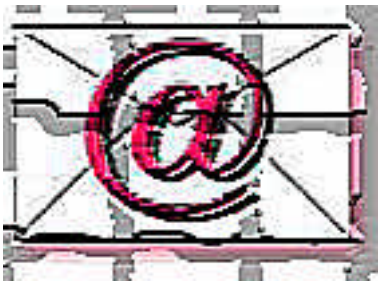
11 septembre 2001 – 11 septembre 2002

Internet en liberté surveillée



Reporters sans frontières
5, rue Geoffroy-Marie – 75009 Paris
Contact : Loïck Coriou
Tel : 33 1 44 83 84 61 – Mail : loick.coriou@libertes-immuables.net
www.rsf.org / www.libertes-immuables.net

Reporters sans frontières défend la liberté d'expression. Celle-ci est indissociable de la liberté de la presse mais aussi de la libre circulation de l'information sur Internet et de la préservation de la confidentialité des échanges sur la Toile. C'est pourquoi, au travers de ce rapport, l'organisation dénonce les graves coups portés à Internet depuis le 11 septembre 2001. Un état des lieux accablant.

Depuis le milieu des années 90, un certain nombre d'Etats et d'institutions internationales ont cherché à contrôler Internet au travers de lois ou de textes de régulation. Avec plus ou moins de succès. La croisade antiterroriste et les dérapages sécuritaires qu'elle engendre ont précipité cette tendance.

Un an après les tragiques événements de New York et de Washington, le Réseau peut être couché sur la liste des « dommages collatéraux » de la dérive sécuritaire généralisée. Et du coup, les libertés numériques fondamentales ont été amputées.

Les pays traditionnellement épinglés pour leur non-respect des droits de l'homme et de la liberté d'expression (Chine, Viêt-nam, Arabie Saoudite, Tunisie, etc.) ont adopté une attitude schizophrénique à l'égard du Réseau. Côté pile, ils ont encouragé son développement pour servir la propagande étatique ou les intérêts économiques. Côté face, ils se sont organisés pour le contrôler et étouffer dans l'œuf les critiques, la contestation et les aspirations démocratiques exprimées en ligne.

Depuis les attentats du 11 septembre 2001, ces "ennemis d'Internet" ont saisi avec opportunisme le contexte de la campagne antiterroriste internationale pour renforcer leurs dispositifs policiers et législatifs d'encadrement de la Toile. Et pour accentuer leurs pressions sur les cyberdissidents.

C'est le cas de la Chine. Le gouvernement de Pékin, qui détenait, le 30 août 2002, trente internautes derrière les barreaux, tente de contrôler le développement des cybercafés. Quatorze mille cafés Internet ont été fermés en l'espace de quelques semaines, depuis la fin du printemps 2002. Par ailleurs, un cyberdissident a été condamné en août 2002 à la plus lourde peine jamais infligée en la matière : onze ans de prison. Enfin, les autorités font signer aux fournisseurs d'accès et aux portails un pacte d'autocensure. Fait grave : le géant américain Yahoo ! l'a ratifié.

En Tunisie, le régime du présiden Ben Ali surfe également habilement sur la vague antiterroriste pour resserrer l'étau autour des cyberdissidents. Il a mis derrière les barreaux et fait condamner à deux ans et quatre mois de prison, le 20 juin 2002, le fondateur d'un site Internet trop critique : Zouhair Yahyaoui, créateur de *Tunezine.com.*

Mais outre les pays ennemis de la liberté d'expression, Internet doit désormais faire face à une nouvelle menace en provenance des démocraties occidentales. Ainsi, de nombreux pays ont adopté des lois, des mesures et des pratiques, qui sont en passe de mettre Internet sous la tutelle des services de sécurité. Ces Etats organisent la conservation généralisée des informations relatives aux e-mails reçus ou envoyés et aux sites consultés sur la Toile. Ce qui métamorphose les fournisseurs d'accès à Internet et les opérateurs de téléphonie en auxiliaires de police potentiels. Enfin, l'accès à cette masse d'informations est désormais accordé avec une déconcertante aisance aux services de police et de renseignements. Cette dérive sans précédent revient à suspecter a priori tous les citoyens.

On peut citer pour exemple la Résolution 1373 relative au combat contre le terrorisme votée par le Conseil de sécurité de l'ONU le 28 septembre 2001 ; l'USA Patriot Act adopté aux Etats-Unis le 24 octobre 2001 et les décrets présidentiels de George W. Bush qui ont précédé ou suivi ce texte ; la révision de la Directive européenne sur la protection des données de télécommunications votée le 30 mai 2002 ; le vote de lois par les Parlements nationaux un peu partout dans le monde ; les recommandations du G8 ou d'Europol (police européenne), etc.

