Chronique etic

CEIM

Gouvernance d'Internet : émergence de nouveaux clivages

Volume 2, numéro 2, novembre 2013 *ISSN 2292-2288*

Résumé analytique

Dans la gouvernance des TIC, deux grands événements diplomatiques sont survenus au cours de la dernière année. Premièrement il y a le grand débat sur le rôle de l'Union internationale des télécommunications dans la gouvernance d'Internet qui suit un modèle multi-parties prenantes plutôt qu'un modèle centré sur la coopération strictement interétatique. Le deuxième est sans aucun doute les révélations de M. Snowden et les découvertes sur la surveillance à grande échelle effectuée par les États-Unis dans le cyberespace. Cette chronique aborde ces deux grands enjeux de la gouvernance d'Internet.

Notons que Michèle Rioux a participé à la réunion de Giganet (Graduate Institute, Geneva) les 17 et 18 mai 2013 où elle a présenté une communication dont le texte sera publié dans **M. Rioux,** B. Company and N. Adam, « Competing Institutional Trajectories of Global Regulation – Internet in a Fragmented World », Rolf H. Weber, Roxana Radu, Jean-Marie Chenou, *The evolution of global Internet policy: new principles and forms of governance in the making?,* Shulthess, 2013, 230 p. Madame Rioux a également rencontré à l'UIT, M. H. Zhao Vice secrétaire –général, M. P. Maloor, conseiller pour les stratégies et les politiques, et M. M. Fall, chef de la division de l'environnement réglementaire et commercial.

Contenu

Nicolas Adam, direction scientifique

Olivier Dagenais, Guillaume Murphy et Thomas Scorticati, rédaction

Centre d'études sur l'intégration et la mondialisation

Projet d'Études sur les technologies de l'information et des communications (ETIC)

Cybersécurité et libertés fondamentales | Tensions entre cybersurveillance et vie privée

Révélations sur la NSA, quels enjeux pour la protection de la vie privée?

Il y a maintenant plus de 10 ans, les événements du 11 septembre 2001 marquaient les esprits et allaient par la suite légitimer d'importantes mesures sécuritaires, dont la création du département de la sécurité intérieure des États-Unis. Parallèlement, les communications et l'échange d'informations sur Internet ont augmenté de façon exponentielle et l'accès au réseau, autrefois réservé à une élite technologique, s'est démocratisé. Une quantité phénoménale d'informations se retrouve à circuler sur un réseau complexe, décentralisé, mais principalement concentré en Occident. En juin 2013, le *Washington Post* et *The Guardian* révélait que la *National Security Agency* (NSA) des États-Unis procédait à la collecte à grande échelle d'informations touchant autant les ressortissants étrangers que des citoyens américains. Ces révélations on remit au goût du jour le débat, propre à nos sociétés modernes, entourant l'arbitrage entre sécurité et vie privée. Nous examinerons avant tout dans ce billet ce qui en est de ces révélations pour ensuite analyser les enjeux entourant la protection de la vie privée aux États-Unis. Ensuite, nous mettrons en lumière quelques autres exemples cas de surveillance impliquant des entreprises américaines de télécommunication depuis le début des années 2000 et axerons notre analyse sur l'élargissement graduel des pouvoirs des agences de renseignement américaines.

PRISM-Gate : Une surveillance à grande échelle

Le 5 juin 2013, le *Guardian* publiait un ordre du tribunal fédéral américain relatif au renseignement étranger (*Foreign Intelligence Surveillance Court*, FISC) ordonnant au fournisseur d'accès *Verizon* de confier à la NSA[1] et au FBI l'accès aux métadonnées d'appels téléphoniques (date, heure, durée et destination des appels) de millions d'étrangers et de citoyens américains transitant sur son réseau. Le jour suivant, le *Washington Post* révélait l'existence d'un programme de surveillance électronique nommé PRISM qui vise, depuis 2007, la collecte, l'archivage et l'analyse des informations et des communications d'internautes (courriels, vidéos, clavardages, photos et requêtes de recherche) résidant à l'extérieur des États-Unis par le biais d'un accès aux données de neuf géants américains de l'Internet, parmi lesquelles figurent Apple, Microsoft, Google, AOL, Yahoo! et Facebook. Ce programme (voir la présentation PowerPoint annotée par le *Washington Post*) aurait permis aux agents et analystes de la NSA et du FBI de se connecter à un portail sécurisé sur les serveurs de ces mêmes entreprises leur permettant d'avoir accès à des données confidentielles, et ce, sans mandat judiciaire spécifique. Le programme PRISM apparaît comme la source principale de

[1] Créée en 1952 par le président Truman durant la guerre de Corée, la NSA avait pour mission de protéger les États-Unis contre de possibles menaces étrangères.

renseignement brute utilisée par les analystes de la NSA. Ces allégations ont fait suite à la sortie publique d'un dénonciateur, Edward Snowden, réfugié à Hong Kong avant que les deux journaux publient les révélations. Informaticien de 29 ans, il résidait en banlieue de Honolulu et travaillait pour des sous-traitants de la NSA et la CIA tels Dell et Booz Allen Hamilton, son dernier employeur. Il fut inculpé par le gouvernement américain sous les chefs d'accusation d'espionnage, vol et utilisation illégale de biens gouvernementaux. Les documents qu'il a confiés aux médias soulèvent d'importantes questions sur les méthodes de collectes de données par la NSA et la protection de la vie privée aux États-Unis, couvert par le 4e amendement à la constitution américaine.

Dès le mois de décembre de l'an 2000, la NSA émettait la volonté d'une réinterprétation du 4e amendement à la constitution dans un mémo confidentiel.[2] Déclassifié, puis mis en ligne par l'Université George Washington, le document, adressé à l'administration Bush nouvellement arrivée à la Maison-Blanche, met la table à un élargissement futur des pouvoirs de la NSA. Le mémo exprime le désir de l'agence d'entamer, sans ambiguïtés législatives indues, le virage des nouvelles technologies d'information et de la communication.

Combattre le feu par le feu

L'administration Bush donna son aval à l'extension des compétences de la NSA. D'emblée, l'adoption en 2001 du *Patriot Act* par le Congrès américain permit notamment l'émission de lettre de sécurité nationale (*National Security Letters*, NSLs) autorisant la collecte, par le FBI ou la NSA par exemple, de renseignements sur un citoyen américain sans ordonnance judiciaire. Bien que ces lettres soient accompagnées d'un bâillon (*gag order*) et que la grande majorité des documents concernant la NSA soient classés secrets, certains cas feront surface et attireront l'attention du public avant les fuites de Snowden.

