Office of the
Privacy Commissioner
of Canada

Commissariat
à la protection de
la vie privée du Canada

Pouvoirs de surveillance, de perquisition ou de saisie élargis par des lois récentes au Canada, au Royaume-Uni, en France et aux États-Unis

Document d'information présenté par le Commissariat à la protection de la vie privée du Canada au Comité permanent de la sécurité publique et nationale

Révision des constatations et des recommandations issues de l'enquête interne sur les actions des responsables canadiens relativement à Abdullah Almalki, Ahmad Abou-Elmaati et Muayyed Nureddin (enquête Iacobucci) et du rapport de la Commission d'enquête sur les actions des responsables canadiens relativement à Maher Arar (enquête Arar)

7 mai 2009
Ottawa (Ontario)

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

Tables des matières

Sommaire

L'objet de cette enquête est d'étudier les pouvoirs de surveillance octroyés aux gouvernements de plusieurs pays qui ont récemment été la cible d'actes terroristes. Nous espérons qu'en étudiant les bases législatives des pouvoirs de surveillance des États-Unis, du Canada, du Royaume-Uni et de la France, un portrait comparatif des tendances juridiques qui ont une incidence sur les pouvoirs de surveillance de l'État s'en dégagera. Il y a actuellement beaucoup de discussions anecdotiques qui opposent les lois d'un pays à celles des autres, mais il existe peu d'analyses basées sur des preuves.

Depuis 2001, dans tous les pays étudiés, les inquiétudes liées à la sécurité et le rôle accru de la police en vue de combattre le terrorisme ont mené à l'octroi de davantage de pouvoirs d'enquête, de collecte de renseignements et de partage d'information aux services de police et aux organismes de renseignements. Cependant, les approches juridiques et logistiques de collecte de renseignements diffèrent d'un pays à l'autre. Les modèles de pouvoir de surveillance judiciaire, d'enquête administrative et d'autorisation ministérielle sont également différents.

Aux États-Unis, la *USA PATRIOT Act* (2001) a modifié de façon importante les lois d'interception, en allongeant leur période d'applicabilité et en imposant des contraintes moins précises sur leur utilisation. Les services de police et les organismes de renseignement ont également reçu le mandat important de recueillir et de partager davantage de renseignements avec les autorités compétentes. Au Canada, en vertu de la *Loi antiterroriste* (2001), les restrictions concernant l'interception des communications pendant les enquêtes relatives à la sécurité nationale ont également été assouplies considérablement. L'organisme canadien de renseignements relatifs aux transmissions, le Centre de la sécurité des télécommunications du Canada (CSTC), a reçu le mandat concret d'aider les organismes policiers et de sécurité dans leurs enquêtes. Au Royaume-Uni, la *Anti-terrorism, Crime and Security Act* (2001) exige explicitement des entreprises de télécommunications qu'elles conservent les données de communication de leurs clients pour les enquêtes criminelles et à des fins de sécurité nationale. Les entreprises doivent aider les organismes à intercepter des renseignements. En France, la *Loi pour la sécurité quotidienne* (2003) comporte des dispositions antiterroristes générales, des dispositions de conservation de données qui obligent les entreprises à noter les activités de leurs clients, et donne au gouvernement l'accès aux clés de chiffrement.

Il est également important de noter que chaque pays possède son propre système d'autorisation de surveillance. Aux États-Unis et en France, les ordonnances autorisant les interceptions au sein du pays sont émises par les juges. Au Canada, tout dépendant de son objectif, la surveillance est autorisée par le ministre compétent ou par des mandats obtenus en Cour supérieure. Au Royaume-Uni, les mandats exécutoires sont délivrés par le ministre de l'Intérieur.

Finalement, dans chacun des pays étudiés, les exigences administratives pour les mandats en matière de sécurité nationale sont beaucoup moins sévères que celles de mandats en matière d'enquêtes criminelles. Au Royaume-Uni et en France, les intérêts précis en matière de sécurité nationale que les enquêtes visent à protéger n'ont pas à être déterminés. Aux États-Unis, les auteurs des requêtes ne doivent pas prouver qu'il y a un motif raisonnable dans les cas liés à la sécurité nationale. De la même façon, au Canada, pour pouvoir délivrer des mandats d'application de la loi, un tribunal doit se demander si la surveillance est le dernier recours possible. Ce n'est plus vrai pour les enquêtes en matière de sécurité nationale.

Introduction

Objet et étendue de l'étude

L'objet de cette enquête est d'étudier les pouvoirs de surveillance octroyés aux gouvernements de plusieurs pays qui ont récemment été la cible d'actes terroristes. Nous espérons qu'en étudiant les bases législatives des pouvoirs de surveillance des États-Unis, du Canada, du Royaume-Uni et de la France, un portrait comparatif des tendances juridiques qui ont une incidence sur les pouvoirs de surveillance de l'État s'en dégagera. Il y a actuellement beaucoup de discussions anecdotiques qui opposent les lois d'un pays à celles des autres, mais il existe peu d'analyses basées sur des preuves.

Compte tenu des contraintes de temps et afin d'en limiter l'étendue, cette étude sera axée exclusivement sur a) les lois qui régissent les activités des organismes de l'État qui surveillent, interceptent, captent, perquisitionnent et analysent des communications, b) la capacité du gouvernement à saisir, recueillir et perquisitionner des documents imprimés et d'autres articles, et c) le mandat statutaire des autorités de partager ces renseignements. Les lois en matière de surveillance sont au cœur de ces pouvoirs. Même si une gamme complète d'instruments intergouvernementaux, de règlements internes et de procédures administratives existent également pour permettre la collecte et le partage de renseignements par les autorités de l'État, aucun de ces éléments n'est codifié dans une loi.

Finalement, c'est plus souvent la nature des programmes nationaux individuels, et non des lois ou des traités, qui a une incidence notable sur la vie privée des citoyens. Par exemple, les policiers français et britanniques peuvent vérifier l'identité de n'importe qui sans justification. Des 15 États membres de l'Union européenne, 11 sont dotés d'un système national de cartes d'identité obligatoires. Il s'agit de différences normatives de longue date qui provoqueraient probablement un tollé chez les citoyens si elles étaient appliquées en Amérique du Nord. D'autres programmes et bases de données de surveillance (comme le NSEERS de l'UE ou l'US-VISIT des États-Unis, par exemple) ont suscité la controverse en raison de leur incidence sur la vie privée des voyageurs. Cependant, les analyses détaillées des programmes de sécurité

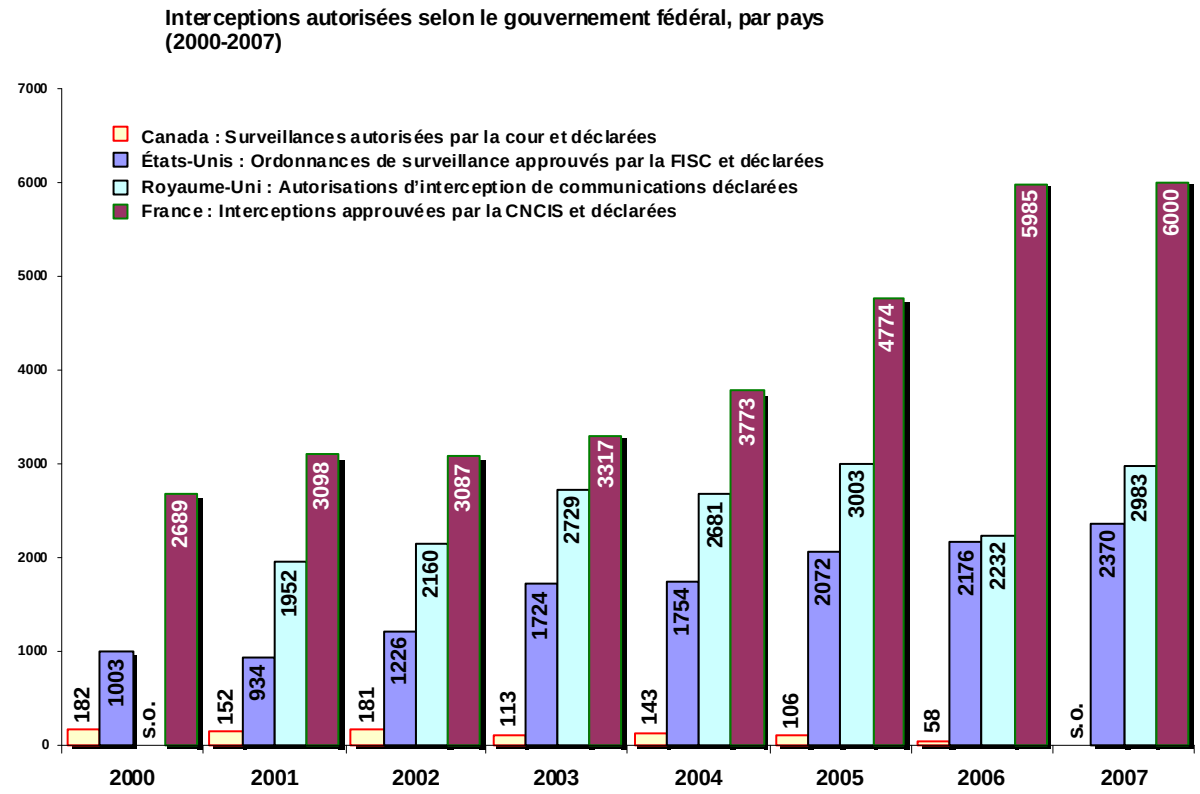
précis (repérage du financement du terrorisme, collecte d'ADN et programmes nationaux de cartes d'identité) ne font pas partie de cette étude.

