 personnes ont été arrêtées lors de la plus grande arrestation de masse que le Canada n'ait jamais connue en temps de paix.

Comme lors des Jeux olympiques de Vancouver, il n'y a eu aucune atteinte grave à la sécurité lors du G20 de Toronto. Néanmoins, « des niveaux élevés de confrontation et de force » - une caractéristique du modèle de Miami – ont été appliqués durant toute la fin de semaine du sommet qui a été marquée par des niveaux de brutalité policière sans précédent.

Selon l'Association canadienne des libertés civiles (2011), la répression durant la fin de semaine du G20 a été « sans précédent, disproportionnée et, par moments, inconstitutionnelle » (4). Elle a entraîné « la pire attaque à l'endroit des libertés civiles de l'histoire du Canada », selon André Marin, l'ombudsman de l'Ontario (Benzie & Ferguson 2010). (NDLR : Voir le rapport sur les violations des droits au G20 présenté par la CIDDH de l'UQAM, la LDL et la FIDH à la Commission interaméricaine des droits de l'Homme.[2])

Modes de surveillance au G20 de Toronto

La surveillance est la pierre angulaire du modèle de Miami et le Sommet du G20 à Toronto en a été une illustration classique. Le dispositif de sécurité incluait une infrastructure de surveillance technique complète mais c'est probablement l'opération HUMINT (le renseignement humain) qui a le plus perturbé les mouvements sociaux et menacé les libertés civiles. Cette opération de renseignement comprenait à la fois de la surveillance secrète et visible et vraisemblablement de la cyber surveillance. Une méthode relativement nouvelle a aussi été utilisée : la surveillance ouverte externalisée.

Un policier prenant des photos des manifestant-e-s circulant tranquillement dans les rues d'Ottawa pour protester contre le Sommet de Montebello.

Surveillance visible Il s'agit de la surveillance physique évidente des militant-e-s par les forces de l'ordre, avec le double objectif de collecte de renseignements et d'intimidation (ACLC). Elle prend la forme d'une surveillance physique : observer et suivre les militant-e-s, téléphoner à leur domicile, faire des entrevues avec leurs ami-e-s et voisin-e-s, visiter leur lieu de travail et participer à des réunions. Avant le G20, le militant montréalais Stefan Christoff a indiqué que ses ami-e-s avaient reçu de telles visites au moins cinq fois dans les semaines précédant le Sommet. Selon Christoff (2010), de telles démarches des forces de l'ordre « ont pour but d'intimider et d'instaurer un climat politique de peur parmi les réseaux de militant-e-s ».

Le recours à des « surveillant-e-s d'événements » est une autre forme de surveillance quasi-visible. L'Unité de surveillance des événements (USE) du G20 avait pour but de « surveiller les foules et les protestataires lors des diverses manifestations » et de « fournir des renseignements en continu et en temps réel par la supervision étroite de tous les grands rassemblements avec un potentiel préexistant de criminalité » (GRC 2011, 53) Les équipes de l'USE, composées de policières et policiers municipaux et provinciaux, « sont en tenue civile et se placent à des endroits stratégiques pour recueillir des renseignements » (ibid). En dépit de leur tenue civile, les surveillant-e-s d'événements sont souvent faciles à repérer comme le montrent clairement plusieurs vidéos YouTube, rappellant aux autres qu'ils peuvent toujours être observés (Stimulator 2010).

La surveillance visible par les forces policières a été renforcée par l'infrastructure technique du dispositif de surveillance du G20. Au centre-ville de Toronto un réseau dense de 86 vidéocaméras, publiquement visibles et montées sur des poteaux, alimentait en continu deux postes de commandement. Les forces policières effectuaient aussi une surveillance visible à bord des auto-patrouilles, équipées de caméras montées à l'intérieur et à l'extérieur ainsi qu'avec des caméras de poing utilisées le long des défilés, derrière les cordons policiers et à l'intérieur des encerclements. Durant le G20, des forces policières ont filmé systématiquement d'honnêtes citoyens qui protestaient, observaient les interventions policières ou simplement passaient par là. En plus de recueillir des images pour de futures identifications par la technologie de reconnaissance faciale, cette surveillance avait un but pédagogique, en envoyant le message menaçant que le rassemblement et l'expression politique sont des comportements qui suscitent l'intérêt des forces policières.

Surveillance secrète Cette forme est beaucoup plus insidieuse, car moins visible. Le GIS du G20 a mis sur pied un Groupe mixte du renseignement (GMR) en janvier 2009 pour effectuer des « enquêtes de renseignement sur des menaces possibles et des activités suspectes » en lien avec le sommet (G8-G20 ISU JIG 2009, 1). L' « image analytique d'une menace », élaborée par le GMR, était un pot-pourri de terrorisme, de militantisme écologique, de « convergence autochtone/ extrémiste », de cyber-espionnage et d'extrémisme de droite. L'Équipe principale d'enquête de renseignement (PIIT) était l'organe d'enquête du GMR responsable de l'identification et du ciblage des « suspect-e-s, personnes d'intérêt et associé-e-s en lien avec ces menaces » et des mesures à prendre pour « détecter, dissuader, prévenir, enquêter et/ou désamorcer les menaces ».

Le PIIT a dirigé une des plus grandes opérations nationales de renseignement dans l'histoire du Canada. Il a « mené des opérations d'infiltration, recruté des informatrices et des informateurs confidentiels et été en contact avec des gouvernements provinciaux et étrangers, des organismes

2. http://liguedesdroits.ca/wp-content/fichiers/rapportfinal-ligue-ciddhu-devant-cidh-25oct20101.pdf

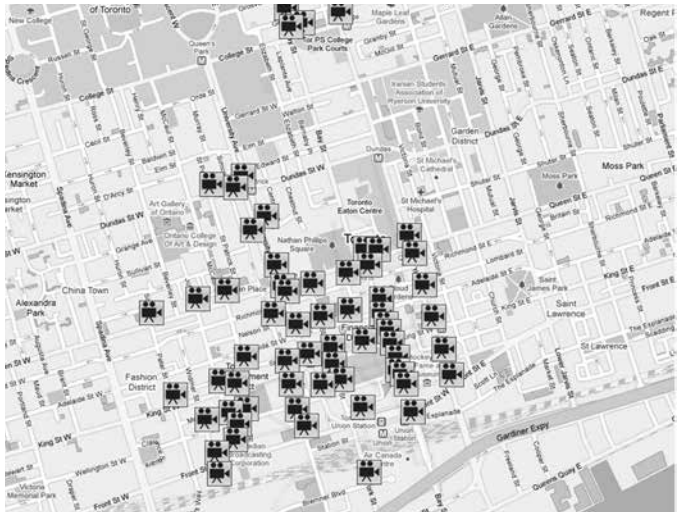


Photo : Surveillance Club TO - https://creativecommons.org

Au centre-ville de Toronto un réseau dense de 86 vidéocaméras, publiquement visibles et montées sur des poteaux, alimentait en continu deux postes de commandement.

Commons Wikimedia

d'application de la loi et même des entreprises » (Groves & Zubinsky 2011). Le PIIT s'est concentré surtout sur la « menace à l'ordre public », définie comme « des extrémistes criminels motivés par un assortiment d'idéologies radicales » telles que l'anarchisme, le socialisme et le communisme (G8-G20 ISU JIG 2009). Douze « enquêteurs dument formés » ont été affectés à l'infiltration des groupes qui prévoyaient manifester au G20 (Groves 2011). Le travail de deux agents de la Police provinciale de l'Ontario qui ont infiltré des groupes militants dans le sud de l'Ontario pendant 18 mois a mené au dépôt de 59 accusations criminelles contre 20 organisatrices et organisateurs communautaires, allégués avoir orchestré des troubles publics pendant le G20.

En demandant une enquête sur la répression policière pendant le G20, l'Association canadienne des libertés civiles (2010a) a fait valoir que « l'infiltration routinière de groupes de protestation légaux pourrait avoir un effet dévastateur sur les droits aux libertés d'expression et d'association ». Comme l'a souligné un militant, « sur le plan légal, la pratique de l'infiltration des manifestations politiques par la police secrète sert à recueillir des preuves en vue d'une condamnation mais sur le plan politique, elle crée une culture de peur envers la dissidence » (Groves & Dubinsky 2011).

La surveillance secrète est essentielle pour permettre aux forces de l'ordre de déstabiliser les mouvements sociaux et décourager l'action politique qui remet en question le statu quo. Elle permet une répression préventive, stratégie essentielle du modèle de Miami qui vise à court-circuiter la dissidence et à nuire à la mobilisation des mouvements sociaux avant même qu'ils ne se manifestent (Costanza-Chock 2004). Les tactiques courantes incluent l'arrestation préventive de militant-e-s, notamment les plus connus, des raids sur les lieux de rassemblement des militant-e-s et des visites dans les centres de média indépendants; toutes ces tactiques ont été appliquées lors du G20 de Toronto.

La répression préventive est facilitée aussi par la **cybersurveillance** qui se définit comme « la saisie, le traitement et la divulgation en ligne de renseignements personnels » (Bennett et al. 2012, 340). Généralement, il est difficile de réunir les preuves de cas précis de cyber surveillance. Cette forme de surveillance hautement technique et largement indétectable est souvent confirmée seulement à l'issue des procès, plusieurs années plus tard ou bien elle est révélée par des dénonciatrices ou des dénonciateurs. Il n'est pas vraiment surprenant d'apprendre que les régimes totalitaires à travers le monde utilisent l'internet pour surveiller et brimer les militant-e-s des droits de la personne et les dissident-e-s politiques (Deibert et al 2008). Toutefois, la découverte que les démocraties occidentales pratiquent des méthodes d'espionnage similaires, a été tout un choc. Des documents très secrets publiés par Snowden ont révélé une alliance mondiale de surveillance dont l'étendue n'avait été détaillée jusqu'à présent que dans des œuvres dystopiques de science-fiction.

Une demande d'accès à l'information a révélé que la GRC a constitué une « unité de surveillance de l'internet » avec l'intention de surveiller « tous les liens internet ouverts reliés aux sommets du G8 et du G20 » (Bowser 2011). Le gouvernement fédéral « a déployé de vastes efforts pour surveiller les conversations et les critiques relatives aux sommets sur l'internet… disséquant, compilant et produisant des rapports sur ce que des individus, des syndicats et des universités disaient sur des blogs, dans les comptes Twitter, sur YouTube et sur les sites de photos comme Flickr.com », selon un autre document obtenu par une demande d'accès à l'information (Chase 2011). Avec, en outre, des cas anecdotiques d'interception de courriels et autres formes de surveillance des télécommunications, il semble raisonnable

Il n'est pas vraiment surprenant d'apprendre que les régimes totalitaires à travers le monde utilisent l'internet pour surveiller et brimer les militant-e-s des droits de la personne et les dissident-e-s politiques. Toutefois, la découverte que les démocraties occidentales pratiquent des méthodes d'espionnage similaires, a été tout un choc.

de conclure que le GIS du G20 a effectué une certaine forme de cyber surveillance dans le cadre de son opération de renseignement.

Surveillance ouverte externalisée Utilisée lors du G20, elle constitue une évolution relativement nouvelle dans le contrôle policier des méga-manifestations qui reflète une tentative d'impliquer activement des citoyen-ne-s dans la collecte de renseignements. Il y a longtemps que les forces policières utilisent les affiches « RECHERCHÉ » pour enrôler les citoyen-ne-s dans l'arrestation de suspects criminels. Le Service de police de Toronto a poussé cette pratique un cran plus loin, en demandant à la population non seulement d'identifier des suspects mais de fournir des images de manifestant-e-s impliqués dans des actes de vandalisme, prises avec des caméras personnelles ou des téléphones cellulaires. Autrement dit, la police a invité la population à collaborer à sa propre activité de surveillance. Avec 40 000 photos et 500 vidéos, la plupart téléchargés par le public, la police a créé des affiches « RECHERCHÉ » et une galerie de media sociaux sur Facebook. Puis, elle a demandé à la population de l'aider à identifier des présumés vandales et délinquant-e-s.

