Après le 11 septembre 2001 : sécurité ou surveillance ? Analyse de la politique canadienne en matière de contrôle du contenu informatique

Éric GEORGE [1]

Résumé : Les technologies ont toujours été employées à des fins de surveillance. En témoigne par exemple le panoptique de Jeremy Bentham, un système technique – rendu célèbre par l'analyse faite par Michel Foucault – qui permettait à un individu d'observer un ensemble de personnes sans que celles-ci ne puissent savoir qu'elles étaient regardées. Dans ce texte, nous proposons de présenter les politiques de surveillance du contenu informatique qui ont été mises en oeuvre au Canada suite au développement d'Internet et depuis les attentats du 11 septembre 2001. Ce sera l'occasion de mettre en évidence les tensions entre les positions des institutions étatiques qui justifient les politiques par la nécessité de renforcer la sécurité dans un contexte de montée en puissance du terrorisme international et les composantes de la « société civile » qui se sont opposées à la mise en place de ces politiques en faisant part de leur inquiétude vis-à-vis des menaces que celles-ci pourraient entraîner sur le plan des libertés en favorisant le développement d'une « société de contrôle ». Nous verrons aussi qu'il n'y a pas unanimité au sein de ces deux ensembles d'acteurs sociaux.

Abstract: Technologies have a long history of being employed for monitoring and surveillance purposes. This is perhaps best exemplified in notion of the panopticon, or the ability to observe large groups of people without without any one individual knowing when s/he was being observed, that emerged from Michel Foucault's analysis of the prison architecture designed by Jeremy Bentham. in the 1800s. In this paper we examine the policies of surveillance of the informatic content implemented in Canada during the past decade, in response to the evolution of Internet in the post-9/11 period. Particular attention is given to the tensions between the justifications provided by political institutions regarding the need to enhance security in the light of threats created by international terrorism and the arguments presented by civil society representatives who are concerned about a potential shift toward the establishment of a surveillance society. We will see also that there is not unanimity within these two sets of social actors.

Mots clés : informatique, TIC, Internet, sécurité, surveillance, contrôle, liberté, 11 septembre 2001, terrorisme.

Key words : informatics, ICT, Internet, security, surveillance, control, freedom, September 11, 2001, terrorism.

[1] Adresse de courriel : george.eric@uqam.ca
Adresse postale : École des médias, Faculté de communication, Université du Québec à Montréal (UQAM)
Case Postale 8888, Succursale Centre Ville, Montréal, Qc, H3C 3P8, Canada

Après avoir étudié l'évolution des discours critiques consacrés à l'informatisation au cours des vingt-cinq dernières années, Dominique Carré a conclu que nous assistons de la part des « mouvements sociaux » à « un revirement, pour ne pas dire un retournement de perspective. [À] la fin des années 1970, la critique sociale portait sur les limites de l'informatisation, les répercussions négatives engendrées par la technique informatique, sur l'utilisation de la technique par le capital pour aliéner davantage les travailleurs exploités » (2004, p.8). Maintenant, les discours dominants ne remettent plus en cause l'orientation du processus d'informatisation mais, au contraire, l'encouragent le plus souvent. Comment expliquer ce changement pour le moins important, si ce n'est radical ? Le chercheur écrit que le développement de la micro-informatique a dû largement contribuer à repousser les craintes – concernant notammment la surveillance – liées au déploiement des gros ordinateurs. À partir de cette explication que nous pensons en effet pertinente, nous proposons de nous interroger dans ce texte sur les positions respectives de deux ensembles d'acteurs sociaux, les représentants de l'État et les composantes de la « société civile » dans le contexte de l'après 11 septembre 2001. Aux États-Unis, mais aussi dans d'autres pays, de nouvelles lois ont été votées après les attentats de New York et de Washington pour favoriser la lutte contre les utilisations criminelles d'Internet et d'autres moyens de communication, comme les téléphones portables, notamment en lien avec le terrorisme. Ci-dessous, en nous concentrant sur le cas du Canada, nous allons aborder d'une part les contenus législatifs et réglementaires ainsi que les justifications des responsables politiques et d'autre part les points de vue des composantes de la « société civile » qui se sont opposées à la mise en place de ces politiques en faisant part de leur inquiétude vis-à-vis des menaces que celles-ci pourraient entraîner sur le plan des libertés en favorisant le développement d'une « société de contrôle ». Nous verrons aussi que l'unanimité n'a pas été de mise de chaque côté de ces deux ensembles d'acteurs sociaux, notamment au sein de l'appareil étatique canadien[2].