Les Etats-Unis, la Grande-Bretagne, la France, l'Allemagne, l'Espagne, l'Italie, le Danemark, le Parlement européen, le Conseil de l'Europe ou le G8 s'en sont pris, au fil des mois, aux libertés numériques. Ces pays et institutions ont pourtant une culture démocratique séculaire. Et leurs citoyens ont gagné de haute lutte le droit à la liberté d'expression ; le droit à la protection de la confidentialité de leurs courriers ; le droit au secret des sources des journalistes.

Que feraient les citoyens, d'Europe ou d'ailleurs, si on leur annonçait qu'une loi permettant de contrôler en toute impunité le courrier qu'ils confient aux services postaux a été votée et qu'en vertu de ce texte, les services de police peuvent à tout moment suivre leurs échanges épistolaires ? Ils s'insurgeraient contre ces actes liberticides. C'est pourtant bien ce type de mesures qui ont été adoptées ou sont en passe de l'être pour Internet. Elles appellent donc une vigilance accrue de notre part.

Allemagne

L' « Otto-Katalog » (en référence à un catalogue fourre-tout de vente par correspondance) : voilà comment la presse et les organisations non gouvernementales ont ironiquement surnommé le train de mesures antiterroristes élaboré par le ministre de l'Intérieur, Otto Schily. Il a été adopté par les parlementaires fin 2001. Le contenu de la loi a été sévèrement critiqué par les organisations de défense des droits civiques, de la liberté d'expression et de protection des données personnelles. Les mesures les plus controversées concernent l'abolition de la séparation entre les services de police et de renseignements. Dans le cadre du nouveau texte, ces derniers ont un accès illimité à la base de données de la police, INPOL.
Ces mêmes services ont également accès aux données de télécommunications stockées sur support numérique : archivage des contenus des communications ; accès aux renseignements relatifs aux échanges de e-mails ; accès à toutes les données permettant de localiser les personnes à l'origine des communications, des courriers électroniques ; accès aux données des entreprises de télécommunications.
Une vingtaine d'organisations se sont regroupées au sein d'un collectif pour dénoncer les efforts d'Otto Schily pour contrôler les communications. Elles ont dénoncé « cette loi dont les concepts juridiques sont discutables, imprécis et difficiles à apprécier. Un texte, de surcroît, inapte à endiguer l'activité terroriste ».
Cette nouvelle législation a valu au ministre de l'Intérieur de recevoir, en Allemagne, le Big Brother Award de l'année "pour sa politique d'espionnage et de restriction des libertés collectives et individuelles". Selon Privacy International, qui a décerné ce "prix", "Otto Schily a contribué, sous couvert de lutte contre le terrorisme, à la restriction des droits des citoyens en Allemagne et principalement la protection de leurs données personnelles".

Canada

La surveillance rapprochée d'Internet et du courrier électronique est l'une des clés de voûte de la loi antiterroriste canadienne baptisée C-36, votée mi-décembre 2001. Ce texte facilite l'obtention par les services de police de mandats permettant d'effectuer des écoutes, téléphoniques et électroniques. Le Centre de la sécurité des télécommunications, un service spécialisé du ministère de la Défense, peut, quant à lui, et pour la première fois de son histoire, procéder à des écoutes électroniques de ressortissants canadiens ainsi que d'étrangers. La confidentialité des échanges de courriers électroniques est clairement battue en brèche.
John Reid, le Commissaire à l'information (autorité indépendante chargée de veiller au respect des libertés civiles au Canada) s'en est ému dans un courrier adressé à la présidente du comité sénatorial de la Justice, Joyce Fairbairn. « Cette loi porte un coup fatal à mon indépendance ; comment pourrais-je protéger le droit à la confidentialité des citoyens face à cette loi ? », a-t-il écrit

Danemark

Le gouvernement danois a présenté au mois d'octobre 2001 un important projet de révision des principales lois nationales pour combattre plus durement le terrorisme. Sous l'intitulé générique de « batterie de mesures antiterroristes », il s'est traduit par l'amendement des lois sur la justice, les affaires intérieures, l'économie et la fiscalité.
Internet et les nouvelles technologies ont particulièrement pâti de ces révisions. Le gouvernement a demandé au ministère de la Justice de prendre de nouvelles dispositions pour légaliser la rétention des données relatives aux télécommunications et aux connexions au Réseau, aux e-mails et permettre à la police d'accéder plus rapidement et plus facilement à ces données personnelles. Le 31 mai 2002, le Danemark a porté à un an la rétention des données. La loi antiterroriste va plus loin : elle permet aux services secrets, PET, et à la police de consulter librement toutes ces informations, sans avoir besoin de saisir la justice. La police peut même brancher sur les terminaux des opérateurs des systèmes d'interception des courriers électroniques du même type que le logiciel américain Carnivore.