USA Today révélait en 2006 que la surveillance sans supervision judiciaire de millions de citoyens et d'entreprises américaines débutait peu après septembre 2001 avec la collecte par la NSA de métadonnées provenant des trois plus grandes compagnies de télécommunication des États-Unis à l'époque, soit *AT&T*, *Verizon* et *Bell South*. Le but ici était de monter une base de données pour tous les appels à provenance ou à destination étrangère afin et pister de potentielles activités terroristes. En vertu de la section 222 du *Communication Act*, les compagnies de télécommunication se voyaient normalement interdire la divulgation d'informations sur les appels téléphoniques de ses clients pour toute demande ne reposant pas sur une ordonnance de la justice, au risque de s'exposer à de sévères amendes. L'exception à cette loi fut permise par la signature du président George W. Bush apposée à un décret présidentiel (*executive order*) en 2002 qui allait permettre aux agences de sécurité américaines

[2] Rappelons que le 4e amendement à la constitution introduit par le *Bill of Rights* le 15 décembre 1791 est central à la question de la protection de la vie privée puisqu'il stipule qu'aucune fouille ne peut être effectuée sur une propriété privée sans ordonnance de la justice. Nous sommes ici face aux valeurs américaines de protection de des droits de l'individu contre une intrusion trop importante d'une tierce partie dans la vie privée d'un citoyen américain. Le souvenir des « Writs of Assistance » allègrement émis par le roi d'Angleterre George 1er durant l'ère coloniale et qui permettait la fouille de toute propriété privée sur le territoire des treize colonies était frais dans la mémoire des législateurs américains. Les droits individuels articulés par 4e amendement nous renvoient au cœur même des valeurs des pères fondateurs et des fondements de l'État de droit.

d'envoyer une demande d'accès aux métadonnées des compagnies de télécommunication concernant les citoyens américains, les résidents permanents, les touristes et tout autre étrangers en sol américain. Le tout afin de faciliter les procédures pour la collecte de renseignements dans la lutte des États-Unis contre le terrorisme. Dans le même ordre d'idée, le *New York Times* affirmait en 2005 que le président Bush avait, à l'aide d'un décret, bel et bien autorisé la NSA à surveiller les appels téléphoniques internationaux de milliers d'Américains sans ordonnance de la justice.

Un autre cas, impliquant la NSA cette fois-ci, fera surface en 2006. Mark Klein, technicien d'AT&T à la retraite, affirme alors dans une déclaration sous serment avoir été témoin à multiples reprises de la visite d'agents de la NSA sur son lieu de travail et relate la construction d'une pièce hautement sécurisée au début des années 2000. Cette pièce aurait servi à héberger de l'équipement réseau visant à intercepter la totalité du trafic Internet transitant sur le point de branchement réseau dont Klein était responsable.

Dernièrement, un litige opposant Google et le gouvernement américain est venu rappeler que le débat est loin d'être résolu. Ce litige a fait l'objet d'une décision en date du 20 mai 2013 dans laquelle Susan Illston, juge de la Cour fédérale, ordonne à la société de *Mountain View* d'adhérer à des demandes en provenance du FBI visant la collecte de renseignements sur des usagers. *Google* plaidait dans cette affaire que la pratique de l'agence gouvernementale d'émettre des lettres de sécurité nationale à des entreprises de télécommunication était inconstitutionnelle en vertu du 4e amendement à la constitution mais cet argument fut rejeté par la Juge qui entérina par sa décision l'émission de ces lettres.

Ce type particulier de demande d'accès à l'information, sans supervision judiciaire, commença à être émis par le FBI suite à l'adoption par le Congrès américain du *Patriot Act*. Ici, le Titre V, intitulé enlèvement des obstacles à l'enquête sur le terrorisme, est en cause puisqu'il a considérablement élargi l'utilisation de ces lettres[3]. En 2012, le FBI aurait envoyé près de 16,000 de ces mêmes lettres pour des demandes d'accès à de l'information impliquant plus de 7,000 citoyens américains.

Les cas Verizon et PRISM

Dans le cas des révélations de Snowden impliquant *Verizon,* le tribunal fédéral américain relatif au renseignement étranger ayant émis l'ordre rendu public par *le Guardian* fut mis sur pied suite à l'adoption du *Foreign Intelligence Surveillance Act* (FISA) en 1978. Il s'est vu accorder le pouvoir d'émettre de tels ordres à l'intention d'entreprises privées depuis l'amendement de la loi FISA par l'article 215 du *Patriot Act* en 2001. Depuis cet amendement, ce tribunal possède le pouvoir d'émettre, suite à des délibérations tenues secrètes entre les 11 juges constituant la cour, un ordre permettant l'accès à l'information réclamé par la NSA et le FBI, sans mandat judiciaire. Pour que la décision de la cour entérine les demandes de ces agences de sécurité, ces dernières doivent en théorie démontrer qu'il y a présence d'un doute

[3] Plus précisément l'article 505 du titre V du *Patriot Act* (2001), en plus des amendements apportés au *Electronic Communication Privacy Act* par le *USA Patriot Reauthorization Acts* (2006), et le *FISA Amendments Act* (2008).

raisonnable légitimant une enquête sur une personne résidant aux États-Unis. Dans ce cas-ci – tel qu'explicitement indiqué dans l'ordre émis par le tribunal fédéral américain relatif au renseignement étranger – un doute raisonnable légitimant la saisie de la totalité des métadonnées d'appels téléphoniques de la totalité des clients de *Verizon*, à l'intérieur des États-Unis et à destination de l'étranger, opérés entre le 25 avril 2013 et le 19 juillet 2013. L'article 215 du *Patriot Act* permet donc, tout comme l'ordre exécutif de 2002, la surveillance de citoyens des États-Unis sur leur territoire pour motifs sécuritaires sans égard aux balises auparavant assurées par le 4e amendement.