Cette délégation à l'ensemble des citoyen-ne-s auxquels il est demandé d'effectuer gratuitement des tâches d'application de la loi est toutefois hautement problématique. Premièrement, c'est l'externalisation de tâches spécialisées - la collecte de preuves – à des individus non formés qui n'ont aucune obligation professionnelle assermentée, ni code d'éthique. De plus, les incitations de la police à dénoncer des concitoyen-ne-s élève la culture de la délation à une forme de responsabilité civique, valorisant un comportement que la culture occidentale décourage chez les enfants : la délation, moucharder. La surveillance ouverte externalisée ouvre la porte à des violations potentielles des droits de la personne et des libertés civiles, incluant l'identification erronée de personnes innocentes et l'encouragement à se faire justice à soi-même (Samuel 2011, Parson 2011).

Résister au regard inquisiteur : le cas troublant de Byron Sonne

Il y a un envers au phénomène croissant de la surveillance ouverte externalisée, alimentée par la quasi-ubiquité des appareils personnels d'enregistrement : les images captées par les citoyen-nes peuvent aussi jouer un rôle crucial pour rendre la police imputable.

La surveillance inversée implique « l'enregistrement ou la surveillance d'un officier de haut rang par une personne de plus faible autorité » (Mann 2004). C'est une forme de surveillance qui met l'accent sur la « surveillance vigilante qui vient d'en-bas » (Mann 2002). « La surveillance inversée intervient dans le processus de surveillance et tente de miner ou de renverser le pouvoir autoritaire associé à la technologie » (Institute for Applied Autonomy, nd). Elle contribue à la « nouvelle visibilité de l'action policière » dans laquelle la capacité technique de surveiller la police par l'enregistrement et la diffusion d'images

Avec 40 000 photos et 500 vidéos, la plupart téléchargés par le public, la police a créé des affiches « RECHERCHÉ » et une galerie de media sociaux sur Facebook. Puis, elle a demandé à la population de l'aider à identifier des présumés vandales et délinquant-e-s.

peut contribuer à sensibiliser davantage le public aux actions policières ainsi qu'à l'imputabilité de la police (Goldesmith 2010, 914).

Le cas de Byron Sonne, un résident de Toronto, spécialiste en sécurité informatique, présente une situation dramatique de surveillance inversée et la menace qu'elle peut susciter pour l'État. Préoccupé par le cirque de la sécurité entourant les préparatifs du G20, Sonne s'est joint au Surveillance Club, un groupe informel de citoyen-ne-s, de militant-e-s et d'universitaires (incluant les auteurs) qui s'intéressait à la réglementation démocratique des technologies et des pratiques de surveillance. Dans le cadre de sa recherche, Sonne prévoyait surveiller légalement les scanners non encryptés de la police pendant le G20 et afficher ses résultats sur Twitter. Il a aussi utilisé les média sociaux pour publier des photos, des vidéos et des tweets qui documentaient et critiquaient la sécurisation de Toronto.

Toutefois, Sonne s'est retrouvé sur l'écran radar de la sécurité du G20, non pas à cause des mesures de surveillance extensive du G20, mais tout à fait par hasard après qu'un agent de sécurité privé ait signalé à la police un « suspect » qui photographiait la clôture de sécurité dans les jours précédant le sommet. Un officier de police de Toronto a piégé Sonne pour l'amener à fournir son identification. Une vérification de sécurité a révélé qu'il détenait un permis de port d'arme à feu. La suite de l'enquête du Service de police de Toronto par « source ouverte » a produit les comptes Twitter et Flickr de Sonne dans lesquels il critiquait le cirque de la sécurité du G20 et la militarisation urbaine de Toronto, ainsi que son blog personnel dans lequel il révélait ses convictions anarchistes. A partir de ces éléments et d'autres données apparemment inoffensives, la police a concocté un scénario de menace présentant Sonne comme un pirate informatique ayant des motivations politiques et qui planifiait une attaque terroriste contre le G20; ce qui a déclenché une opération de surveillance secrète intensive pendant 5 jours qui s'est terminée par l'encerclement par les forces de police d'un autobus municipal dans lequel se trouvait Sonne qui fut arrêté sur le champ. Sonne a passé 11 mois en prison avant d'être libéré et d'attendre son procès avec assignation à résidence. En mai 2012, près de deux ans après son arrestation, il a été trouvé non coupable de toutes les accusations portées contre lui.

Ambivalence de la surveillance inversée

Les implications de la surveillance inversée sont ambigües. Certes le cauchemar de Sonne sert de mise en garde aux militant-e-s, aux dissident-e-s politiques et autres critiques des actions de l'état. Comme Jaggi Singh, militant de longue date arrêté lui aussi pendant le G20 de Toronto, le mentionnait dans un tweet après le procès de Sonne : « la peine, c'est le processus et non le verdict lui-même (ou la condamnation) ». La peine par le processus a caractérisé la plupart de la répression policière lors du G20 puisque les forces de l'ordre cherchaient à contenir la surveillance inversée. De nombreuses et nombreux journalistes indépendants ont été arrêtés tandis qu'ils tentaient de documenter le harcèlement des militant-e-s et des passant-e-s par les forces policières avec des contrôles d'identité ou des interpellations et des fouilles illégales. Des vidéos et des photos prises par des centaines de spectatrices, de spectateurs, de bloqueuses, de blogueurs, de citoyen-ne-s journalistes et d'artisan-ne-s des média indépendants affichés sur l'internet ont confirmé la brutalité policière choquante ainsi que le mépris des libertés civiles et du protocole légal pendant le G20.

Plusieurs séquences recueillies par des citoyen-ne-s, affichées sur l'internet et largement diffusées via les media sociaux sont devenues des éléments de preuves photographiques dans deux enquêtes criminelles sur la violence policière durant le G20. Toutefois, un cas seulement a débouché sur une condamnation : celui de Adam Nobody (son vrai nom) qui a été vicieusement agressé par le policier Babak Andalib-Goortani du Service de police de Toronto (Di Manno 2011). En dépit du fait que de nombreux abus commis par des forces policières aient été largement documentés et diffusés sur You Tube et d'autres sites de réseaux sociaux, la surveillance inversée s'est finalement avérée largement inefficace.

CC Creative Commons

Conclusion

La surveillance des mouvements sociaux par l'État est problématique pour la démocratie. Les libertés civiles, gagnées de haute lutte, dont jouissent les Canadien-ne-s telles que la liberté de parole, de pensée, de croyance et d'association favorisent l'engagement civique dans une société ouverte et démocratique. Le droit constitutionnel à l'autonomie personnelle et à la protection contre l'intrusion de l'État dans nos vies privées est essentiel à la dignité humaine. Mais un vaste état de surveillance indiscriminée et perpétuelle du type de celle révélée par Edward Snowden a un effet dévastateur. Il engendre une réticence à participer aux mouvements sociaux, ce qui affecte de manière négative leur viabilité et leur efficacité. De plus en plus, au fur et à mesure que la technologie permet aux gouvernements de recueillir davantage de renseignements sur ses citoyen-ne-s, ceux-ci perdent confiance dans l'intention des gouvernements de respecter leurs protections constitutionnelles.

La cybersurveillance, de concert avec la surveillance ouverte et secrète, enseigne la crainte de représailles contre la mobilisation politique et les expressions publiques de dissidence. Cette pédagogie contribue à normaliser la mise de côté de la loi et la restriction de la citoyenneté qui accompagnent les mégaévénements et en particulier les mégamanifestations, préparant ainsi les citoyen-ne-s à accepter de futurs empiètements sur leurs libertés civiles. La résistance spontanée de la base, incarnée par la surveillance inversée, semble à première vue porteuse d'espoir pour rendre imputables les organismes d'application de la loi. En réalité, les résultats de l'enregistrement omniprésent et le partage sur les média sociaux sont ambivalents car cette nouvelle visibilité de la répression est largement réduite à de la téléréalité.

La véritable bataille passe par la modification des politiques et par des amendements législatifs pour lesquels les défenseurs de la vie privée et des libertés civiles se battent sur de nombreux fronts, incluant des procès et des recours collectifs, la résistance massive, l'éducation, les activités contre une législation favorable à la surveillance, tel que proposée dans la *Loi sur la protection des renseignements personnels numériques* et la *Loi sur la protection des Canadiens contre la cybercriminalité*. Des groupes de défense des droits, des universitaires engagés et des défenseurs des libertés civiles se sont lancés dans cette bataille. Reste à savoir si une vaste opposition émanera des citoyen-ne-s canadiens car ultimement ce sont eux qui doivent livrer la bataille contre l'État de surveillance.

Résistance à la surveillance : le cas de l'UQAM

Samuel Ragot, étudiant à la maîtrise en science politique
Université du Québec à Montréal

René Delvaux, étudiant à la maîtrise en science politique
Université du Québec à Montréal

La question de l'utilisation de plus en plus fréquente de dispositifs de surveillance vidéo est une problématique importante pour les mouvements sociaux. La situation de l'Université du Québec à Montréal (UQÀM) témoigne des impacts de l'apparition et de la multiplication de ces dispositifs dans nos milieux de vie et de travail, mais aussi des formes de résistance qui peuvent leur être opposées.

La vidéosurveillance et le contexte plus large de la sécurisation

Les sociétés libérales ont tendance à se tourner vers une « sécurisation » de plus en plus importante. Si Orwell voyait un danger dans la manipulation du langage par les États, alors que Bernays dans Propaganda considérait que « la propagande devient un auxiliaire indispensable de la vie publique »[1], on remarque que la « sécurisation » de nos sociétés se déploie notamment par un processus d'hyperbolisation et d'euphémisation dans le discours politique. Selon Pierre Tevanian et Sylvie Tissot[2], ces processus opèrent de façon à exposer « la violence des dominé-e-s, ayant pour effet d'une part de disqualifier leur parole » pour mieux «occulter, minimiser et relativiser une violence [de l'État], et ainsi la rendre acceptable ». Pour Bourdieu, l'euphémisation vise notamment à vider les termes de leur « substance » afin de procéder à un « effet d'occultation par la mise en forme »[3]. Il s'agit de modifier et déposséder la réalité telle qu'elle existe pour en projeter une autre, plus convenable. C'est dans ce cadre que se déroulent les contestations sociales comme celle contre la vidéosurveillance à l'UQÀM.

La surveillance : un système dans le système

La surveillance vidéo en tant qu'outil s'inscrit dans un système de surveillance plus large, visant notamment à enregistrer des données et images captées par un ensemble de dispositifs techniques. Ce caractère systémique et systématique est important puisqu'il vient non seulement appuyer un ensemble d'autres dispositifs, mais aussi créer de nouveaux réseaux (little brothers) visant le contrôle social. Cette surveillance est par ailleurs très insidieuse puisqu'elle a un aspect de permanence et de continuité dans le temps et dans l'espace (pouvant donc agir et servir a posteriori), qui a, de facto, un effet de dissuasion de l'action politique (« chilling effect »).

Dans les faits, le « chilling effect » vise à dissuader, par des moyens répressifs ou « préventifs », des personnes de faire usage notamment de leur liberté d'expression dans différentes situations, que ce soit de militance ou de contestation juridique. Dans un cadre de modification et de mutation du langage, le « chilling effect » prend une dimension toute particulière : certaines pratiques de résistance ou d'utilisation de droits reconnus sont maintenant présentées comme des actes inacceptables.

Le cas de l'UQÀM

À l'UQÀM, le phénomène général de « sécurisation » et ses effets se déploient depuis un certain nombre d'années avec notamment l'importante croissance des budgets alloués à la sécurité du campus.[4] Depuis janvier 2013, plus de 2,5 millions de dollars ont été dépensés afin de mettre en place un nouveau parc de vidéosurveillance à l'UQÀM. Des coûts récurrents supplémentaires de plus de 200 000$ par année seront dorénavant perçus à même les budgets de l'université pour l'utilisation et l'entretien de ces dispositifs. Des chiffres qui, dans le contexte d'un sous-financement universitaire, n'ont pas manqué de susciter la colère des membres de la communauté de l'UQÀM.