1. La situation avant les attentats du 11 septembre 2001

Il importe tout d'abord de mentionner que le Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC) a décidé en 1999 de ne pas réglementer le réseau Internet estimant d'une part que celui-ci ne pouvait pas être considéré comme un média de masse et d'autre part que des textes juridiquement contraignants pouvaient s'appliquer moyennant éventuellement quelques adaptations. Ainsi, le Code criminel canadien a été légèrement modifié pour intégrer certaines crimes tels que la pornographie infantile en ligne. Mais en ce qui concerne les pratiques de surveillance des contenus transmis par voie informatique, deux lois ont un rôle essentiel. La Loi sur la protection des renseignements personnels, en vigueur depuis 1983, encadre les usages des informations personnelles recueillies par des institutions gouvernementales [Canada, Ministère de la Justice, 2007a]. Les informations collectées par ces institutions doivent l'être pour des raisons précises, uniquement pour les besoins identifiés avant la collecte. Elles doivent aussi être consultables et modifiables par toutes les personnes concernées. Quant à la Loi sur la protection des renseignements personnels et les documents électroniques, elle date de 2000 et vise à gérer les renseignements colligés par les entreprises privées dans le cadre de leurs activités commerciales [Canada, Ministère de la Justice, 2007b]. D'une part, les citoyens et citoyennes ont le droit de connaître les objectifs poursuivis par l'organisme et la teneur des informations qui sont connues d'eux, tout en demandant éventuellement à corriger celles-ci. D'autre part, les organisations doivent obtenir le consentement de la personne concernée pour recueillir,

[2] L'auteur de ce texte tient à remercier Renée Marchand, étudiante au département de communication à l'Université d'Ottawa, pour son travail de recherche sur la réglementation d'Internet dont il a repris quelques éléments dans ce texte. Il reste toutefois entièrement responsable de son contenu.

utiliser ou communiquer des renseignements personnels, sauf dans certaines circonstances, notamment les cas de sécurité nationale et les menaces à la sécurité d'autrui [Canada, Commissariat à la protection de la vie privée, 2000].

Il incombe au Commissariat à la protection de la vie privée du Canada d'assurer la surveillance des deux lois fédérales grâce à la réception de plaintes à propos du contenu et du traitement des renseignements collectés. Après réception des plaintes, il enquête sur celles-ci et les règle, tout en pouvant aussi prendre l'initiative de déposer lui-même des plaintes. Il sensibilise également le public aux questions relatives à la protection des renseignements personnels. Il peut rendre toute information publique mais n'a pas de pouvoir de sanction. Toutefois, il peut soumettre les problèmes graves à la Cour fédérale du Canada, laquelle peut ensuite ordonner aux organisations de cesser certaines pratiques et accorder des dommages et intérêts, parfois considérables. Cette institution a un ou une commissaire à sa tête, un haut fonctionnaire qui relève directement du Parlement et qui fait office d'*ombudsman*. Il importe de noter par ailleurs que dans le cas des actions menées par les entreprises privées, le Commissariat n'intervient pas dans les provinces qui ont adopté des lois similaires à la loi fédérale en matière de protection des renseignements personnels. Le Québec a été la première province à promulguer une loi dont les objectifs globaux et l'intention générale ont été jugés par le Commissaire à la protection de la vie privée du Canada « essentiellement similaires » à la LPRPDÉ. C'est maintenant aussi le cas en Alberta et en Colombie-Britannique [Canada, Commissariat à la protection de la vie privée, 2007].

2. La situation après les attentats du 11 septembre 2001

2.1 Les États-Unis, premier pays à légiférer

Logiquement, c'est aux États-Unis que les attentats du 11 septembre 2001 ont eu l'impact le plus rapide en termes législatifs quant aux politiques de contrôle des activités sur le territoire. Le 26 octobre suivant, George W. Bush signait le USA Patriot Act voté auparavant par le Congrès. Ce texte de loi visait à renforcer les pouvoirs des différentes agences gouvernementales, à savoir le Federal Bureau of Investigation (FBI), la Central Intelligence Agency (CIA), la National Security Administration (NSA) et l'armée. Suivront d'autres textes comme le Homeland Security Act (HSA) en 2002 qui stipule qu'il est possible de demander aux fournisseurs d'accès des renseignements personnels, tels que les sites Internet visités par une adresse IP quelconque, sans mandat autorisé par une Cour de justice et le Controlling the Assault of Non-Solicited Pornography and Marketing Act de 2003, ou CAN-SPAM Act, qui a pour but de protéger les internautes des pourriels abusifs.