Contexte historique

En étudiant les lois qui régissent la surveillance dans chacun des pays choisis, il est important de souligner que chacun d'eux a eu sa part d'expériences importantes (et traumatisantes) de terrorisme intérieur et étranger depuis plusieurs décennies. Par exemple, l'expérience du Royaume-Uni aux prises avec des ultranationalistes violents (le Front national, par exemple) ou des mouvements indépendantistes (l'Armée républicaine irlandaise, par exemple), reflète les inquiétudes nord-américaines concernant les extrémistes politiques aux États-Unis et au Canada (la milice de droite et le FLQ, par exemple). De la même façon, les États-Unis ne sont pas les seuls à avoir été la cible du terrorisme international, car le Canada (Air India), le Royaume-Uni (vol 103 de Pan-Am) et la France (attentats à la bombe à Paris) ont également été la cible d'attaques meurtrières dans les années 1980.

Cependant, depuis septembre 2001, on remarque des développements juridiques généralisés dans chacun des pays. Les lois ont changé soit graduellement (Royaume-Uni et France) soit rapidement (États-Unis et Canada) alors que les politiciens, les bureaucrates et d'autres responsables ont cherché à réorganiser les structures de surveillance juridique et administrative pour les opérations de surveillance. Aux États-Unis et au Canada, ces changements ont été en grande partie engendrés par des projets de loi-cadre individuels, comme l'*USA PATRIOT Act* et la *Loi antiterroriste*. Réciproquement, depuis l'année 2000, en France et au Royaume-Uni, un flux constant de nouvelles lois a modifié ou élargi les pouvoirs de surveillance déjà en place.

Pour avoir un bon indicateur brut de ces activités de surveillance accrues, il suffit de repérer les cas de surveillance autorisée. Pour répondre aux demandes de transparence des législateurs, chaque pays a en place une forme de communication publique concernant l'utilisation de la surveillance par les autorités de l'État (voir ci-dessous). En tenant compte de la superficie relative de chaque pays, il est intéressant de noter l'augmentation (ou la diminution) relative du nombre de surveillances approuvées depuis 2000.



Cependant, il est important de souligner que ces chiffres ne comprennent pas les activités de surveillance qui ne requièrent aucune autorisation juridique, notamment les pouvoirs d'interception utilisés pour la contre-ingérence ou pour contrer le terrorisme. Au Royaume-Uni et en France, l'information concernant ces activités est encore considérée comme un secret d'État. De plus, les interceptions purement étrangères ont lieu dans une zone grise en dehors des exigences intérieures quant aux renseignements à fournir. Depuis le début de la guerre froide, la cueillette mondiale de renseignements a évolué en partant du principe que l'interception faite à l'étranger tombe en dehors des lois nationales qui régissent la confidentialité des communications. Comme pour le cas des eaux internationales, les interceptions de communications externes ne sont pas assujetties aux mêmes surveillances juridiques, judiciaires et administratives que l'on retrouve dans le pays. De la même façon, au moins trois des quatre pays étudiés (États-Unis, Royaume-Uni et Canada) ont mis en place l'infrastructure nécessaire au partage de renseignements en tant qu'alliés, sans égard aux contraintes juridiques nationales.

Comparaison des nouveaux pouvoirs

Atténuer les limites des opérations de renseignements

- Aux États-Unis, plusieurs lois qui ont été promulguées depuis le 11 septembre 2001 permettent une cueillette élargie de renseignements de nature criminelle et étrangère au pays.

- Notamment, la *USA PATRIOT Act* de 2001 a permis aux organismes gouvernementaux de recueillir des renseignements étrangers auprès de citoyens américains ou non, a éliminé les distinctions juridiques entre les enquêtes criminelles et la surveillance visant à recueillir des renseignements étrangers, et a aboli l'exigence de la loi voulant que le gouvernement ait à prouver qu'une cible qu'il surveille n'est pas un citoyen américain[1].
- En 2007, le Congrès américain a modifié la *Foreign Intelligence Surveillance Act* (FISA) pour permettre la surveillance sans mandat des citoyens américains lorsqu'une des parties d'une conversation pourrait avoir eu lieu en dehors des États-Unis. De plus, le secrétaire à la Justice et le directeur du renseignement national « peuvent, en collaboration, autoriser pour une période pouvant aller jusqu'à un an, le ciblage de personnes que l'on croit raisonnablement être à l'extérieur des États-Unis, afin de recueillir des renseignements étrangers » [traduction], même si le point d'origine ou d'arrivée de toutes les communications à recueillir se trouve aux États-Unis[2].
- En 2001, la *Loi antiterroriste* du Canada a élargi les pouvoirs de l'organisme canadien de renseignements relatifs aux transmissions, le Centre de la sécurité des télécommunications du Canada (CST). Dans des circonstances particulières, en vertu de l'article révisé 273.65 de la *Loi sur la défense nationale* du Canada, le CST peut maintenant intercepter des communications dont le point d'origine ou d'arrivée se trouve au Canada[3].
- Le Royaume-Uni a également grandement assoupli ses contraintes juridiques concernant les opérations de surveillance intérieure, notamment dans la *Regulation of Investigatory Powers Act* (RIPA) de 2000. Cette loi permet au ministre de l'Intérieur ou à certains responsables délégués qui gèrent des renseignements de nature criminelle ou nationale de délivrer des mandats pour l'interception de communications, et exige de tous les fournisseurs de services de communications qu'ils offrent une « capacité d'interception raisonnable » [traduction] dans leurs réseaux, à des fins de surveillance dans les enquêtes en matière de sécurité nationale[4].
- La RIPA permet également aux hauts gradés de la police civile et militaire, de l'administration douanière, ainsi qu'aux membres de l'organisation judiciaire de demander qu'on leur remette le texte en clair de matériel chiffré, ou dans certains cas, les clés de chiffrement elles-mêmes.
- De plus, la *Prevention of Terrorism Act* de 2005 donne au ministre de l'Intérieur du Royaume-Uni le pouvoir d'émettre des directives de conservation des données pour tous les fournisseurs de communications, dans le but de protéger la sécurité nationale ou de prévenir ou détecter les crimes qui y sont liés.
- En vertu de ces lois de conservation des données, les données de communications doivent être conservées et rendues accessibles aux autorités pour une période pouvant aller jusqu'à un an. Récemment, le gouvernement a proposé de modifier la loi (et la RIPA) afin de rendre la conservation de données obligatoire et d'élargir son utilisation pour qu'elle comprenne les crimes sérieux et non seulement les infractions de terrorisme.
- La France a employé une tactique similaire. La *Loi pour la sécurité quotidienne* (LSQ), quoiqu'introduite en septembre 2001, a été promulguée en 2003 et

contenait certaines modifications antiterroristes concernant la conservation de données. La LSQ exige des fournisseurs de services Internet (FSI) qu'ils stockent les fichiers historiques des activités de leurs clients pour une période pouvant aller jusqu'à un an et elle offre l'accès au gouvernement à des clés de chiffrement privées[5]. Même si ces mesures devaient prendre fin en décembre 2003 et être limitées aux enquêtes terroristes, la *Loi pour la sécurité intérieure* (LSI) subséquente a élargi ses dispositions, en leur donnant une application générale et définitive.

- La *Loi relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers* (2006) impose une obligation aux FSI, aux compagnies de téléphone et à tout organisme qui donne un accès public à Internet, soit de fournir sur demande des renseignements sur les clients aux autorités antiterroristes, y compris les adresses IP, l'endroit où l'équipement est utilisé, des listes d'appels effectués, les personnes impliquées et les dates de communications. À la suite de la mise en œuvre de la loi, les médias français ont rapporté que la police et les services de renseignements avaient mis sur pied une plateforme technique leur permettant de recueillir facilement des données de trafic liées aux messages textes, aux téléphones mobiles et à Internet[6].
- Aussi, la *Loi relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers* offre aux services de renseignements antiterroristes un accès aux bases de données administratives nationales françaises, auxquelles ils n'avaient pas accès avant 2006.
- En vertu des lois françaises de conservation des données, les services de sécurité peuvent déterminer précisément qui a communiqué avec qui, et quand et où c'est arrivé; ils peuvent également obtenir, auprès des compagnies de téléphone, les listes de tous les appels qu'un abonné a effectués ou reçus, des documents d'abonnement, des adresses et des renseignements bancaires, et les adresses de sites Internet ou de forums qu'une personne a visités.

Permettre la collecte de renseignements des citoyens

- Depuis le 11 septembre 2001, les États-Unis ont réduit un grand nombre de mesures de protection juridique et administrative qui empêchaient les organismes de surveiller les citoyens américains. Notamment, la *USA PATRIOT Act* a éliminé l'exigence de la loi voulant que le gouvernement ait à prouver qu'une cible qu'il surveille n'est pas un citoyen américain et a expressément autorisé les ordonnances de surveillance de citoyens américains dans les enquêtes liées aux activités terroristes internationales ou aux activités clandestines de renseignements[7].
- De la même façon, dans la foulée de la controverse liée à l'écoute téléphonique sans mandat aux États-Unis, le Congrès a modifié la FISA en 2008 afin de laisser tomber cette dernière clause. Le gouvernement n'a plus à démontrer que ses cibles sont des agents étrangers ou des personnes impliquées dans des activités criminelles ou terroristes[8].