Au cours de la dernière année, les caméras se sont donc multipliées dans les pavillons de l'université. Elles se

1. Edward L Bernays, *Propaganda : comment manipuler l'opinion en démocratie* (Paris : Zones, 2007), 93.

2. Pierre Tevanian, Sylvie Tissot, *Les mots sont importants 2000-2010* (Paris : Libertalia, 2010), 274.

3. Pierre Bourdieu, *Ce que Parler veut dire : L'économie des échanges Linguistiques* (Paris : Fayard, 1982).

4. « La sécurité, ce puits sans fond », Montréal Campus, 11 mars 2011. En ligne: http://montrealcampus.ca/2011/03/la-securite-ce-puit-sans-fonds/

comptent aujourd'hui par centaines.[5] Leur apparition soulève des enjeux reliés à la gestion budgétaire et à la légitimité des processus décisionnels, mais elle inaugure surtout de nouvelles possibilités de contrôle et de surveillance des activités et des personnes sur le campus. En guise de riposte, les associations étudiantes ont alors procédé à l'organisation de différentes actions directes, mais aussi institutionnelles afin de forcer l'UQÀM à retirer certaines caméras et mieux encadrer l'utilisation de la surveillance vidéo. Parallèlement aux démarches entreprises au sein des canaux institutionnels de l'université, une campagne d'information et de sensibilisation a été conçue et mise en place sur internet (www.souslescameras.ca) et dans le campus. Via leurs syndicats et leurs représentant-e-s au sein des instances universitaires les professeur-e-s, chargé-e-s de cours et employé-e-s ont appuyé l'initiative.

À l'UQÀM, comme ailleurs, on note une opacité dans la gestion des enjeux de sécurité. Ces enjeux semblent se soustraire aux règles de transparence et aux processus décisionnels qui s'appliquent pourtant à tout autre domaine du vivre ensemble. Cet état d'exception cherche à se justifier par un discours qui s'appuie sur la peur et la menace. En agitant d'abord le spectre des « tueurs fous » et d'une criminalité endémique au centre-ville, puis en évoquant ensuite la prolifération de l'itinérance et de la toxicomanie au cours de la dernière année, la direction de l'UQÀM semble vouloir imposer une logique sécuritaire anxiogène et écarter les inquiétudes légitimes de la communauté universitaire. À ce jour, il n'existe toujours aucun encadrement de la surveillance vidéo. L'arbitraire de l'utilisation de ces dispositifs intrusifs est laissé au Service de la prévention et de la sécurité, seul maître à bord de l'État dans l'État.

La direction de l'université, à corps défendant, accepte aujourd'hui de discuter de la question et envisage l'adoption d'une politique institutionnelle sur la vidéosurveillance à partir d'un document rédigé par des membres de la communauté[6]. Il s'agit d'un moindre mal pour celles et ceux qui s'opposent à la surveillance vidéo, mais l'initiative pourrait à terme assurer un encadrement restrictif de l'utilisation des caméras et permettre ultimement aux membres de la communauté de prendre la place qui leur revient dans la gestion de ces dispositifs.

L'impact de la vidéosurveillance dans le cas de l'UQÀM

Dans le cas de l'UQAM, il semble que le problème de la vidéosurveillance pourrait engendrer un « chilling effect » important sur l'activisme politique ou syndical dans le cadre de l'exercice de droits acquis et reconnus. L'effet dissuasif de ces dispositifs repose sur le sentiment d'être surveillé en permanence, mais aussi sur le fait que les actes de désobéissance civile ou les actions politiques deviennent de moins en moins acceptables aux yeux de l'institution. Bien que de nombreuses actions directes continuent d'avoir lieu (perturbations d'un discours du recteur, occupation des bureaux du Service de la prévention et de la sécurité, bris de caméras lors de manifestations, etc.), on constate que les risques liés à la désobéissance sous surveillance dissuadent une partie des personnes qui auraient autrement été promptes à participer à ces contestations.

L'UQÀM procède donc par l'euphémisation de la menace que représentent ces dispositifs de surveillance et l'hyperbolisation de la menace que représenterait l'action politique au sein de l'université ou l'intrusion sur le campus de personnes étrangères à la communauté. De plus, en choisissant d'utiliser des moyens légaux pour répondre à ces résistances, l'UQÀM cherche à décourager l'activité de ces personnes au sein du mouvement militant, mais aussi à créer un exemple. En utilisant les moyens techniques liés à la vidéosurveillance, l'UQÀM pourrait ainsi faire planer le spectre de la menace judiciaire ou disciplinaire contre les membres de la communauté universitaire. Ces signes nous exposent à l'important risque d'abus de la possibilité d'utiliser et de multiplier des technologies de surveillance sans aucun cadre réglementaire.

Un enjeu qui touche tout le monde, mais face auquel il est difficile de réagir collectivement

Il est pertinent de se demander comment faire en sorte de renverser la tendance et de mobiliser la population si l'État ou l'institution est en mesure de contrôler le discours public tout en réprimant de façon très efficace tout embryon de contestation? Alors que, pour reprendre les mots d'Anselm Jappe, « tout est fait pour rendre impossible un changement de direction »[7] historique au niveau de l'État et de la société en général, il est absolument fondamental de se questionner sur notre capacité à arrêter la machine.

Comme nous l'avons vu dans le cas de l'UQÀM, il est possible de s'organiser et de résister. Il s'agit, en forçant le débat, de se réapproprier des questions qui nous ont été confisquées, car faisant partie de la sphère des « objets de sécurisation »[8]. L'exemple de l'UQÀM indique que c'est la perspective de perturbations continues et une mobilisation politique soutenue qui ont permis de désamorcer le langage sécuritaire et d'exposer l'euphémisation des dangers de la vidéosurveillance. Résister aux dérives de la vidéosurveillance, c'est aussi résister à son effet dissuasif et ne pas reculer sur l'exercice de nos libertés individuelles et collectives.

5. Leur nombre exact est encore inconnu, le Service de prévention et de sécurité (SPS) de l'établissement refuse en effet de divulguer cette information, comme plusieurs autres, sous prétexte que cela pourrait compromettre l'efficacité de leur dispositif de sécurité.

6. Julien Pieret et al., Politique Alternative En Matière de Surveillance Vidéo À l'Université Du Québec À Montréal," n.d.,

7. Jappe, Crédit à mort, 79.

8. Buzan, Barry. 1998. *Security : a new framework for analysis*. Boulder, Colo : Lynne Rienner Pub.

Dérives sécuritaires et profilages des populations marginalisées

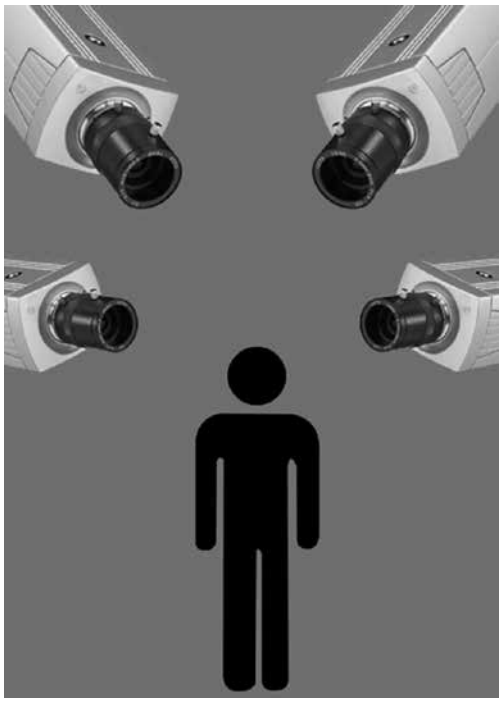
Céline Bellot, professeure
École de service social, Université de Montréal

Marie-Ève Sylvestre, professeure
Faculté de Droit, Université d'Ottawa

Si la question de la sécurité est un enjeu majeur de nos sociétés, les dérives sécuritaires le sont tout autant. Qu'on songe au programme d'accès aux communications des internautes par l'Agence Nationale de sécurité américaine (NSA), à la multiplication des caméras de surveillance dans nos villes, au déploiement et au croisement de nombreuses banques de données tant gouvernementales, que commerciales; à l'accroissement des mesures judiciaires de surveillance (probation, conditions avant et après procès) des populations judiciarisées. En effet, malgré une diminution notable de la criminalité dans notre pays, les effectifs associés à la sécurité sont toujours en augmentation, que ce soit en regard de la sécurité publique ou de la sécurité privée.

Dans ce contexte, la gestion selon les risques éventuels plutôt que selon le danger réel par les acteurs de la sécurité est devenue le cadre quotidien des politiques et des pratiques de surveillance et contrôle. Or, si l'idée du risque est en apparence proche de celle de danger, il importe cependant de considérer qu'elle s'en distancie fortement lorsqu'il est question d'assurer le contrôle du comportement humain et de promouvoir la protection de l'ordre public. En effet, de manière rationnelle, le risque impose un calcul de probabilité, qui dans une logique actuarielle permet d'évaluer les pertes et les gains associés à une situation, un évènement dont la survenue est plus ou moins probable. Ainsi, dans le registre des assurances, la protection à l'égard du risque de maladie, d'invalidité, ou d'accident, vient soutenir les pertes financières associées à la réalisation du risque. Pour autant, lorsqu'il est question d'ordre public et de contrôle de la criminalité, la notion de risque devient plus fuyante dans la mesure où elle contribue à développer des pratiques de contrôle et de surveillance en amont de l'existence même d'un danger.

Or, loin de s'inscrire dans une logique préventive, ces pratiques de contrôle et de surveillance associées à l'idée de risque alimentent une dynamique d'encadrement de populations ou de personnes ciblées, qui seraient à risque de commettre éventuellement des crimes. En effet, l'ordre public est d'abord et avant tout assuré par la protection de la population contre des infractions définies par le code criminel. En cherchant à agir sur des populations et des



Etienne Vallieres-Chartrand, Concepts pour tous

personnes, dont on décide qu'elles pourraient éventuellement commettre des crimes, dans la mesure où elles sont qualifiées de dérangeantes, en mobilisant des outils juridiques à cette fin, les acteurs de la sécurité publique et privée portent le plus souvent atteinte à la liberté des individus et à leurs droits fondamentaux. Certes, le couple liberté/contrôle s'impose comme le paradoxe de nos sociétés modernes.

Pour autant, l'élargissement des pratiques de contrôle et de surveillance à l'égard de situations jugées à risque, parce que dérangeantes, constitue une dérive majeure contemporaine. En effet, au cœur du paradoxe entre la liberté et le contrôle, s'inscrit à la fois la définition du « vivre ensemble » mais aussi « les pouvoirs coercitifs » qu'exerce la société pour maintenir l'ordre établi. À ce titre, la double définition du contrôle social, tantôt ce qui assure la conformité, tantôt ce qui réagit à la déviance vient rendre compte de cette tension paradoxale. Les analyses récentes sur l'élargissement du contrôle social,

CC Creative Commons

à l'aune de la gestion des risques, montrent à quel point, la discipline mise en place dans nos sociétés s'alimente à travers les rapports sociaux de pouvoir en réduisant, de facto, la portée universaliste et démocratique des droits fondamentaux. En somme, face à la gestion des risques développée à travers les pratiques de surveillance et de contrôle des acteurs de la sécurité publique et privée, se dessinent l'identification, le suivi de personnes ou de populations qui auraient moins le droit de vivre librement dans nos sociétés.

Ainsi, la judiciarisation par exemple, des populations itinérantes constitue une atteinte directe à leur droit à l'occupation de l'espace public, mais aussi à leur liberté de circuler librement dans nos sociétés. En soutenant une surveillance accrue de ces populations, on leur impose des infractions pénales pour des comportements que de nombreux citoyens adoptent aussi dans l'espace public, qu'il s'agisse de consommer de l'alcool dans l'espace public, de flâner dans les rues, etc. Ce traitement pénal des populations itinérantes révèle une logique différentielle des actrices et des acteurs de la sécurité publique à leur endroit. Or, cette logique différentielle construite sur la base d'une condition sociale particulière contrevient aux chartes des droits et libertés en réalisant un profilage de ces populations. Cet exemple illustre en effet, de manière concrète et marquante, les conséquences de l'utilisation de la notion de risque en matière de production de l'ordre public. Dans le cadre de leur judiciarisation, il ne s'agit pas de réprimer des actes criminels mais des actes certes répréhensibles en regard des législations pénales (provinciales ou municipales). Cependant ces pratiques, en ciblant les populations itinérantes, réalisent un profilage et donc un traitement discriminatoire.

