

LES ENTRAVES
À LA CIRCULATION DE L'INFORMATION
SUR LE RÉSEAU

INTERNET SOUS SURVEILLANCE

REPORTERS SANS FRONTIÈRES
RAPPORT 2003



www.rsf.org

Avec le soutien du ministère français des Affaires étrangères,
de la Caisse des dépôts et consignations et de la Fondation Hachette

Les statistiques "population" proviennent de :
L'état du monde 2003, © Editions La Découverte & Syros, 2002

Les statistiques "internauts" sont les chiffres de l'Union Internationale
des Télécommunications.

Les cartes proviennent de :
L'atlas des drapeaux du monde, de Patrick Mérienne,
© Editions Ouest-France, 1998

Conception graphique : Nuit de Chine
ndc@nuitdechine.com

ISBN : 2-90-8830-88-4

Copyright : Reporters sans frontières 2003

La libre circulation des informations à un prix

Par VINTON G. CERF

La vérité est un solvant redoutable. Des murs de pierre fondent devant sa puissance irrésistible. Internet est l'un des vecteurs les plus solides de la liberté. Il offre la vérité à ceux qui veulent la voir et l'entendre. On ne s'étonnera donc pas que certains gouvernements et organismes craignent Internet et sa capacité à faire connaître la vérité. Le terme "liberté d'expression" est souvent utilisé pour qualifier un aspect clé des sociétés démocratiques : la libre communication et tout particulièrement la transparence des gouvernements. Mais la liberté d'expression ne constitue que la moitié de l'équation : il est également essentiel que les citoyens puissent disposer du droit à entendre et à voir librement. De nombreux gouvernements sont intervenus dans ce dernier domaine pour tenter d'interdire aux citoyens l'accès à des informations qu'ils préféreraient dérober à leurs regards.

En fait, l'équation est complexe et comporte bien plus d'éléments que parler et écouter ou écrire et lire. Internet ressemble à une feuille de papier, inconsciente de ce qu'on écrit sur elle. De même, Internet est oublieux ; il livre information et désinformation avec la même facilité. Ainsi, il peut servir d'intermédiaire dans la fourniture de données erronées.

Pire, celles-ci peuvent être propagées, par ignorance plutôt que par malice. Je suis surpris par la fréquence à laquelle je reçois des avertissements paniqués dans ma boîte de courrier électronique, transmis par quelque ami qui aurait dû être mieux informé, selon lesquels les services postaux vont bientôt faire payer les messages électroniques ou que Microsoft facturera chaque copie envoyée d'un message donné. Ce sont immanquablement des canulars mais les lecteurs sont trop paresseux ou peut-être trop idiots pour prendre le temps de vérifier l'information avant de la relayer.

L'antidote à la mauvaise information n'est cependant pas la censure, mais une information meilleure et plus abondante. Bien sûr, ceci impose au consommateur d'informations un effort supplémentaire, celui de faire attention et de garder un esprit critique sur ce qu'il lit et entend. De toute évidence, c'est ce qu'un citoyen responsable devrait faire. C'est aussi incontestablement ce que nous devrions enseigner à nos enfants, tant à la maison qu'à l'école.

Malgré la grande promesse qu'il constitue, Internet n'est pas en lui-même une garantie de libre circulation des informations. Le célèbre financier George Soros s'évertue à nous rappeler que la liberté prodiguée par Internet peut être reprise. Ce que vous allez lire dans les pages qui suivent illustre tout juste cela. De nombreux gouvernements cherchent à limiter l'accès de leurs citoyens à l'information. Dans certains cas, les motivations sont compréhensibles et même louables. Je ne vois pas ce que peut apporter la pornographie mettant en scène des enfants, par exemple, et j'apporte mon soutien aux actions destinées à la faire disparaître d'Internet. Mais ceux d'entre nous qui vivent dans une société libre savent, pour l'avoir de nombreuses fois entendu, que la censure est une pente savonneuse et doit être abordée avec les plus grandes précautions.

Même dans les pires cas de contenus abusifs, il faut rester vigilant. Par exemple, on est en présence d'une grave menace lorsque les gouvernements tentent d'étendre leur juridiction au-delà de leurs frontières nationales. Il arrive souvent que des fournisseurs d'accès Internet reçoivent de la part des tribunaux d'un pays X l'ordre d'éliminer certains contenus de serveurs dans un pays Y. Une telle manœuvre extraterritoriale entraîne un imbroglio juridique semé de pièges dans lequel aucune personne normalement constituée ne devrait avoir envie de se retrouver.

Pour emprunter une phrase au monde du capital-risque, les citoyens libres doivent faire preuve de diligence raisonnable pour s'assurer que leur gouvernement ne cache pas de censure politique derrière une façade morale putative. On se rappelle la tentative d'un certain gouvernement de fermer des milliers de cybercafés sous prétexte que l'un d'entre eux avait enfreint la loi de protection contre les incendies et que, par conséquent,

tous les autres pouvaient être dangereux. J'ai trouvé que cela était au mieux une hypocrisie, au pire une insulte à l'intelligence des citoyens.

L'usage efficace d'Internet implique de nombreuses responsabilités. Les citoyens doivent faire leur possible pour se préserver de la censure d'Etat à des fins politiques. Parallèlement, ils ont pour mission d'essayer de différencier les renseignements fiables et utiles des informations de mauvaise qualité et doivent par conséquent jeter un regard critique sur ce qu'ils voient et entendent. Cette responsabilité ne se limite pas à Internet, elle concerne tous les médias. De plus, confrontés à la désinformation, les citoyens attentifs se doivent d'attirer l'attention sur le problème, voire de fournir des informations correctes pour faire échec à celles qui ne le sont pas. Ils doivent en outre être conscients du fait que toutes les informations pertinentes ne sont pas en ligne et que, pour un examen approfondi, il convient d'examiner des documents issus de sources autres qu'Internet avant de conclure que toute la diligence raisonnable a été mise en œuvre. Imaginez les problèmes juridiques inextricables auxquels seraient confrontés les médecins s'ils ne devaient se fier qu'à des informations trouvées sur Internet pour poser un diagnostic et administrer un traitement à leurs patients. Ceux-ci ne doivent pas non plus s'imaginer qu'ils sont au fait des traitements types grâce à une simple recherche sur le Web ou qu'ils ont trouvé le remède miracle sur un site annonçant tambour battant un traitement aussi obscur qu'incertain.

Aucun logiciel de filtrage ne peut distinguer la vérité de la fiction. Aucune "puce antiviolence" cognitive ne peut séparer le bon grain de l'ivraie. Le seul outil à appliquer est la pensée critique. Cet aphorisme s'applique tant à Internet qu'aux autres modes de communication. Peut-être le Réseau nous force-t-il à comprendre cela plus clairement que les autres médias. La juxtaposition brute de contenus utiles et inutiles force la réflexion. Voilà l'occasion pour nous tous de nous instruire. Nous devons réfléchir en profondeur à ce que nous voyons et entendons. Nous devons évaluer et sélectionner, et choisir nous-mêmes nos guides.

En ce XXI^e siècle, ère de l'information, les internautes sont investis de responsabilités importantes. Ils doivent se préserver contre une censure abusive et lutter contre la désinformation. Ils ont un rôle à assumer dans l'usage judicieux d'Internet et du Réseau, ainsi que de tous les services et outils d'information à venir. La libre circulation de l'information a un prix et les internautes responsables le supporteront ensemble.