Plus récemment, en 2005, l'USA Patriot Act est revenu sur le devant de la scène car bon nombre de ses dispositions n'étaient valides que pendant quatre ans. Un véritable débat a alors eu lieu à la Chambre des représentants et au Sénat. Mais malgré l'opposition d'un nombre important de parlementaires, les pouvoirs des agences ont encore été renforcés, la plupart des mesures adoptées en 2001 sur une base temporaire en tant que procédures d'urgence ayant été transformées en dispositions permanentes. Jean-Claude Paye estime en conséquence que : « le renouvellement du Patriot Act permet d'inscrire dans la durée des mesures qui, lors de leur première adoption en 2001, furent justifiées par une situation d'urgence. En devenant permanentes, ces mesures de surveillance intrusives deviennent la base d'un nouvel ordre politique qui donne à l'administration des prérogatives revenant au pouvoir judiciaire. Cependant, contrairement à la première version, votée par la Chambre en Juin 2005, la forme juridique adoptée reste celle de l'état d'exception permanent et non

directement celle de la dictature » [Paye, 2007]. Et il ajoute que « la résistance du Sénat a permis de garder et d'introduire quelques possibilités formelles de contrôle et de recours judiciaires » mais « sans que celles-ci entament réellement les prérogatives du FBI et du gouvernement » [Paye, 2007].

2.2 La loi antiterroriste au cœur des politiques au Canada

Tout comme aux États-Unis, les politiques canadiennes en matière de contrôle des activités prétenduement dangereuses pour la collectivité ont pris de l'ampleur suite aux attentats du 11 septembre 2001, et ce même si les discours ont varié selon les moments. Le gouvernement a parfois affirmé que les nouveaux projets de loi n'étaient pas liés directement aux attentats à New York et Washington, les premières études sur les problèmes de criminalité et les graves menaces à la sécurité nationale perpétrées à l'aide des technologies de l'information et de la communication (TIC) remontant au mois d'octobre 2000 [Canada, Ministère de la Justice, 2006]. Mais à d'autres moments, le gouvernement a justifié ses orientations de lutte contre le terrorisme en mentionnant non seulement les attentats du 11 septembre 2001 mais aussi les attentats à l'explosif dans une discothèque de Bali en 2002, dans une gare ferroviaire de Madrid en 2004, la tragédie survenue dans une école de Russie la même année et l'attentat à l'explosif d'un autobus à Londres en juillet 2005, autant d'« exemples saisissants des dangers posés par le terrorisme » Avant d'ajouter qu'« aucun pays n'est à l'abri, pas même le Canada » [Canada, Ministère de la Justice, 2007c].

Concrètement, le gouvernement canadien a rapidement présenté sa stratégie autour de la Loi antiterroriste. Celle-ci a reçu la sanction royale dès le 18 décembre 2001 et est entrée en vigueur 16 jours plus tard, ce qui a placé le Canada juste après les États-Unis et la Grande-Bretagne en termes de rapidité à légiférer. La loi antiterroriste a consisté en une loi d'ensemble comprenant de nouvelles mesures et modifiant six lois existantes : le Code criminel, la Loi sur la protection de l'information (modifiant et remplaçant la Loi sur les secrets officiels), la Loi sur la preuve au Canada, la Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes, la Loi sur l'enregistrement des organismes de bienfaisance (renseignements de sécurité) et la Loi sur la défense nationale. De plus, la loi a comporté de nombreuses modifications importantes à d'autres mesures législatives. [Canada, Ministère de la Justice, 2007c]. L'objectif principal consistait à pouvoir prendre des mesures susceptibles d'anticiper les actions terroristes. Cette loi a été présentée comme le moyen pour le pays de respecter ses obligations internationales en matière de lutte contre le terrorisme après qu'il ait ratifié deux conventions des Nations Unies sur le terrorisme et après la mise en œuvre de la Résolution 1373 du Conseil de sécurité des Nations Unies qui a enjoint les États à prendre des mesures, notamment contre le financement du terrorisme [Organisation des Nations Unies, Conseil de sécurité, s.d.]. Grâce à la loi, de « nouvelles infractions sur le terrorisme ont été ajoutées aux pouvoirs prévus dans le Code criminel relativement à la surveillance électronique » [Canada, Ministère de la Justice, 2007c]. Il n'a notamment plus été obligatoire de faire appel à la surveillance électronique uniquement en tant que « dernier recours » dans le cadre d'enquêtes sur des terroristes.