Espagne

Le 27 juin 2002, le Congrès des députés espagnols a adopté la LSSICE ou "Loi de l'Internet". Un texte destiné à combattre la cybercriminalité et le terrorisme sur la Toile ibérique. Cette loi, concoctée par le ministère des Sciences et Technologies, comporte des articles liberticides aux yeux des supporters d'un Réseau soumis à un minimum de surveillance. Elle oblige en effet les fournisseurs d'accès à Internet à conserver les données de connexions et de trafic de leurs clients pendant au moins un an. Mais, grâce à l'introduction d'un amendement par l'opposition, ces dernières ne seront utilisées par les services de police ou de renseignements qu'avec l'aval d'un magistrat.
Les détracteurs du projet sont d'autant plus déçus qu'ils espéraient que son impact serait édulcoré après l'examen des parlementaires. Le résultat final s'est révélé pire que le texte initial. C'est principalement le cas pour le stockage des données de connexions par les fournisseurs d'accès. Ainsi les modalités pratiques de cette rétention généralisée n'ont pas été précisées, ce qui laisse craindre des dérives. Reste par ailleurs à savoir quelle autorité administrative aura la possibilité de fermer des sites qui « attentent à une série de valeurs ». Et ce, sans porter atteinte à la liberté d'expression. Une liberté reconnue et défendue par la Constitution, dont l'article 20 protège particulièrement le droit "à communiquer ou recevoir librement une information véridique par tout moyen de communication".

Etats-Unis

Les attentats du 11 septembre 2001 et l'utilisation présumée d'Internet par les membres du commando terroriste pour communiquer et préparer leur action ont fait triompher les chantres d'une politique ultrasécuritaire et d'un Réseau encadré par des textes de régulation stricts.
La campagne de reprise en main d'Internet a débuté quelques heures seulement après les attentats, lorsque des agents de la police fédérale (FBI) ont investi les sièges des principaux fournisseurs d'accès à Internet du pays (Hotmail, AOL, Earthlink, etc.) pour y intercepter des informations sur d'éventuels échanges par e-mail entre les terroristes. Le journal en ligne *Wired* a affirmé dans une enquête que les agents du FBI avaient également tenté d'installer le système de surveillance électronique « Carnivore » (rebaptisé depuis DCS 1000) sur les principaux serveurs informatiques des fournisseurs d'accès basés aux Etats-Unis. « Ces agents du FBI se sont présentés dans les locaux de ces sociétés afin d'installer leurs machines. Ils ont assuré que la prise en charge des frais d'installation et d'exploitation de leurs systèmes était assurée. Le FBI aurait encore exigé et obtenu de responsables de ces compagnies des informations provenant de comptes dont l'adresse Internet comportait le mot « Allah ». Tous les grands fournisseurs d'accès semblent avoir suivi l'exemple de Hotmail et pleinement collaboré avec les services de sécurité américains. »

Carnivore : un logiciel qui « ratisse » large

Carnivore est le premier grand logiciel « d'écoute électronique » utilisé par la police d'un Etat. Créé par les services du FBI, il permet, après avoir été installé chez un fournisseur d'accès, d'enregistrer et de stocker toutes les données échangées par ses utilisateurs. Combattu par les défenseurs des libertés civiles aux Etats-Unis, ce système n'était utilisé jusqu'alors qu'avec l'accord préalable d'un juge. Un texte intitulé « Combating Terrorism Act », voté en toute urgence par le Sénat le 13 septembre, a exempté les services de sécurité américains de l'aval de la justice pour l'utilisation de Carnivore.
Dans la foulée, de nombreux responsables américains ont attaqué la cryptographie. Ce procédé permet aux internautes de protéger la confidentialité des informations échangées sur le Net en les chiffrant à l'aide de logiciels. Le 13 septembre toujours, le sénateur républicain Judd Gregg a proposé, dans un discours prononcé devant le Congrès, l'interdiction des logiciels de cryptographie dont les diffuseurs n'auraient pas fourni à l'autorité publique la clé permettant de déchiffrer les messages. Il a justifié cette requête par le fait que le FBI avait mis dix mois pour déchiffrer les fichiers cryptés sur l'ordinateur du principal responsable du premier attentat contre le World Trade Center, en 1993.
Le créateur de PGP, le principal logiciel de cryptographie, David Zimmerman, a souligné pour sa part : « La société a plus à gagner qu'à perdre d'une cryptographie forte. Elle sauve des vies dans le monde entier. Le logiciel PGP est utilisé par des organisations de défense des droits de l'homme partout dans le monde, et spécialement dans les pays soumis aux dictatures. »