VINT CERF
MACLEAN, VIRGINIE



Afghanistan

POPULATION : 22 474 000

INTERNAUTES : STATISTIQUES NON DISPONIBLES

FOURNISSEURS D'ACCÈS PRIVÉS : OUI

Conséquence de vingt ans de guerre et de la censure extrême des taliban, Internet est quasi inexistant en Afghanistan. Le nouveau régime en place depuis novembre 2001 affiche son souhait de défendre la liberté d'expression et le pluralisme des médias. C'est sa capacité à reconstruire les infrastructures de communication qui décidera du développement d'Internet.

L'émirat islamique d'Afghanistan créé par les taliban, depuis leur prise de contrôle de Kaboul en 1996, a été l'un des régimes les plus répressifs à l'égard de la liberté d'expression. Dans ce contexte, Internet ne pouvait être considéré par les "étudiants en théologie" que comme un média hérétique et dangereux. Par ailleurs, plus de deux décennies de guerre civile ont ravagé les infrastructures téléphoniques. Le Web était donc, au-delà même des entraves imposées à son développement par les mollahs, quasiment inexistant dans le pays. A l'horizon 2000-2001, seuls les dignitaires du pouvoir taliban, les hauts fonctionnaires des ministères, les cadres d'organisations humanitaires internationales et certains dirigeants de l'opposition de l'Alliance du Nord pouvaient surfer sur la Toile, via le Pakistan ou des liaisons satellite.

Fantomatique, Internet a pourtant été formellement interdit par les taliban le 13 juillet 2001. Selon le ministère des Affaires étrangères, cette interdiction devait alors permettre "d'empêcher l'accès à tout contenu vulgaire, immoral et anti-islamique". Fin août 2001, un nouveau décret signé par le mollah Omar précisait que "sur le territoire de l'émirat islamique d'Afghanistan, aucune organisation gouvernementale ou non gouvernementale, afghane ou internationale, ni aucun particulier ne peut utiliser Internet". Le gouvernement taliban a ordonné dès lors à la police religieuse de punir les contrevenants conformément à la loi islamique. Seul le quartier général de la milice des "étudiants en théologie" était habilité à utiliser le Réseau et à valider le courrier électronique des différents ministères.

La chute, en novembre 2001, du régime taliban a ouvert une ère nouvelle. Lors de son discours d'investiture, le 22 décembre, le président du nouveau gouvernement intérimaire d'Afghanistan, Hamid Karzaï, a martelé que "la liberté d'expression et de

croissance est un droit de tous et de chacun des citoyens afghans, et il est de notre responsabilité de le défendre". Une prise de position qui augure peut-être de l'avènement progressif d'Internet en Afghanistan. Le chemin sera néanmoins long. S'il n'existe dans le pays aucune législation qui réglemente ou limite l'accès au Réseau, encore faut-il pouvoir se connecter. Toujours délabré, le réseau de télécommunications ne permet pas d'utiliser Internet. Aucun fournisseur d'accès ne peut donc proposer de services sur le sol afghan. La seule option restante est la connexion satellite. Si les officiels du régime, les reporters étrangers, les ONG ou les militaires l'utilisent abondamment, la population n'y a pas ou peu accès, compte tenu du coût exorbitant de la connexion.

En mars 2003, le ministère de la Communication et le Programme des Nations unies pour le développement inaugurent le nom de domaine "af" réservé aux utilisateurs afghans d'Internet. "C'est notre drapeau national sur Internet", affirme le ministre de la Communication. Il n'existe encore aucune réglementation concernant Internet, mais le ministère travaille, avec l'aide d'organisations internationales, à la rédaction d'une loi sur les télécommunications.

En août 2002, le premier café Internet a ouvert ses portes à Kaboul, à l'initiative de la compagnie de télécommunications Afghan Wireless Communication. Peu de temps après, l'ONG d'aide aux médias AINA a inauguré à Kaboul une salle Internet pour les journalistes afghans. Selon un décompte de l'Agence France-Presse, on compte, en mars 2003, cinq cafés Internet dans la capitale.

Le Net est pourtant un vecteur d'information crucial pour l'importante diaspora afghane. Des dizaines de milliers d'Afghans sont aujourd'hui installés aux Etats-Unis, au Canada, en Australie, en France, en Allemagne, etc. En fin d'année 2001, ils ont décidé de recourir à Internet pour participer à la reconstruction du pays et pour ressouder la communauté éparpillée. Des exilés installés dans la Silicon Valley, en Californie, ont ainsi créé le site Virtual Nation. Il sert de lien entre les Afghans du monde entier et les organisations qui cherchent à lancer des programmes de développement en Afghanistan.

LIENS :

• L'Afghan Reconstruction Development Center
www.virtualnation.org

• L'agence de presse *Afghanistan*
<http://francais.afgha.com>

• Le ministère de la Communication
www.af-com-ministry.org



Afrique du Sud

POPULATION : 43 792 000

INTERNAUTES : 3 100 000

FOURNISSEURS D'ACCÈS PRIVÉS : OUI

Moteur du développement du Web sur le continent, l'Afrique du Sud s'est dotée, au début du mois de juin 2002, d'une loi très controversée de lutte contre le cyberterrorisme. Les opposants à ce texte ont également dénoncé "la nationalisation par le gouvernement de l'administration des noms de domaines en ".za" des sites sud-africains".

La croissance d'Internet dans la patrie de Nelson Mandela fait rêver tous les amoureux du Net sur le continent. L'Afrique du Sud est, de très loin, le pays le plus avancé en la matière. Connecté à la Toile depuis le milieu des années 90, il a un atout de taille : la quasi-totalité des flux Internet des autres pays du continent transite par ses backbones (nœuds de connexions permettant de router mondialement les messages et requêtes). Le pays possède donc une infrastructure technologique à même d'encourager la croissance de son Internet.

La marche vers la démocratisation de la Toile s'est amorcée il y a deux ans environ. Les résultats commencent à être probants : le secteur d'activités de la fourniture d'accès est tonique et la concurrence est acharnée. Surtout, le gouvernement affiche une volonté de connecter le plus rapidement possible toutes les couches sociales du pays au Réseau. Si cette démocratisation n'est pas encore avérée, la croissance régulière du nombre d'utilisateurs est prometteuse.

Quels contrôles, dans quels systèmes ?

Deux événements ont pourtant assombri, début juin 2002, ce tableau : le vote d'une loi destinée à lutter contre le cyberterrorisme et la décision du gouvernement de s'approprier l'administration de l'attribution des noms de domaines nationaux (en .za).

L'Assemblée nationale sud-africaine a adopté une loi sur les transactions et communications électroniques (The Electronic Communications and Transactions Bill) visant à "protéger le pays contre le cyberterrorisme". Le 23 novembre 2001, à Budapest, l'Afrique du Sud avait déjà signé la première convention internationale contre la cybercriminalité aux côtés d'une trentaine de pays (membres du Conseil de l'Europe, Etats-Unis, Canada, Japon).