Cela dit, l'article 145 stipulait que la loi devait être réexaminée par un comité du Sénat ou un comité de la Chambre des communes avant une période de trois ans. À la Chambre des communes, le Comité permanent de la justice, des droits de la personne, de la sécurité publique et de la protection civile a chargé son sous-comité de la sécurité publique et nationale de procéder à l'examen. Au Sénat, un comité spécial a été mis sur pied en décembre 2004 pour effectuer aussi un examen. Mais ni l'un, ni l'autre des comités n'ont présenté de

rapport à cet égard avant la dissolution du 38e Parlement décidé par le premier ministre libéral sortant, Paul Martin. Et le gouvernement conservateur de Stephen Harper, nouvellement élu, a décidé de ne pas considérer le dossier comme prioritaire lors de la 39e législature, aucune réunion n'ayant eu lieu depuis le 3 avril 2006.

2.3 Le projet d'« accès légal » promu par les autorités politiques

En plus des projets de loi présentés ci-dessus, le gouvernement canadien a tenté de légiférer davantage sur les techniques d'enquêtes et la surveillance électronique. La législation en matière d'accès légal devait faciliter les interceptions de communications, les perquisitions et la saisie de données, notamment informatiques. Étaient considérées les télécommunications, avec ou sans fil ainsi que la « technologie Internet ». Des textes de loi avaient déjà prévu des cas de ce genre à l'image des dispositions actuelles du Code criminel qui portent sur l'interception des communications promulguées pour la première fois en 1974. Par la suite, le Code criminel a été modifié dans les années 1980 afin que les dispositions qui portent sur les saisies et les perquisitions visent spécifiquement les systèmes informatiques. En 1984, le Parlement a adopté la Loi sur le Service canadien de renseignement de sécurité (SCRS), qui a donné au SCRS le pouvoir d'intercepter légalement les communications privées, à des fins de sécurité nationale. Mais depuis, selon le Ministère de la Justice « si la technologie a évolué de manière considérable […], les lois canadiennes en matière d'accès légal n'ont pas suivi. Les technologies de plus en plus complexes posent un défi aux méthodes conventionnelles d'accès légal » [Canada, Ministère de la Justice, 2006]. Par ailleurs, toujours selon le Ministère, étant donné que les TIC se répandaient de plus en plus à une échelle internationale et que la criminalité avait aussi une dimension globale croissante, il devenait nécessaire de coopérer internationalement afin d'élaborer des solutions efficaces.

Le Canada avait d'ailleurs participé à l'élaboration de la Convention sur la cybercriminalité avec le Conseil de l'Europe, l'Afrique du sud, les États-Unis et le Japon. Mais alors que le projet avait donné lieu à de nombreuses discussions avant les attentats du 11 septembre 2001, le texte définitif fut adopté très vite après ceux-ci, soit le 23 novembre 2001 à Budapest. Il avait pour but de favoriser l'établissement d'une politique commune en vue de protéger la société contre la cybercriminalité, notamment par le truchement de lois et à l'aide d'une plus grande coopération internationale [Conseil de l'Europe, 2001]. En conséquence, le gouvernement canadien présenta l'accès légal comme « l'aboutissement d'une étude globale entamée en octobre 2000… [qui visait] la recherche de solutions au problème de la criminalité et des menaces à la sécurité nationale graves perpétrées à l'aide des nouvelles technologies » [Canada, Ministère de la Justice, 2006] et comme le moyen de ratifier la Convention sur la cybercriminalité.

C'est l'année suivante que le gouvernement fédéral publia un premier document de consultation intitulé « Accès légal ». Ce document présentait les principes d'une future législation permettant, d'une part, d'augmenter les capacités de surveillance électronique en les adaptant aux technologies actuelles et futures des systèmes informatique et télécommunicationnel et, d'autre part, de contraindre les fournisseurs d'accès, à stocker les données disponibles sur leurs serveurs afin de les remettre éventuellement aux personnes chargées d'appliquer les lois. Étaient mentionnées parmi les raisons en faveur de ce plan la lutte contre la pornographie infantile, la lutte contre les virus informatiques et bien entendu la lutte contre le terrorisme.

Il s'agissait donc de pouvoir utiliser les systèmes informatiques à des fins de surveillance et d'enquête en assurant l'accès à tout un ensemble de données. Les fournisseurs d'accès devaient garder les communications au cas où. Le gouvernement souhaitait en plus d'une part qu'il ne soit plus nécessaire qu'une autorisation judiciaire fasse appel à des motifs raisonnables pour avoir accès aux données et d'autre part qu'aucune autorisation judiciaire ne soit nécessaire au début d'une enquête. Enfin, le projet prévoyait aussi d'autoriser des organismes de police étrangers à faire ce que certains corps policiers n'auraient pas pu faire sur leur propre territoire selon le principe de l'indissociabilité entre la sécurité nationale et la mise en place d'une police internationale.