Le même genre de collecte de données sans supervision judiciaire prend une toute autre ampleur avec le programme PRISM. Sa portée est si vaste qu'il peut être tentant de tomber dans une interprétation orwellienne face à une surveillance mondiale institutionnalisée de la sorte. Il faut éviter cet écueil si nous voulons conserver un regard objectif sur la question. Du côté des principaux intéressés, Google et Facebook, tout comme les autres compagnies associées à PRISM, se sont empressés de nier l'existence d'un « accès direct » à leurs serveurs à des agences gouvernementales. Par exemple, Mark Zuckerberg écrivait au lendemain des révélations du *Washington Post* « Facebook n'est pas et n'a jamais été touché par un programme donnant au gouvernement américain un accès direct à nos serveurs ». Larry Page, PDG de Google, affirmait de son côté que le géant de l'Internet n'avait pas donné accès à ses serveurs au gouvernement. « Google prend au sérieux la sécurité des données de ses usagers. Nous divulguons des données sur nos utilisateurs au gouvernement en conformité avec la loi et nous examinons toutes les demandes avec soin ». De son côté, Microsoft affirmait « Nous acceptons de répondre aux ordonnances pour les demandes concernant des comptes ou des identifiants spécifiques. Si le gouvernement a un programme plus large de sécurité nationale pour recueillir des données sur les clients, nous ne participons pas à celui-ci ».

On note un certain degré de dissonance entre ce que les compagnies affirment par voie de communiqué officiel et ce qui est rapporté via les fuites de Snowden. Bien que les entreprises ciblées aient démenties la présence d'« accès direct » ou encore de « porte dérobée » (*back door*), le *New York Time* affirme qu'un portail sécurisé fut tout de même mis en place spécifiquement pour combler les besoins en renseignement des agences gouvernementales. Hormis quelques contorsions sémantiques d'usage, il appert qu'un outil a bel et bien été élaboré. Les enjeux sont importants puisqu'il en va de la réputation de ces entreprises par rapport à la protection des données personnelles de leurs utilisateurs.

Chez certaines firmes, la coopération a vraisemblablement été plus difficile à obtenir, mais, ultimement, l'environnement légal développé ne leur laissait guère le choix. En effet, c'est en vertu de la loi FISA amendée par le titre V du *Patriot Act* et l'article 702 du *FISA Amendment Act* de 2008, que le programme PRISM fut mis en place par la NSA. Ce dernier amendement à la loi FISA (initialement prévu pour 5 ans et renouvelée pour 5 années supplémentaires en décembre 2012) autorise la collecte de renseignements électroniques à grande échelle incluant les communications internationales et les communications entre les États-Unis et l'extérieur du pays du moment que l'intention est de récolter de l'information sur des individus ou des puissances à l'étranger. De plus, les ordres du tribunal fédéral américain relatif au renseignement étranger mis sur pied par le FISA, tout comme les lettres de sécurité nationale, sont accompagnés d'un bâillon qui empêche les bénéficiaires d'en parler publiquement. Ce qui

pourrait expliquer dans une certaine mesure la langue de bois des entreprises éclaboussées par les révélations. Microsoft et Google ont par ailleurs entamé des procédures judiciaires afin de faire lever le bâillon qui les vise en invoquant le 1er amendement à la constitution américaine touchant à la liberté d'expression.

On constate donc une démultiplication des outils de collecte d'information au profit des agences de renseignement américaines démultipliant les compromis à la protection de la vie privée pour des fins sécuritaires. Ordre du tribunal instauré par le FISA, lettre de sécurité nationale et demande directe sur la base d'un décret présidentiel sont autant de nouveaux moyens d'accéder aux informations confidentielles des citoyens américains comme des étrangers, sans pour autant avoir de supervision judiciaire autre que celle des 11 juges du tribunal mis sur pied par le FISA. Pour le renseignement américain, la collecte automatisée de données électroniques à grande échelle est un mal nécessaire afin de garantir la sécurité des citoyens américains. Le général Keith Alexander, Directeur de la NSA, défendait le programme PRISM dans les médias, arguant que la collection et l'analyse de métadonnées téléphoniques qui en a résulté avaient contribué à déjouer une cinquantaine d'attentats dans le monde depuis le 11 septembre 2001. Même son de cloche du côté du président Obama, qui a défendu la pertinence des méthodes de l'agence dans une entrevue à l'émission *Current Affairs* le 17 juin dernier.

Débordement du mandat de la NSA

Deux directives émises à l'endroit du tribunal fédéral américain relatif au renseignement étranger par le procureur général Eric Holder, mis en ligne par le journal *The Guardian* le 20 juin 2013, mettent en lumière les politiques de la NSA concernant la collecte et l'utilisation de données d'Américains. L'agence est, entre autres choses, autorisée à :

- Conserver pour 5 ans toute donnée susceptible de comprendre des informations sur des citoyens américains;
- Conserver indéfiniment et à utiliser des communications domestiques « acquises par inadvertance » si elles contiennent des renseignements ou des informations sur des activités criminelles, des menaces à l'encontre d'une personne ou d'une propriété, si elle sont encrypté ou si elles contiennent des éléments en lien avec la cyber sécurité;
- Préserver les renseignements contenus dans les communications entre un avocat et son client si l'un ou l'autre est à l'étranger.

Ces documents démontrent que la NSA possède une latitude considérable dans la collecte de données électroniques à grande échelle. Ceux-ci stipulent que s'il s'avérait qu'il y a des doutes à savoir si des données auraient été récoltées sur une personne qui est citoyen américain, l'analyste de la NSA est autorisé à écouter le contenu d'appels téléphoniques et à lire le contenu de messages pour s'en assurer. De plus, cette procédure ne s'applique pas à la collecte à grande échelle d'informations puisque la NSA n'est pas en mesure de filtrer les données domestiques de l'ensemble de l'échantillon et qu'en conséquence, la totalité des données saisies de la sorte peut être conservée pendant 5 ans. A la lumière des révélations de

Snowden concernant *Verizon* et le programme PRISM, force est de constater que les pouvoirs de collecte d'information de la NSA ont affiché une nette augmentation depuis septembre 2001. À la base mise sur pied pour étudier et contrer les menaces étrangères, certains gardes-fous légaux – à commencer par le 4eamendement – limitaient l'autorité de l'agence auprès des citoyens américains. Or, nous assistons à une érosion progressive et soutenue de cette protection et tout indique que la NSA jouisse désormais d'un large pouvoir discrétionnaire quant à ses demandes d'accès à l'information concernant les citoyens américains.

Quel écho à l'international?