La nouvelle loi sud-africaine a été durement critiquée, notamment par l'Alliance démocratique (DA) qui a voté contre son adoption, mais aussi par les organisations de défense de la libre circulation de l'information sur Internet ou les entreprises privées. Elle permet en effet à la ministre des Télécommunications, Ivy Matsepe-Casaburri, de nommer des inspecteurs chargés de contrôler les systèmes de télécommunications et leurs contenus, et de procéder à d'éventuelles saisies de données.

Les entreprises s'inquiètent de l'ingérence de l'Etat dans le secteur du commerce en ligne, même si Ivy Matsepe-Casaburri a déclaré devant l'Assemblée "qu'elle n'entend pas le contrôler". Au-delà des acteurs économiques, les défenseurs du droit à la confidentialité et à la liberté d'expression s'interrogent sur l'opacité des méthodes de travail des inspecteurs qui vont être nommés, ou sur la liste exacte des systèmes de télécommunications qu'ils seront à même de contrôler et des données auxquelles ils auront accès.

Résistance autour des noms de domaines

Autre sujet de polémique : la décision du gouvernement de s'approprier l'attribution des noms de domaines des sites Internet nationaux. Jusqu'au vote du texte par l'Assemblée, ils étaient administrés par une organisation d'usagers d'Internet "Nom de Domaine ZA" (Namespace ZA), dirigée par Mike Lawrie. Les griefs du gouvernement sont clairs : "Les noms de domaine sud-africains ne doivent plus être administrés par une seule personne travaillant dans le secteur privé." Pour Mike Lawrie, il s'agit, ni plus ni moins, "d'une nationalisation de ces noms". "C'est inacceptable car le niveau de surveillance et de contrôle que va imposer l'Etat, s'il les gère, mettra en péril l'indépendance du Web sud-africain", rétorque-t-il. Refusant de céder, il a transféré, courant juin, une partie de ses informations et de ses serveurs hors des frontières afin, dit-il, "de les mettre à l'abri, quitte à m'exposer à des poursuites".

LIENS :

- L'organisation d'usagers d'Internet Namespace ZA
www.namespace.org.za
- L'association des fournisseurs d'accès d'Afrique du Sud ISPA
www.ispa.org.za



MAGHREB

Algérie

POPULATION : 30 841 000

INTERNAUTES : 500 000

FOURNISSEURS D'ACCÈS PRIVÉS : OUI

Contrairement à son voisin tunisien, l'Algérie ne soumet Internet à aucun contrôle spécifique. Seuls des dispositifs législatifs traduisent la volonté des autorités de réglementer davantage la Toile, voire de la surveiller. Mais dans les faits, rien encore n'a été mis en œuvre.

C ourant 2001, le quotidien *Liberté* a rapporté qu'à Boufarik, une petite ville à l'ouest d'Alger, un policier avait tenté d'obtenir du gérant d'un cybercafé qu'il enregistre les noms et les adresses des internautes, ainsi que les sites qu'ils visitent. Ce dernier avait refusé et déposé une plainte. Après la révélation de l'affaire dans la presse, le responsable local de la police avait affirmé qu'il s'agissait d'une initiative personnelle du policier et que ce dernier avait été suspendu.

Depuis, aucun cas de censure n'a été signalé. Cependant, l'article 14 d'un décret sur les télécommunications publié en 1998 stipule que les fournisseurs d'accès "doivent assumer les responsabilités du contenu des pages et des serveurs de données qu'ils gèrent ou qu'ils hébergent". Surtout, il leur est demandé "de prendre toutes les dispositions nécessaires afin d'assurer une surveillance constante du contenu et des serveurs accessibles à leurs abonnés". Ce, "afin d'empêcher l'accès aux serveurs contenant des informations contraires à l'ordre public et à la morale".

En mai 2001, l'Assemblée a par ailleurs adopté un projet d'amendement du code pénal qui a soulevé un tollé au sein de la communauté journalistique. L'article 144 bis prévoit des peines de deux à douze mois de prison et des amendes variant de 750 à 3 750 euros en cas "d'atteinte au président de la République en termes contenant l'injure, l'insulte ou la diffamation, soit par l'écrit, le dessin ou par voie de déclaration. Et ce, quel que soit le moyen utilisé : diffusion sonore, image, support électronique, informatique ou autre". Les poursuites peuvent désormais être engagées directement par le ministère public, sans dépôt préalable d'une plainte. En cas de récidive, les peines d'emprisonnement et les amendes sont "portées au double". Toutes ces sanctions sont également applicables quand les délits sont commis à l'encontre du "Parlement ou de l'une de ses deux Chambres, de l'ANP" (l'Armée nationale populaire) mais aussi de toute "autre institution publique ou tout autre corps constitué". Si plusieurs journalistes ont été condamnés à des peines de prison à cette période, cette mesure n'entrave pas, pour l'heure, le développement d'Internet.

LIENS :

- Le site d'informations Algeria Interface
www.algeria-interface.com

- Le site d'informations sur les droits de l'homme Algeria Watch
www.algeria-watch.de

- Le site Maghreb des droits de l'homme
www.maghreb-ddh.org



Allemagne

POPULATION : 82 007 000

INTERNAUTES : 35 000 000

FOURNISSEURS D'ACCÈS PRIVÉS : OUI

Le programme "Internet pour tous" impulsé, en 2000, par le chancelier Gerhard Schröder est un moteur incontestable du succès populaire d'Internet en Allemagne. Une politique volontariste de développement de la Toile qui s'accompagne néanmoins d'un encadrement législatif strict.

Depuis juillet 1996 et la loi sur les télécommunications, les fournisseurs d'accès doivent rendre possible la consultation des communications Internet par les services secrets. La loi sur l'information et la communication d'août 1997 rend les hébergeurs responsables de leur contenu propre et de celui des sites qu'ils accueillent, seulement s'ils en ont connaissance. En 2001, la loi G-10, qui impose des limitations à la politique de protection des communications, a été amendée. Il a été demandé aux providers de tout mettre en œuvre pour permettre aux services de renseignements de surveiller ou d'intercepter les communications électroniques ou vocales, nationales comme internationales. Il a également été fortement conseillé à ces même hébergeurs de faire un effort pour "autoréguler" les contenus diffusés sur le Web. Cette loi comporte une liste des crimes justifiant la surveillance des télécommunications. Longue et floue, cette liste ne cible pas seulement le suspect, mais aussi toute personne susceptible d'avoir un échange d'informations avec le suspect.

Les attentats du 11 septembre ont débouché par ailleurs sur le vote, fin 2001, d'une loi antiterroriste concoctée par le ministre de l'Intérieur, Otto Schily. Entrée en vigueur en janvier 2002, l'Ordonnance sur l'interception des télécommunications permet notamment aux services de renseignements et à la police d'accéder aux données de télécommunications stockées sur support numérique : informations sur les services utilisés par les clients ; accès aux renseignements relatifs aux échanges de e-mails ; accès à toutes les données permettant de localiser les personnes à l'origine des communications ou des courriers électroniques ; accès aux données des entreprises de télécommunications.

Une vingtaine d'organisations de défense des droits civiques, de la liberté d'expression et de protection des données personnelles, se sont regroupées au sein d'un collectif pour dénoncer ce contrôle des communications. Elles jugent cette loi inapte

à dénigrer l'activité terroriste et ont dénoncé les concepts juridiques invoqués pour adopter de telles mesures.