La question des dérives sécuritaires actuelles dans les politiques et les pratiques de surveillance et de contrôle pose précisément cet enjeu. Puisque tout peut être risque éventuel, les politiques et les pratiques de sécurité ont nécessairement besoin de circonscrire les « menaces » qu'elles cherchent à contrôler. Or, la construction de cette menace en renonçant à des faits tangibles et raisonnables en regard de la criminalité réelle, se développe à travers un mécanisme d'identification, de désignation, de suivi des personnes, des groupes, des populations qui pourraient être menaçantes, et surtout sont perçues comme menaçantes. Dans cette dynamique, loin d'être dans un contrôle direct et transparent des populations, la construction de cette menace se fait en souterrain, le plus souvent à l'insu même des populations. Comment, en effet, dire publiquement que certaines populations ou personnes, en raison de leur origine ethnique, de leur condition sociale, de leurs convictions politiques, de leur orientation sexuelle, doivent être surveillées et contrôlées, sont surveillées et contrôlées, sans l'existence même d'un soupçon raisonnable de croire qu'elles pourraient commettre un crime. Le dire serait porter une atteinte fondamentale à notre État de droit. Et pourtant, la banalisation de la surveillance en s'appuyant sur une multiplicité de profilages effrite au quotidien l'État de droit et contribue à gouverner par l'inquiétude plutôt que par la certitude. Par conséquent, rétablir l'État de droit et assurer la sécurité de tou-te-s signifie bien moins contrôler davantage des populations construites comme menaçantes, que de soutenir le renforcement des libertés et des droits fondamentaux de tout-e citoyen-ne à vivre sans surveillance tant que ses gestes ne peuvent être considérés comme criminels. Rendre visible la surveillance et le contrôle, dénoncer leurs conséquences discriminatoires, renforcer les solidarités entre les citoyen-ne-s, sont autant d'avenues susceptibles de maximiser la liberté de chacun-e à vivre dans une société sécure.

Lorsque code et design font la loi et permettent la surveillance

Assujettir l'informatique à la démocratie

Pierrot Péladeau, chercheur invité chez Communautique
et chroniqueur au Journal de Montréal

L'informatisation de nos sociétés vient à peine de commencer. Nous ne sommes qu'au seuil d'une révolution où nos rapports interpersonnels et collectifs passeront de plus en plus par des machines numériques. L'un des enjeux est l'avenir même de la démocratie et des droits de la personne. En conséquence, le développement même de l'informatique doit devenir une question de démocratie et de droits de la personne.

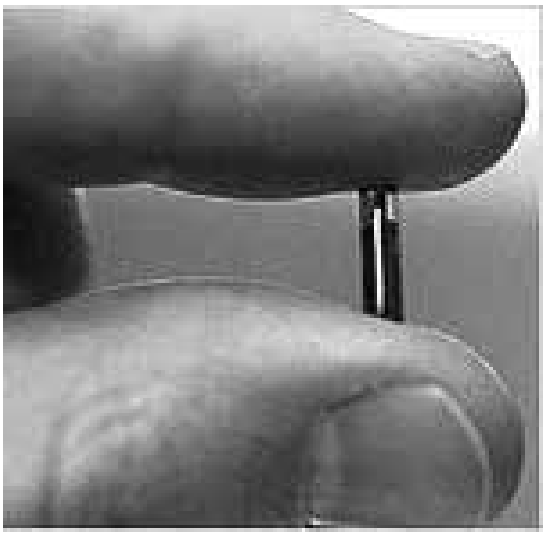
L'informatique transforme les institutions humaines. Car ce qui caractérise l'animal social humain est sa capacité à manier des représentations symboliques à l'aide d'images et de sons, de lettres et de mots, de chiffres ainsi que d'opérateurs logiques et mathématiques. Or, l'informatique augmente et élargit spectaculairement la capacité de produire et manier ces symboles servant la pensée, la communication et l'action humaines. L'informatique ne peut donc que s'immiscer dans tous les domaines de la vie sociale et les transformer.

Voilà pourquoi on ne peut pas simplement parler des effets de l'informatique sur la démocratie et sur les droits de la personne en particulier. Ou réciproquement, d'*application* de ces derniers à l'informatique. Nous assistons plutôt à des coévolutions qui exigent de penser ensemble ces réalités, non seulement entre elles, mais avec plusieurs autres, tel la mondialisation ou le droit avec lesquels l'informatique coévolue également.

En outre, l'informatisation des activités humaines implique comme condition et résultat nécessaires une production d'informations en quantités et détails sans précédent. Cependant, rien ne prédétermine la nature des informations produites ni leurs utilisations possibles ou non.

La liberté dans l'universalité

À l'origine de l'informatique moderne, il y a l'ordinateur, incarnation physique du concept de *machine de Turing universelle*. En répondant à un problème de philosophie mathématique, Alan Turing a inventé le concept d'une machine capable d'exécuter n'importe quelle suite finie, non



Puce d'identification radio fréquence pour implantation sous-cutanée.

ambigüe, d'instructions sur n'importe quel type de données[1]. Cette machine est dite universelle puisqu'elle peut exécuter n'importe quel algorithme sur n'importe quelles informations. C'est pourquoi les premiers ordinateurs s'appelaient *calculateurs universels* : ils pouvaient exécuter n'importe quel *programme*.

Cette universalité d'application est un fait politique capital à partir de l'instant où l'informatique supporte les rapports entre êtres humains. De la même manière qu'il est possible avec les mots et règles d'une langue de concevoir une quasi-infinité de textes législatifs des plus émancipateurs aux plus asservissants, il est également possible de concevoir une quasi-infinité de désign et d'algorithmes régissant les rapports entre personnes physiques et légales. Et une fois confiées à une machine, les règles et opérations énoncées dans le programme seront automatiquement et impitoyablement mises en œuvre avec une remarquable efficacité. Le juriste Lawrence Lessig l'a bien résumé dans sa formule le *code fait loi*[2]. En fait, l'informatique transforme le droit lui-même en lui offrant de nouveaux médias et espaces d'expression et d'application, de nouvelles logiques, de nouveaux lieux, acteurs, actrices et processus de production[3].

Bien sûr, durant une génération, l'informatique a été confinée à d'immenses et couteuses machines centralisant nécessairement leur puissance chez quelques très grandes organisations. Cependant, la miniaturisation des processeurs et l'omniprésence d'Internet ont définitivement ouvert l'horizon à toutes les formes de régulation et de surveillance imaginables. Le pouvoir que les dispositifs numériques offrent sur les rapports interpersonnels peut donc, d'une quasi-infinité de manières, être distribué entre acteurs et actrices autonomes, ou partagé avec de tiers surveillants, ou concentré en des mains contrôlantes, voire autoritaires. Aucune option n'est prédéterminée. Aux humain-e-s de décider ce qu'ils souhaitent commander à leurs machines.

Exemple à l'échelle intime

Les autorités européennes et états-uniennes ont commencé à autoriser la commercialisation de pilules avec micropuce électronique sans fil. Certains « modèles » de pilules enregistrent automatiquement l'instant précis où nous les prenons. Ces informations peuvent ensuite être communiquées à distance à tout intéressé : nous-mêmes, un-e proche aidant-e, notre médecin, notre pharmacien-ne, notre établissement de santé, l'assureur qui paie le traitement.

On imagine aisément de nombreuses situations où un tel dispositif serait manifestement utile. Pour aider patient-e-s et proches à garder trace de la prise de plusieurs médicaments en même temps. Pour aider médecins et pharmacien-ne-s à ajuster une prescription individuelle comportant risques et effets secondaires importants, et éventuellement le protocole pour toutes les personnes recevant ce traitement.

On imagine autant de nombreuses situations qui, au contraire, seraient controversées. Pour permettre aux médecins de talonner et réprimander ces nombreux patient-e-s qui ajustent ou interrompent de leur propre chef un traitement prescrit. Ou à un assureur de suspendre le paiement d'un médicament pour indiscipline des patient-e-s dans sa prise.

Or qui décidera du mode précis de surveillance confié au dispositif? Nous les patients consommateurs et consommatrices du médicament sur une base ad hoc, avec ou sans nos médecins? Les médecins collectivement à travers des protocoles standardisés? Le fabricant de la pilule? Le fabricant du dispositif numérique? L'agence gouvernementale qui en autorise la commercialisation? L'assureur? Nos député-e-s par voie de législation? Un gouvernement par voie règlementaire? C'est précisément le caractère inédit du dispositif qui en fait une question ouverte, imprévue par le droit existant.

Un exemple planétaire

À une tout autre échelle, Internet est aujourd'hui l'une des infrastructures clés sur laquelle repose l'informatisation des sociétés à travers presque toute la planète. Les révélations d'Edward Snowden sur les pratiques de la NSA ont cependant souligné à quel point Internet facilite la surveillance de masse. Car les conceptrices et les concepteurs de son désign initial et de ses développements subséquents, comme le Web, n'avaient pas imaginé une telle possibilité.

1. A. Turing, « On computable numbers, with an application to the Entscheidungs problem » (*problème de la décidabilité, NdA), Proceedings of the London Mathematical Society*, Série 2, 42 (1936-7), 230–265.

2. L. Lessig, *Code and Other Laws of Cyberspace*, New York, Basic Book, 2000,

3. P. Péladeau, « L'informatique ordinatrice du droit et des procès d'information sur les personnes », *Technologie de l'information et société*, vol. 1, no. 3 (1989), 35-56.

Or, Edward Snowden lui-même a rappelé à plusieurs reprises qu'il est dès aujourd'hui techniquement possible de reconfigurer Internet pour rendre impossible la surveillance de masse. Premièrement, en chiffrant (cryptant) par défaut les communications de bout en bout afin de les rendre illisibles même si interceptées. Deuxièmement, en «routant» par défaut ces mêmes communications « en oignon » afin d'en camoufler les emplacements des participant-e-s.

De telles mesures ne peuvent immuniser totalement contre la surveillance ciblée d'individus ou organisations en particulier. Mais elles peuvent rendre économiquement irréalisable la surveillance de masse de populations entières.

Comment les parlements, gouvernements et sociétés civiles peuvent-ils orienter l'informatique et la surveillance qu'elle permet et, non pas seulement préserver les libertés et la démocratie, mais bien les renforcer?

Qui actuellement en discute et en décidera? Ce sont, notamment, quelques milliers d'individus qui se sont autodésignés membres de l'*Internet Engineering Task Force*, un groupe international sans aucun statut légal, ni mode d'adhésion formalisés.

Or, où sommes-nous, citoyen-e-s québécois-es ou d'ailleurs dans le monde, dans cette délibération qui nous concerne directement? Plutôt dans un rôle de spectatrices ou de spectateurs. Car la gouvernance démocratique d'Internet, innovation technique devenue mondiale, reste encore largement à inventer. Il n'en tient qu'à l'État québécois ou d'ailleurs et aux sociétés civiles de prendre les moyens d'y participer.

Par contre, certains États comme la Chine et l'Iran ont décidé de balkaniser partiellement Internet afin d'en contrôler la portion existant sur leur territoire, et leur population à travers elle. En Europe, on discute également d'une semblable approche mais, au contraire, pour mieux protéger leur population contre la surveillance.

L'avenir d'Internet, y compris sa survie même, s'inscrit aussi dans un horizon ouvert.

La surveillance fait société

Un autre fait incontournable est que la surveillance est une composante indissociable de toute vie sociale. Ceci est vrai de toutes les sociétés humaines, tout comme de nombreuses sociétés animales. Et même de communautés végétales comme le démontrent des découvertes biologiques récentes.

Il s'ensuit qu'une société informatisée est, nécessairement, une société de surveillance accrue. Et comme l'illustre l'exemple des pilules à micro puce sans fil, la surveillance permise par l'informatique peut prendre d'innombrables formes entrainant des conséquences très différentes, voire radicalement opposées.

De même, le fait que les activités d'agences comme la NSA ou notre *Centre de la sécurité des télécommunications Canada* sont conduites essentiellement par des moyens informatiques qui les rendent aisées à surveiller par ces mêmes moyens informatiques. Au lieu de s'en tenir aux déclarations de leurs administrateurs, laconiques ou carrément mensongères, leurs métadonnées peuvent automatiquement fournir un portrait exact et détaillé, même en temps réel si on le souhaitait, de tous les types d'activités de surveillance réalisées par ces agences.

D'où la question : comment les parlements, gouvernements et sociétés civiles peuvent-ils orienter l'informatique et la surveillance qu'elle permet et, non pas seulement préserver les libertés et la démocratie, mais bien les renforcer?