Toutefois, très vite, des oppositions se sont fait sentir. C'est ainsi que le commissaire à la protection de la vie privée George Radwanski critiqua le texte en ces termes : « En vertu de la proposition dite d'"accès légal" que le gouvernement fédéral met de l'avant, l'utilisation que nous faisons d'Internet et nos communications électroniques seraient scrutées d'une manière sans précédent. L'interception et la surveillance des communications privées constituent une activité hautement envahissante qui frappe au cœur même du droit à la vie privée. Si les Canadiennes et les Canadiens ne peuvent plus être assurés que leurs activités d'internautes et leurs communications électroniques sont réellement privées, le droit à la vie privée que défend notre pays sera gravement atteint, et ce, de manière inutile et injustifiable » [Canada, Commissariat à la protection de la vie privée, 2004]. Il ajoutait qu'il considérait positivement le fait que le projet ne prévoyait pas de collliger les données portant sur les communications par Internet et par téléphonie cellulaire de façon systématique.

Puis il faisait la mise en garde suivante : « nous n'accepterions pas une proposition visant à permettre aux organismes d'application de la loi et de la sécurité nationale de photocopier la correspondance de toutes les Canadiennes et de tous les Canadiens ou d'enregistrer les appels téléphoniques au cas où ils ou elles voudraient lire cette correspondance ou écouter ces appels ultérieurement. Une ordonnance générale de rétention serait tout autant une attaque contre la vie privée » [Canada, Commissariat à la protection de la vie privée, 2004].. Avant d'être très sévère avec la mesure suivante: « le document de consultation propose la création d'"ordonnances de conservation des données" qui "exige du fournisseur de services qu'il stocke et conserve toutes les données existantes qui se rapportent à une transaction ou à un client spécifique". L'objet d'une telle ordonnance est de faire en sorte que les fournisseurs de services de communication, en tant que gardiens des données sur les communications, ne suppriment pas l'information relative à un abonné jusqu'à ce qu'ils aient reçu un mandat de saisie ou une ordonnance de production des données. Les ordonnances de conservation sont tout aussi dangereuses et non appropriées, du point de vue de la protection de la vie privée, que peuvent l'être les ordonnances de rétention » (ibid.). Avant d'ajouter que le danger principal résidait dans la banalisation possible de ce genre de pratique intrusive : « l'ingérence dans la vie privée des Canadiennes et des Canadiens à un niveau sans précédent ne devrait pas être rendue pratique ou facile à un point tel qu'elle encouragerait de telles activités de façon générale plutôt que dans les situations les plus graves et inévitables » [Canada, Commissariat à la protection de la vie privée, 2004]. On a pu constater qu'il n'y avait pas unanimité au sein de l'appareil étatique canadien.

2.4 Un projet très controversé au sein de la « société civile »

Les positions du Commissariat à la protection de la vie privée du Canada ont d'ailleurs souvent servi de justificatif dans l'argumentaire des composantes de la société civile qui se sont élevées contre le projet de loi. Des mémoires ont été déposés dans le cadre de la

consultation sur l'accès légal en 2003. 14 d'entre eux émanaient de groupes de la société civile[3]. À la lecture de ceux-ci, un reproche majeur ressort : le manque crucial d'arguments susceptibles de montrer que le projet de loi contribuerait à lutter efficacement contre le crime organisé ou le terrorisme alors qu'il apparaît plutôt susceptible de favoriser l'accès à la vie privée des Canadiens. Il n'a pas été démontré selon plusieurs organismes que l'élargissement de l'accès légal aux communications privées entraineraît plus d'avantages sur le plan de la sécurité que d'inconvénients liés à une atteinte à la vie privée. De plus, certains groupes ont mentionné que si le projet de loi et la convention sur la cybercriminalité allaient finalement à l'encontre des valeurs et des droits garantis par la Charte des droits et libertés et interprétés par la Cour suprême du Canada, il serait alors nécesssaire de renoncer aux deux textes. D'autres arguments ont été évoqués avec une fréquence moindre, à commencer par le fait qu'il était anormal que les exigences soient moins fortes à l'égard de l'interception légale, des perquisitions et des saisies de communications en ligne que dans le cas des communications téléphoniques ou postales. Enfin, notons qu'un organisme s'est inquiété de la possibilité de surveiller les échanges d'opinions sur la politique, la religion et la culture, et qu'en conséquence la future loi ne menace pas seulement la le droit à la vie privée mais aussi la liberté d'expression et la liberté d'association [Canada, Ministère de la Justice, 2003].