Déjà, en juin 2001, la presse avait égratigné le gouvernement en révélant qu'il avait laissé se développer sur son sol un "maillon" du réseau-espion américain Echelon. Selon le quotidien bavarois *Merkur*, qui a rendu public un rapport des services secrets de l'armée des Etats-Unis, la base américaine implantée à Bad Aibling (Bavière) serait l'une des plus importantes stations d'écoute et d'interception des communications électroniques du système Echelon en Europe, derrière la base américaine de Menwith Hill, en Grande-Bretagne. Elle permettrait aux Etats-Unis d'espionner les courriers électroniques émis depuis une grande partie de l'Europe, dont tout l'ancien bloc soviétique de l'Est. Une révélation qui a fait d'autant plus de bruit que l'Allemagne n'est pas signataire du pacte UKUSA, qui organise la répartition des tâches entre les Etats-Unis, la Grande-Bretagne, le Canada, l'Australie et la Nouvelle-Zélande.

Depuis octobre 2001, les autorités régionales de Westphalie du Nord dressent une "liste noire" de sites Internet et demandent à plus de 80 hébergeurs locaux d'en bloquer l'accès grâce à un système de filtrage, adopté par les compagnies Bocatel, Intranet et Webwasher. Ainsi, le 8 février 2002, les autorités ont demandé de bloquer l'accès à deux sites américains à caractère néonazi. La FITUG (organisation allemande de défense des droits électroniques), ainsi que de nombreux internautes, ont protesté contre le blocage de l'accès à certains sites, qui affecte moins les auteurs des sites au contenu contraire à la Constitution ou aux droits de l'homme que les infrastructures de communication elles-mêmes. D'autant plus que cette interdiction est facilement contournable à partir d'un autre département, les autorités de Düsseldorf n'ayant de compétence que sur les hébergeurs locaux.

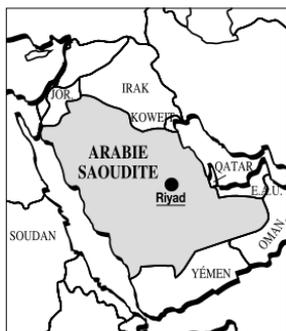
LIENS :

- Le site du gouvernement fédéral

www.bundesregierung.de

- La FITUG, association de défense des droits électroniques (en allemand)

www.fitug.de



Arabie Saoudite

POPULATION : 21 028 000

INTERNAUTES : 1 600 000

FOURNISSEURS D'ACCÈS PRIVÉS : OUI

Le royaume saoudien n'a autorisé l'usage public d'Internet qu'en 1999. Un retard qui s'explique par la volonté des autorités de mettre en place un système de censure efficace avant même de libéraliser les connexions au Réseau.

La parade mise en place par le pouvoir : un "fire wall", autrement dit un dispositif permettant de contrôler les requêtes formulées vers la Toile par les internautes saoudiens et de bloquer l'accès aux sites jugés "immoraux". Installé à la Cité du roi Abdulaziz pour la science et la technologie à Djeddah, ce dispositif a officiellement pour vocation de bloquer l'accès aux sites pornographiques. Dans la réalité, cette censure frappe tous les sites "violant les valeurs sociales, culturelles, politiques, économiques et religieuses de l'Etat". Les portails d'opposition, comme celui du Mouvement pour la réforme islamique en Arabie (MIRA) sont inaccessibles, de même qu'un grand nombre de sites d'organisations politiques ou d'organisations non gouvernementales qui défendent les droits de l'homme.

Début 2001, les autorités ont affirmé avoir bloqué deux cent mille sites. En avril de la même année, elles ont annoncé qu'elles allaient en bloquer deux cent mille autres, dont les contenus sont jugés "contraires aux bonnes mœurs". A la même période, le mufti d'Arabie Saoudite a appelé les internautes du royaume à boycotter le site de Yahoo!, opérateur "qui a décidé de promouvoir la pornographie", selon les instances religieuses.

S'il n'existe pas de loi spécifique à Internet dans le pays, la Toile est de fait encadrée par la loi sur la presse. Celle-ci impose d'obtenir une autorisation avant d'exploiter un média, quel qu'il soit. En outre, la famille royale a le pouvoir de révoquer les journalistes et nomme les responsables des journaux et des organes médiatiques. La liberté d'expression n'existe pas en Arabie Saoudite : ni dans la presse, ni sur Internet.

Le contournement de la censure semble néanmoins connaître un frémissement. Les internautes saoudiens utilisent de plus en plus des serveurs relais (proxys) pour se connecter aux sites bloqués et surfer en conservant l'anonymat.

LIENS :

- Saudi Center for Human Rights Studies
www.saudihr.org

- Saudi Institute for Development and Studies, qui travaille à la promotion de la société civile en Arabie saoudite
www.saudiinstitute.org

- Site d'informations sur les pays du Golfe (en arabe)
www.gulfissues.net



Australie

POPULATION : 19 338 000

INTERNAUTES : 8 400 000

FOURNISSEURS D'ACCÈS PRIVÉS : OUI

Le Broadcasting Services Act, entré en vigueur le 1er janvier 2000, définit les contenus prohibés sur Internet : pornographie mettant en scène des enfants, bestialité, violence excessive, représentations précises d'actes sexuels, informations sur le crime, la violence et l'usage de stupéfiants. L'appréciation des contenus a été confiée à l'Australian Broadcasting Authority (ABA - organisme qui réglemente les services de radio et télédiffusion) qui demande au fournisseur d'accès de chaque site concerné "de prendre les mesures raisonnables pour en bloquer l'accès". Ces dispositions inquiètent les associations de défense des libertés civiles. Elles dénoncent également l'obligation faite aux fournisseurs d'accès à Internet de proposer des logiciels de filtrage de contenus à leurs clients. Les fournisseurs d'accès font d'ailleurs de la résistance. Ils refusent pour la plupart d'obtempérer sous la contrainte et se bornent à aiguiller leurs abonnés vers des sites proposant ces produits.

En octobre 2001, le gouvernement promulgue le Cybercrime Act qui autorise notamment les juges à obliger un suspect à révéler ses codes de cryptage. Quelques mois plus tard, le Sénat rejette un amendement à la loi sur les télécommunications qui aurait permis aux services de sécurité d'intercepter des communications électroniques sans l'aval de la justice.

Le 28 mai 2002, huit des plus importants médias internationaux, notamment *Yahoo*, *CNN*, *Reuters*, *The Guardian*, sont représentés par un groupe d'avocats pour soutenir le groupe de presse Dow Jones' jugé en appel pour "diffamation" devant la Haute Cour du pays. Cette procédure fait suite à une plainte de l'homme d'affaires australien Joseph Gutnick qui estime avoir été diffamé par un article publié sur la version Internet du magazine *Barrons*, détenu par Dow Jones'. Dow Jones' a été condamné en première instance pour "diffamation" par la Cour suprême de l'Etat de Victoria, qui avait jugé la plainte recevable car l'article pouvait être consulté depuis cet Etat. Selon l'avocat de Dow Jones', cette jurisprudence fait courir un grand risque à la presse en ligne, menacée d'être poursuivie en justice aux quatre coins de la planète.