Assouplissement des procédures d'écoute électronique

La surveillance de l'information sur la Toile a été définitivement légalisée, le 24 octobre 2001, avec l'adoption par la Chambre des représentants américains de l' « USA Patriot Act », rebaptisé plus tard « USA Act ». Cette loi antiterroriste confirme l'autorisation accordée au FBI de brancher le système Carnivore sur le réseau d'un fournisseur d'accès à Internet pour surveiller la circulation des messages électroniques et conserver les traces de la navigation sur le web d'une personne suspectée de contact avec une puissance étrangère. Pour cela, seul l'aval d'une juridiction spéciale est nécessaire.
Les dérapages redoutés par les organisations de défense de la liberté d'expression se sont produits. Au printemps 2002, l'organisation américaine Electronic Privacy Information Center (EPIC), après un bras de fer juridique avec le FBI, a obtenu le droit d'accéder à certains dossiers relatifs à Carnivore. Ses spécialistes ont découvert que, dans le cadre de la « croisade antiterroriste », les courriers électroniques privés de citoyens au-dessus de tout soupçon avaient été interceptés et espionnés « par erreur », selon la police fédérale. De mauvaises manipulations techniques seraient à l'origine de ces bavures…
Quant aux logiciels de cryptographie, ils sont mis à mal par le programme « Lanterne magique » (« Magic Lantern ») du FBI. Envoyé par e-mail, ce virus, du type « espion de clavier », enregistre à leur insu les touches sur lesquelles frappent les internautes. Il permettrait ainsi au FBI d'identifier la clé de chiffrement des utilisateurs de logiciels de cryptographie et de récupérer les messages écrits par le propriétaire de l'ordinateur.
Si les autorités tentent de contrôler la circulation de l'information sur la Toile et de surveiller ce qu'il s'y dit et s'y échange, elles cherchent aussi à tirer profit d'Internet pour assurer la propagande des Etats-Unis dans la lutte antiterroriste. Le 19 février 2002, le *New York Times* révèle que le Bureau de l'influence stratégique (OSI, Office of Strategic Influence), un service du département d'Etat à la Défense, propose de recourir à la diffusion de fausses informations auprès des médias étrangers. Notamment en les diffusant sur des sites Internet créés dans ce but, et administrés en réalité par le service, ou via des e-mails adressés à des journalistes ou des rédactions. Peu après le tollé provoqué par ces révélations, Ari Fleischer, porte-parole de la Maison Blanche, affirme que M. Bush ignorait tout du projet de l'OSI et a ordonné la fermeture de ce bureau.

Gendarme mondial du Net

Le département de la Justice s'est en outre arrogé le droit de poursuivre les « pirates » de l'Internet, qu'ils soient ou non Américains, qu'ils agissent sur le sol des Etats-Unis ou en dehors. Le raisonnement

des autorités est simple : dans la mesure où la majeure partie des communications Internet transite par les Etats-Unis, elles entendent désormais poursuivre quiconque, dans le monde, contreviendrait aux lois des USA dans le domaine du cyberespace, dès lors que l'objet des " délits " électroniques circulerait par les « tuyaux américains ».
Cette mesure, sans précédent dans le monde, confère de facto aux Etats-Unis « le rôle de gendarme mondial du Net », s'alarment les défenseurs des libertés.
D'autant que les termes « hackers » ou « pirates » peuvent englober de multiples activités. « Les auteurs de n'importe quel délit basique sur Internet, du vol de données informatiques, du petit piratage de sites, à l'envoi d'images pornographiques, pourraient ainsi être inquiétés par les autorités américaines », explique Mark Rasch, un expert en sécurité sur Internet.
Par ailleurs, un fait rarissime dans les annales d'Internet illustre la détermination des Etats-Unis : en novembre 2001, la Somalie a été totalement déconnectée de la Toile. L'unique fournisseur d'accès, Somalia Internet Company, ainsi que la principale entreprise de télécommunications al-Barakaat, ont été contraints de cesser leurs activités. Motif : les deux compagnies ont été accusées par les autorités américaines de soutenir financièrement le réseau Al-Qaida d'Oussama ben Laden et placées sur la liste des soutiens au terrorisme. Durant deux mois, les Somaliens ont donc été isolés du reste du monde numérique. Courant janvier 2002, l'arrivée d'un nouvel opérateur sur le marché somalien, NetXchange, a réintroduit le pays dans la cybercommunauté.
Le ministre de la Justice, John Ashcroft, et le directeur du FBI, Robert Mueller, ont présenté un plan de réforme de la police fédérale le 30 mai 2002. Selon ce plan, le FBI recentre ses activités sur la lutte antiterroriste aux dépens de celles sur la lutte contre la criminalité. L'une des principales nouveautés est l'autorisation donnée aux agents fédéraux de placer sur écoutes les communications téléphoniques et électroniques de toute personne qui pourrait posséder des informations liées aux affaires terroristes. Et ce, sans demander de mandat à un juge. Le FBI peut également pénétrer dans les bases de données informatiques qui recèlent des informations d'ordre commercial, économique ou scientifique. Ces enquêtes peuvent être réalisées à titre « préventif », même si aucune preuve n'existe à l'encontre des personnes ou organisations surveillées.