- Comme il a été mentionné, la *Loi antiterroriste* du Canada permet au ministre de la Défense nationale d'autoriser le CSTC d'intercepter des renseignements confidentiels, sous certaines conditions[9].
- Par le passé, il était interdit au CSTC d'intercepter toute communication dans laquelle un des participants se trouvait au Canada. Par exemple, une communication dans laquelle une personne présentant un intérêt pour le renseignement étranger communique avec un collaborateur au Canada (comme une personne soupçonnée de financer des terroristes qui se trouve au Pakistan et qui envoie un courriel à une personne qui se trouve à Montréal).
- La loi n'*exclut* pas expressément l'interception de communications des citoyens canadiens ni ne *limite* expressément les interceptions de ces communications qui surviennent en dehors du Canada.
- Comme le souligne l'expert canadien en renseignements Wesley Wark, « il s'agit d'un changement historique dans le mandat du CSTC, qui depuis sa mise sur pied, au début de la guerre froide, vise exclusivement les communications étrangères » [traduction]. Depuis 2001, l'effectif du CSTC est passé d'environ 1 000 employés à 1 700 employés en 2008.
- Cependant, d'autres pays anglo-américains semblent avoir adopté ce changement. Comme le souligne Stanley Cohen, « l'autorisation ministérielle semble maintenant être la norme dans les pays de la *common law* avec lesquels on compare souvent le Canada […] partenaires dans les exercices de collecte de renseignements qu'entreprendrait normalement le CSTC » [traduction]. Comme l'a expliqué un responsable de la sécurité publique devant un comité sénatorial en 2001, « lorsqu'il y a une connexion canadienne, par exemple, si la cible est étrangère mais que l'appel est reçu au Canada ou vient du Canada, faut-il une autorisation judiciaire? D'après nous, clairement non ».
- L'approche de surveillance et d'interception des communications au Royaume-Uni est également teintée par la tradition. Historiquement, l'interception de communications par le gouvernement est une pratique qui existe depuis longtemps et qui est connue du public. Avant 1985, il n'existait pas de cadre légal qui régissait cette pratique, seulement des dispositions isolées dans différentes ordonnances. Le secrétaire d'État était investi d'un pouvoir qui lui permettait d'autoriser, par mandat, l'interception de toute communication postale ou télégraphique, en supposant que le processus était assujetti à un contrôle par le pouvoir exécutif plutôt qu'à un règlement.
- Par conséquent, à ce jour, les surveillances effectuées par les autorités britanniques en vertu de la RIPA ne requièrent pas de mandat pour identifier une personne ou des lieux, si elles sont liées à l'interception de communications à l'extérieur du Royaume-Uni[10].
- Même pour les opérations intérieures, l'interception de communications de personnes ou de lieux précis peut être exigée par le service de sécurité, le service secret de renseignements, le Service gouvernemental d'écoutes et de transmission, la Serious Organised Crime Agency, la police, les Douanes et Accise, l'organisme de renseignements de défense et d'autres organismes gouvernementaux, en autant que l'objectif de la surveillance soit lié à la sécurité nationale, à la prévention et à la détection de crimes sérieux et à la protection du

bien-être économique du Royaume-Uni, ou aux dispositions de tout accord international d'assistance mutuelle[11].

- En France, la LSI (2003) donne aux autorités le mandat d'ajouter des données dans la base de données nationale de recherche de criminels, y compris dans la base de données nationale d'empreintes digitales. Notamment, la LSI allonge la liste d'infractions et de personnes qui peuvent mener à des dossiers dans la base de données nationale d'empreintes digitales, y compris les personnes pour lesquelles la police a de bonnes raisons de soupçonner qu'elles ont presque commis un crime[12].
- Toujours en France, la *Loi relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers* (2006) prévoit la collecte de renseignements personnels de tous les passagers qui voyagent en provenance ou à destination d'un État à l'extérieur de l'UE. Ces renseignements peuvent être sous forme de cartes de débarquement et de codes à barres sur les documents de voyage, et peuvent être recueillis par les systèmes de réservation.
- La même loi s'applique à la vidéosurveillance à des fins antiterroristes et donne à la police un accès à toutes les cassettes de surveillance en dehors du contexte d'une enquête en cours, sans mandat. En vertu de la loi, les autorités publiques peuvent utiliser la vidéosurveillance dans les endroits publics à des fins de « prévention d'actes terroristes », et les organismes privés peuvent installer des systèmes de vidéosurveillance pour protéger leurs locaux lorsqu'ils « risquent d'être la cible d'actes terroristes ». La police et d'autres organismes de surveillance des travaux publics et du transport peuvent également mettre en place des systèmes de surveillance pendant quatre mois, en cas d'urgence.
- Aussi, la même loi prévoit la *Lecture automatisée des plaques d'immatriculation* (LAPI), qui permet l'installation de dispositifs fixes et mobiles partout en France afin de prévenir les actes de terrorisme et d'aider à combattre le vol des véhicules. Ces dispositifs peuvent lire automatiquement les plaques d'immatriculation et comparer leurs données avec celles comprises dans la base de données nationale des véhicules volés et les bases de données des autorités de l'UE, et ils peuvent également photographier les occupants des véhicules.

Permettre les perquisitions et la surveillance sans avis

- La *USA PATRIOT Act* prévoit également plusieurs moyens traditionnels de surveillance judiciaire dans l'acte de procédure américain concernant les perquisitions. La loi permet des perquisitions sans être vus par les autorités fédérales, c'est-à-dire que ceux qui font l'objet d'une perquisition mandatée sont sujets à un avis retardé et ils ne savent pas ce qui a été perquisitionné, ou si quelque chose a été saisi pendant le processus[13].
- De la même façon, la *Loi antiterroriste* du Canada a ajouté les « infractions terroristes » à la liste des circonstances pour lesquelles un procureur général peut retarder l'avertissement d'une personne qui fait l'objet d'écoute téléphonique, pour une période pouvant aller jusqu'à trois ans[14].

- La *Loi antiterroriste* élimine la nécessité de démontrer que la surveillance est le dernier recours pour les enquêtes en matière de terrorisme, bien que la plupart des écoutes téléphoniques doivent être approuvées par un juge de cour supérieure.
- Cela étant dit, la *Loi sur la sécurité publique* a modifié la LPRPDE pour permettre aux organisations du secteur privé de recueillir des renseignements personnels à l'insu et sans le consentement d'une personne, si a) la collecte est à des fins de divulgation subséquente exigée par la loi, b) le SCRS, la GRC ou tout autre organisme gouvernemental autorisé en fait la demande et que les renseignements sont liés à la sécurité nationale, à la défense du Canada ou à la tenue d'affaires internationales, et c) l'organisme croit que les renseignements peuvent être pertinents pour la sécurité nationale, la défense du Canada ou la tenue d'affaires internationales et entend divulguer ces renseignements à un organisme d'enquête ou une institution gouvernementale.
- En plus de ces révisions juridiques, le Canada a récemment mis sur pied divers programmes de surveillance « passive », notamment le Programme de protection des passagers parrainé par la *Loi sur la sécurité publique*. La loi a ajouté un article dans la *Loi sur l'aéronautique,* qui exige des compagnies aériennes qu'elles divulguent les renseignements personnels de tous leurs passagers à destination ou en provenance du Canada aux autorités désignées à des fins de « sécurité des transports », et qui permet au ministre des Transports d'exiger de tout transporteur ou exploitant aérien faisant partie d'un système de réservation de lui divulguer des renseignements spécifiques qu'il a en sa possession à des fins de sécurité des transports ou d'enquêtes sur des « menaces envers la sécurité du Canada »[15].
- Au Royaume-Uni, la *Terrorism Act* de 2000 élargit grandement les pouvoirs de perquisition discrétionnaires des autorités, permettant aux responsables d'effectuer des perquisitions dans des maisons après avoir reçu un mandat d'un juge de paix, basé sur des « doutes raisonnables » [traduction][16]. La loi permet également à un policier d'arrêter et de perquisitionner un véhicule ou des personnes dans des zones préalablement autorisées, à sa discrétion, et donne le pouvoir de recherche détaillée dans une zone précise pendant une certaine période de temps si cette activité est considérée comme « propice à la prévention d'actes terroristes » [traduction][17].
- Par suite de ces pouvoirs, la totalité du Grand Londres a été déclarée zone de perquisition par la police aux mois d'août et de septembre 2003.
- Le Royaume-Uni a également élargi ses activités de surveillance de ses citoyens au nom de la sécurité publique et du maintien de l'ordre de routine. En 2001, l'*Anti-terrorism, Crime and Security Act* a permis à la police britannique des transports du ministère de la Défense d'autoriser la recherche détaillée de certaines zones pour une période pouvant aller jusqu'à 28 jours, tout en permettant la documentation importune de suspects par la police pendant leur détention, allant de l'échantillonnage d'ADN à des photos détaillées de caractéristiques physiques (tatouages, grains de beauté et cicatrices, par exemple)[18].
- De plus, la *Prevention of Terrorism Act* de 2005 permet aux tribunaux du Royaume-Uni d'imposer des « mesures de contrôle » sur un suspect, « qui placent

une obligation sur ce dernier à des fins de protection du public contre un risque de terrorisme » [traduction]. Comme pour le cas des injonctions aux États-Unis et au Canada, elles déterminent comment une personne peut communiquer, voyager, interagir, etc. La traçabilité électronique et la surveillance permanente de suspects non jugés deviennent de plus en plus fréquentes en vertu de cette disposition de la loi.

- Comme il a été souligné, la LSI de France permet l'accès immédiat, par les autorités d'application de la loi, aux données d'entreprises de télécommunications et permet la perquisition sans mandat de tout système de renseignements, en autant que le système en question soit connecté à un ordinateur perquisitionné à la suite de l'émission d'un mandat.
- Aussi, la *Loi relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers* (2006) prévoit une procédure administrative pour l'accès à des renseignements électroniques des FSI sans autorisation juridique préalable.