Toujours en 2003, une série d'organismes de la société civile a signé au Québec la Déclaration contre le projet du gouvernement fédéral « Accès légal ». Y figuraient la Ligue des droits et libertés du Québec, la Fédération des infirmières et des infirmiers du Québec, l'Association étudiante facultaire de sciences politiques et droit de l'UQAM, le Centre de documentation sur l'éducation des adultes et la condition féminine (CDEACF) et le Carrefour mondial de l'Internet citoyen (CMIC). Ils se sont opposés au contenu du projet en estimant que celui-ci allait permettre de surveiller non seulement les courriels, mais aussi les transactions bancaires, les prescriptions pharmaceutiques, les informations médicales, etc. « Le projet a des conséquences dépassant de loin la simple répression de ces crimes particuliers. Il risque de nous faire basculer dans un monde où nos courriers électroniques, nos consultations et visites sur Internet, où nos moindres gestes pourraient être épiés, où nous serions comme des microbes sous le microscope » [Ligue des droits et libertés du Québec et ali., 2003].

Notons enfin la présence d'une autre association, cette fois à l'ouest du pays en Colombie-Britannique, la Freedom of Information and Privacy Association (FIPA) qui, tout en prenant position contre le projet d'accès légal, a participé avec le Ministère fédéral de la Justice à la tenue de rencontres en 2005 avec une trentaine de groupes de la région de Vancouver. L'opinion majoritaire s'est avérée nettement défavorable au projet considéré comme susceptible de porter atteindre à la vie privée ds citoyens et citoyennes du pays. Néanmoins, tout en s'opposant au fait que les règlements prévus diffèrent selon les modes de communication, par Internet, par téléphone ou par courrier postal, l'association n'était pas forcément contre le recours de la police aux contenus informatiques [BC Freedom of Information and Privacy association, 2005]. Cette position nuancée a témoigné de l'existence de certaines différences de points de vue parmi les organismes de la « société civile ».

---

[3] Les associations étaient les suivantes : B.C. Civil Liberties Association, British Columbia Freedom of Information and Privacy Association, Association du Barreau canadien, Association canadienne des libertés civiles, Canadian Library Association, Civil Liberties Association, NCR / Association des droits civils, région de la capitale nationale, Electronic Frontier Canada et Electronic Frontier Foundation (É.U.), Internet Law Group-Université du Manitoba, Option consommateurs, PovNet, Privaterra - Computer Professionals for Social Responsibility, Public Interest Advocacy Centre / Centre pour la défense de l'intérêt public, Vancouver Community Network.

3. La situation actuelle et à venir

Une première lecture du projet de loi a eu lieu en 2005 à la Chambre des communes mais ce dernier n'est jamais passé à l'étape suivante suite à la dissolution de la Chambre sur décision du premier ministre Paul Martin le 23 janvier 2006. Depuis, le parti libéral a laissé la place à la tête du pays au parti conservateur. On peut se demander si la situation changera avant les prochaines élections étant donné que le gouvernement est minoritaire et qu'en conséquence, les votes à la Chambre des communes sont l'occasion de voir à l'œuvre des majorités fragiles. Or, comme nous l'avons vu, les mesures de lutte contre le terrorisme ne font pas l'unanimité, loin de là. Certains experts s'attendent toutefois à ce que le projet de loi soit à nouveau prochainement au programme de la Chambre des communes. Michael Geist estime même que dans un tel cas, la nouvelle loi serait probablement plus musclée [Geist, 2006a]. Par ailleurs, il faut noter que certains compagnies n'ont pas attendu l'adoption de lois pour prendre des décisions. Ainsi, la compagnie Bell Canada, la plus importante entreprise de communications du pays, a ajouté une clause à son entente avec ses usagers qui permet la surveillance des usages de ses services dans le cadre des lois, des réglementations et de toute autre requête effectuée par le gouvernement [Geist, 2006b].

Cela dit, si un nouveau projet de loi était déposé, il y a de fortes probabilités qu'il soit à nouveau critiqué. La nouvelle Commissaire à la protection de la vie privée du Canada, Jennifer Stoddart, adopte en effet une position aussi critique que son prédécesseur sur ce dossier. En réponse aux consultations du gouvernement précédent, elle a questionné ouvertement la nécessité de revoir les lois déjà existantes et pense que les propositions avancées pourraient remettre en question les droits des internautes et des fournisseurs de services Internet. Elle dénonce, par exemple, les perquisitions sans mandat auprès des fournisseurs pour obtenir des informations au sujet de leurs abonnés et les ambigüités concernant la saisie et l'interception des courriels personnels [Canada, Commissariat à la protection de la vie privée, 2005]. De plus, un autre acteur d'importance, la Cour Suprême du pays, a adopté une position critique par rapport à une autre loi visant les terroristes, en jugeant en février 2007 à l'unanimité que la loi sur les certificats de sécurité devait être revue sous le prétexte qu'il était déraisonnable de refuser aux suspects l'accès à la preuve retenue contre eux. Toutefois, ni l'existence des certificats, ni l'emprisonnement indéfini qui en découle parfois n'ont été remis en question à cette occasion [Buzzetti, 2007].