Les nouveaux législateurs

Le premier défi vient du fait que si code et désign font loi alors un pouvoir social de plus en plus considérable échappe actuellement aux institutions démocratiques classiques. Il se retrouve plutôt entre les mains de technocrates, ingénieur-e-s, bidoulleuses et bidouilleurs et firmes informatiques commerciales.

Cela peut être des organisations informelles privées internationales comme l'Internet Engineering Task Force dans le cas d'Internet. Ou des entreprises commerciales ou des organisations professionnelles dans celui des pilules à micro puce.

Un tel détournement est facilité par le fait que, contrairement aux textes de lois et règlements qui sont écrits en langage naturel (français et anglais au Canada), codes et désign sont écrits dans des langages mathématiques et formels qui sont actuellement incompris par la quasi-totalité des citoyen-ne-s, y compris chez ceux qui forment la société civile, les législatures et les gouvernements.

Un exemple troublant est celui du Dossier Santé Québec en cours d'implantation. Dans les 10 dernières années, le gouvernement et l'Assemblée nationale ont tenu plusieurs consultations publiques sur l'implantation d'un résumé électronique d'informations médicales. Chaque fois, il y eut quasi-unanimité à maintenir le principe fondamental du consentement des patient-e-s à la communication de ses renseignements médicaux. Député-e-s, patient-e-s,

professionnel-le- de la santé, pratiquement tous étaient d'accord sur le maintien du principe.

Sauf, qu'une fois amorcé le déploiement du Dossier Santé Québec, il a fallu admettre que le coûteux dispositif ne permettait pas l'exercice concret du consentement ad hoc du patient. D'où l'adoption en 2012 du projet de loi 59 qui abolit pratiquement ce consentement lorsque les renseignements médicaux passent par la machine Dossier Santé Québec. C'est désormais tout ou rien. Ou bien tous les professionnel-le-s et établissements de santé ont accès à tout le contenu du Dossier Santé Québec. Ou bien personne n'y a accès. Bref, le désign du système adopté nous a imposé de renoncer à un principe de droit fondamental sur lequel nous faisions consensus.

Pourtant, bien d'autres systèmes d'informations médicales existants ou possibles, non seulement maintiennent le consentement de la patiente ou du patient, mais rehaussent le contrôle que peuvent exercer patient-e-s et professionnel-le-s de la santé sur la communication d' informations médicales.

Sauf que les député-e-s ont, sans en avoir jamais eu véritablement conscience, abdiqué leur pouvoir législatif au profit des technocrates réunis par *Inforoute Santé Canada,* l'organisation parapublique pancanadienne qui a conçu ce modèle de résumé électronique d'informations médicales.

En 2012, il n'était absolument pas trop tard pour que l'Assemblée nationale reprenne ce pouvoir. Mais cela impliquait de reprendre à neuf des développements informatiques qui avaient déjà coûté des centaines de millions de dollars.

L'informatique est politique

Si l'informatique peut mettre en œuvre n'importe quelle sorte d'instructions sur n'importe quel type d'informations supportant et organisant des rapports entre êtres humains, alors le choix d'un type particulier de dispositif numérique et des détails de son désign et de son code n'est pas prédéterminé par la technique. Un tel choix est fondamentalement de nature politique. Pareillement, pour le type de surveillance que permet ou non ce dispositif.

Premièrement le défi démocratique exige de nous, de collectivement apprendre à distinguer les dimensions des innovations informatiques qui impliquent l'exercice d'un pouvoir social. Or, ces dimensions politiques ont souvent un caractère émergeant. Ainsi Internet, avant d'être l'infrastructure sociale qu'il est aujourd'hui, a été des protocoles de communications numériques développés indépendamment dans des réseaux interuniversitaires, interbancaires, téléphoniques et militaires. De même Facebook, avant de s'imposer mondialement comme aujourd'hui, n'a été qu'une proposition de réseautage social parmi des dizaines d'autres disponibles sur un marché ouvert.

Deuxièmement, il faut obliger les concepteurs à communiquer à la citoyenne et au citoyen concernés ces dimensions politiques de leurs innovations numériques d'une manière compréhensible, fiable et vérifiable.

Troisièmement, enfin, il faut démocratiser ces innovations, soit en amenant leur délibération dans des institutions démocratiques existantes ; soit en développant la capacité des citoyens et de la société civile à participer aux instances nouvelles.

Sur le plan des moyens, cela exige de développer :

- dans la population une culture informatique et société qui va bien au-delà du savoir utiliser des dispositifs numériques professionnels ou personnels ;

- une citoyenneté active des niveaux local jusqu'à international dans les forums de discussion où se discutent l'organisation et la régulation du social à travers le désign et le code numériques ;

- une expertise et veille sociale publiques qui, en matière de surveillance, dépasse très largement la compétence des commissariats à la protection des renseignements personnels, car si cette problématique constitue un critère d'évaluation nécessaire, il demeure totalement insuffisant (donc inefficace seul) pour préserver les libertés, les droits de la personne et la démocratie; et enfin

- une préférence pour des technologies ouvertes qui permettent, d'une part à tous d'en inspecter le détail du désign et du code source — ce qu'ils permettent à qui de faire ou non exactement, notamment en matière de surveillance — ainsi que de librement les adapter à des besoins démocratiquement définis.

Nous ne sommes qu'au seuil de la révolution numérique. À nous de la façonner en réinventant la démocratie elle-même.

Lettre ouverte : 500 écrivain-e-s dénoncent la surveillance numérique

À l'occasion de la Journée internationale des droits de l'Homme, 562 écrivain-e-s, dont 5 lauréat-e-s du Prix Nobel*, dans 80 pays, ont lancé un appel pour dénoncer l'espionnage institutionnalisé des citoyen-ne-s à l'ère numérique. Cet appel a été publié dans 30 journaux à travers le monde. Voir le texte ci-dessous. (NDLR Martine Eloy)

« Ces derniers mois, l'étendue de la surveillance de masse est devenue notoriété publique. De quelques clics de souris, l'État peut accéder à votre portable, à votre adresse e-mail, à vos réseaux sociaux et à vos recherches sur Internet.

« Il peut suivre vos penchants et vos activités politiques et, en partenariat avec des sociétés de l'Internet, il recueille et stocke vos données et il peut donc prédire votre consommation et vos comportements.

« Le pilier fondamental de la démocratie est l'intégrité inviolable de l'individu. L'intégrité humaine s'étend bien au-delà du corps physique. Dans leurs pensées et dans leurs environnements personnels et de communication, tous les êtres humains ont le droit à une intimité sans encombre.

« Ce droit fondamental est rendu caduc par l'abus de l'évolution technologique par les États et par les sociétés organisées à des fins de surveillance de masse.

« Une personne placée sous surveillance n'est plus libre; une société sous surveillance n'est plus une démocratie. Pour rester valides, nos droits démocratiques doivent s'appliquer aussi bien dans le virtuel que dans le concret.

** La surveillance viole la sphère privée et compromet la liberté de pensée et d'opinion.*

** La surveillance des masses traite chaque citoyen comme un suspect potentiel. Elle remet en question un de nos triomphes historiques : celui de la présomption d'innocence .*

** La surveillance rend l'individu transparent, tandis que l'État et la société fonctionnent dans le secret. Comme nous l'avons vu, ce pouvoir est systématiquement abusif.*

** La surveillance est un vol. Ces données ne sont pas un bien public : elles nous appartiennent. Quand elles sont utilisées pour prédire notre comportement, nous sommes spoliés d'autre chose : du principe de la libre volonté, essentiel à la liberté démocratique.*

NOUS EXIGEONS LE DROIT pour tous les peuples à déterminer, comme citoyens démocratiques, dans quelle mesure leurs données personnelles peuvent être légalement collectées, stockées et traitées et par qui; d'obtenir des informations sur l'endroit où leurs données sont stockées et comment elles sont utilisées; d'obtenir la suppression de leurs données si elles ont été illégalement recueillies et stockées.
NOUS APPELONS TOUS LES ÉTATS ET SOCIÉTÉS à respecter ces droits.
NOUS APPELONS TOUS LES CITOYENS à se lever en défense de ces droits.
NOUS APPELONS LES NATIONS UNIES à reconnaître l'importance centrale de la protection des droits civils de l'ère numérique et de créer une Charte internationale des droits numériques.
NOUS APPELONS LES GOUVERNEMENTS à signer et à adhérer à une telle convention. *»*

http://www.change.org/fr/pétitions/pour-une-défense-de-la-democratie-à-l-ère-numérique

* Les 5 Prix Nobel signataires sont : *Orhan Pamuk, J.M. Coetzee, Elfriede Jelinek, Günter Grass et Tomas Tranströmer. Parmi les signataires, se trouvent également Umberto Eco, Margaret Atwood, Don DeLillo, Daniel Kehlmann, Nawal El Saadawi, Arundhati Roy, Henning Mankell, Richard Ford, Javier Marias, Björk, David Grossman, Arnon Grünberg, Angeles Mastretta, Juan Goytisolo, Nuruddin Farah, João Ribeiro, Victor Erofeyev, Liao Yiwu et David Malouf.*

Au niveau international

La résistance citoyenne s'organise

Martine Eloy
Ligue des droits et libertés

Le 31 juillet 2003, à l'initiative de Privacy International, Access et Electronic Frontier Foundation, une centaine d'organisations de divers pays à travers le monde ont lancé un appel à l'endossement de principes internationaux pour encadrer la collecte et l'utilisation de données personnelles dans le respect des droits humains. Cet appel a été rédigé suite à une vaste consultation échelonnée sur une période de plus d'un an auprès d'ONG et d'expert-e-s internationaux sur les aspects juridiques, politiques et technologiques de la surveillance des communications.

Le développement de nouvelles technologies des communications et la capacité qui existe maintenant de numériser l'activité humaine ont rendu possible une collecte sans précédent de données sur tous les aspects de la vie des individus. Toutefois, un consensus général s'est développé au niveau international à savoir que les pratiques actuelles de surveillance sont allées trop loin. Il est urgent de prendre des mesures pour les encadrer, de façon à protéger les droits à la vie privée et à la liberté d'expression. S'appuyant sur le fait que les États ont des obligations à ce chapitre, les 13 principes proposent des balises pour la collecte et l'utilisation de données dans l'environnement numérique actuel.

En décembre 2013, le Conseil d'administration de la LDL a endossé Les principes internationaux pour l'application des droits humains à la surveillance des communications. Ces principes sont généraux, il est vrai, mais il nous incombe de les traduire en lois et règlements applicables ici.

Principes internationaux pour l'application des droits humains à la surveillance des communications

Préambule

Le respect de la vie privée est un droit de l'homme (ndlr : un droit humain) fondamental, indispensable au bon fonctionnement des sociétés démocratiques. Il est essentiel à la dignité humaine et renforce d'autres droits, tels que la liberté d'expression et d'information, ou la liberté d'association. Il est reconnu par le droit international des droits de l'homme. Les activités qui restreignent le droit au respect de la vie privée, et notamment la surveillance des communications, ne sont légitimes que si elles sont à la fois prévues par la loi, nécessaires pour atteindre un but légitime et proportionnelles au but recherché.

Avant la démocratisation d'Internet, la surveillance des communications par l'État était limitée par l'existence de principes juridiques bien établis et par des obstacles logistiques inhérents au contrôle des communications. Au cours des dernières décennies, les barrières techniques à la surveillance se sont estompées. Dans le même temps, l'application des principes juridiques aux nouvelles technologies a perdu en clarté. L'explosion des communications numériques et des informations relatives à ces communications, également appelées « métadonnées des communications » (termes qui désignent les informations portant sur les communications d'une personne ou sur son utilisation d'appareils électroniques), la baisse des coûts de stockage et d'exploration de grands ensembles de données, ou encore la mise à disposition de données personnelles par le biais de prestataires de service tiers, ont conféré à l'État des pouvoirs de surveillance sans précédent. Parallèlement, notre conception des droits de l'homme n'a pas encore intégré les récentes évolutions et la modernisation des moyens de surveillance des communications utilisés par l'État, de la capacité de ce dernier à combiner et organiser les informations obtenues par différentes techniques de surveillance, ou de la sensibilité croissante des informations accessibles.

(…) Malgré le risque élevé d'intrusion dans la vie privée des personnes et l'effet d'intimidation qu'il peut avoir sur les associations politiques ou autres, les instruments législatifs et réglementaires accordent souvent aux métadonnées une protection moindre. Ils ne limitent pas suffisamment la façon dont les agences gouvernementales peuvent manipuler ces informations, notamment pour les explorer, les partager et les conserver.