Un débat sur la portée de ce qui est possible de réaliser sous l'égide du *Patriot Act* ainsi que sur l'interprétation du 4eamendement à la constitution américaine est toujours en cours aux États-Unis même plusieurs mois après les révélations initiales. L'union américaine des libertés politiques (American Civil Liberties Union, ACLU) a d'ailleurs entamé des procédures judiciaires à l'endroit de l'administration Obama concernant l'affaire *Verizon* et la collecte des métadonnées d'appels téléphoniques. Ce que les révélations sur PRISM nous indiquent, c'est que les citoyens de tous les pays du monde sont visés par les enquêtes et la collecte de données à grande échelle de la NSA. Un malaise diplomatique s'est installé entre les États-Unis et la communauté internationale, d'autant plus que les plus grandes entreprises de la toile sont américaines et que l'actuelle structure d'Internet fait en sorte que la majorité du trafic passe par le territoire américain. La quantité de personnes susceptibles d'être concernées par PRISM est immense.

Flux mondial de transmission de données (2005)

Source : Telegeography et Wired.com

Les Européens furent parmi les premiers à exprimer leurs préoccupations face à ces révélations. Évidemment, toute personne qui n'est pas citoyen des États-Unis n'est pas protégée par le 4e amendement. Devant une vulnérabilité apparente, le Parlement européen avait déjà travaillé à la protection des données européennes touchant à la vie privée. La Commission européenne exige aujourd'hui des garanties de la part des États-Unis par rapport à la protection des données européennes au moment où un accord de libre-échange est négocié

entre les deux puissances. Des politiciens anglais,[4] allemands, néerlandais, suisses et belges sont parmi les voix qui s'élèvent et qui en appellent à une enquête au niveau européen de l'impact du programme. Antonio Soro, commissaire italien à la protection des données personnelles, déclarait à l'intention de l'administration Obama : « S'il est vrai que la relation entre la sécurité et la vie privée est une figure incontournable de notre modernité, le prétexte de protéger la démocratie par la compression de la liberté des citoyens est susceptible de remettre en cause l'essence même du bien que vous souhaitez défendre ».

Selon la Haute-Commissaire des Nations unies aux droits de l'homme, Navanethem Pillay, les programmes de surveillance qui contreviennent au droit de la personne à la vie privée au nom de la sécurité risquent au contraire de nuire à la lutte contre le terrorisme en nuisant à l'implantation de l'état de droit. Jeffrey Feltman, vice-secrétaire général des Nations unies et directeur de l'*Équipe spéciale de la lutte contre le terrorisme*, affirme pour sa part que « si des compromis sont faits par les États quant au respect des droits de l'homme, nous ne sommes pas en train de combattre le terrorisme, nous lui traçons la voie ». D'emblée, le respect de la vie privée d'un individu, à son domicile comme dans ses correspondances, est protégé au niveau du droit international par l'article 12 de la Déclaration universelle des droits de l'homme de l'ONU : « Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes ».

Du côté canadien, le commissaire à la protection de la vie privée, Jennifer Stoddart, a annoncé qu'elle allait se pencher sur l'impact au Canada de la surveillance à grande échelle des États-Unis et que cette affaire soulevait de grandes inquiétudes. Elle interpelle du même coup le commissaire chargé de la surveillance du *Centre de la sécurité des télécommunications du Canada* (CST), l'équivalent de la NSA, responsable des activités de renseignement électromagnétique (SIGINT), pour tenter d'évaluer à quel point les informations personnelles des Canadiens pourraient être affectées par les activités américaines de surveillance. Par ailleurs, suite aux révélations sur le renseignement britannique, Peter Mackay, ministre canadien de la Défense, se voulait rassurant et affirmait que le CST ne disposait pas d'accès semblable à celui du *Government Communication Headquarters* (GCHQ) au système PRISM. Selon le ministre, le programme de collecte de métadonnées du CST, mis en place depuis 2005, « n'est pas autorisé à faire la collecte de données personnelles de citoyens et ressortissants Canadiens. (Il) se concentre plutôt sur les activités extérieures au pays, sur les menaces étrangères. Il existe un mécanisme de surveillance rigoureux. Il y a un processus législatif en place qui indique spécifiquement ce qui peut et ce qui ne peut être examiné ». Devant les révélations sur ce même type de procédures aux États-Unis, qui vraisemblablement laisse une large part de discrétion aux analystes de la NSA, il pourrait être révélateur de se pencher sur les règles qui encadrent la CST ici même, au Canada.

[4] D'autres révélations du journal *The Guardian* sur le renseignement anglais ont toutefois mis en cause le *Government Communication Headquarters* (GCHQ) qui aurait eu accès au réseau de fibre optique transportant le trafic Internet et les appels téléphoniques du monde entier. Le GCHQ aurait partagé ses données avec la NSA pendant au moins trois ans et produit plus d'une centaine de rapports tout en ayant accès au données du programme PRISM.

En bref, l'environnement légal aux États-Unis s'est considérablement transformé depuis 2001, élargissant la marge de manœuvre des agences de renseignement comme la NSA. Des outils légaux contraignants ont vu le jour, obligeant les plus grandes entreprises présentent sur Internet à livrer des informations confidentielles sur leurs usagers. Les révélations de Snowden nous auront permis d'apprécier l'impressionnante capacité de surveillance des États-Unis et de confirmer que certains compromis entourant l'interprétation du 4e amendement, que l'on associait à l'administration Bush, ont été reconduits par l'administration Obama. Ceci pose la question difficile de l'arbitrage entre sécurité et protection de la vie privée puisque la création même de l'État moderne repose justement sur ce compromis qu'acceptent les individus entre liberté individuelle et sécurité. Les théories du contrat social postulent la nécessité de délaisser certains droits au profit d'un souverain qui assure en contrepartie la sécurité de ses citoyens. Mais existe-t-il une ligne à ne pas franchir? Snowden affirmait dans une entrevue qu'il livra à *The Guardian* que sa plus grande crainte est que rien ne change. Si on peut souscrire au principe selon lequel certains compromis sont nécessaires pour la sécurité du plus grand nombre, il demeure primordial pour la suite des choses de se pencher sur ce qui sera effectivement fait par les autorités américaines pour répondre aux critiques qui leur sont adressées quant à l'ampleur et la systématicité de la surveillance qu'ils opèrent.

Recherche et rédaction : Guillaume Murphy

Pour en savoir plus :

Bloom, Robert et William J. Dunn. 2006. « Constitutional Infirmity of Warrantless NSA Surveillance: The Abuse of Presidential Power and the Injury to the Fourth Amendment, The ». *William and Mary Bill of Rights Journal*, vol. 15, no 1, pp. 147-202.