En novembre 2002, l'Australian Broadcasting Authority refuse de censurer trois sites antimondialisation qui ont notamment demandé aux manifestants contre le Sommet

de l'Organisation mondiale du commerce de Sydney de s'armer de "battes de baseball et de masques à gaz." Les autorités, et plus particulièrement la police, avaient fait cette demande de censure depuis septembre, estimant qu'il s'agissait d'appels explicites à la violence contre les forces de l'ordre. En réaction à la décision de l'Australian Broadcasting Authority, le gouvernement aurait entamé la rédaction d'une loi mettant en place un Centre des crimes technologiques. Selon le journal *The Courier-Mail*, ce texte donnerait au gouvernement fédéral le pouvoir de censurer directement des sites Internet.

LIENS :

- Les pages d'Electronic Frontier Australia consacrées à la censure sur Internet
www.efa.org.au/Analysis/aba_analysis.html
- L'Australian Broadcasting Authority
www.aba.gov.au
- Le site de *Zdnet* sur les nouvelles technologies
www.zdnet.com.au



EUROPE

Azerbaïdjan

POPULATION : 8 096 000

INTERNAUTES : 300 000

FOURNISSEURS D'ACCÈS PRIVÉS : OUI

Le retard du développement d'Internet dans le pays s'explique par le prix élevé des ordinateurs et des abonnements aux fournisseurs d'accès, ainsi que par la qualité médiocre des lignes téléphoniques et du matériel de télécommunications. Et ce, même si le coût de l'heure passée sur le Web ne cesse de baisser (moins de un dollar). Si de plus en plus d'Azerbaïdjanais surfent dans les cybercafés des grandes villes, il est encore difficile de se connecter hors des agglomérations.

Une douzaine de fournisseurs d'accès, publics ou privés, occupent le marché. Mais le ministère des Communications oblige ces derniers à lui céder 51 % des parts de leurs entreprises. C'est également ce ministère qui leur alloue les licences leur permettant de se lancer sur le marché et les transmissions demeurent sous son contrôle. Le secteur est par ailleurs encadré par les services du ministère de la Sécurité nationale qui contrôle le trafic et les communications des opposants, des intellectuels ou des hommes d'affaires étrangers. Selon une source non officielle, l'Etat justifie cette mainmise par sa lutte contre les hackers arméniens qui lancent des attaques contre les sites officiels azerbaïdjanais depuis quelques années déjà. En mars 2002, le site d'informations *Virtualnyi Monitor*, basé en Russie, a été bloqué temporairement après la publication d'articles critiquant le gouvernement.

En juillet, le Forum Internet Azerbaïdjan a lancé une campagne de protestation virtuelle contre la censure sur Internet exercée par les autorités, qui retarde le développement du web dans le pays.

LIENS :

- Le service azerbaïdjanais de *Radio Free Europe/Radio Liberty*
www.rferl.org/bd/az
- Le site d'informations *Eurasianet*
www.eurasianet.org
- L'agence de presse indépendante *Turan*
www.turaninfo.com



Bahreïn

POPULATION : 652 000

INTERNAUTES : 165 000

FOURNISSEURS D'ACCÈS PRIVÉS : NON

A l'occasion de la Journée mondiale de la liberté de la presse, le 3 mai 2003, l'Association pour l'entente nationale islamique (AENI), principal groupe d'opposition et émanation politique des chiites, a dénoncé le blocage par les autorités de l'accès à plusieurs sites Internet. Des sites dont les contenus "irritaient" le pouvoir. Lors du 3 mai 2002, l'AENI avait organisé un rassemblement devant les locaux de la Bahrain Telecommunications Company (Batelco), pour dénoncer "ce blocage qui revient à bâillonner la liberté d'expression". La Batelco, unique fournisseur d'accès du pays, bloque certains sites et surveillerait les échanges de courriers électroniques.

Selon le ministère de l'Information, qui a décidé cette censure, ces sites "sont devenus des tribunes pour la diffusion d'informations tendancieuses, de rumeurs et de mensonges". Le ministre, Nabeel Yacoub el Hamer, a déclaré en mars 2002 qu'il lèverait ce blocage lorsque les sites auront changé leur contenu. Parmi les sites censurés figuraient www.vob.org, du Mouvement de libération du Bahreïn (MLB, opposition basée à Londres), www.bahrainonline.org, de Bahrain online, www.al-manama.net, du journal en ligne *Al Manama* ou encore un site de l'islamiste Abdel Wahab Hussein.

LIENS :

• La Bahrain Telecommunications Company
www.batelco.com.bh

• Site d'informations sur les pays du Golfe (en arabe)
www.gulfissues.net

• Le quotidien anglophone *Bahrain Tribune*
www.bahraintribune.com



ASIE

Bangladesh

POPULATION : 140 369 000

INTERNAUTES : 204 000

FOURNISSEURS D'ACCÈS PRIVÉS : OUI

Au Bangladesh, une dizaine de médias en bengali et en anglais disposent de versions en ligne. Mais on ne comptabilise qu'une petite poignée de fournisseurs d'accès et un nombre infime d'internautes par rapport à la population totale. La police a étendu sa surveillance aux courriers électroniques de certains journalistes et militants politiques.

Le 27 février 2001, dans les vingt-quatre heures qui ont suivi le lancement du portail banglarights.com, spécialisé dans l'information sur les droits de l'homme, les communications téléphoniques et fax ont été suspendues par le Bangladesh Telegraph and Telephone Board (BTTB). L'organisme de régulation nie que cette coupure soit liée aux activités militantes de l'organisation non gouvernementale DRIK qui héberge le site. L'autorité de régulation la justifie par les besoins d'une enquête du ministère du Téléphone et du Télégraphe suite à des plaintes spécifiques contre les fournisseurs d'accès à Internet.

DRIK héberge également un site d'activisme antiglobalisation très critique à l'égard de la politique gouvernementale, [Meghbart](http://Meghbart.com). A la période du lancement de banglarights.com, [Meghbart](http://Meghbart.com) avait mis en ligne des articles sur la situation des droits de l'homme au Bangladesh et relaté des incidents dont avaient été victimes des militants des droits de l'homme. Des articles qui auraient irrité un certain nombre d'hommes politiques.

En novembre 2001, le gouvernement a par ailleurs fait couper les lignes téléphoniques d'une soixantaine de sociétés proposant des services liés à Internet. Le ministre des Télécommunications a motivé cette coupure par l'incapacité de ces sociétés à faire renouveler leurs licences professionnelles. Mais l'association des sociétés de services Internet a présenté une autre version des faits. Selon ses dirigeants, cette opération visait à mettre un terme à l'utilisation du réseau Internet par les usagers pour téléphoner à l'étranger. Une pratique qui permet de ne pas passer ses appels par le réseau téléphonique national. Répandue au Bangladesh et autorisée dans la plupart des pays du monde, elle est cependant proscrite par le gouvernement bangladais.