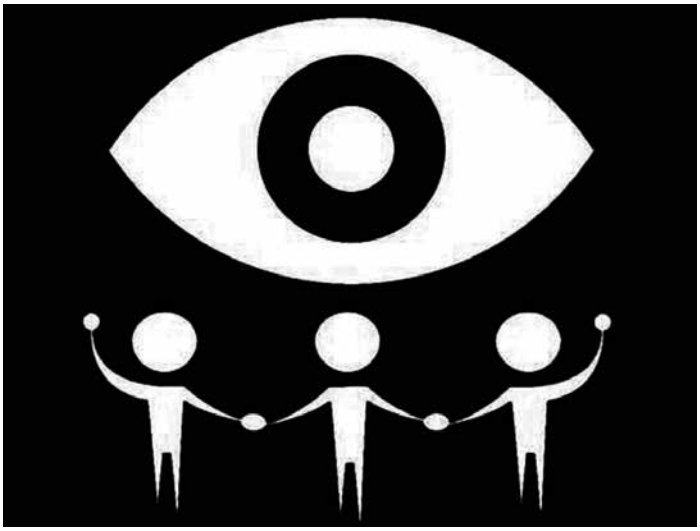
Pour que les États respectent réellement leurs obligations en matière de droits de l'homme au plan international dans le domaine de la surveillance des communications, ils doivent se conformer aux principes présentés ci-dessous. Ces principes s'appliquent à la surveillance exercée au sein d'un État ou la

surveillance extraterritoriale. Ils sont mis en œuvre quel que soit l'objectif de la surveillance : application de la loi, sécurité nationale ou toute autre fin réglementaire. Ils concernent également l'obligation qui incombe à l'État de respecter les droits de chaque individu et de protéger ces droits contre d'éventuels abus commis par des acteurs non étatiques, et en particulier des entreprises privées. Le secteur privé assume une responsabilité équivalente en termes de respect des droits de l'homme, car il joue un rôle déterminant dans la conception, le développement et la diffusion des technologies, dans la mise à disposition des services de communication et, le cas échéant, dans la coopération avec les activités de surveillance des États. Néanmoins, le champ d'application des présents principes est limité aux obligations des États.

Des technologies et des définitions en pleine évolution

Dans un contexte moderne, le concept de « surveillance des communications » désigne le contrôle, l'interception, la collecte, l'analyse, l'utilisation, la préservation, la conservation, la modification ou la consultation d'informations qui contiennent les communications passées, présentes ou futures d'une personne, ainsi que de toutes les informations qui sont relatives à ces communications. Les « communications » désignent toute activité, interaction ou transaction transmise de façon électronique, telle que le contenu des communications, l'identité des parties impliquées, les données de localisation (adresses IP, par exemple), les horaires et la durée des communications, ainsi que les identifiants des appareils utilisés.

Le caractère intrusif de la surveillance des communications est traditionnellement évalué sur la base de catégories artificielles et formelles. Les cadres légaux existants font la distinction entre le « contenu » et les « données hors contenu », les « informations sur l'abonné » et les « métadonnées », les données stockées et celles en transit, les données conservées dans leur emplacement d'origine et celles transmises à un prestataire de services tiers. Pourtant, ces distinctions ne sont plus appropriées pour mesurer le niveau d'intrusion entraîné par la surveillance des communications dans la vie privée et les relations sociales des individus. Il est admis de longue date que le contenu des communications nécessite une protection légale importante dans la mesure où il peut révéler des informations sensibles. Toutefois, il est maintenant clair que d'autres informations issues des communications d'un individu, telles que les métadonnées et d'autres formes de données hors contenu, peuvent fournir plus de renseignements sur cette personne que le contenu lui-même. Elles doivent donc bénéficier d'une protection équivalente. (…) Par conséquent, toutes les informations qui contiennent les communications d'une personne ou sont relatives à ces communications, et qui ne sont pas publiquement et facilement accessibles, doivent être considérées comme des « informations protégées ». Elles doivent donc, à ce titre, bénéficier du plus haut niveau de protection au regard de la loi.



Logo de la campagne *Exigez la fin de la surveillance de masse*..

Pour évaluer le caractère intrusif de la surveillance des communications par l'État, il convient de prendre en considération non seulement le risque de divulgation des informations protégées, mais également les raisons pour lesquelles l'État recherche ces informations. Si la surveillance des communications a pour conséquence de révéler des informations protégées susceptibles d'exposer une personne à des enquêtes, des discriminations ou des violations des droits de l'homme, elle constitue à la fois une violation sérieuse du droit au respect de la vie privée et une atteinte à la jouissance d'autres droits fondamentaux tels que la liberté d'expression, d'association et d'engagement politique. En effet, ces droits ne sont effectifs que si les personnes ont la possibilité de communiquer librement, sans subir l'effet d'intimidation qu'engendre la surveillance gouvernementale. Il est donc nécessaire de rechercher, pour chaque cas particulier, tant la nature des informations collectées que l'usage auquel elles sont destinées.

Lors de l'adoption d'une nouvelle technique de surveillance des communications ou de l'extension du champ d'action d'une technique existante, l'État doit vérifier préalablement si les informations susceptibles d'être obtenues entrent dans le cadre des « informations protégées ». Il est ensuite tenu de se soumettre à un examen par le pouvoir judiciaire ou à un mécanisme de supervision démocratique. Pour déterminer si les informations obtenues par le biais de la surveillance des communications doivent être considérées comme des « informations protégées », il est judicieux de prendre en compte non seulement la nature de la surveillance, mais aussi sa portée et sa durée. Une surveillance généralisée ou systématique peut entraîner la divulgation d'informations privées au-delà des données collectées individuellement. Elle est donc susceptible de conférer à la surveillance des informations non protégées un caractère intrusif nécessitant une protection renforcée.

Résumé des 13 principes internationaux *

Pour déterminer si l'État peut ou non entreprendre une surveillance des communications faisant intervenir des informations protégées, il convient de se conformer aux principes ci-dessous.

Légalité :
Toute limitation au droit à la vie privée doit être fixée par la loi.

Objectif légitime :
Les lois doivent seulement autoriser la surveillance des communications par des autorités étatiques identifiées afin d'atteindre le but légitime qui correspond à un intérêt légal essentiel, nécessaire dans une société démocratique.

Nécessité :
Les lois autorisant la surveillance des communications par l'État doivent limiter la surveillance à ce qui est strictement et manifestement nécessaire au but légitime.

Pertinence :
Tout cas de surveillance des communications autorisé par la loi doit concourir à la réalisation du but légitime spécifique identifié.

Proportionnalité :
Les décisions concernant la surveillance des communications doivent assurer un équilibre entre les bénéfices recherchés et les atteintes aux droits des utilisateurs et des intérêts en présence.

Autorité judiciaire compétente :
Les décisions concernant la surveillance des communications doivent être prises par une autorité judiciaire compétente impartiale et indépendante.

Procédure équitable :
Les États doivent respecter et garantir le respect des droits fondamentaux de chaque individu en s'assurant que des procédures légales régissant les atteintes aux droits de l'homme sont correctement édictées par la loi, systématiquement appliquées, et mise à disposition du public.

Notification à l'utilisateur :
Les individus doivent se voir notifier toute décision autorisant la surveillance de leurs communications dans un délai suffisant et avec assez d'informations pour leur permettre de faire appel de la décision, et doivent avoir accès à tous les documents présentés pour soutenir la demande d'autorisation.

Transparence :
Les États doivent faire preuve de transparence à l'égard de l'utilisation et de l'étendue des techniques et des possibilités de surveillance des communications.

Contrôle public : Les États doivent établir des mécanismes de contrôle indépendants afin de garantir la transparence et la redevabilité dans le cadre de la surveillance des communications.

Intégrité des communications et des systèmes :
Les États ne doivent pas contraindre les fournisseurs de services et les vendeurs de matériel informatique ou de logiciel à développer au sein de leurs systèmes des capacités de surveillance ou de contrôle, ou à collecter ou à stocker des informations.

Garanties relatives à la coopération internationale :
Les traités d'assistance judiciaire mutuelle en vigueur entre les États doivent garantir qu'en matière de surveillance des communications la loi applicable soit celle présentant le plus haut degré de protection.

Garanties relatives à l'accès illégitime :
Les États doivent adopter une législation criminalisant la surveillance illégale des communications par des acteurs publics ou privés.

La résistance prend de l'ampleur

Depuis la rédaction de cet article, deux autres nouvelles coalitions d'organisations de défense des droits humains ont vu le jour.

Le 4 avril, la Coalition contre l'exportation illégale de technologies de surveillance (CAUSE), qui regroupe Amnistie Internationale, Digital Gesellschaft, la FIDH, Human Rights Watch, New America Foundation's Open Technology Institute, Privacy International et Reporters sans frontières, a publié une lettre ouverte par laquelle les organisations sonnent l'alerte face au commerce mondial très peu réglementé des équipements de surveillance des communications.

Puis le 15 mai dernier, un vaste groupe de scientifiques, d'universitaires et de défenseurs des libertés civiles ont rendu publique une déclaration commune, la Déclaration d'Ottawa sur la surveillance au Canada, appelant le gouvernement à une plus grande retenue en matière de surveillance de ses citoyens, mais aussi à la mise en place de balises plus claires et à la mise à jour des lois protégeant la vie privée.

* Pour la version intégrale, la liste complète des signataires ou endosser les principes : rendez vous sur le site https://www.necessaryandproportionate.org

Les recommandations de la Commission O'Connor Plus pertinentes que jamais

Dominique Peschard, président
Ligue des droits et libertés

Rappel des faits

Né en Syrie en 1970, Maher Arar arrive au Canada à titre d'immigrant reçu en 1987 et devient citoyen canadien en 1995. Le 26 septembre 2006, de retour vers le Canada sur un vol d'American Airlines en provenance de Zurich, M. Arar est arrêté lors de l'escale à New York. Le 8 octobre on le fait monter à bord d'un avion privé et il est amené à Amman en Jordanie d'où il est transféré au tristement célèbre centre de détention de Far Falestin dirigé par le Renseignement militaire syrien (RMS). Il est interrogé, torturé et enfermé dans un sordide cachot pendant dix mois avant de pouvoir revenir au Canada. Il devra attendre la sortie du premier rapport de la Commission d'enquête, le 18 septembre 2006, pour être définitivement blanchi. Ce rapport révèle, entre autres, une enquête de la GRC qui trace un portrait de M. Arar fondé sur des faits inexacts ou carrément erronés, qui le décrit sans fondement comme un islamiste extrémiste lié à Al-Qaïda et une pratique d'échange d'information sans restrictions avec les autorités américaines qui ne respecte même pas les propres règles de la GRC.

Le deuxième rapport

Le 12 décembre 2006, le Commissaire de l'enquête Arar, le juge Dennis O'Connor remettait un deuxième rapport intitulé *Un nouveau mécanisme d'examen des activités de la GRC en matière de sécurité nationale*. Ce rapport contient des recommandations importantes pour la protection des droits et libertés, recommandations auxquelles le gouvernement canadien a toujours refusé de donner suite.

L'enquête sur les faits entourant la déportation de Maher Arar vers la torture[1] révélait que 24 agences ou ministères du gouvernement fédéral étaient impliqués dans des questions de sécurité nationale. Des services de police provinciaux ou municipaux, de même que des services de renseignement provinciaux[2] sont susceptibles de travailler en étroite

collaboration avec d'autres agences ou services de police gouvernementaux ou encore de participer à des équipes intégrées d'enquête dont peuvent même faire partie le FBI et la CIA.

Parmi les agences et ministères impliqués en matière de sécurité nationale, seul le *Service canadien du renseignement de sécurité* (SCRS), le *Centre de la sécurité des télécommunications Canada* (CSTC)[3] et la GRC sont dotés chacun d'un organisme chargé de l'examen de leurs activités. Dans le cas de la GRC, il s'agit de la *Commission civile d'examen et de traitement des plaintes* (CCETP)[4] relatives à la GRC dont les pouvoirs sont limités.

Le Commissaire propose donc de remplacer l'ancienne CPP par un organisme indépendant d'examen doté de pouvoirs

1. Voir *Maher Arar : quand les droits humains sont sacrifiés au nom de la liberté,* Bulletin de la Ligue des droits et libertés, automne 2006.