Prorogation des mandats de perquisition et de surveillance

- Les États-Unis, dans une succession de révisions législatives, ont prorogé le délai prescrit pour l'utilisation de mandats de perquisition en vertu de la FISA. Au départ, la *USA PATRIOT Act* fixait le délai des fouilles manuelles à a) 90 jours (comparativement à 45) ou b) 120 jours pour les agents d'une puissance étrangère (employés ou membres d'une puissance étrangère, non citoyens américains)[19].
- En 2005, avec la USA *PATRIOT Improvement and Reauthorization Act* le délai pour les enregistreurs graphiques et les dispositifs de piégeage et de suivi est passé de 90 jours à un an[20].
- Enfin, en 2008, le délai fixé pour la surveillance sans mandat est passé de 48 heures à 7 jours par suite des modifications à la FISA.
- Dans le même ordre d'idées, la *Loi antiterroriste* canadienne a prorogé jusqu'à un an le mandat d'écoute électronique utilisé pour enquêter sur de présumées activités terroristes, au lieu du délai de 60 jours pour la plupart des infractions.
- Comme il a été mentionné précédemment, en France, diverses lois ordonnent aux fournisseurs de service Internet et aux compagnies de téléphone de conserver les renseignements personnels des clients et de les stocker pour une période allant jusqu'à un an. En outre, la LSI permet aux autorités d'accéder immédiatement aux données informatiques des entreprises de télécommunications et autorise les perquisitions sans mandat et permet la perquisition sans mandat de tout système de renseignements, en autant que le système en question soit connecté à un ordinateur perquisitionné à la suite de l'émission d'un mandat. Conformément à la *Loi pour la confiance dans l'économie numérique* (LEN), les fournisseurs de services Internet doivent également tenir un registre des données des abonnés et les personnes qui désirent afficher du contenu sur Internet doivent s'identifier à leur fournisseur de services.

Échange de renseignements entre organismes

- La reformulation globale de la façon dont les organismes gouvernementaux échangent et exploitent les renseignements constitue l'un des changements les plus profonds en matière de renseignement et d'application de la loi depuis les attentats du 11 septembre aux États-Unis.
- L'un des principaux objectifs de la *USA PATRIOT Act* était la libre circulation des renseignements entre les divers organismes. La *USA PATRIOT Act* autorise la divulgation de résultats d'écoute électronique, d'information obtenue durant une audience devant un grand jury et d'autres renseignements recueillis dans les affaires pénales aux organismes de renseignement lorsque ceux-ci sont du renseignement étranger[21].
- La *USA PATRIOT Act* autorise également la collecte et la mise en commun de renseignements n'ayant pas un lien direct avec des activités criminelles par les organismes d'application de la loi. Ainsi, une importante restriction législative, imposée aux États-Unis à la fin des années 1970, est abolie entre les organismes d'application de la loi et de renseignement.
- Enfin, le renseignement étranger, la contre-ingérence et le renseignement étranger obtenus dans le cadre d'une enquête criminelle peuvent être communiqués à tout représentant de l'application des lois fédérales, du renseignement, de la protection, de l'immigration, de la défense nationale ou de la sécurité nationale afin de l'aider dans l'exercice de ses fonctions officielles.
- En 2005, découlant du changement historique et dans la foulée du rapport de la Commission du 11 septembre, le Congrès américain a passé la *Intelligence Reform and Terrorism Prevention Act* (IRTPA). Cette loi autorise la création d'un « environnement de mise en commun des renseignements » afin d'« établir un lien entre toutes les entités fédérales, locales et tribales appropriées et le secteur privé » [traduction].
- Plus particulièrement, aux fins de mettre en commun les renseignements dans les bases de données publiques et privées, l'IRTPA ne comporte aucune garantie de sécurité contre l'exploration de données autre que d'enjoindre le président à publier des lignes directrices[22].
- Comme le soulignait le commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique dans son rapport de 2004 sur la *USA PATRIOT Act*, « le manque de distinctions entre les fonctions d'application de la loi et de sécurité nationale est l'une des caractéristiques déterminantes des États policiers, de sorte que la primauté du droit donne lieu tôt ou tard à une prise de décision arbitraire par les autorités chargées de l'application des lois et que les droits des citoyens ordinaires perdent leur signification. Les démocraties reposent sur des règles claires et efficaces adaptées aux activités de l'État qu'elles sont censées régir et qui reflètent les valeurs essentielles d'une société libre » [traduction].
- Des tendances semblables se dessinent dans les milieux du renseignement canadiens. En vertu des dispositions de la *Loi sur la sécurité publique*, les données sur les passagers recueillies par Transports Canada peuvent être divulguées à la GRC, au SCRS, à Citoyenneté et Immigration Canada, à l'Agence du revenu du Canada et à l'Administration canadienne de la sûreté du transport

aérien dans le but d'assurer la sécurité du transport. Des dispositions similaires sur l'échange des renseignements ont été étendues au Centre d'analyse des opérations et déclarations financières du Canada (CANAFE) à des fins de mise en commun des renseignements financiers au sein des organismes de sécurité nationale et d'application de la loi.

- De façon encore plus générale, les modifications à l'article 7 de la LPRPDE prévues dans la *Loi sur la sécurité publique*, qui permettent la collecte et l'utilisation des renseignements sans le consentement de l'intéressé à des fins de sécurité nationale, montrent une fois de plus la possibilité qu'ont les organisations privées de divulguer des renseignements de nature délicate aux organismes canadiens d'application de la loi.
- Pour citer Kent Roach, plusieurs dispositions de la *Loi sur la sécurité publique* « autorisent la mise en commun des renseignements sans un examen et une surveillance poussés de la nécessité de l'échange des renseignements, de l'exactitude et de la fiabilité des renseignements échangés ou des répercussions de l'échange des renseignements sur la protection de la vie privée[23] » [traduction].
- Au Royaume-Uni, les législateurs ont aussi donné aux autorités le mandat d'accroître la mise en commun des renseignements. L'*Anti-terrorism, Crime and Security Act* offre aux autorités publiques toute la latitude voulue en matière d'échange de renseignements se rapportant aux enquêtes criminelles ou aux procédures contre des présumés terroristes, au Royaume-Uni ou à l'étranger, une fois cet échange approuvé en principe par le ministre de l'Intérieur.

Échange de renseignements intergouvernemental

- La *USA PATRIOT Act* permet également aux milieux du renseignement américains d'établir le contact au sens large avec des partenaires internationaux. Ainsi, tout renseignement qui se rapporte à la capacité des États-Unis à se protéger d'un attentat réel ou potentiel, du sabotage ou du terrorisme international ou des activités clandestines de renseignement ainsi que tout renseignement qui se rapporte à la défense ou la sécurité nationales ou à la tenue d'affaires étrangères peut être divulgué à *tout* représentant du gouvernement, y compris les organismes de renseignement, de défense nationale et de sécurité nationale[24].
- Les dispositions subséquentes de l'IRTPA (2005) renforcent la divulgation de renseignements aux représentants de gouvernements étrangers, le cas échéant[25].
- Dans le même ordre d'idées, conformément à la *Loi antiterroriste* au Canada, les renseignements obtenus d'un gouvernement étranger ou d'un organisme international peuvent également être présentés par l'État et être pris en considération par un juge afin qu'il détermine si un groupe doit figurer sur la liste des organisations terroristes. Les personnes visées peuvent recevoir un résumé des preuves pour autant que l'information divulguée ne porte pas atteinte à la sécurité nationale.

Pouvoirs étendus d'ordonnances de production

- Le fait que le Federal Bureau of Investigation (FBI) puisse, en vertu de la *USA PATRIOT Act*, délivrer une ordonnance pour « avoir accès à des "objets tangibles" (y compris des livres, des dossiers, des papiers, des documents et d'autres objets) à des fins d'enquête de protection contre le terrorisme international ou les activités clandestines de renseignement » [traduction] constitue un autre aspect prêtant énormément à controverse.
- En gros, la disposition en question prévoit l'établissement des mandats autonomes signés par un enquêteur. Dénommées lettres de sécurité nationale (National Security Letters, NSL), il s'agit en quelque sorte d'ordonnances administratives utilisées par le FBI et, selon les informations obtenues, par d'autres organismes gouvernementaux américains, dont l'Agence centrale de renseignement (Central Intelligence Agency, CIA) et le département de la Défense[26].
- La NSL équivaut à une ordonnance de production de dossiers et de données concernant des personnes, délivrée à une entité ou à un organisme particulier. En vertu de la loi, toute personne peut être tenue de remettre des documents sur ses clients aux autorités. Le gouvernement fédéral des États-Unis dispose ainsi d'un pouvoir sans pareil pour accéder aux documents financiers, aux antécédents médicaux, à l'historique d'utilisation d'Internet, aux tendances touristiques et à d'autres documents sur une personne et pour les examiner.
- En 2005, l'IRTPA a commencé à exiger l'approbation des hauts fonctionnaires pour les NSL des dossiers des bibliothèques, des librairies et des ventes d'armes à feu, des dossiers médicaux et scolaires, et des déclarations de revenus. Sur le fondement des NSL, les autorités ont présenté des demandes de renseignements sur 3 501 personnes différentes aux États-Unis en 2005. Au cours de la même période, le nombre total de demandes de renseignements en vertu des NSL concernant des personnes aux États-Unis s'est chiffré à 9 254.
- En 2006, 12 583 demandes de NSL ont été présentées sur 4 790 personnes différentes aux États-Unis. Le nombre de NSL a augmenté de façon remarquable depuis que le FBI a le pouvoir de les délivrer en vertu de la *USA PATRIOT Act*.
- En mars 2007, l'inspecteur général du département de la Justice des États-Unis a déterminé que le FBI avait abusé de son pouvoir relativement aux NSL dans 22 % des affaires examinées. Le FBI n'a en outre pas rapporté au Congrès le nombre réel de lettres de sécurité délivrées. La Cour de district américaine a plus tard déclaré la disposition relative aux NSL de la *USA PATRIOT Act* comme étant inconstitutionnelle.
- Au Canada, un nouveau précédent jurisprudentiel en matière d'ordonnances de production dans les enquêtes sur la sécurité nationale a vu le jour. La *Loi antiterroriste* a modifié la *Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes* afin d'habiliter le directeur du SCRS ou tout membre de l'organisme à présenter à un juge une demande d'ordonnance de divulgation de toute information lorsqu'il y a des « motifs raisonnables » de croire que la sécurité du Canada est menacée. L'ordonnance autorise tous les employés du SCRS nommés dans l'ordonnance à accéder à tous les renseignements ou documents ayant trait à l'ordonnance et à les examiner.