La police a développé la surveillance des courriers électroniques de journalistes et de militants politiques. Ainsi, début 2002, le journal islamiste *Inqilab* publie des

courriers électroniques privés du journaliste Shahriar Kabir, visiblement interceptés par les services de sécurité bangladaise. Le quotidien, qui soutient le gouvernement, est alors engagé dans une campagne contre Shahriar Kabir, accusé d'être un "traître vendu à l'Inde". De même, fin 2002, lors d'une vague d'arrestations menée par le gouvernement conservateur, la police saisit les ordinateurs de plusieurs journalistes dont Saleem Samad, correspondant de Reporters sans frontières. Un climat de peur s'installe et plusieurs reporters et militants des droits de l'homme affirment à l'époque à l'organisation ne plus oser utiliser d'adresses électroniques de providers nationaux, de peur qu'ils ne soient surveillés par la police.

LIENS :

- Le quotidien en ligne *News from Bangladesh*
<http://bangladesh-web.com/news>
- L'organisation DRIK
www.drik.net



EUROPE

Bélarus

POPULATION : 10 147 000

INTERNAUTES : 808 700

FOURNISSEURS D'ACCÈS PRIVÉS : OUI

Tout en plaidant pour le développement des technologies numériques dans son pays, le président Alexandre Loukachenko a initié une surveillance étroite d'Internet.

Les internautes biélorusses soupçonnent le régime d'exercer un contrôle strict sur les connexions via la procédure de "certification" de tout modem mis en utilisation. Cette procédure de vérification du matériel, exigée par le ministère des Communications, dure au minimum une semaine. L'Etat exerce un monopole sans partage à travers Beltelekom, le principal opérateur public. Si plusieurs fournisseurs d'accès privés sont apparus, tels Global one, filiale de l'opérateur américain Sprint, ou Open Contact, ils sont, en réalité, relayés par Belpak (la division Internet de Beltelekom). Pour obtenir une licence, il est nécessaire de s'engager à utiliser le réseau Beltelekom, d'accepter des "inspections techniques" impromptues des inspecteurs du ministère des Communications et de lui fournir chaque année la liste de ses abonnés. Les providers s'engagent par ailleurs à ne pas échanger de trafic les uns avec les autres.

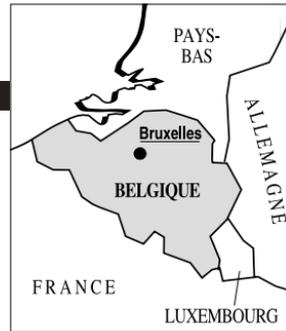
Les sites d'informations indépendants ne font l'objet d'aucune censure. Probablement parce que l'audience d'Internet est encore limitée en Biélorussie.

Le 22 mai 2002, le Parlement a fini par rejeter un projet de loi sur la "sécurité de l'information", dénoncé par l'Association des journalistes biélorusses (BAJ) comme renforçant le contrôle des autorités sur le contenu et la circulation de l'information.

Le 5 novembre, la police a interrogé Iulia Doroshevich et Andrey Pachobut, deux journalistes du quotidien *Pagonya*, interdit en 2001, au sujet de la version Internet de la publication, toujours accessible. Le rédacteur en chef de *Pagonya* et un de ses journalistes ont purgé, de septembre 2002 à mars 2003, des peines de travaux forcés pour avoir "insulté" le président Loukachenko dans un article.

LIENS :

- L'association des journalistes biélorusses BAJ : baj.ru/indexe.htm
- Etude de la législation liée à la liberté d'expression par l'organisation Article 19 www.article19.by/publications/instrumentscontrol/index.html



Belgique

POPULATION : 10 264 000

INTERNAUTES : 3 400 000

FOURNISSEURS D'ACCÈS PRIVÉS : OUI

A lors qu'en 1998, on recensait seulement cinq cent mille internautes dans le royaume, les internautes représentent aujourd'hui près de 30 % de la population. Ce sont principalement des hommes (90 %), âgés de 24 à 45 ans, dont les deux tiers sont en possession d'un diplôme universitaire ou équivalent.

Cette croissance rapide s'explique en partie par le fait que Bruxelles, capitale européenne, siège des grandes institutions de l'Union, a été précoce et pionnière en matière de conversion aux nouvelles technologies. La dynamique de développement de la Toile est par ailleurs soutenue par le nombre important d'offres commerciales portées par le très concurrentiel secteur des fournisseurs d'accès à Internet.

Pays attaché à la liberté d'expression et aux droits de ses citoyens, la Belgique a néanmoins été l'un des premiers États européens à légiférer pour instituer la conservation des données de connexion au Réseau. En 2001, avant même les attentats du 11 septembre, cette conservation a été portée à un an. Cette volonté de pouvoir garder et exploiter ces informations s'explique vraisemblablement par le fait que la Belgique a été traumatisée par les affaires de pédophilie et d'exploitation sexuelle de la jeunesse via les nouvelles technologies de l'information.

LIENS :

- L'Association Electronique Libre

www.ael.be

- L'Observatoire des droits de l'Internet

www.internet-observatory.be



Birmanie

POPULATION : 48 364 000

INTERNAUTES : 10 000

FOURNISSEURS D'ACCÈS PRIVÉS : NON

La Birmanie reste l'un des pays les plus hermétiques à Internet. Les Birmans doivent se contenter d'un ersatz de Réseau, le Myanmar Wide Web, un Intranet national mis en place par la junte militaire. Les quelques milliers de comptes e-mails autorisés sont contrôlés. Le pouvoir a lâché timidement du lest en 2002 en autorisant l'activité d'un second fournisseur d'accès et l'ouverture d'un cybercafé à Rangoon.

Si la situation d'Internet en Birmanie a quelque peu évolué depuis 2000, seuls quelques centaines de privilégiés - officiels du pouvoir, militaires de haut rang ou chefs d'entreprises dont l'activité est tournée vers l'export - ont le privilège de pouvoir surfer sur le Web. Sous une étroite surveillance, s'entend. Pour près d'une dizaine de milliers de personnes, Internet se limite à l'utilisation du courrier électronique, qui leur est accordée pour raisons professionnelles uniquement. Courrier rigoureusement filtré par les hommes de l'organisme de tutelle, le Myanmar Posts and Telecommunications (MPT) et des services de renseignements militaires qui utiliseraient le logiciel de filtre "Dans Guardian".

Un Intranet national contrôlé par la junte militaire

Moins de dix mille personnes se contentent de l'ersatz de réseau qu'est le Myanmar Wide Web, une sorte d'Intranet national mis en place par la dictature militaire. Quelques dizaines de sites, essentiellement des sites de services ou des sites administratifs dûment accrédités par le pouvoir, y sont proposés. Pour autant, ce réseau national est peu accessible. A Rangoon, par exemple, seul le "I-café" de l'université proposait, en 2002, un accès libre au Myanmar Wide Web.

Quant au courrier électronique, seuls les grands hôtels, les agences de voyage et les hommes d'affaires birmans et étrangers peuvent y avoir recours. Les courriers arrivent sur un serveur national et les messages sont triés et contrôlés par le MPT avant d'atteindre leurs destinataires. Cette entreprise publique aurait déjà ouvert plus de cinq mille comptes e-mails.

La prison guette les contrevenants

Une loi promulguée dès 1996 proscrit toute importation, détention ou utilisation d'un fax ou d'un modem sans autorisation de l'administration. Les contrevenants à cette loi s'exposent à quinze années d'emprisonnement. Une peine aussi lourde peut être prononcée à l'encontre de quiconque recourt au Réseau pour "porter atteinte à l'Etat, à l'ordre, à la loi, à l'unité nationale, à la culture ou à l'économie". Enfin, toute personne créant un lien vers un site sans autorisation risque également la prison.