2. Plusieurs services de police municipaux et provinciaux ont leur propre agence de renseignements. Par exemple citons le cas québécois de la *Direction des enquêtes et renseignements de sécurité* (DERS).

3. Il s'agit du *Bureau du commissaire du Centre de la sécurité des télécommunications Canada*. Comme nous l'avons vu dans l'article sur le CSTC, ce mécanisme est totalement inadéquat.

4. Le projet de loi C-42 qui a reçu la sanction royale le 19 juin 2013 a remplacé la *Commission des plaintes du public contre la GRC*, en fonction au moment de l'affaire Arar, par la CCETP. La nouvelle commission n'a toujours pas les pouvoirs recommandés par la Commission Arar.

renforcés, la *Commission indépendante d'examen des plaintes contre la GRC et des activités en matière de sécurité nationale* (CIE). La CIE examinerait également les activités relatives à la sécurité nationale de l'*Agence des services frontaliers du Canada* (ASFC). Les personnes désignées à la CIE devraient être des personnalités tenues en haute estime et qui inspirent au public confiance en leur jugement et leur expérience.

Par ailleurs, le mandat de l'actuel mécanisme de surveillance du SCRS, le *Comité de surveillance des activités de renseignement de sécurité* (CSARS), serait élargi afin de recevoir les plaintes et d'examiner les activités des différents ministères et agences impliqués dans des activités de renseignement relatives à la sécurité nationale, soit le *Centre de la sécurité des télécommunications Canada, Citoyenneté et Immigration Canada, Transports Canada, le Centre d'analyse des opérations et déclarations financières du Canada et le ministère des Affaires étrangères et du Commerce international.*

Enfin, le Commissaire recommande au gouvernement de mettre en place un autre nouveau mécanisme qu'il désigne *Comité de coordination pour l'examen intégré des questions de sécurité nationale* (CCEISN). Le mandat de ce Comité serait, notamment :

• d'offrir un mécanisme de réception centralisé des plaintes concernant les activités relatives à la sécurité nationale d'organisations fédérales;

• de faire rapport sur la reddition de comptes concernant les pratiques et tendances dans le domaine de la sécurité nationale au Canada, notamment les effets de ces pratiques et tendances sur les droits et libertés individuels ;

• de mettre en œuvre des programmes d'information du public concernant le mandat du Comité, en particulier le mécanisme de réception des plaintes;

• d'entamer la discussion sur la collaboration avec les organismes indépendants d'examen des forces policières provinciales et municipales qui participent aux activités relatives à la sécurité nationale.

Le Commissaire recommande que le gouvernement aménage « *[…] des passerelles législatives entre les organismes d'examen des activités relatives à la sécurité nationale, la CIE y compris, pour permettre l'échange d'informations, le renvoi d'enquêtes à un autre organisme, l'institution d'enquêtes conjointes et la coordination de la préparation des rapports.* »

Les mécanismes recommandés par le juge O'Connor augmentent considérablement la protection offerte aux citoyens contre les abus. Afin d'éviter que ces mécanismes ne deviennent des coquilles vides, le gouvernement devra leurs fournir les ressources appropriées afin de permettre la pleine réalisation de leur mandat de surveillance[5].

La situation n'a fait qu'empirer depuis l'affaire Arar. L'accord canado-américain sur la sécurité du périmètre rendu public en mars 2012 représente ni plus ni moins que l'intégration du Canada à l'appareil sécuritaire des États-Unis, sans aucune protection pour les canadien-ne-s des abus qui pourraient en découler. C'est l'abandon pur et simple des normes canadiennes en matière de protection de la vie privée. Le projet donne aux États-Unis un accès à des quantités encore plus grandes de renseignements personnels sur les voyageuses et les voyageurs, y compris l'information biométrique et biographique. De plus, l'entente prévoit l'instauration de listes communes, c'est-à-dire étasuniennes: listes d'interdiction de vol, listes anti-terroristes et autres. Dans tout le document, pas un mot sur la surveillance et l'imputabilité des agences de sécurité, ni sur les droits de recours et de réparation pour les personnes dont les droits seraient violés. L'entente va même à l'encontre des recommandations de la Commission Arar et vise à « encourager les échanges informels de renseignements », ce qui permet aux agences de sécurité d'échapper à tout mécanisme d'imputabilité.

Comme nous l'avons constaté à la Commission Arar, plusieurs États sont souvent impliqués dans les enquêtes en matière de sécurité nationale. Dans le cas de Maher Arar, autant les États-Unis que la Syrie se déchargeaient sur les autres États de leur responsabilité quant au partage d'information et au renvoi vers la torture. Lorsqu'un abus est dévoilé, il est machinal, pour les gouvernements, de « pelleter dans la cour du voisin » et d'accuser les autres États impliqués. En décembre 2004, plusieurs organisations internationales de défense des droits de la personne, dont la Fédération internationale des droits de l'Homme (FIDH), signaient une déclaration conjointe affirmant « *la nécessité d'un mécanisme international de contrôle de la compatibilité des mesures de lutte contre le terrorisme avec les droits de l'homme*[6] ». À moyen terme, le Canada devrait promouvoir la création d'un organisme international pouvant enquêter sur toutes les agences d'enquête quel que soit l'État dont elles dépendent.

5. Coalition pour la surveillance internationale des libertés civiles (CSILC), *Mémoire relatif à l'examen de la politique, déposé devant la Commission d'enquête sur les actions des responsables canadiens relativement à Maher Arar*, le 21 février 2005 : paragraphe 17- N.

6. *Déclaration conjointe sur la nécessité d'un mécanisme international de contrôle de la compatibilité des mesures de lutte contre le terrorisme avec les droits de l'homme*, décembre 2004.

Hors dossier

Le Plan Nord Plus
Rompre avec l'idéologie du « tout à la croissance »

Vincent Greason, vice-président
Ligue des droits et libertés

http://allianceromaine2.wordpress.com

En 2012, des militantes innues soutenus par Alliance Romaine ont occupé l'autoroute 138 près de Sept-Îles pour protester contre Hydro-Québec et le Plan Nord.

Dans un court article publié au lendemain de la victoire électorale du parti Libéral, Bruno Massé observe :

« Durant les élections provinciales, le sujet de l'environnement a été volontairement écarté du débat […] Lors de sa campagne électorale, le nouveau premier ministre Philippe Couillard annonçait que l'environnement n'est pas une priorité pour lui. Ce qui est important, c'est les emplois, par exemple ceux que pourrait créer le Plan Nord (+)[1]*. »*

Philippe Couillard veut reprendre le pari économique nordique de son prédécesseur afin de dégager des centaines de millions de dollars de fonds publics pour promouvoir le développement industriel du Nord québécois. Ainsi, le nouveau gouvernement québécois est sur le point de reproduire un exemple flagrant de la tendance de « tout à la croissance » dénoncée par la LDL dans son récent rapport sur l'état des droits humains au Québec[2]. À moins d'un revirement inattendu, *le Plan Nord* ne s'annonce pas comme un (+) ni pour les peuples autochtones, ni pour les Québécois-e-s, ni pour l'environnement, ni pour les droits humains au Québec.

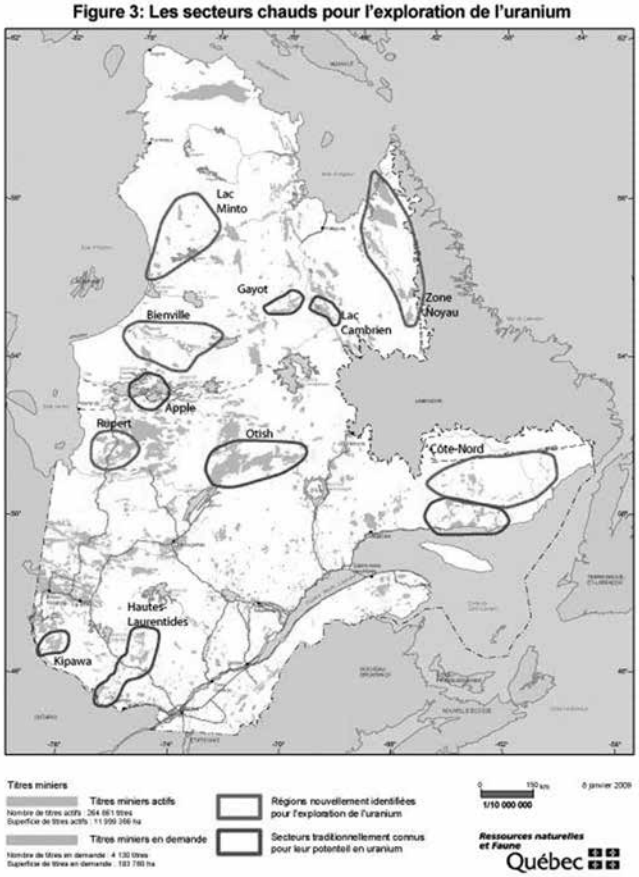
Le Plan Nord : une atteinte aux des droits de la personne

De la manière qu'il a été lancé, le Plan Nord (+) accentue la rupture du lien de confiance entre le peuple et le gouvernement en matière d'exploitation des ressources, de projets de développement et de protection de l'environnement. Il porte atteinte aux droits à l'autodétermination, à l'accès à l'information et à la participation. Par ailleurs, les activités extractives promues par le Plan entraîneront inévitablement des atteintes aux droits économiques, sociaux et culturels de communautés autochtones et québécoises.

1. Massé Bruno, « *L'effondrement de la civilisation et les «vraies affaires»*, Huffington Press, 24/04/2014.

2. Ligue des droits et libertés, Rapport sur l'état des droits humains au Québec et au Canada, 2013, disponible à www.liguedesdroits.ca

Figure 3: Les secteurs chauds pour l'exploration de l'uranium



Les atteintes au droit à l'autodétermination du peuple québécois

L'article premier des deux principaux instruments internationaux relatifs aux droits humains auxquels le Québec s'est déclaré lié en 1976 statue que les peuples « ont le droit de disposer d'eux-mêmes » et de « disposer librement de leurs richesses et ressources ». Ainsi, les choix de modes de développement d'un pays doivent être faits par les peuples ou avec leur consentement. Les gouvernements ne peuvent pas leur imposer des formes de développement allant à l'encontre de leur volonté. Or, dans le cas du Plan Nord (+), aucune tentative sérieuse n'a été entreprise jusqu'à ce jour pour connaitre la volonté des peuples concernés face à ce « chantier d'une génération ».

Que ce soit dans sa version libérale ou péquiste, l'objectif du Plan Nord est de « développer » le vaste territoire du Grand Nord afin de permettre aux entreprises privées, souvent étrangères, d'accéder aux ressources naturelles du peuple québécois et des Premières Nations et d'en tirer profit. Pour faciliter ceci, on propose de nationaliser des investissements en énergie et en infrastructure, un cas classique de collectiviser les risques pour privatiser les profits. De nombreux citoyens, de tous les milieux, s'y opposent. C'est la mobilisation de plus de 250 000 citoyen-ne-s dans les rues de Montréal, le 22 avril 2012, qui a transformé une grève étudiante en un vaste mouvement social qui a fini par faire tomber le gouvernement Charest. Une demande au cœur de cette mobilisation demeure actuelle : « *Que le gouvernement du Québec se dote d'une véritable stratégie, pour le Nord et l'ensemble du territoire où le développement de nos ressources naturelles et énergétiques répond à nos exigences les plus hautes en matière de partage de la richesse, de respect de l'environnement et des populations, maintenant et pour les générations à venir*[3]. »

Le gouvernement Couillard doit prendre acte de cette opposition et mettre en place des mécanismes qui permettront à l'ensemble de la population de se prononcer sur un projet de développement aussi majeur que celui du Plan Nord (+). L'engouement du milieu des affaires ne permet pas au gouvernement du Québec de faire fi d'un débat éclairé, qui respecte le droit à l'information et qui permet aux peuples du Québec de choisir leurs modes de développement et de disposer librement de leurs richesses et de leurs ressources naturelles. Et ce, avant que le Projet aille plus loin.