France

La dérive sécuritaire générée par les attentats du 11 septembre a débouché, dans l'Hexagone, sur le vote de deux lois qui restreignent les libertés numériques. Le gouvernement Jospin a présenté en novembre 2001 un ensemble de mesures destinées à lutter contre le terrorisme : la Loi sur la sécurité quotidienne (LSQ). Ce dispositif n'a pas été " taillé sur mesure " pour combattre la menace terroriste. Des dispositions ont été ajoutées à la hâte à une ossature de texte existante : la LSI, Loi sur la société de l'information.
Votée le 15 novembre 2001 en urgence, et quasiment à l'unanimité au terme d'un débat inexistant, la LSQ a porté à un an la durée de conservation des données de connexions à la Toile et les données relatives aux envois et réceptions de e-mails par les fournisseurs d'accès à Internet. Elle autorise les juges à recourir aux « moyens de l'Etat soumis au secret de la Défense nationale » pour décrypter les messages et elle oblige les fournisseurs de moyens de cryptographie à fournir aux autorités leurs protocoles de chiffrement, afin qu'elles puissent décrypter à leur aise les messages. Autant de dispositions qui reviennent à placer Internet sous haute surveillance et à jeter l'anathème sur la cryptographie.
Les organisations de défense de la liberté d'expression sur Internet, *Reporters sans frontières, LSIjolie, IRIS, Bug Brother, etc.*, se sont indignées du vote aussi rapide d'un texte qui n'a fait l'objet d'aucune concertation et remet en cause le principe de la confidentialité des échanges professionnels et privés, notamment du secret des sources des journalistes.

Perquisitions et saisies des données « en ligne »

Le nouveau gouvernement de Jean-Pierre Raffarin a soumis aux parlementaires, dès juillet 2002, sa Loi d'orientation et de programmation sur la sécurité intérieure (LOPSI) qui comporte des dispositions inquiétantes pour la liberté d'expression en ligne et le droit à la confidentialité des citoyens.

Des mesures contenues dans la LOPSI, adoptée le 31 juillet 2002, soulèvent des questions brûlantes. Elles concernent principalement la possibilité pour les officiers de police judiciaire de procéder « à distance, en ligne » aux perquisitions des serveurs informatiques des fournisseurs d'accès, dans lesquels sont stockées les informations relatives aux connexions des citoyens au Réseau mais aussi l'envoi et la réception de e-mails professionnels et privés. « Il sera élaboré un texte permettant aux officiers de police judiciaire, agissant dans le cadre d'une enquête judiciaire, sur autorisation d'un magistrat, d'accéder directement à des fichiers informatiques et de saisir à distance par la voie télématique ou informatique, les renseignements qui paraîtraient nécessaires à la manifestation de la vérité », dit la loi d'orientation.
Questions posées par les détracteurs de la LOPSI, au rang desquels *le Syndicat de la magistrature*, *IRIS* ou la *Fédération Informatique et Libertés* (*FIL*) : ce « texte » à venir, précisant les modalités d'application de la loi, fera-t-il l'objet d'un débat parlementaire de fonds ? Les officiers de police judiciaire abilités à accéder aux fichiers informatiques et à saisir leurs contenus seront-ils spécialement formés et équipés pour réaliser ces opérations ? Seront-ils contraints, à l'instar des procédures de perquisitions classiques, d'informer les suspects de la procédure en cours ? Les magistrats appelés à délivrer ces autorisations seront-ils formés à ces actes et sensibilisés à leur nature intrusive ?
La LOPSI précise par ailleurs : « Les textes nécessaires seront adoptés dans le but d'autoriser sous contrôle judiciaire l'emploi des techniques les plus modernes indispensables à l'interception des messages et à la mise en place de dispositifs de surveillance élaborés rendus nécessaires en raison du recours de plus en plus systématique des délinquants aux possibilités de brouillage de leurs échanges ou au camouflage de leurs rencontres. » Une mesure qui vise directement les internautes qui utilisent des moyens de cryptographie pour préserver leur anonymat sur la Toile.