D'autres prises de position invitent aussi à demeurer attentifs. Ainsi, l'Asssociation canadienne des professeurs et professeures d'Université (ACPPU) qui se donne pour mission d'être vigilante par rapport à toutes les lois et autres mesures qui compromettent les libertés civiles et les droits des Canadiens et des Canadiennes porte un jugement très négatif sur la période récente : « Au Canada, depuis le 11 septembre 2001, on a vu une prolifération de mesures censées se justifier par la nécessité du secret et du pouvoir arbitraire. […] Et dans de nombreux cas, le gouvernement en a prescrit l'usage à des fins autres que la lutte contre le terrorisme » [ACPPU, 2005]. Dans son argumentaire critique, l'association fait notamment référence au caractère ambigü du terme même de terrorisme car celui-ci ne fait l'objet d'aucun consensus au sein de la communauté internationale. Pour illustrer son propos, elle rappelle que l'administration Bush ne considère pas les personnes revendiquant agir au compte de l'armée républicaine irlandaise (IRA) ou bien pour Israël et la Palestine comme des terroristes au nom de la « courtoisie internationale ». Au final, l'ACPPU va jusqu'à considérer que les lois proposées par le gouvernement puis votées par le parlement « mènent à l'état policier et à la société de surveillance » (ibid.). La position présentée en 2001 par la

Confédération des syndicats nationaux (CSN) dans son mémoire sur la Loi antiterroriste conduisait déjà à s'interroger. La centrale syndicale estimait aussi que cette loi comprenait une définition trop large du terme « terrorisme ». « La CSN est d'avis que la définition d'activité terroriste prévue au projet de loi doit être revue pour ne pas entretenir d'ambiguïté permettant d'assimiler des groupes démocratiques tels les syndicats et les groupes communautaires à des groupes terroristes » [CSN, 2001].

Selon ces prises de position, il conviendrait en conséquence de rester vigilants. Or, il y a quelques semaines, l'une des membres du collectif formé au Québec en 2003 reconnaissait qu'il ne serait pas évident de remobiliser des citoyens et des citoyennes si un nouveau projet de loi était déposé au Parlement canadien prochainement. Pourtant, si d'un côté le développement de la micro-informatique a pu grâce à sa dimension distribuée calmer les inquiétudes de citoyens et citoyennes soucieux du respect de la vie privée, de l'autre il importe de rappeler que notamment depuis le développement d'Internet, la mise en réseau de plus en plus systématique a rendu possible de nouvelles formes de surveillance, notamment autour du recoupement des données et des traces laissées de façon régulière. Une recherche effectuée à l'Université Queen's à Kingston en Ontario a indiqué que presque la moitié des Canadiens et des Canadiennes considèrent les nouvelles lois comme intrusives. Mais moins d'un tiers d'entre eux pensent avoir un mot à dire sur les informations collectées sur leur vie privée[4] [Lyon et al., 2007].

4. Bibliographie

Asssociation canadienne des professeurs et professeures d'Université (ACPPU) : *Mémoire présenté au sous-comité de la sécurité publique et nationale concernant l'examen de la loi terroriste,* 28 février 2005, http://www.caut.ca/fr/publications/briefs/2005antiterrorism.pdf, 2005.

BC Freedom of Information and Privacy association (FIPA) : « Canadian government readies legislation to increase Internet snooping powers » ; http://fipa.bc.ca/library/Law_Reform_Activities/LAWFUL_ACCESS_(police_surveillance_of_electronic_communication)/Canadian_govt_readies_legislation_to_increase_Internet_snooping_powers.doc, 2005.

Buzzetti Hélène : « Ottawa devra refaire ses devoirs », *Le Devoir,* http://www.ledevoir.com/2007/02/24/132398.html, 2007.

Canada, Commissariat à la protection de la vie privée : « À propos de nous. Mandat et mission du CPVP », http://www.privcom.gc.ca/aboutUs/index_f.asp, 2007.

Canada, Commissariat à la protection de la vie privée : « Réponse à la consultation du gouvernement sur l'accès légal. Présentation du Commissariat à la protection de la vie privée du Canada au ministre de la Justice et procureur général du Canada », le 5 mai 2005, http://www.privcom.gc.ca/information/pub/sub_la_050505_f.asp, 2005.