Accès aux communications téléphoniques (contenu)

- Aux États-Unis, l'interception des communications par les autorités est chose courante depuis longtemps. Les organismes d'application de la loi pratiquent l'écoute clandestine depuis l'invention des communications par télégraphe en 1844 et l'écoute téléphonique, depuis le début des années 1890. En 1928, la Cour suprême a statué, dans l'affaire *Olmstead c. États-Unis*, que l'interception des conversations téléphoniques par des agents fédéraux ne constituait pas une perquisition ou une saisie aux termes du quatrième amendement de la Constitution.
- Il faut attendre les années 1960 pour que la Cour suprême des États-Unis protège les personnes des perquisitions et saisies abusives en limitant les poursuites fondées sur l'interception des communications. Dans la cause faisant jurisprudence *Katz c. États-Unis* (1967), la Cour a établi la doctrine de l'attente raisonnable en matière de respect de la vie privée en statuant que l'interception sans mandat contrevenait au quatrième amendement.
- De plus, il convient de le souligner, l'interception des conversations téléphoniques aux États-Unis nécessite toujours un mandat, malgré tout ce qui a été écrit sur la *USA PATRIOT Act*[27]. Les modifications de 2008 à la FISA autorisent les autorités à effectuer de la surveillance injustifiée de personnes pour une période allant jusqu'à une semaine seulement si le tribunal de la FISA est avisé du début de la surveillance et qu'une demande d'autorisation est présentée dans la semaine même.
- Au Royaume-Uni, le nombre de communications interceptées a augmenté depuis l'entrée en vigueur de la *Regulation of Investigatory Powers Act* (RIPA), en 2004. Plus de 200 organismes, services de police et prisons ont maintenant le droit d'intercepter des communications. En 2005-2006, 2 407 mandats d'interception de téléphone et de courrier ont été délivrés en Angleterre et en Écosse conformément à la RIPA, comparativement à 1 466 en 2002. De même, 5 143 modifications de mandats ont été apportées. Les autorités refusent de divulguer le nombre d'interceptions liées à la sécurité nationale.

Accès aux communications électroniques

- La *USA PATRIOT Act* permet aux organismes d'application de la loi d'installer des dispositifs pouvant intercepter le courrier électronique et les activités sur Internet (avec une ordonnance en vertu de la FISA) et élargit la portée de la surveillance au paquet de données et aux données des destinataires. La loi « accroît considérablement le type et la quantité d'information que les autorités peuvent obtenir sur les utilisateurs de leurs fournisseurs de services Internet (FSI) » [traduction][28].
- Au Royaume-Uni, l'*Anti-terrorism, Crime and Security Act* (2001) habilite le ministre de l'Intérieur à diffuser un code de pratique sur la conservation des données par les fournisseurs de services de communications dans le but d'assurer la sécurité nationale ou de prévenir ou détecter les crimes ayant trait à la sécurité

nationale. La conservation se limite aux données que les fournisseurs de services de communications détiennent déjà à des fins commerciales[29].

- Les données sur les communications peuvent être conservées jusqu'à un an. Le gouvernement a proposé de modifier la loi (et la RIPA) afin que la conservation des données soit obligatoire et que son utilisation soit élargie aux crimes graves en plus des infractions de terrorisme[30].
- En France, les dispositions d'accès légal de la *Loi pour la sécurité intérieure* (LSI) s'étendent maintenant à toutes les données stockées par les entreprises de télécommunications (y compris les FSI) ainsi qu'à la plupart des instituts, organismes ou entreprises publics ou privés. La loi autorise les recherches sans mandat dans les données de tout système à distance, pour autant que les données soient accessibles par un réseau d'un ordinateur perquisitionné sur présentation d'un mandat. L'accès aux données stockées dans un ordinateur situé dans un pays étranger demeure assujetti aux accords internationaux applicables en la matière.

Accès aux dossiers de communications

- En vertu de la *USA PATRIOT Act*, les FSI peuvent communiquer toute donnée sur les transactions aux organismes d'application de la loi sans ordonnance d'un tribunal ou assignation. Les données comprennent le nom, l'adresse, les dossiers de facturation d'appels locaux et interurbains, le numéro de téléphone ou le numéro ou l'identité d'autres abonnés et la durée du service d'un abonné, mais aussi les heures et durées des sessions, les types de services utilisés, l'information relative à l'adresse du dispositif de communication (par exemple les adresses IP), le mode de paiement ainsi que les numéros de comptes bancaires et de cartes de crédit[31].
- Les modifications de 2008 à la FISA permettent au secrétaire à la Justice et au directeur du renseignement national d'ordonner à tout fournisseur de services de communication électronique à immédiatement « fournir aux autorités tous les renseignements, les ressources et l'aide nécessaires pour accomplir l'acquisition » [traduction]. Cette nouveauté a conduit à de nombreux reportages des médias sur des organismes de renseignements américains accédant « à califourchon » à leurs propres dispositifs de surveillance sur des réseaux privés en installant les dispositifs de façon permanente[32].
- Au Canada, les dispositions concernant le CSTC dans la *Loi antiterroriste* stipulent que l'organisme détient les pouvoirs d'« acquérir l'information provenant de l'infrastructure mondiale d'information dans le but de fournir des renseignements étrangers » à l'aide de moyens comprenant l'interception des communications visant des cibles étrangères, et de veiller à la protection des renseignements électroniques et des réseaux informatiques du gouvernement.
- Le renseignement doit être acquis dans le but de fournir des données provenant du renseignement étranger, conformément aux priorités du gouvernement du Canada en matière de renseignement, de fournir des avis, des conseils et des services pour aider à protéger les infrastructures d'information et les renseignements électroniques essentiels pour le gouvernement du Canada et

d'apporter une assistance technique et opérationnelle aux organismes fédéraux chargés de l'application de la loi et de la sécurité, dans l'exercice des fonctions que la loi leur confère[33].

- Les dispositions sur la conservation des données une fois la RIPA passée au Royaume-Uni fournissent également aux autorités britanniques un accès étendu aux dossiers de communications. Ces dispositions autorisent toute autorité publique désignée par le ministre de l'Intérieur à accéder aux « données sur les communications » [traduction] sans mandat.
- Les données accessibles comprennent les renseignements sur les abonnés, les relevés des appels effectués et reçus, le courrier électronique envoyé et reçu, les sites Web consultés, la localisation des téléphones cellulaires, les renseignements identificateurs d'une personne, d'un appareil ou d'un lieu, par exemple l'identification de la ligne appelante et les données sur la localisation de téléphones cellulaires, les données d'identification ou de sélection d'appareils, par exemple les données de routage.
- En vertu du paragraphe 22(2) de la RIPA, il est possible d'accéder aux données sur les communications pour les raisons suivantes: (a) sécurité nationale; (b) prévention ou détection du crime ou prévention des désordres publics; (c) bien-être économique du Royaume-Uni; (d) sécurité publique; (e) protection de la santé publique; (f) fixation ou perception d'impôt, de droit, de taxe ou d'autre contribution, ou charge payable à un ministère; (g) en cas d'urgence, prévention de décès ou de blessures ou de tout préjudice à la santé physique ou mentale ou atténuation de blessures ou de tout préjudice à la santé physique ou mentale[34].
- En 2005-2006, 439 000 demandes de données sur les communications ont été présentées. D'après le ministère de l'Intérieur, la plupart des demandes portaient sur les informations d'adresse. Qui a accès aux données sur les communications a fait l'objet d'une importante controverse.
- Là encore, à l'instar du Royaume-Uni, les autorités françaises ouvrent l'accès aux données sur les transactions à des fins d'enquête. La *Loi sur la sécurité quotidienne* établit à un an la période de conservation des données dans le but de la prévention, de l'enquête, de la détection et de la poursuite des crimes.
- Les données ne doivent pas révéler le contenu des communications, que ce soit le contenu du courrier électronique ou le contenu des sites Web consultés. Les FSI fautifs sont passibles d'un an de prison et d'une amende de 75 000 euros.
- L'Association des fournisseurs d'accès et de services Internet (France) a publié un document évaluant les demandes de données qu'elle a reçues des autorités judiciaires. Le document public fait état d'une réception mensuelle d'environ 500 demandes.
- Les dispositions françaises sur la conservation et la divulgation des données pourraient être prorogées. D'après une version provisoire publiée en avril 2007, les webmestres, les fournisseurs d'hébergement, les compagnies de téléphonie fixe et mobile et les fournisseurs de services Internet devront conserver tous les renseignements sur les internautes et les abonnés au téléphone et les communiquer à la police ou à l'État sur demande. Ils devront en plus conserver les mots de passe fournis au moment de l'inscription à un service téléphonique ou à

un compte Internet ou les renseignements de paiement comme le montant, la date ou le mode.