Les atteintes au droit à l'autodétermination des peuples autochtones

Le droit de disposer librement de ses richesses et de ses ressources naturelles s'applique tout autant aux peuples autochtones qu'au peuple québécois. Alors qu'il est vrai que le gouvernement Charest a obtenu l'accord de principe de la part des nations inuite, naskapie et crie en échange de promesses d'investissements dans les domaines sociaux, l'ancien gouvernement a faussement laissé entendre que son Plan Nord procédait avec l'aval des Premières Nations du Québec.

Dans les faits, l'aval était au mieux partiel. Les communautés innues de Pessamit, de Maliotenam, de La Romaine, de Natashquan et du Labrador ont carrément rejeté le projet de développement qui se déroulera sur des terres dont les titres autochtones n'ont jamais été cédés. Deux autres nations autochtones, les Algonquins et les Attikameks qui vivent au sud du 49e parallèle, mais qui revendiquent des terres au nord de cette ligne, n'ont jamais eu leur mot à dire sur le Plan Nord puisqu'elles n'ont même pas été consultées.

Le droit à l'autodétermination des peuples autochtones est d'ailleurs réaffirmé et spécifiquement protégé par la *Déclaration sur les droits des peuples autochtones* que le Canada a endossée. Le gouvernement du Québec a donc l'obligation de respecter le droit à l'autodétermination de tous les peuples autochtones, y compris de ceux qui s'opposent à ce « projet d'une génération ». L'accord de certains peuples autochtones ne lui permet pas d'ignorer la volonté d'autres peuples, dont celle de la majorité du peuple innu.

3. Déclaration de 22avril.org, signée par 58,947 personnes au 30 mai 2012, http://22avril.org/declaration/

De plus, selon la *Déclaration*, le Québec a l'obligation non seulement de consulter, mais aussi d'obtenir **le consentement** de l'ensemble des peuples autochtones concernés **avant** d'approuver quelconque projet de développement. L'obligation d'obtenir un consentement entraîne la possibilité pour les peuples concernés de refuser l'utilisation ou l'exploitation de leurs ressources.

Le droit d'accès à l'information

Afin de pouvoir disposer librement de leurs richesses et de leurs ressources naturelles, tous les peuples concernés – autochtones et québécois - doivent pouvoir accéder à l'ensemble de l'information relative au Plan Nord (+). Ceci comprend tous les projets s'effectuant sur le territoire du Québec ainsi que sur les territoires ancestraux des peuples autochtones. Le gouvernement et les différents acteurs impliqués doivent faire preuve d'une totale transparence et veiller à l'accessibilité de l'information.

Or, l'opacité avec laquelle s'est effectuée la signature des ententes existantes entre le gouvernement et les entreprises minières est extrêmement préoccupante. Qu'il s'agisse des termes des contrats signés avec les compagnies extractives, des quantités de minerai extraites par celles-ci, des redevances encaissées par l'État en fonction de chaque projet minier ou des obligations de restauration, le gouvernement a jusqu'à maintenant refusé de fournir l'information aux citoyens québécois et aux autochtones, alors que les ressources exploitées leur appartiennent.

Le *Pacte international relatif aux droits civils et politiques* précise pourtant clairement que le droit à la liberté d'expression « comprend la liberté de rechercher, de recevoir et de répandre des informations et des idées de toute espèce ».

L'argument consistant à dire que des informations concernant l'exploitation des ressources naturelles du peuple québécois sont confidentielles en vertu du droit minier ou du droit de la concurrence n'est tout simplement pas recevable dans une société démocratique où les droits humains des citoyens doivent primer sur les intérêts économiques des entreprises privées.

Par ailleurs, très peu d'information existe sur les impacts environnementaux qu'aura le Plan Nord sur ce vaste territoire qui héberge les derniers écosystèmes intacts en territoire forestier. À cet égard, de nombreux groupes écologiques demandent au gouvernement de procéder non seulement à des études d'impact environnemental pour chacun des projets proposés, mais aussi à une évaluation environnementale stratégique plus globale permettant d'étudier l'impact des contaminants générés par l'ensemble des activités extractives, des modes de transport et des projets énergétiques sur les cours d'eau, la santé publique, les changements climatiques, etc.

Le droit à la participation

Le public québécois doit être impliqué dans le processus de prise de décisions relatif au Plan Nord (+). Le droit à la participation est protégé par certains instruments internationaux, en particulier par le *Pacte international relatif aux droits civils et politiques* qui garantit à tout citoyen le droit « de prendre part à la direction des affaires publiques, soit directement, soit par l'intermédiaire de représentants librement choisis ». Par ailleurs, la *Convention sur l'élimination de toutes les formes de discrimination à l'égard des femmes* protège le droit des femmes de « participer pleinement à l'élaboration et à l'exécution des plans de développement à tous les échelons ». Aussi, la *Déclaration des Nations Unies sur les droits des peuples autochtones* stipule que « Les peuples autochtones ont le droit de participer à la prise de décisions sur des questions qui peuvent concerner leurs droits ». La participation du public est également reconnue comme une condition essentielle non seulement à la protection de l'environnement, mais aussi à la protection du droit à la santé.

Les atteintes potentielles aux droits économiques, sociaux et culturels

Au vu des informations scientifiques sur la question, l'exploitation et l'éventuelle transformation des minerais exploités dans le cadre du Plan Nord (+) comportent des risques réels pour l'environnement et, par conséquent, sur le droit à la santé et à l'eau.

Le droit à l'eau et le droit à la santé mis à risque

De nombreuses études démontrent que des risques existent pour la santé de la population dans l'exploitation de certains métaux comme l'or ou l'uranium. L'exploitation de l'uranium génère d'immenses quantités de résidus miniers radioactifs qui doivent être entreposés sur le territoire, et pour lesquels les risques de contamination demeurent présents à perpétuité. Un des résidus de l'uranium, le gaz radon, est d'ailleurs la deuxième cause de cancer du poumon après le tabac au Canada, étant responsable de plus 2000 décès par année au pays. Les travailleurs de mines d'uranium sont particulièrement à risque du cancer du poumon. Une concentration accrue de cette poussière radioactive dans l'atmosphère en cas d'accident ou de dégradation des mesures d'entreposage pourrait avoir un impact réel sur la santé humaine.

C'est également à travers les risques de contamination des cours d'eau que des violations au droit à la santé et au droit à l'eau risquent de survenir. Les méthodes utilisées pour confiner les résidus miniers uranifères, soit l'entreposage dans des fosses à ciel ouvert ou l'entreposage dans des

bassins construits à cet effet à l'aide de digues de rétention, présentent des défis techniques importants sur le long terme et ne sont pas à l'abri de fuites qui pourraient atteindre les cours d'eau.

Quant à l'exploitation d'autres métaux, il est connu que l'extraction et la transformation de ceux-ci nécessitent des quantités importantes d'énergie, d'eau et de produits chimiques de toutes sortes (dont le cyanure dans le cas de l'extraction aurifère). Même le ministère du Développement durable, de l'Environnement et de la Lutte contre les changements climatiques du Québec reconnait que les cours d'eau dans les régions minières, dont celles touchées par le Plan Nord (+) présentent des concentrations de métaux préoccupantes en raison de l'activité extractive. Par conséquent, il est essentiel que chacun des projets miniers fasse l'objet d'une étude d'impact environnementale.

Le fait que le territoire du Grand Nord se situe dans une région peu peuplée, loin des grands centres urbains, ne justifie pas de prendre à la légère les obligations inscrites dans les instruments internationaux de protection des droits humains. Non seulement une contamination des cours d'eau risque-t-elle de violer les droits à la santé et à l'eau des populations du Grand Nord, mais elle pourrait également atteindre les nappes phréatiques et par là, le reste de la population québécoise.

Les droits sociaux (logement, alimentation)

Une recherche récente, menée par l'*Institut de recherches et d'informations socio-économiques* (IRIS), a pris en cas d'espèce la ville albertaine de Fort McMurray pour étudier les bouleversements sociaux qui peuvent accompagner un « boom économique » associé au développement rapide des industries extractives. L'IRIS suggère d'examiner le Plan Nord à la lumière du cas de cette ville nordique de l'Alberta. Les villes québécoises de Baie-Comeau, Sept-Iles et Port-Cartier, points de service au développement nordique, rapportent déjà les faits troublants prévus par l'IRIS : explosion des prix, pénurie de logements, phénomène nouveau d'itinérance, prix alimentaires inabordables… Un tel dérapage affecte surtout la population d'origine, et plus particulièrement les personnes vulnérables : personnes âgées, monoparentales, prestataires d'aide sociale dont les droits économiques et sociaux sont particulièrement fragilisés.

Le droit des générations futures

Malgré le fait qu'il n'existe pas à ce jour un traité de protection des droits humains qui consacre spécifiquement le droit des générations futures, rappelons que tous les droits humains sont interreliés, interdépendants et universels, comme l'a rappelé avec force la *Conférence de Vienne* de 1993[4]. Ceci signifie qu'ils s'appliquent à tous les êtres humains et s'appliqueront dans l'avenir à tous les êtres humains qui naîtront. Or, avec le Plan Nord (+), l'enjeu essentiel est celui du legs nordique que nous laisserons à nos enfants et petits-enfants. À maints égards, la manière dont le Québec choisira de « développer » le Grand Nord québécois en dira long sur les valeurs que porte notre peuple. Aura-t-on le courage de rompre avec la tendance de « tout à la croissance »?

4. Conférence mondiale sur les droits de l'homme, article 5, Vienne, 14 au 25 juin 1993 : « *Tous les droits de l'homme sont universels, indissociables, interdépendants et intimement liés. (…)* »

* L'auteur tient à reconnaitre l'apport important d'Alexa Leblanc et de Maude Prud'homme à la rédaction d'un texte inédit qui a largement inspiré le présent texte. Les lecteurs qui voudraient obtenir des références plus précises de certains points sont invités à communiquer avec l'auteur. vtrovepo@bellnet.ca

Une série de fascicules sur des enjeux de droits et libertés

La liste noire de passagers aériens

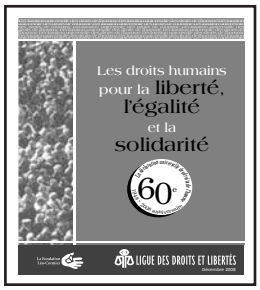
La Loi antiterroriste

Les certificats de sécurité

Le « Taser » une arme inoffensive?

La laïcité

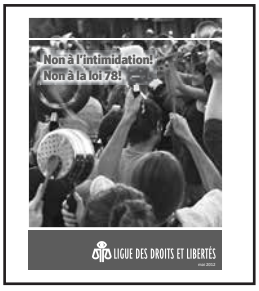
La surveillance de nos communications



Le 60e de la DUDH

Vie privée et renseignements personnels

Droits humains, droit d'asile et immigration



Non à l'intimidation! Non à la loi 78!

La liberté d'expression

L'environnement un enjeu de droits humains

Les droits humains, j'y adhère!

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

Nom : Prénom :

Adresse : Ville : Prov. : Code postal :

Courriel : Tél. maison : Tél. travail :

Ligue des droits et libertés
50 ans d'action

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 LDL par courriel plutôt que par la poste.

*** La LDL accepte les adhésions individuelles, quelle que soit la somme versée.**
En devenant membre de la LDL, vous recevrez ses publications ainsi que l'infolettre (courriel). Faites parvenir votre coupon dûment rempli à :
LDL, 516 rue Beaubien Est Montréal (QC) H2S 1S5 ou au bureau de votre section régionale. Les renseignements nominatifs que vous fournissez demeurent confidentiels.

LDL – SIÈGE SOCIAL
516, rue Beaubien Est, Montréal,
(Québec), H2S 1S5
Téléphone : 514-849-7717 poste 21
Télécopieur : 514-849-6717
Courriel : info@liguedesdroits.ca
Site internet : www.liguedesdroits.ca

LDL – SECTIONS RÉGIONALES

LDL – Section Estrie
187, rue Laurier, bureau 313
Sherbrooke, Québec, J1H 4Z4
Téléphone : 819-346-7373
Télécopieur : 819-566-2664
Courriel : ldlestrie2005@yahoo.ca

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
363, rue de la Couronne, 5e étage,
Québec (QC) G1K 6E9
Téléphone : 418-522-4506
Télécopieur : 418-522-4413
Courriel : info@liguedesdroitsqc.org
Site internet : www.liguedesdroitsqc.org

Ligue des
droits et libertés

FONDATION LÉO-CORMIER
pour l'éducation aux droits et libertés