Canada, Commissariat à la protection de la vie privée : « Lettre du commissaire à la protection de la vie privée du Canada, George Radwanski à l'honorable Martin Cauchon, ministre de la Justice et procureur général du Canada, à l'honorable Wayne Easter, solliciteur général du Canada, ainsi qu'à l'honorable Allan Rock, ministre de l'Industrie, au sujet des propositions relatives à "l'accès légal" », http://www.privcom.gc.ca/media/le_021125_f.asp, 2004.

[4] Le pourcentage est un peu supérieur au tiers au Québec. Au-delà des chiffres portant sur le Canada, cette étude est aussi consacrée à d'autres pays, dont la Chine, les États-Unis et la France.

Canada, Commissariat à la protection de la vie privée : « Législation. Document d'information. La Loi sur la protection des renseignements personnels et les documents électroniques », http://www.privcom.gc.ca/legislation/02_06_07_f.asp, 2000.

Canada, Ministère de la Justice : *Loi sur la protection des renseignements personnels,* http://lois.justice.gc.ca/fr/P-21/index.html, 2007a.

Canada, Ministère de la Justice : *Loi sur la protection des renseignements personnels et les documents électroniques,* http://lois.justice.gc.ca/fr/showtdm/cs/P-8.6//20070310, 2007b.

Canada, Ministère de la Justice : « La loi anti terroriste. Foire aux questions (FAQ) », http://www.justice.gc.ca/fr/anti_terr/faq.html, 2007c.

Canada, Ministère de la Justice : « FAQ sur l'accès légal », http://www.justice.gc.ca/fr/cons/la_al/summary/faq.html, 2006.

Canada, Ministère de la Justice : *Résumé des mémoires présentés dans le cadre de la consultation sur l'accès légal,* http://www.justice.gc.ca/fr/cons/la_al/summary/6.html, 2003.

Carré Dominique : « Des dégâts du progrès… au marketing de l'usage. Revirement de perspectives en matière de critique sociale dans le champ Informatique et société », dans *Société de l'information, société du contrôle ?, Évolution de la critique de l'informatisation,* actes du 13e colloque international du Centre de coordination pour la Recherche et l'Enseignement en Informatique et Société (CREIS), Paris. http://www.creis.sgdg.org/colloques%20creis/2004/IS04programme%20et%20actes.htm, 2004.

Confédération des syndicats nationaux (CSN) : *Mémoire sur le projet de loi C-36,* http://www.csn.qc.ca/memoires/TerrorismeC36FrSet.html, 2001.

Conseil de l'Europe, *Convention sur la cybercriminalité* : Budapest, le 23 novembre 2001, http://conventions.coe.int/Treaty/fr/Treaties/Html/185.htm, 2001.

Geist Michael : « Big Brother watching you surf ? », *The Globe and Mail,* http://www.theglobeandmail.com/servlet/story/RTGAM.20060627.gtsecurity0627/BNStory/Technology/home, 2006a.

Geist Michael : « Bell Controversy Puts Spotlight on Net Surveillance », *Toronto Star,* http://www.michaelgeist.ca/content/view/1314/159/, 2006b.

Ligue des droits et libertés : « La Loi antiterroriste de 2001 : une loi toujours aussi inutile, trompeuse et… dangereuse », http://www.liguedesdroits.ca/documents/surveillance/c36/abbendum_c36_oct2006.pdf, 2006.

Ligue des droits et libertés : *Mémoire sur l'« accès légal » en réponse à la consultation menée par le Ministère de la Justice du Canada,* http:// www.liguedesdroits.ca/documents/surveillance/acces_legal/memoire_acces_legal.pdf, 2002.

Ligue des droits et libertés du Québec (LDL), Fédération des infirmières et des infirmiers du Québec (FIIQ), Association étudiante facultaire de sciences politiques et droit de l'UQAM, Centre de documentation sur l'éducation des adultes et la condition féminine (CDEACF) et Carrefour mondial de l'Internet citoyen (CMIC) : *Déclaration contre le projet du gouvernement fédéral « Accès légal »,* http://www.liguedesdroits.ca/documents/surveillance/acces_legal/decl_acceslegal.pdf, 2003.

Lyon David, Elia Zureik et Yolande Chan : *The Surveillance Project and the Globalization of Personal Data,* Queen's University at Kingston, http://www.queensu.ca/sociology/Surveillance/?q=media, 2007.

Organisation des Nations Unies (ONU), Conseil de sécurité : *Actions prises par le Conseil de sécurité,* http://www.un.org/french/terrorism/sc2.htm, s.d.

Paye Jean-Claude : « Le "Patriot Act Reauthorization" : un état d'urgence permanent », http://multitudes.samizdat.net/article2762.html, 2007.