- D'après le texte provisoire, les données conservées par les FSI et les fournisseurs d'hébergement, puis communiquées à la police pourraient être conservées par cette dernière pendant trois ans dans les systèmes de traitement automatique fournis par les ministères de l'Intérieur et de la Défense.
- Comme il a déjà été mentionné, la LEN autorise d'autres exigences relatives à la conservation de données dans les télécommunications, nommément la clause pour les renseignements personnels (y compris le nom, l'adresse et les données enregistrées) devant être recueillis sur les utilisateurs par tous les fournisseurs de réseaux électroniques. En outre, conformément à la LEN, toute personne qui désire afficher du contenu sur Internet doit s'identifier au public, en indiquant son nom et son adresse sur son site Web (dans le cas d'une entreprise), ou à son fournisseur d'hébergement (dans le cas d'une personne).
- L'Union européenne (UE) a ajouté depuis une directive sur la conservation des données à des fins d'application de la loi et de sécurité nationale aux dispositions sur la conservation des données au Royaume-Uni et en France par les fournisseurs en télécommunications. Les entreprises de communications européennes doivent ainsi conserver et rendre accessibles les données de trafic « pour les enquêtes, la détection et les poursuites de crimes graves, comme le prévoit le droit national de chaque État membre » [traduction], pour une période allant jusqu'à deux ans.
- À ce jour, seuls l'Allemagne, le Danemark, l'Italie et l'Irlande ont mis la directive en œuvre. Dans certains cas, la période de conservation exigée est de 24 mois. Cela dit, la Commission européenne a avisé officiellement par écrit 19 États membres de l'UE de leur non-respect de l'échéance pour mettre en œuvre la directive. Aux États-Unis et au Canada, l'approche a été accueillie avec beaucoup de réserve.

Accès aux documents financiers

- Aux États-Unis, la *USA PATRIOT Act* a également modifié les lois en matière de protection des renseignements financiers des personnes en accordant un vaste pouvoir aux enquêteurs pour exiger les livres comptables[35].
- Auparavant, seuls les dossiers des transporteurs publics et des installations d'accueil au public, d'entreposage et de location de véhicule pouvaient être obtenus avec l'ordonnance d'un tribunal. La loi permet maintenant de demander au tribunal de la FISA d'ordonner la production de tout livre comptable ou objet tangible en vue d'une enquête destinée à assurer une protection contre le terrorisme international ou les activités clandestines de renseignement.
- La *USA PATRIOT Act* a également accru la portée de la *Bank Secrecy Act* pour mettre l'accent sur la lutte au financement d'activités terroristes et au blanchiment d'argent, accordant au Financial Crimes Enforcement Network (FinCEN) un nouveau pouvoir de surveillance et d'établissement de rapports.
- Dans une certaine mesure, la surveillance des opérations financières des personnes s'est aussi répandue au Canada. La *Loi antiterroriste* a modifié les lois canadiennes sur le recyclage de l'argent, ajoutant le financement d'activités

terroristes à la liste des infractions par la *Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes*[36].

- La loi subséquente en 2005 a également autorisé l'organisme principal, le CANAFE, à demander des renseignements sur des transactions, des comptes et des personnes suspects au moyen d'échange de renseignements avec le CSTC, le SCRS et les services de police du Canada[37].
- Dans la même veine, au Royaume-Uni, en vertu du *Terrorism Act* (2000), les services de police peuvent ordonner aux institutions financières de divulguer les adresses actuelles et précédentes, les numéros de compte financier et la date de naissance d'un client afin de bloquer ou saisir des actifs suspects qui fournissent un soutien matériel à des activités terroristes. Il est également possible de surveiller les mouvements sur un compte grâce à l'obtention d'un mandat judiciaire[38].
- Les pays de la présente étude étant tous membres du Groupe d'action financière sur le blanchiment de capitaux, ils ont mis sur pied une unité de renseignement financier semblable au CANAFE. Les États-Unis ont créé le FinCEN en 1990, le Royaume-Uni, la Serious Organized Crime Agency en 2000 et la France, le Traitement du renseignement et action contre les circuits financiers clandestins (TRACFIN) en 1990.

Sources consultées

- ABELE, Robert P. *A user's guide to the USA Patriot Act Act and beyond*, 2005.
- ALEXANDER, Yonah et Edgar H. BRENNER, éd., *United Kingdom's legal responses to terrorism*, 2003.
- AMERCIAN CIVIL LIBERTIES UNION. « Surveillance Under the USA PATRIOT ACT Act », mis à jour en avril 2003), <http://www.aclu.org/safefree/general/17326res20030403.html>.
- BAKER, Stewart A. et John KAVANAGH, éd., *Patriot Act Debates: Experts debate the USA PATRIOT Act*, 2005.
- BAZAN, E. B. *The Foreign Intelligence Surveillance Act*, 2002.
- BECKMAN, James. *Comparative legal approaches to homeland security and anti-terrorism*, 2007.
- BROWN, Ian. « UK government surveillance powers », 2006, <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1026974>.
- CANADA. SOLLICITEUR GÉNÉRAL. *Annual Report on the Use of Electronic Surveillance*, 1996-2006.
- CANADA. BUREAU DU COMMISSAIRE DU CENTRE DE LA SÉCURITÉ DES TÉLÉCOMMUNICATIONS. *Rapports annuels 1997-2008*.
- CANADA. SÉNAT. « Comité spécial sénatorial sur la teneur du projet de loi C-36 », 29 octobre 2001.
- CENTRE FOR TECHNOLOGY AND DEMOCRACY. « PATRIOT Act Overview », mis à jour en avril 2008, <http://www.cdt.org/security/usala Patriot Act/overview2005.php>.
- CHALK, Peter. *Confronting "the enemy within": security intelligence, the police, and counterterrorism in four democracies*, 2004.
- COHEN, Stanley. *Privacy, Crime and Terror: Legal Rights and Security in a Time of Peril*, 2005.

- COMMISSAIRE À L'INFORMATION ET À LA PROTECTION DE LA VIE PRIVÉE DE LA COLOMBIE-BRITANNIQUE. *Privacy and the USA Patriot Act: Implications for British Columbia Public Sector Outsourcing*, 2004.
- COMMISSAIRE À L'INFORMATION ET À LA PROTECTION DE LA VIE PRIVÉE/ONATRIO. *National Security in a Post-9/11 World: The Rise of Surveillance… the Demise of Privacy?*, 2003.
- COUSENS, Michael. *Surveillance law*, 2004.
- ELECTRONIC FRONTIER FOUNDATION. « Analysis Of The Provisions Of The USA PATRIOT Act », mis à jour en octobre 2003, <http://w2.eff.org/Privacy/Surveillance/Terrorism/20011031_eff_usa_la Patriot Act_analysis.php>.
- ELECTRONIC PRIVACY INFORMATION CENTRE. « The USA PATRIOT Act », mis à jour en novembre 2005, <http://epic.org/privacy/terrorism/usala Patriot Act/default.html>.
- ELECTRONIC PRIVACY INFORMATION CENTRE et PRIVACY INTERNATIONAL. *Privacy and Human Rights*, 2006, <http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-559458>.
- ÉTATS-UNIS. DÉPARTEMENT DE LA JUSTICE. *FISA Annual Reports to Congress 1979-2007*.
- FORCESE, Craig. *National security law: Canadian practice in international perspective*, 2008.
- FRANCE. COMMISSION NATIONALE DE CONTRÔLE DES INTERCEPTIONS DE SÉCURITÉ. *Rapports annuels 2000-2008.*
- FRIEDLAND, Martin L. « Police powers in Bill C-36 », *The Freedom of Security: Essays on Canada's Anti-Terrorism Bill*, 2001.
- *Guide to Homeland Security: 2005 edition*, 2005.
- HUBBARD, Robert W., Peter M. BRAUTI et Scott K. FENTON. *Wiretapping and Other Electronic Surveillance: Law and Procedure*, 2008.
- JACOBSON, Michael. *The West at war: U.S. and European counterterrorism efforts, post-September 11*, 2006.
- LYON, David. *Surveillance after September 11*, 2003.
- MARZOUKI, Meryem. « Cybercrime and Data Retention: French Situation and Articulation with the International Context », 2002, <http://www-polytic.lip6.fr/article.php3?id_article=77>.
- MOORE, John Norton et Robert F. TURNER. *National Security Law*, 2005.
- PERELMAN, Marc. « How the French Fight Terror », *Foreign Affairs*, janvier 2006, <http://www.foreignpolicy.com/story/cms.php?story_id=3353>.
- ROACH, Kent. *September 11: Consequences for Canada*, 2003.
- ROACH, Kent. « Must We Trade Rights For Security? The Choice Between Smart, Harsh or Proportionate Security Strategies in Canada and Britain », 2006, <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=899280>.
- ROYAUME-UNI. OFFICE OF THE INTERCEPTION OF COMMUNICATIONS COMMISSIONER. *Report of the Interception of Communications Commissioner 2001-2007.*
- SOLOVE, Daniel J., Marc ROTENBERG et Paul M. SCHWARTZ. *Information privacy law*, 2006.
- *Terrorisme, droit et démocratie : comment le Canada a-t-il changé depuis le 11 septembre?*, 2002.
- WARK, Wesley. « Intelligence requirements and Anti-Terrorism Legislation », *The Freedom of Security: Essays on Canada's Anti-Terrorism Bill*, 2001.

- WEINER, Eric. « Wire-tapping, European style », *Slate*, février 2006, <http://www.slate.com/id/2136147/>.
- WESTBY, Jody R. *International Guide to Privacy*, 2004.
- WILLIAMS, Victoria. *Surveillance and intelligence law handbook*, 2006.
- WISPINSKI, Jennifer. « Droit à l'information et à la protection de la vie privée : les changements apportés par la *Loi antiterroriste* et la *Loi de 2002 sur la sécurité publique* », 2006, <http://www.parl.gc.ca/information/library/PRBpubs/prb0535-e.html>.
- WISPINSKI, Jennifer. « La Patriot Act » des États-Unis et la *Loi antiterroriste* du Canada : Principales différences entre les deux approches législatives », 2006, <http://dsp-psd.pwgsc.gc.ca/Collection-R/LoPBdP/PRB-f/PRB0583-f.pdf>.
- WOLFSON, S.M. « The NSA, AT&T, and the Secrets of Room 641A », *I/S: A Journal of Laws and Policy for the Information Society*, hiver 2007-2008, p. 411-441.
- WONG, Thomas. « Regulation of Interception of Communications in Selected Jurisdictions », février 2005, <http://www.legco.gov.hk/yr04-05/english/sec/library/0405rp02e.pdf>.