Depuis le 20 janvier 2000, les écrits politiques sont interdits sur le Réseau et la création de pages web est soumise à autorisation. La réglementation interdit "tout écrit en ligne susceptible de nuire aux intérêts de l'Union de Myanmar" et tout message "directement ou indirectement nuisible à la politique actuelle et aux secrets d'Etat en matière de sécurité."

Ces dispositions visent à empêcher la population de s'informer librement ou de consulter les sites de l'opposition birmane en exil, très active sur le Net. Le site Free Burma Coalition fédère par exemple plusieurs mouvements d'opposants de la diaspora.

Une avancée à pas comptés

"Certains des hommes au pouvoir sont convaincus que la Toile est un passage obligé, en matière de développement économique. En même temps, ils sont conscients que l'accès à une information pluraliste et à une richesse culturelle représente un danger réel. Le débat est donc vif et le sujet sensible au sein même de la junte militaire", affirme sous couvert d'anonymat un journaliste birman. L'avancée se fait donc à pas comptés.

Au printemps 2002, le monopole du provider étatique MPT a été battu en brèche par l'arrivée d'un second opérateur : Bagan Cybertech Company. Une concurrence en trompe-l'œil : cette compagnie est, en fait, une société semi-publique. Le pouvoir n'a donc pas beaucoup à craindre de ce nouveau fournisseur d'accès et de services, dont le directeur, Ye Naung Win, est le fils du très puissant chef des services secrets militaires, le lieutenant général Khin Nyunt. Bagan Cybertech Company a affirmé que le pouvoir a autorisé la création de dix mille nouveaux comptes e-mails et de plusieurs milliers d'accès à Internet. L'entreprise aurait déjà vendu plus de trois mille connexions. Les responsables de Bagan Cybertech ont ajouté que l'Intranet national devrait compter plusieurs centaines de sites dans un futur proche.

Selon un article du magazine *Irrawaddy* (basé en Thaïlande), les demandes d'ouverture de cybercafés doivent systématiquement passer par Bagan Cybertech. Le prix d'un accès au Réseau pour un particulier, qui doit disposer d'une autorisation de la junte militaire, est de 260 euros. Il est de 600 euros pour les entreprises.

En septembre 2002, le magazine économique birman *Living Color* annonce l'ouverture

prochaine au grand public du premier cybercafé de Rangoon. Mais les clients ne pourront pas y consulter leurs comptes e-mails. Les détenteurs d'adresses e-mails peuvent lire leurs messages dans les rares "e-mail shops" de la capitale. Mais il s'agit d'une activité illégale tout juste tolérée par la junte.

La presse profitera-t-elle de cette "ouverture" ? Au cours de l'année 2001, la plupart des hebdomadaires et des mensuels birmans ont mis en ligne leurs publications sur l'Intranet. Mais la presse indépendante et les organisations d'opposition doivent toujours lancer et gérer leurs sites depuis l'étranger pour pouvoir les faire exister.

LIENS :

- Le magazine indépendant en exil *Irrawaddy*
www.irrawaddy.org

- Site officiel du pays
www.myanmar.com

- La Burma Media Association
www.bma-online.net

- La lettre électronique *Burmanet news*
www.burmanet.org

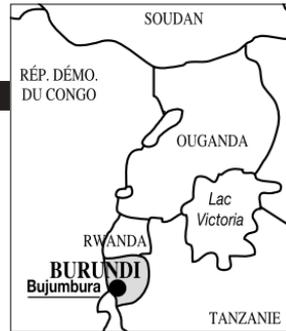
- Etude sur l'impact d'Internet en Birmanie
www.firstmonday.dk/issues/issue6_5/krebs

Burundi

POPULATION : 6 502 000

INTERNAUTES : 6 000

FOURNISSEURS D'ACCÈS PRIVÉS : OUI



Début janvier 2002, plusieurs journalistes de l'agence de presse en ligne *In-Burundi.net* sont brutalisés par des gendarmes à Bujumbura. Ils enquêtaient sur la torture d'un vigile par des agents de la Documentation nationale (services de renseignements). Celui-ci avait été arrêté dans le cadre de l'assassinat de Kassi Malan, le représentant de l'Organisation mondiale de la santé (OMS) au Burundi en décembre 2001. Les gendarmes menacent les journalistes de "subir le même sort".

Le 26 août, le Conseil national de la Communication (CNC) interdit aux sites Internet des médias burundais d'héberger "des documents ou autres communiqués d'organisations politiques faisant la propagande de la haine et de la violence". Cette mesure vise notamment le site de l'agence *Net Press, Rugamba*, dont une rubrique publie des communiqués de mouvements d'opposition. Le CNC menace de fermer l'agence *Net Press* si le site *Rugamba* ne cesse pas "toute reproduction de document ou déclaration (...) portant atteinte à la paix et à la sécurité publique".

LIENS :

- L'agence de presse en ligne *In-Burundi.net*
www.in-burundi.net
- *Rugamba*, le site de l'agence *Net Press*
www.netpress.bi



Canada

POPULATION : 31 153 000

INTERNAUTES : 15 200 000

FOURNISSEURS D'ACCÈS PRIVÉS : OUI

A la suite des attentats du 11 septembre, le Canada a adopté, le 18 décembre 2001, une loi antiterroriste qui met notamment à mal le principe de protection des sources journalistiques.

Cette loi modifie plusieurs textes, dont le Code criminel, la Loi sur la défense nationale, la Loi sur les secrets officiels et celle sur les droits de la personne. En modification du Code criminel, elle étend aux groupes terroristes les facilités de surveillance électronique jusqu'alors employées dans les enquêtes sur les organisations criminelles. Ainsi, dans le cadre d'une enquête sur des organisations terroristes, la police n'a plus à démontrer que la surveillance électronique est un dernier recours. La décision reste néanmoins soumise à l'approbation d'un juge de la Cour supérieure. La période de validité de l'autorisation d'interception des communications passe quant à elle de 60 jours à un an.

Une modification apportée à la Loi sur la défense nationale permet au ministre de la Défense nationale d'autoriser le Centre de la sécurité des télécommunications (CST) à "intercepter des communications privées [y compris électroniques] liées à une activité ou une catégorie d'activité que [le ministre] mentionne expressément" (article 273.65.1). De fait, le principe de la confidentialité des communications, et donc celui de la protection du secret des sources journalistiques, sont battus en brèche. Néanmoins, les activités du CST "ne peuvent viser des Canadiens ou toute personne au Canada".

En outre, le 25 août 2002, le gouvernement a lancé une consultation sur l'adaptation aux technologies modernes des législations permettant "l'accès légal" des enquêteurs à des documents privés, au nom de la défense de "la sécurité et du bien-être" des Canadiens. "Il est proposé que tous les fournisseurs de services Internet soient tenus de s'assurer que leurs systèmes ont la capacité technique de fournir un accès légal aux organismes d'application de la loi et de sécurité nationale", expose le document officiel. Autrement dit : les fournisseurs d'accès seraient obligés de stocker certaines données sur leurs abonnés et d'en donner l'accès aux enquêteurs.