Chronologie des événements impliquant la NSA par l'*Electronic Frontier Fondation*: https://www.eff.org/nsa-spying/timeline

Jordan, David Alan. 2005. « Decrypting the Fourth Amendment: Warrantless NSA Surveillance and the Enhanced Expectation of Privacy Provided by Encrypted Voice over Internet Protocol ». *Boston College Law* Review, vol. 47, no 3, pp. 505-546.

Slobogin, Christopher. 2008. « Government Data Mining and the Fourth Amendment ». *The University of Chicago Law Review*. Vol. 75, no 1 (hiver), pp. 317-341.

À suivre dans la prochaine chronique : le plan Obama sur la réforme de la cybersurveillance aux États-Unis

Après le scandale de la surveillance électronique par l'agence américaine, *National Security Agency (NSA)*, le président Barack Obama a décidé de constituer un groupe de réflexion afin de réajuster les pratiques de surveillance. Le *Review group on Intelligence and Communications Technology* rassemble 5 membres experts du renseignement et des libertés civiles nommés par le président Obama. Tous se sont entendus qu'il fallait un meilleur contrôle judiciaire de la *Foreign Intelligence Surveillance Court* (FISC). Mais aucun des membres n'a discuté de la carte blanche accordée à la NSA. L'une des principales critiques adressées à ce comité d'experts est qu'il n'est pas indépendant. Deux des 5 membres nommés par le président Obama, M. Morell et R. Clarke, sont respectivement, ancien vice-directeur de la CIA et ancien coordinateur de la lutte antiterroriste à la Maison-Blanche. La société civile critique le fait que la séance se déroule à huit clos et que le rapport final serait présenté au président avant de le rendre public. Face à ces critiques, le Congrès a décidé de créer une commission. Pour pallier au manque d'engagement du comité exécutif, trois sénateurs démocrates ont décidé d'élaborer un projet de loi pour limiter la surveillance électronique. *The Intelligence Oversight and Surveillance Reform Act* propose:

1. Qu'il soit interdit de récolter les données sans soupçon.
2. Qu'en cas d'état d'urgence, la NSA puisse récolter les données de tous les suspects mais que l'agence fasse une demande de confirmation au procureur général 7 jours après du début de la collecte.
3. Qu'un « avocat constitutionnel » soit membre du FISC pour protéger les droits et libertés.
4. Que la NSA fasse un rapport des métadonnées enregistrées auprès des Américains.
5. Qu'il soit interdit aux agents de surveiller un Américain sans mandat
6. Que les responsabilités des entreprises soient précisées.

Selon le sénateur Saxby Chambliss, le projet de loi n'avancera pas car il n'y a aucun contrôle technique de la surveillance faite par la NSA. Un amendement similaire a été présenté à la Chambre des Représentants en juillet dernier et il fut rejeté par 217 voix contre et 207 pour. Voici, une liste, en ordre chronologique, des documents publiés en juin concernant le scandale.

- **5 juin 2013** : ordre du tribunal fédéral américain relatif au renseignement étranger (*Foreign Intelligence Surveillance Court*, FISC) à destination de l'entreprise de télécommunication *Verizon*.

- **6 juin 2013** : Publication par *The Washington Post* de quelques diapositives provenant d'une présentation PowerPoint décrivant un programme de surveillance de portée mondiale nommé PRISM et qui impliquerait 9 entreprises américaines.

- **7 juin 2013** : Publication par *The Guardian* d'un décret présidentiel du président Barack Obama qui demande à diverses agences de sécurité américaines de dresser une liste de cibles potentielles pour la *Offensive Cyber Effects Operations* américaine, un organe de cyber sécurité ayant le potentiel de mener des attaques à destination de structures et systèmes informatiques situés en territoire étranger.

- **11 juin 2013** : Quatre diapositives d'une présentation de la NSA sont publiées par *The Guardian*. Elles démontrent l'existence d'un programme informatique nommé *Boundless Informant* utilisé pour identifier l'origine des données recueillies par la NSA.

- **17 juin 2013** : *The Guardian* met en ligne quelques extraits de documents produits par le *Government Communication Headquarter* (GCHQ), une agence de renseignement britannique, qui aurait surveillé les communications des délégués de différents pays lors du G20 de Londres en 2009.

- **20 juin 2013** : Publication par *The Guardian* de deux documents signés par Eric H. Holder, procureur général des États-Unis, à l'intention de la NSA. Le premier document dépeint les procédures à suivre pour enquêter sur des cibles qui ne seraient pas citoyens américains. Le deuxième document traite des directives visant à minimiser la collecte d'informations sur des citoyens américains.

- **21 juin 2013** : *The Guardian* publie quelques diapositives d'une présentation de la GCHQ intitulé *Mastering the internet*. L'agence de renseignement britannique surveillerait et archiverait les données transitant par des câbles de fibre optique dans le cadre d'un programme nommé *Tempora.*

- **29 juin 2013** : Publication par *The Washington Post* de nouvelles diapositives provenant de la même présentation PowerPoint à l'origine des révélations sur PRISM. Elles détaillent les liens entre divers départements de la NSA et du FBI ainsi que les procédures lorsqu'un analyste de la NSA envoie une requête d'information sur une cible par le biais du programme PRISM.

Recherche et rédaction: Thomas Scorticati

La gouvernance d'Internet et l'Union internationale des télécommunications

Gouvernance d'Internet, présence des agences de renseignement sur la Toile ou encore la crainte de guerres cybernétiques, plusieurs dossiers illustrent l'intérêt croissant des États pour la gouvernance d'Internet.

En 1962, les États-Unis prenaient conscience de leur vulnérabilité lors de la crise des missiles de Cuba. Le système centralisé de communication militaire risquait de mettre le pays en ruine si rien n'était fait pour le sécuriser. La réponse fut la création d'un réseau décentralisé qui serait en mesure de survivre à d'éventuelles attaques contre un ou plusieurs points géographiques ciblés. Une demande en recherche et développement du Département de la Défense est lancée à la RAND Corporation[5]. Le premier réseau décentralisé est créé, *ARPAnet*, par des scientifiques du secteur militaire, mais aussi, par des universitaires américains et européens, donc par la société civile[6]. En 1972, le réseau est divisé en deux avec du côté militaire, *Milnet*, et du côté civil, *ARPAnet* qui deviendra Internet, la forme abrégée de *Interconnecting Network*.