Grande-Bretagne

Le « Anti-Terrorism, Crime and Security Act », la loi britannique antiterroriste adoptée mi-décembre 2001, a porté la durée de conservation des données de connexions des internautes par les fournisseurs d'accès à un an au moins. Le ministère de l'Intérieur a également annoncé qu'il entendait « avoir un droit de regard sur les transactions financières en ligne, ou contrôler les e-mails privés ». En vertu de la nouvelle loi, la police est dispensée dans de nombreux cas de figure de l'autorisation préalable d'un juge pour agir. Il lui suffit d'obtenir le feu vert du ministre de l'Intérieur ou de l'un de ses hauts fonctionnaires pour le faire. Autant de mesures qui ont provoqué un tollé, outre-Manche. Des fournisseurs d'accès ont même annoncé qu'ils envisageaient la délocalisation de leurs serveurs informatiques hors de Grande-Bretagne.
Les craintes d'une dérive sécuritaire majeure exprimées par les ONG semblent fondées. Mi-juin 2002, David Blunkett, ministre de l'Intérieur, a présenté un projet de révision d'une loi très controversée adoptée en 2000 : the « Regulation of Investigatory Powers Act » (RIPA). Il souhaite permettre aux administrations locales (impôts, Sécurité sociale, services municipaux, etc.) d'accéder aux données relatives aux connexions des citoyens au Réseau et à leurs envois et réceptions de e-mails. D'abord programmée pour courant juin ou début juillet 2002, cette révision a provoqué une telle levée de boucliers, tant dans la presse qu'un niveau des groupes de défense des libertés civiles, que le gouvernement a décidé de reporter cette révision législative à l'automne.

Des lois « anticonstitutionnelles » ?

Elizabeth France, commissaire à l'Information en Grande-Bretagne (autorité indépendante qui veille à ce que les droits des citoyens, en matière d'accès à leurs informations personnelles, soient préservés), a jeté un pavé dans la mare, début août 2002, en déclarant que ces deux textes « entrent en conflit » et que certaines des mesures qu'ils contiennent sont anticonstitutionnelles.
Ses services expliquent que « la loi antiterroriste précise que les données de connexions peuvent être retenues pendant une période plus longue que ne le réclament les besoins de facturation des

opérateurs, mais seulement si ces données sont nécessaires à des enquêtes impliquant la sécurité nationale. Mais le RIPA, lui, autorise bon nombre d'instances, sans réel mandat judiciaire, à pouvoir accéder à ces même données, alors que la plupart de ces instances n'ont pas vocation à protéger la « sécurité nationale ». Il y a donc de grandes chances « que les conditions d'accès à ces données soient déclarées illégales, selon les textes régissant la vie privée et les droits de l'homme ».

Inde

Le *POTO*, l'Ordonnance sur la prévention du terrorisme, la loi promulguée dans la foulée des attentats antiaméricains du 11 septembre, permet au gouvernement indien de surveiller tous types de communications, et a fortiori les communications électroniques telles que les e-mails. Et ce, sans contrôle judiciaire ou administratif. Les éléments recueillis au terme des interceptions de messages décrétées par les services de sécurité peuvent être utilisés à charge contre un suspect, devant une cour.
Utilisateurs privilégiés d'Internet et du courrier électronique en Inde, les journalistes étaient particulièrement menacés par la première mouture de la loi. Elle stipulait en effet que les reporters qui ne transmettraient pas aux autorités les éléments en leur possession sur des terroristes ou des organisations répertoriées comme telles, étaient passibles de cinq années d'emprisonnement.
Durement critiqué par l'opposition et par les organisations de défense des droits de l'homme et de liberté d'expression, le texte a été modifié. Les députés ont finalement retiré l'article obligeant les journalistes à révéler leurs informations liées aux dossiers terroristes.

Italie

Pour lutter contre le terrorisme, le gouvernement italien a fait adopter, mi-décembre 2001, une loi qui permet d'assouplir considérablement le processus de mise sur écoutes d'un suspect et, surtout, qui autorise l'interception des courriers électroniques ou la conservation des données de connexions et de télécommunications.
Grâce à ce texte**,** le nombre des fonctionnaires des services de police et de sécurité à même de recourir à ces procédures a considérablement augmenté. En revanche, le grade ou le niveau hiérarchique des fonctionnaires en question, désormais habilités à traiter ces missions, ont été abaissés. Enfin, le nom desdits fonctionnaires ou les informations concernant les modalités de ces interceptions et réquisitions ne peuvent être divulgués. Les contrevenants s'exposent à des peines de prison ferme. D'où les inquiétudes des ONG quant à l'intrusion d'un grand nombre de fonctionnaires dans les données relatives aux connexions à la Toile.
En fin d'année 2001, une autre loi visant à réformer les services de renseignements a été promulguée. En vertu de ce texte, les agents des services secrets civils (SISDE) et militaires (SISMI) peuvent, en toute impunité, commettre des délits au cours de leurs missions, excepté tuer ou blesser des personnes. Le vol, les perquisitions « secrètes », les écoutes « sauvages », téléphoniques et électroniques, sont désormais autorisés.