Notes

[1] Voir la *USA PATRIOT Act (U.S. H.R. 3162, Public Law 107-56), titre II, article 218.*

[2] En vertu de l'alinéa 702*a*), le secrétaire à la Justice et le directeur du renseignement national « peuvent, en collaboration, autoriser pour une période pouvant aller jusqu'à un an, le ciblage de personnes que l'on croit raisonnablement être à l'extérieur des États-Unis, afin de recueillir des renseignements étrangers » [traduction], même si le point d'origine ou d'arrivée de toutes les communications à recueillir se trouve aux États-Unis.

[3] L'article 102 de la *Loi antiterroriste* a modifié la *Loi sur la défense nationale* (article 273.65, 1 à 4), et permet au ministre, dans le seul but d'obtenir des renseignements étrangers, d'autoriser par écrit le Centre de la sécurité des télécommunications à intercepter des communications privées, s'il est convaincu que les conditions suivantes sont réunies : l'interception vise des entités étrangères situées à l'extérieur du Canada; les renseignements à obtenir ne peuvent raisonnablement être obtenus d'une autre manière; la valeur des renseignements étrangers que l'on espère obtenir grâce à l'interception justifie l'interception envisagée; il existe des mesures satisfaisantes pour protéger la vie privée des Canadiens et pour faire en sorte que les communications privées ne seront utilisées ou conservées que si elles sont essentielles aux affaires internationales, à la défense ou à la sécurité.

[4] La partie 1, article 5, de la *Loi* exige des fournisseurs de services de communications qu'ils offrent une « capacité d'interception raisonnable » [traduction] dans leurs réseaux, à des fins de surveillance dans les enquêtes en matière de sécurité nationale. La partie III exige la production de texte en clair de matériel chiffré, ou dans certains cas l'offre des clés de chiffrement elles-mêmes.

[5] Les dispositions de la LSQ portent sur l'utilisation de la cryptographie et établissent des conditions de déchiffrement de données chiffrées : un accusateur public ou un juge peut demander à un expert de déchiffrer des données. S'ils soupçonnent un crime ou une infraction qui mérite plus de deux ans de prison, ils peuvent exiger des fournisseurs d'outils de déchiffrement qu'ils fournissent les clés de déchiffrement aux responsables autorisés (par le premier ministre), sur demande. S'ils refusent, les fournisseurs peuvent écoper de deux ans de prison et d'une amende de 30 000 euros. Les clés de chiffrement doivent être fournies à la suite d'une requête juridique, dans les cas où la cryptographie a été utilisée à des fins de commande, de préparation ou de facilitation d'un crime ou d'une infraction.

[6] Selon les rapports des médias, les services de sécurité peuvent déterminer précisément qui a communiqué avec qui, et quand et où c'est arrivé; ils peuvent également obtenir, auprès des compagnies de téléphone, les listes de tous les appels qu'un abonné a effectués ou reçus, des documents d'abonnement, des adresses et des renseignements bancaires, et les adresses de sites Internet ou de forums qu'une personne a visités.

[7] Avec une mise en garde concernant le fait que ces enquêtes ne sont pas effectuées seulement en fonction des activités liées au premier amendement : culte religieux, liberté d'expression, liberté de regroupement et protestation. Voir la *USA PATRIOT Act (U.S. H.R. 3162, Public Law 107-56), titre II, article 214.*

[8] En fait, il ne doit pas déterminer de cible précise du tout. La loi stipule expressément que les requêtes du gouvernement doivent seulement déterminer les installations, les lignes téléphoniques, les adresses de courriel, les lieux, les locaux ou les propriétés qui feront l'objet d'une surveillance.

[9] La démarche législative canadienne de surveillance n'a pas été grandement modifiée par la loi; comme dans la plupart des cas, une autorisation juridique est toujours requise. Cependant, de nouveaux pouvoirs introduits par la loi éliminent le besoin de démontrer que la surveillance représente le dernier recours des enquêtes antiterroristes. Comme le souligne Kent Roach dans son étude de la *Loi antiterroriste*, l'État peut empiéter sur la vie privée s'il démontre qu'il a des motifs raisonnables de croire qu'une infraction grave a été commise et qu'une surveillance révèlerait des preuves de cette infraction. Notamment, l'article 6 et le paragraphe 133(8) de la loi ont fourni aux organismes d'application de la loi et de sécurité nationale des nouveaux outils d'enquête en modifiant le *Code criminel*, pour éliminer le besoin de démontrer que la surveillance électronique représente le dernier recours dans une enquête liée au terrorisme (cette exigence a également été mise de côté pour les enquêtes liées au crime organisé). La loi a modifié le paragraphe 186(1.1) du *Code criminel* pour permettre des enquêtes par écoute téléphonique liées aux infractions de terrorisme, sans devoir se conformer aux seuils d'enquête habituels. Un juge d'une cour supérieure doit toujours approuver la surveillance.

[10] L'interception du contenu (d'une lettre, d'un appel téléphonique ou d'un courriel) est autorisée pour une période allant de trois à six mois par le ministre de l'Intérieur en vertu de la partie 1, chapitre 1, de la *Loi*.
[11] Un mandat ne doit pas nécessairement identifier une personne ou un lieu s'il est lié à l'interception de communications à l'extérieur du Royaume-Uni.
[12] En France, la question des bases de données nationales demeure controversée. Ce pays a exploré l'idée de créer une base de données nationale sur la santé, et plus récemment, a présenté EDVIGE, une nouvelle base de données à être utilisée par les services de renseignements français et par la police administrative, et qui classera les personnes, les groupes, les organisations et les personnes morales qui, en raison de leurs activités individuelles ou collectives, sont plus propices à déranger l'ordre public, peu importe s'ils ont déjà commis une infraction ou non. EDVIGE renfermera des données sur l'état civil et la profession; des adresses physiques, des numéros de téléphone, des adresses de courriel; des caractéristiques physiques, des photos et des traits de comportement; des pièces d'identité; des numéros de plaque d'immatriculation; des données fiscales et patrimoniales; des données sur les déménagements et les antécédents judiciaires, ainsi que des données sur l'orientation sexuelle et la santé. EDVIGE contient seulement les données de personnes âgées de 13 ans et plus.
[13] Voir la *USA PATRIOT Act (U.S. H.R. 3162, Public Law 107-56), titre II, article 213.*
[14] Elle permet également aux pouvoirs de la police d'effectuer des arrestations préventives et de faire comparaître les personnes concernées devant une audience, au cours de laquelle le droit de garder le silence est perdu. La loi permet également au gouvernement de soumettre des renseignements obtenus d'un gouvernement étranger ou d'une organisation internationale, qu'un juge peut prendre en compte pour déterminer si on doit identifier tel groupe comme une organisation terroriste. Les personnes concernées peuvent recevoir un sommaire de la preuve, seulement si les renseignements divulgués ne peuvent nuire à la sécurité nationale.
[15] La loi ajoute un nouvel article (4.81) à la *Loi sur l'aéronautique*, qui exige des compagnies aériennes qu'elles divulguent les renseignements personnels de tous leurs passagers en provenance ou à destination du Canada.
[16] L'article 42 permet aux responsables de perquisitionner des maisons s'ils ont des doutes raisonnables. L'article 44 de la loi donne à n'importe quel agent de police le droit d'arrêter et de perquisitionner un véhicule ou des personnes, à sa simple discrétion. L'article 44 (paragraphe 3) octroie des pouvoirs de recherche détaillée.
[17] Les articles 33 à 36 donnent à la police le pouvoir de délimiter une certaine zone, à des fins d'enquêtes terroristes, dans laquelle elle a de grands pouvoirs de perquisition et de saisie discrétionnaires.
[18] La partie X, articles 98 à 101, de la *Loi* permet à la police britannique des transports du ministère de la Défense d'autoriser des recherches détaillées de certaines zones pour une période pouvant aller jusqu'à 28 jours. Elle remet également en vigueur le « règlement de coopération des témoins » [traduction], qui les oblige à aider la police dans leurs enquêtes, même au détriment de leurs pairs ou des membres de leur famille, sans quoi ils feront face à des poursuites. Cela élimine de façon efficace le droit de garder le silence. La partie X, articles 90 et 96, de la *Loi* permet la documentation des suspects pendant leur détention, de l'échantillonnage de leur ADN aux photographies détaillées de leurs caractéristiques physiques.
[19] Voir la *USA PATRIOT Act (U.S. H.R. 3162, Public Law 107-56), titre II, article 207.*
[20] Prorogation des ordonnances de surveillance et de fouilles manuelles; surveillance des terroristes « loups solitaires » [traduction] en vertu de l'article 207 de la *PATRIOT Act* prorogée à 120 jours pour une ordonnance initiale. Prorogation des enregistreurs graphiques et des dispositifs de piégeage et de suivi de 90 jours à un an, avec une date butoir établie au 31 décembre 2009. Voir la *USA PATRIOT and Terrorism Prevention Reauthorization Act de 2005 (U.S. H.R. 3199, Public Law 109-177), titre I, article 107.*
[21] La *USA PATRIOT Act* autorise tout organisme fédéral à échanger des renseignements avec des organismes d'application de la loi; tout fonctionnaire qui obtient des renseignements au moyen de surveillance électronique ou de fouilles manuelles peut consulter des organismes d'application des lois fédérales à des fins de coordination des enquêtes ou de protection contre les attaques, le sabotage, le terrorisme ou les activités relatives au renseignement potentiels par un service de renseignement extérieur. Voir la *USA PATRIOT Act (U.S. H.R. 3162, Public Law 107-56), titre II, article 203* et la *USA PATRIOT Act (U.S. H.R. 3162, Public Law 107-56), titre V, article 503. Amended 50 U.S.C. § 1825*. Pour la collecte et la mise en commun de renseignements par des organismes d'application de la loi n'ayant pas trait à des activités criminelles, voir la *USA PATRIOT Act (U.S. H.R. 3162, Public Law 107-56), titre II, article 218.*
[22] L'article 1016 autorise la création d'un « environnement de mise en commun des renseignements » afin d'« établir un lien entre toutes les entités fédérales, locales et tribales appropriées et le secteur privé » [traduction].
[23] Kent Roach, « Must We Trade Rights for Security? The Choice between Smart, Harsh or Proportionate Security Strategies in Canada and Britain », *Cardozo Law Review*, vol. 27, p. 2157-2221 (2006), 2161.
[24] Voir la *USA PATRIOT Act (U.S. H.R. 3162, Public Law 107-56), titre II, article 203.*
[25] L'article 6501 incorpore des révisions pour l'échange d'information obtenue durant une audience devant un grand jury ayant trait au renseignement étranger ou à la contre-ingérence avec tout représentant fédéral (article 203 de la *USA PATRIOT Act*) et les dispositions de l'article 895 de la *Homeland Security Act* autorisent la divulgation de cette information à des représentants de gouvernements étrangers, le cas échéant.
[26] Permet au F.B.I. de délivrer une ordonnance « exigeant l'accès à des "objets tangibles" (y compris des livres, des dossiers, des papiers, des documents et d'autres objets) à des fins d'enquête de protection contre le terrorisme international ou les activités clandestines de renseignement » [traduction] en vertu de la *USA PATRIOT Act (U.S. H.R. 3162, Public Law 107-56), titre II, article 215*. L'un des pouvoirs les plus controversés afférent aux pouvoirs en question aux termes de la *PATRIOT Act* a trait aux lettres de sécurité nationale (NSL), une forme d'ordonnance administrative utilisée par le F.B.I. et, selon les informations obtenues, par d'autres organismes gouvernementaux américains, dont l'Agence centrale de renseignement (CIA) et le département de la Défense. La disposition a été autorisée à nouveau en 2005, mais des modifications ont été apportées afin de prescrire un processus de révision judiciaire des NSL et de permettre au destinataire d'une NSL de révéler la réception de la lettre à un avocat dans le but de se conformer à l'ordonnance ou de la contester. Cela dit, en 2007, la Cour de district américaine a déclaré la disposition comme étant inconstitutionnelle. Voir la *USA PATRIOT Act (U.S. H.R. 3162, Public Law 107-56), titre V, article 505. Amended 18 U.S.C. § 2709(b*).
[27] Voir la *USA PATRIOT Act (U.S. H.R. 3162, Public Law 107-56), titre II, articles 204 et 209.*