En 1974, le protocole TCP/IP (*Transmission Control Protocol / Internet Protocol*) est créé lors de la diffusion des énoncés techniques RFC 791 et RFC 793. Ce protocole est formellement implanté en 1983. Le TCP/IP visait à assurer une certaine fiabilité dans la transmission des données, à faciliter l'interconnexion entre des réseaux aux architectures différentes et à fournir un registre global au sein duquel chaque ordinateur est doté d'une adresse IP unique.

Comme l'explique Massit-Folléa, « Le processus de normalisation technique s'est développé sous une forme de coopération décentralisée entre des informaticiens bénévoles qui partageaient une même (contre)culture académique et technologique ».[7] Ces informaticiens se sont organisés sous des organisations informelles telles que l'IETF (*Internet Engineering Task Force)*, l'IAB (*Internet Architecture Board*) ou l'ISOC (*Internet Society)*. Leurs visions étaient novatrices et rompaient avec les arrangements bureaucratiques traditionnels en implémentant des approches pragmatiques, communautaires, et échappant largement à toute logique de territorialité.

---

[5] Pour de plus amples détails sur la contribution de Paul Baran, chercheur à la RAND et un des principaux architectes de la réseautique par commutation de paquets (packet-switching), voir : http://www.rand.org/about/history/baran.html

[6] Le développement de l'informatique par commutation de paquets est considéré comme étant le point zéro de l'histoire du Net, par contre, comme le souligne l'historien Ian Peter, plusieurs autres théories sur ses origines subsistent. Toutes, par contre, s'accordent sur l'importance de la contribution élargie des secteurs civils et académiques. Voir : (http://www.nethistory.info/History%20of%20the%20Internet/origins.html)

[7] Françoise Massit-Folléa « La gouvernance de l'Internet. Une internationalisation inachevée », *Le Temps des médias* 1/2012 (n° 18), p. 29-40.

À la fin des années 1990, la guerre des noms de domaines (« *DNS war* ») est amorcée![8] Face à des velléités de contrôle émanant du gouvernement des États-Unis, qui confie en sous-traitance le processus d'inscription au registre DNS, ce que certains pourraient qualifier de la « veille garde » du Net se mobilise pour développer et signer le gTLD-MoU. Ce processus, appuyé par l'UIT, vise à jeter les premières bases d'une gestion internationale des enjeux du réseau Internet.

Les États-Unis pensent autrement. L'ICANN (*Internet Corporation on Assigned Names and Numbers*) fut créée, une société de droit à lut non lucratif incorporée en Californie sous le contrôle du Département du Commerce des États-Unis et qui se charge de l'administration du registre DNS à l'échelle mondiale. La gestion d'Internet demeure donc d'une certaine manière enracinée aux États-Unis. Plusieurs sommets et forums ont, depuis la création de l'ICANN, discuté des enjeux entourant la gouvernance d'Internet mais depuis quelques années, le niveau d'intérêt, autant chez les décideurs qu'au sein de la société civile, a connu une hausse notable. La dernière s'est déroulée du 14 au 16 mai 2013, lors du Forum mondial des politiques de télécommunications (FMPT) à Genève.

Une nouvelle gouvernance difficilement intégrée

Le Sommet mondial de la société de l'information (SMSI), organisé par l'Union internationale des télécommunications (UIT), s'est déroulé en deux phases. La première (Genève, 2003) avait pour objectif de « formuler de façon parfaitement claire une volonté politique et prendre des mesures concrètes pour poser les bases d'une société de l'information accessible à tous, tout en tenant pleinement compte des différents intérêts en jeu »[9]. La deuxième phase du SMSI (Tunis 2005) avait, elle, pour objectif la mise en œuvre du plan d'action adopté à Genève et d'arriver à un accord sur la gouvernance d'Internet.

Selon l'engagement issu du Sommet de Tunis, il fallait encourager les gouvernements, les organisations internationales, le secteur privé ainsi que la société civile à développer l'accès aux TIC. Ainsi, les grandes décisions liées à la gouvernance du cyberespace étaient ouvertes à toutes les parties prenantes.

Plus récemment, en décembre dernier, l'UIT et son Secrétaire général, Hamadoun Touré, ont tenté de procéder à une révision du Règlement des télécommunications internationales (RTI – *International Telecommunication Regulations* ou *ITR*) lors de la Conférence mondiale des télécommunications internationales (CMTI – *World Conference on International Telecommunication ou WCIT*) pour faciliter l'interconnexion et l'interopérabilité des services de communication nationaux. La révision a provoqué de vifs débats sur la régulation d'Internet et a divisé les États en deux camps distincts et aura finalement été signée par 89 États et refusée

[8] Les noms de domaine sont la version littéraire sur une adresse IP. Chaque site internet comporte une adresse IP. Pour faciliter l'accès à tous, le nom de domaine traduit l'adresse IP sous forme de mot. Exemple : www.ceim.uqam.ca. La « guerre des DNS » a commencé le 14 septembre 1995, lorsque les noms de domaines ayant pour suffixe .com ont été soumis à des frais d'inscription au profit d'un entrepreneur de la sécurité informatique SAIC. Ce fut la course aux noms de domaines à des buts de revente.

[9] http://www.itu.int/wsis/newsroom/1/pc1/jul2-fr.html, consulté le 8 novembre 2013

par 55 autres. Parmi les principaux États ayant refusé de signer la révision du règlement se trouvent les États-Unis, le Canada, la France ou encore le Japon.

Selon le témoignage de Robert McDowell, ancien commissaire de la commission fédérale des communications (*Federal Communications Commission ou FCC*) aux États-Unis, le traité de Dubaï aurait offert davantage de pouvoirs aux États dans la gouvernance d'Internet. Ces derniers auraient eu pour rôle de coopérer afin d'assurer la sécurité et de contrôler la prolifération des courriels indésirables (*spam)* sur la toile. Par ailleurs, bon nombre de commentateurs émanant de la société civile ont critiqué le manque de transparence de cette conférence. On assista aussi à la création du site WCITleaks.org par des chercheurs à l'Université George Mason en janvier 2013 qui visait justement à rendre disponible au public certains documents qui furent gardés secrets tout au long de la conférence et de sa phase préparatoire.