Silvio Berlusconi mène le bal au sein du G8

L'Italie, qui assurait la présidence du G8 au moment des attentats, a également posé la première pierre, dans une déclaration officielle du 19 septembre 2001, d'une politique de « lutte contre la criminalité sur Internet et dans le domaine de la haute technologie ».
Cette politique s'est traduite par le renforcement des prérogatives, des moyens et des activités du réseau ad hoc du G8. « Le réseau, qui, à l'origine, comptait seize États participants et en comprend aujourd'hui vingt-six, facilite une coopération rapide des autorités policières internationales lorsqu'elles doivent réagir d'urgence à des situations de crime liées aux hautes technologies, y compris à des communications de terroristes et d'autres criminels au moyen de réseaux informatiques », ont

expliqué les experts de l'organisation, lors d'un bilan dressé à l'occasion de la réunion au Canada des huit chefs d'Etats et de gouvernement, fin juin 2002.
Sans donner plus d'explication, le G8 a rappelé que « les experts juridiques et les autorités policières ont développé une série de mesures concrètes permettant de déterminer l'origine, la destination et le cheminement des communications de nature terroriste et criminelle sur Internet ; de faciliter l'obtention de preuves électroniques nécessaires à cette fin ; d'assurer la préservation des preuves électroniques existantes afin d'empêcher qu'elles ne soient effacées ou modifiées ». Les organisations de défense des libertés numériques, notamment certaines organisations membres du collectif *GILC, Global Internet Liberty Campaign*, rappellent en outre que l'Italie est l'un des Etats qui a le plus énergiquement fait pression sur le Parlement européen pour qu'il adopte la révision de la Directive sur la protection des données de télécommunications (voir chapitre Union européenne). Ce texte, voté le 30 mai 2002, institue la rétention des données de télécommunications et de connexions à Internet (logs de connexions). Ces mêmes ONG mettent l'accent sur le fait que la liste des logs à conserver dans l'Union, suite à la révision de la Directive, est quasi identique aux recommandations formulées par… les experts du G8. De là à voir l'ombre de l'Italie se profiler derrières les grandes mesures internationales, il n'y a qu'un pas, qu'un grand nombre d'experts ont franchi.

Union Européenne

Jusqu'alors opposée à toute forme de « surveillance électronique générale ou exploratoire pratiquée à grande échelle », l'Union européenne a diamétralement changé de cap depuis les attentats de New York et Washington. Le Conseil européen a ferraillé durement contre le Parlement pour imposer les vues des quinze gouvernements. A savoir : légiférer pour imposer, sous la pression des autorités américaines, la rétention généralisée des données de télécommunications et de connexions à Internet.

Bush use de son influence

Mi-octobre 2001, le président Bush a demandé au Premier ministre belge, Guy Verhofstadt, président en exercice de l'Union, la modification d'un projet de Directive européenne pour tenir compte du contexte antiterroriste. Cette Directive prévoit d'instituer la « rétention préventive » des données de connexions à Internet (logs de connexions).

Dans son courrier, le président américain a apporté son soutien au gouvernement britannique (qui, comme la France, a instauré cette rétention des données de connexions à la Toile) et aux différentes polices judiciaires de l'Union qui réclament de nouveaux pouvoirs afin de mieux surveiller le trafic et les échanges sur les réseaux de communication électroniques.
George W. Bush a ainsi expliqué au Premier ministre belge que les États-Unis s'opposent au principe de l'effacement automatique des données de connexions, un principe pourtant inscrit dans le projet de directive "Vie privée et protection des données personnelles dans les communications électroniques", en cours d'examen au Parlement de Strasbourg. Pour les ONG impliquées dans ce dossier, telle *Statewatch*, « c'est une ingérence des Etats-Unis dans les affaires européennes qui vise uniquement à soutenir les propositions formulées, mais peu entendues, par le groupe de travail du Conseil des 15 (Enfopol). Ce groupe milite depuis près de deux ans pour que ce principe de l'effacement automatique disparaisse de la Directive en question ».
La position de ce Conseil, comme celle du président américain, va à l'encontre de celle de la Commission des libertés et des droits du citoyen du Parlement européen. Celle-ci a approuvé, en juillet 2001, un premier rapport du député radical Marco Cappato, en faveur d'un encadrement strict du droit d'accès des forces de l'ordre aux logs collectés par les compagnies de téléphone et les fournisseurs d'accès Internet.