[28] Permet aux organismes d'application de la loi d'installer des dispositifs pouvant intercepter le courrier électronique et les activités sur Internet (avec une ordonnance en vertu de la FISA) et élargit la portée de la surveillance au paquet de données et aux données des destinataires; consulter la *USA PATRIOT Act (U.S. H.R. 3162, Public Law 107-56), titre II, article 216.* Comme le concluait la commissaire à l'information et à la protection de la vie privée/Ontario dans son rapport de 2003 sur la *USA PATRIOT Act*, la loi « accroît considérablement le type et la quantité d'information que les autorités peuvent obtenir sur les utilisateurs de leurs FSI. Elle autorise les FSI à fournir volontairement aux organismes d'application de la loi tous les renseignements n'étant pas du contenu, sans ordonnance d'un tribunal ou assignation. La loi élargit également l'éventail des dossiers pouvant être demandés par les autorités sur présentation d'une simple assignation (aucune ordonnance d'un tribunal nécessaire) afin qu'ils puissent comprendre les heures et durées des sessions, les adresses IP temporaires, les modes et sources de paiement, y compris les numéros de comptes bancaires et de cartes de crédit. » [traduction].

[29] Voir la partie XI, articles 102 à 107.

[30] Le chapitre XI donne le pouvoir au ministre de l'Intérieur d'ordonner aux compagnies de téléphone et de services Internet de conserver les données sur les communications (mais pas le contenu des communications) pour des périodes données. Subséquemment, le *Code of Practice on Data Retention* approuvé par le Parlement en décembre 2003 établit la période à 12 mois et englobe les éléments suivants : données sur l'abonné (par exemple nom, date de naissance, adresse postale et de facturation, modes de paiement, données de compte bancaire et de carte de crédit); coordonnées (renseignements sur l'abonné non vérifiés par le CSP), par exemple numéro de téléphone, adresse électronique; services de l'abonné (renseignements déterminés par le fournisseur de services de communications), par exemple fiche du client, numéro de compte, liste des services; numéro(s) de téléphone, identité internationale d'équipement mobile; adresse électronique, IP à l'enregistrement; gestionnaire de messages Internet, IP à l'enregistrement; fournisseur de services Internet-disque mobile : ouverture de session, identification de l'appelant à l'enregistrement (si conservée); fournisseur de services Internet-bande permanente : identificateurs uniques, adresse MAC (si conservée), extrémités de ligne d'abonné numérique asymétrique, adresse de tunnel IP; date et heure des débuts d'appels, durée des appels/date et heure des fins d'appels, type d'appels (si disponible), données d'emplacement en début et/ou en fin d'appel, référence longue; données de site cellulaire au moment où le cellulaire cesse d'être utilisé, etc. Le contenu du courrier électronique doit être conservé six mois, le courrier envoyé (nom d'authentification de l'utilisateur, adresses électroniques expéditeur, destinataire et copie conforme, date et heure d'envoi) comme le courrier reçu (nom d'authentification de l'utilisateur, adresses électroniques expéditeur et destinataire, date et heure de réception). Les données des FSI doivent être conservées six mois, par exemple ouverture de session (nom d'authentification de l'utilisateur, date et heure de l'ouverture et de la fermeture de session, adresse IP attribuée). Enfin, le registre des activités Internet doit être conservé quatre jours, y compris, par exemple, les données de serveur mandataire (date et heure, adresse IP utilisée, adresses URL visitées et services).

[31] Voir la *USA PATRIOT Act (U.S. H.R. 3162, Public Law 107-56), titre II, article 212*. La *Loi* permet en outre la divulgation des communications électroniques aux organismes d'application de la loi. Les entreprises exploitant un « ordinateur protégé » peuvent aussi permettre aux autorités d'intercepter les communications acheminées par la machine, contournant les exigences d'ordonnance, en vertu de la *USA PATRIOT Act (U.S. H.R. 3162, Public Law 107-56), titre II, article 217*. Pour les assignations étendues délivrées aux fournisseurs de services Internet, voir la *USA PATRIOT Act (U.S. H.R. 3162, Public Law 107-56), titre II, article 210*.

[32] Une fois autorisé aux termes de la *Loi*, le secrétaire à la Justice et le directeur du renseignement national peuvent ordonner à tout fournisseur de services de communication électronique à immédiatement « fournir aux autorités tous les renseignements, les ressources et l'aide nécessaires pour accomplir l'acquisition »; voir *H.R. 3773: FISA Amendments Act of 2008,* division 702*h)*(1)(A).

[33] Les activités ne peuvent viser des Canadiennes et Canadiens ou toute personne au Canada et doivent être soumises à des mesures de protection de la vie privée lors de l'utilisation et de la conservation des renseignements interceptés. Voir l'article 273.64 de la *Loi sur la défense nationale*.

[34] L'accès aux données se rapportant à l'utilisation de services de communications peut être auto-autorisé par un grand nombre d'organismes gouvernementaux en vertu de la partie I, chapitre 2. En juin 2002, le ministère de l'Intérieur a annoncé que la liste des organismes gouvernementaux autorisés en vertu de la RIPA à accéder aux données sur les communications était élargie à plus de 1 000 ministères différents, y compris les autorités locales, les ministères de la Santé, de l'Environnement et du Commerce et de nombreuses autres autorités publiques.

[35] L'article 215 accorde un vaste pouvoir pour l'exigence de livres comptables. Auparavant, seuls les dossiers des transporteurs publics et des installations d'accueil au public, d'entreposage et de location de véhicule pouvaient être obtenus avec l'ordonnance d'un tribunal. La *Loi* autorise maintenant de demander au tribunal de la FISA d'ordonner la production de tout livre comptable ou objet tangible en vue d'une enquête destinée à assurer une protection contre le terrorisme international ou les activités clandestines de renseignement. Les dossiers de bibliothèque, les achats en librairie et autres données sur les transactions peuvent tous être obtenus sans approbation judiciaire ou surveillance. L'article 505 autorise le F.B.I. à exiger des dossiers de téléphone et de transactions, des dossiers financiers et des renseignements sur les consommateurs en vue d'une enquête destinée à assurer une protection contre le terrorisme international ou les activités clandestines de renseignement, si l'enquête n'est pas uniquement fondée sur des activités protégées par le premier amendement. Le pouvoir en question fera l'objet d'un examen du Congrès en 2010.

[36] L'article 72 de la *Loi* modifie la *Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes* afin de permettre au directeur du SCRS ou à tout membre de l'organisme de présenter à un juge une demande d'ordonnance de divulgation de toute information lorsqu'il y a des « motifs raisonnables » de croire que la sécurité du Canada est menacée. L'ordonnance autorise tous les employés du SCRS nommés dans l'ordonnance à accéder à tous les renseignements ou documents ayant trait à l'ordonnance et à les examiner.

[37] La partie IV, articles 47 à 75, de la loi modifie la *Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes* afin d'autoriser le Centre d'analyse des opérations et déclarations financières du Canada à recueillir et divulguer des renseignements sur les opérations financières qui pourraient constituer des menaces pour la sécurité du Canada au SCRS et autres organismes d'application de la loi.

[38] Annexe 6 (par. 7); également les pouvoirs de surveiller les mouvements sur un compte grâce à l'obtention d'un mandat judiciaire (alinéa 38*a*).