Un clivage entre deux mondes

Avec cette naturelle dérive propre à l'esprit humain, certains parleront de « nouvelle Guerre froide » puisque le monde, dans le sillage du sommet de Dubaï, s'est à nouveau divisé en deux. D'un côté, ceux qui revendiquaient une prédominance des acteurs étatiques dans la gouvernance de la société de l'information (Arabie Saoudite, Chine, Russie) et de l'autre, ceux qui préféraient une perpétuation du modèle multi-parties-prenantes au sein duquel l'État n'est qu'un acteur parmi d'autres (États-Unis, Canada, France). Cette vision de nouvelle Guerre froide n'était pas fausse. Mais, en réalité les avis divergeaient au sein même des pays n'ayant pas même signé la Convention. Jacques Pellet, représentant adjoint de la France à l'ONU reconnaissait qu'il fallait « plus de transparence et d'accessibilité de la part des institutions chargées de la gestion de l'Internet ou [une] meilleure prise en compte de la voix des gouvernements ». Entendons ici que la France refuse le traité de Dubaï puisqu'il ne correspondait pas à ses propres valeurs, mais aussi parce que le pays restait très critique face au mode de gestion actuel du système DNS assuré par l'ICANN.

Mais est-ce vraiment une opposition de deux mondes ? Richard Hill, ancien haut fonctionnaire de l'UIT et aujourd'hui consultant indépendant, a récemment publié un article[10] expliquant en quoi les articles 5A et 5B[11], portant sur la coopération contre les courriels indésirables, ne signifiaient pas un accroissement des prérogatives de l'UIT ou une diminution de la souveraineté des États. Ils ne donnaient pas plus de pouvoir juridique à l'UIT qu'avant l'existence de ce traité. Pour lui, le refus de signer le traité n'était aucunement d'ordre juridique mais bien politique. Quoi qu'il en soit, la révision du traité fut un échec.

[10] Richard Hill, « WCIT: Failure or success impasse or way forward? », *International journal of law and information technology*, 2/2013 (n°21), p.1-16.

[11] Les articles 5A et 5B du traité consistaient à limiter la circulation des *pourriels* et encourageaient la coopération entre les États pour assurer la cybersécurité. Toutefois, certains États ont interprété ces articles de manières différentes. Ils y ont vu un risque de violation des droits individuels en permettant de lire le contenu des courriels par les États. Et, la coopération était vue comme une extension des pouvoirs de l'UIT.

Le FMPT-13 : Un retour à la paix?

Après l'échec de décembre à Dubaï, le Secrétaire général de l'UIT a littéralement enfilé son casque bleu pour que les parties prenantes à la gouvernance d'Internet reviennent à une certaine quiétude. Durant le Forum mondial des politiques de télécommunication/TIC (FMPT – *World Telecommunication/ICT Policy Forum* ou *WTPF*)[12] à Genève étaient présents autour de la table ronde plus de 175 États, l'ICANN, des petites et moyennes entreprises du secteur des TIC, des firmes telles que *CISCO* ou encore *Microsoft* ainsi que plusieurs organisations et représentants de la société civile en tant que membres observateurs. Ce forum a abouti sur un rapport rédigé par la direction de l'UIT, qui constituera la ligne conductrice pour la Conférence plénipotentiaire de 2014 à Busan en République de Corée, où les parties seront appelées à adopter un plan stratégique et financier pour la gouvernance d'Internet durant les quatre années à venir. On y présente six avis.

Un Groupe d'experts informel (GEI – *Informal Experts Group ou IEG)* avait été mis en place pour donner les projets d'avis appelés à être discutés durant le forum de 2013. Comme la gouvernance d'Internet se veut ouverte, le GEI était composé de membres d'États souverains, du secteur privé et d'associations telles que l'ICANN.

Le premier avis concernait le développement de points d'échange Internet (IXP) à l'échelle internationale. Sur ce point, tous les acteurs présents reliés au monde du cyberespace ont convenu du fait qu'il s'agisse de la meilleure solution pour rendre la société globale de l'information véritablement globale. Traditionnellement, les fournisseurs d'accès Internet concluaient des ententes d'échange de trafic (*peering*) de manière souvent ad hoc. L'UIT souligne le déploiement récent de plusieurs points d'échange Internet, installations techniques utilisées par les FAI afin de réduire le nombre de sauts inter-réseaux et réduire les coûts de transmission de données par la centralisation des interconnexions. Les participants, ainsi que l'UIT, voient dans la multiplication de ces mêmes IXP une manière efficace de réduire les coûts d'exploitation pour les fournisseurs[13]. Le deuxième avis portait sur le développement de la connectivité à large bande. À la vitesse où circulent les informations en ce XXIe siècle, il est plus qu'important de développer cette technologie dans les pays en développement. Dans son avis, l'UIT encourageait la prise d'initiatives politiques en matière d'investissement d'infrastructures de large bande. Ces initiatives doivent être prises tant par le secteur public que privé.

Les avis 3 et 4 sont conjoints puisqu'ils abordent la pénurie des adresses IP disponibles sous la version actuelle de l'*Internet Protocol*. Chacune des machines présentes sur Internet est en effet dotée d'une adresse IP. Ces adresses IP ont été déployées lors du protocole de l'IPv4 en 1983. À cette époque, les pionniers n'avaient pas prévu que le réseau allait se développer aussi rapidement. Selon ce protocole, seulement 4,3 milliards d'adresses IP sont disponibles. Ainsi, il

[12] Le FMPT est une instance de haut niveau visant à favoriser les échanges de point de vue sur les politiques publiques relatives à internet. Ces discussions non contraignantes ont pour but de trouver un consensus.

[13] Voici une courte vidéo expliquant le fonctionnement des points d'échange Internet réalisé par l'association européenne des points d'échange. (http://www.youtube.com/watch?v=V1H9QI-w18g)

est plus qu'urgent de développer une nouvelle version pour fournir d'autres adresse IP, c'estun des buts derrière l'implémentation de l'IPv6. Celui-ci est déployé depuis mars 2011, mais le processus d'implantation reste très insuffisant. C'est pourquoi l'UIT a pris pour rôle d'encourager les acteurs à développer ce nouveau protocole. Toutefois, le passage de l'IPv4 à l'IPv6 est délicat puisqu'ils ne sont pas compatibles entre eux. Par conséquent, les acteurs participants au déploiement d'Internet doivent prendre les meilleures décisions afin de gérer convenablement le passage de l'IPv4 à l'IPv6.