Contre l'avis de la Commission des libertés et des juristes

Le rapport Cappato indique en outre que, pour que de telles pratiques soient autorisées, « les États membres de l'Union sont tenus d'agir en vertu d'une loi précise qui soit compréhensible du grand public et les mesures qu'ils prennent doivent être tout à fait exceptionnelles, autorisées par les autorités judiciaires ou compétentes dans des cas particuliers et pour une durée limitée, appropriées, proportionnées et présenter un caractère de nécessité lié à la société démocratique.
Et ce, en adéquation avec les droits fondamentaux de l'Union, selon lesquels toute forme de surveillance électronique générale ou exploratoire pratiquée à grande échelle est interdite ».
La position du Parlement évolue pourtant notablement en moins d'un an. Soumis à l'intense pression du Conseil européen (le Conseil réunissant les Etats membres), les députés adoptent, le 30 mai 2002 et contre l'avis de Marco Cappato, rapporteur du projet initial de révision, la nouvelle Directive. L'article 15.1 du nouveau texte impose en effet aux gouvernements européens qui ne se sont pas encore dotés d'arsenal législatif en la matière, de légiférer (dans les quinze mois à venir) pour obliger les fournisseurs d'accès à Internet et les opérateurs de télécommunications (téléphonie) à conserver toutes les données de communications : e-mails, Internet, télécopie, téléphone. Et à en garantir le libre accès aux services de police, de justice et à certaines administrations.
Un rapport du service juridique du Conseil des 15, dévoilé le 15 octobre 2001, précisait pourtant que les gouvernements de l'Union avaient déjà les pouvoirs législatifs nécessaires pour intercepter les télécommunications en vue de combattre le terrorisme… Un texte inutile à l'échelon européen, écrivait en substance le service juridique.
La Convention sur la cybercriminalité plébiscitée par les Etats

Le 26 novembre 2001, la première Convention internationale sur la cybercriminalité a été ratifiée à Budapest (Hongrie) par trente Etats. En gestation depuis quatre ans, ce dispositif devait initialement concerner les Etats européens. Attentats du 11 septembre obligent, il a été paraphé (entre autres) par les Etats-Unis, le Canada, le Japon et l'Afrique du Sud. Vingt-six des quarante-trois membres du Conseil de l'Europe y ont adhéré. « Cet instrument vient vraiment à point nommé pour lutter contre le cyberterrorisme, après les terribles attaques qui ont frappé les Etats-Unis », a déclaré Hans Christian Krueger, secrétaire général adjoint du Conseil de l'Europe. Le dispositif permet de rassembler des preuves électroniques sur les infractions liées au terrorisme et au crime organisé sur la Toile.
Ce dispositif est dénoncé par les défenseurs des libertés, les fournisseurs d'accès à Internet et, plus généralement, les professionnels du cyberespace qui le qualifient de « liberticide, interventionniste, complice d'une nouvelle ère de surveillance généralisée ». Les articles 18, 19, 20 et 21 sont particulièrement mis à l'index. Ils organisent notamment la réquisition des informations ou des supports informatiques privés ou des informations intéressantes pour les services de sécurité dans le cadre de leurs enquêtes ; la réquisition des informations stockées chez les fournisseurs d'accès et de services ; la perquisition des sites et serveurs de ces derniers et l'extension de ces perquisitions à des réseaux informatiques si nécessaire ; la conservation et le stockage des données saisies ; la collecte en temps réel d'informations et de logs de connexions si besoin (les autorités judiciaires pouvant exiger que ces opérations soient accomplies par les fournisseurs d'accès et de services) ; etc.

« Surveillance généralisée des Européens »

La situation risque encore de se dégrader. Le député européen Marco Cappato a révélé que la présidence danoise de l'Union européenne avait soumis, le 24 juin 2002, une proposition de mesures qui pourraient être portées par le Conseil européen, intitulée : « Acte relatif aux technologies de l'information et mesures concernant les investigations et poursuites contre le crime organisé ». Elle stipule que « dans un futur proche, tous les Etats membres devront avoir adopté les mesures adéquates pour contraindre les opérateurs de télécommunications et les fournisseurs d'accès à Internet à conserver toutes les données de trafic afin d'en garantir la consultation par les services de sécurité dans le cadre d'enquêtes ». Pour Marco Cappato, « la présidence danoise de l'Union entend renforcer la surveillance généralisée et systématique des citoyens européens. »