Les avis 5 et 6 étaient les plus controversés et les plus politisés au sujet du futur de la gouvernance d'Internet. C'est ici où tout se joue, où chacun des mots a son importance. Pour l'UIT, ce qui est contesté dans ces deux derniers avis n'est pas la présence des gouvernements dans la nouvelle gouvernance, mais sur leur degré d'implication dans le processus de régulation. Le cinquième avis suit les initiatives prises dans l'Agenda de Tunis en 2005. Cet avis portait sur l'importance d'un mode de gouvernance « multi-parties-prenantes » pour Internet. Tous les acteurs publics, privés ou civils sont invités à prendre part dans la bonne gouvernance de l'Internet. La « toile d'araignée » du Net a été tissée d'elle-même, de la société civile, du secteur privé et indirectement par les États, particulièrement par le département de la Défense des États-Unis. Pour ainsi dire, c'est inscrit dans ses gênes. Maintenant, il faut savoir à quel degré les États seront appelés à intervenir. Le dernier avis porte sur la coopération entre les différentes parties prenantes. Les États, les entreprises, les organisations intergouvernementales et la société civile doivent s'entendre sur une pleine coopération afin de trouver des solutions sur les problèmes sécuritaires et de *spam* ainsi que pour l'accès à internet dans les pays en développement.

Beaucoup des participants se sont montrés optimistes face à l'atteinte d'un nouveau consensus dans un futur proche. Les États-Unis sollicitent fermement le modèle « multi-parties-prenantes » et le libre marché autorégulateur pour la gouvernance de l'Internet. Le *Council on Foreign Relations*, prestigieux Think Tank étatsunien, offre 90 recommandations aux décideurs américains. Le Brésil avait lui aussi décidé de proposer son avis 7 qui avait été refusé par le groupe d'experts informel puisqu'il n'y avait pas consensus. Cette proposition avait pour objectif de définir l'importance du rôle des États dans la gestion du « modèle multi-parties-prenantes ». De plus, le texte proposé par le Brésil avait pour but d'améliorer les relations entre l'ICANN et l'UIT. Enfin, l'UIT n'aurait que pour fonction d'assistance aux gouvernements pour la gestion du système multi-parties-prenantes. L'Europe a plutôt bien accueilli le texte proposé alors que les États-Unis et l'ICANN sont restés plus prudents en déclarant qu'il serait préférable d'étudier le projet dans un prochain Forum vu la complexité de cet enjeu.

Les représentants de l'ICANN, se sont dits plutôt satisfaits de la rencontre. Selon Nigel Hickson, un des membres du conseil d'administration de l'ICANN, les participants ne sont certes pas arrivés à un consensus, mais une coopération est envisageable.

Les représentants de la société civile, tels que le *Center of Democracy and Technology* (CDT) ont un pouvoir d'influence sur ces dossiers. Dans un communiqué, certaines organisations de la société civile, telles que l'Internet Society, se sont dit très satisfaites que les parties aient choisi de favoriser le « modèle multi-parties prenantes » et de rendre ces conférences transparentes à l'aide des webdiffusions produites par l'Agence onusienne. Toutefois, la

principale critique adressée à l'Union Internationale des Télécommunications est que la société civile n'a qu'un statut d'observateur et ne peut ni donner son opinion, ni s'opposer à un quelconque avis.

L'UIT, une organisation innovatrice?

L'UIT a tenté de créer des ponts entre les parties prenantes. Une entente entre les acteurs étatiques, privés et civils est nécessaire afin de rendre le pilotage du Net cohérent. Reste cependant à savoir si, au-delà, des mots, il existe bel et bien un consensus sur des pistes concrètes et une entente opérationnelle. Il existe certains indicateurs qui permettent d'être optimiste, en voici quelques exemples :

1. À la sortie des réunions de l'UIT, la Protection en ligne des enfants (*CPO – Child Online Protection*), le programme mondial cybersécurité (*GCA – Global Security Agency*) et le Partenariat multilatéral international contre les cybermenaces (*IMPACT - International Multilateral Partnership Against Cyber Threats*) se sont mis d'accord sur l'importance d'une coopération entre le secteur public, privé et la société civile afin d'assurer la sécurité et la confiance dans cette société globale de l'information.

2. Suite à la conférence, Edward Omane Boamah, ministre des communications du Ghana, a conclu un accord avec l'UIT pour assurer la sécurité contre toutes tentatives de cyberattaques. Le projet d'une durée de six mois a pour but de mettre en place une équipe nationale d'intervention en cas d'incident informatique.

3. Un accord a été signé pour un partenariat avec le cabinet de renseignement numérique *ABI Research pour* un Indice de la cybersécurité (*Global Cybersecurity Index ou GCI*) permettra de mesurer le niveau de développement de la cybersécurité des États souverains à partir d'un calcul entre cinq catégories : mesures juridiques, techniques, organisationnelles, renforcement des capacités et des coopérations entre les États et le secteur privé.

Chose certaine, le scandale de la NSA, l'attaque du laboratoire nucléaire iranien par le ver informatique *Stuxnet* ou encore les cyberattaques contre les institutions financières démontrent l'importance d'un débat sur la question de la gouvernance et surtout l'importance des États.

Recherche et rédaction : Thomas Scorticati

Direction

Nicolas Adam, chercheur au CEIM.

Michèle Rioux, professeure et directrice du CEIM.

Rédaction

Olivier Dagenais, adjoint de recherche au CEIM.

Guillaume Murphy, adjoint de recherche au CEIM.

Thomas Scorticati, adjoint de recherche au CEIM.

Abonnez-vous

À la liste de diffusion

Au fil RSS

Bulletin réalisé par le Centre d'études sur l'intégration et la mondialisation dans le cadre du projet d'Études sur les technologies de l'information et des communications (ETIC)

Centre d'études
sur l'intégration
et la mondialisation

Adresse civique :
UQAM, 400, rue Sainte-Catherine Est
Pavillon Hubert-Aquin, bureau A-1560
Montréal (Québec) H2L 2C5 CANADA

Adresse postale :
Université du Québec à Montréal
Case postale 8888, succ. Centre-Ville
Montréal (Québec) H3C 3P8 CANADA

Téléphone : (514) 987-3000, poste 3910
Télécopieur : (514) 987-0397
Courriel : ceim@uqam.ca
Site web : www.ceim.uqam.ca