Par ailleurs, le texte rappelle que le Code criminel interdit d'intercepter volontairement une communication privée. Mais pour justifier une éventuelle interception des

e-mails, il souligne que "lorsqu'une communication est consignée par écrit, il ne s'agit plus réellement d'une communication privée" étant donné que "le document peut facilement se retrouver entre les mains d'un tiers".

Ces propositions ont été violemment critiquées par George Radwanski, commissaire à la protection de la vie privée, dans un rapport publié fin janvier 2003. "Le gouvernement utilise les événements du 11 septembre comme excuse pour justifier de nouvelles collectes et utilisations de renseignements personnels sur nous tous", explique-t-il. D'après ce dernier, de telles mesures "n'ont pas leur place dans une société libre et démocratique" et témoignent du "mépris du gouvernement pour des droits à la vie privée".

LIENS :

- Electronic Frontier Canada
www.efc.ca
- La Ligue des droits et libertés
www.liguedesdroits.ca
- Le site du commissaire à la protection de la vie privée
www.privcom.gc.ca
- Le Centre de la sécurité des télécommunications
www.cse-cst.gc.ca
- Le Conseil de la radiodiffusion et des télécommunications canadiennes
www.crtc.gc.ca
- La Loi antiterroriste C-36
www.parl.gc.ca/37/1/parlbus/chambus/house/bills/government/C-36/C-36_4/C-36_cover-F.html
- Texte sur l'accès légal
http://canada.justice.gc.ca/fr/cons/la_al



Chine

POPULATION : 1 284 972 000

INTERNAUTES : 59 100 000

FOURNISSEURS D'ACCÈS PRIVÉS : NON
 INTERNAUTES ET CYBERDISSIDENTS EMPRISONNÉS : 42

Si le nombre d'internautes chinois double pratiquement tous les six mois, et celui des sites tous les ans, cette croissance fulgurante de la Toile s'accompagne d'un effort de contrôle, de censure et de répression à la mesure de cette dynamique. Lois liberticides, cyberdissidents emprisonnés, sites bloqués, surveillance des forums de discussion, cybercafés fermés, toute la panoplie répressive est utilisée pour museler le Réseau.

Le développement exceptionnel d'Internet ne permet plus techniquement de contrôler le contenu des millions d'e-mails qui transitent dans le pays. Pour autant, les autorités n'ont pas renoncé à interdire aux internautes chinois de se rendre sur des sites jugés dangereux pour "l'ordre social et le système socialiste". A cet effet, elles se sont dotées d'un arsenal juridique destiné à punir la cybercriminalité et la cyberdissidence.

En janvier 2001, l'agence de presse officielle *Xinhua* a annoncé que toute personne "impliquée dans des activités d'espionnage telles que "voler, découvrir, acheter ou divulguer des secrets d'Etat", grâce entre autres à Internet, risque une condamnation à mort ou une peine de prison allant de dix ans à la perpétuité. Le même mois, le ministère de la Sécurité publique a créé un site d'informations sur les lois en vigueur qui avertit les internautes des risques qu'ils encourent s'ils diffusent des informations "subversives". Cela concerne autant les douze millions de Chinois qui possèdent un ordinateur connecté au réseau que les utilisateurs des cybercafés.

Début janvier 2002, le ministre de l'Information et de la Technologie a mis en place une nouvelle régulation en matière de surveillance sur Internet. Les fournisseurs d'accès opérant dans des "domaines stratégiques et sensibles", notamment les sites d'actualité ou les forums, doivent désormais enregistrer des renseignements sur leurs visiteurs tels leurs identifiants Internet, leurs adresses postales ou leurs numéros de téléphone. Il leur est également ordonné d'installer des systèmes logiciels permettant de surveiller et de copier le contenu des e-mails "sensibles". Selon cette nouvelle loi, les fournisseurs d'accès doivent donc interrompre le transfert des courriers électroniques contenant des propos obscènes ou "subversifs", prônant le

terrorisme ou menaçant la sécurité et l'unité nationale. Les auteurs de ces e-mails doivent être dénoncés aux services du ministère de l'Information et de la Technologie, au ministère de la Sécurité publique et au bureau pour la protection des secrets d'Etat. Enfin, les fournisseurs d'accès doivent disposer de systèmes officiels, inaptes à l'espionnage ou au hacking. Cette législation complète la soixantaine de dispositions adoptées le 31 janvier 2001. Enfin, les compagnies étrangères qui vendent des logiciels en Chine doivent s'engager par écrit à ne pas installer des systèmes d'espionnage sur les ordinateurs chinois.

Les opérateurs et les responsables des sites d'information doivent ainsi censurer eux-mêmes les contenus contraires aux lois promulguées. Au sein des principaux sites, des employés ont pour mission de traquer les commentaires et autres messages subversifs. Pour autant, les forums de discussion restent un lieu privilégié d'échanges d'opinions politiques et de critiques de l'action gouvernementale. Si les responsables des sites ne pratiquent pas l'autocensure, les autorités s'en chargent. Ainsi, le moteur de recherche Google.com a été bloqué, en août 2002, pendant douze jours. Cette décision a provoqué des réactions très critiques des experts et des investisseurs étrangers et chinois, d'habitude moins disert sur les pratiques des autorités de Pékin en la matière.

Le 15 novembre, le gouvernement promulgue une loi sur l'exploitation des cybercafés, qui tient les propriétaires pour responsables des pages consultées par les clients. Ils risquent des fermetures administratives et des amendes.

Cette évolution autoritaire a conduit dix-huit intellectuels chinois à signer, en juillet 2002, une "déclaration des droits des internautes chinois". Ils demandent la liberté d'expression sur Internet (création de sites Internet), la liberté de l'information en ligne (accès à tous les sites) et la liberté d'association (création de cybercafés). L'un des initiateurs déclare à l'*Agence France-Presse* : " Si les grands sites se soumettent à la volonté du gouvernement chinois, cela affaiblira considérablement les capacités de résistance des organisations non gouvernementales qui ont trouvé un espace pour s'exprimer sur Internet." Cet acte fondateur d'un Internet chinois libre est soutenu par les signatures de milliers d'internautes chinois.

Confronté à un développement exponentiel d'Internet, le gouvernement chinois a définitivement tourné la page de la "Grande muraille électronique" pour s'engager dans la réalisation du "Bouclier doré". Ce projet très secret a été proposé par le ministère de la Sécurité publique et le ministère de l'Industrie de l'information. Des moyens financiers et humains importants - près de trente mille personnes - ont été mobilisés pour protéger l'Etat d'une utilisation subversive de l'Internet. Ainsi, en avril 2002, Jia Chunwang, alors le ministre de la Sécurité publique, a convoqué à Pékin une réunion de travail sur la sécurité et la protection des informations d'Etat. Les discussions ont porté sur les moyens de combattre les délits commis sur Internet, particulièrement les délits à caractère subversif. Selon des témoins présents à la réunion, le ministre aurait affirmé que "les organes de surveillance sur Internet sont devenus des outils indispensables à la sécurité nationale, à la stabilité politique et à

notre souveraineté". Les autorités, mécontentes de la diffusion d'articles critiques sur le web par le mouvement spirituel Falungong ou par le Parti démocrate chinois (PDC), ont décidé d'accélérer le recrutement de spécialistes chargés de combattre les "forces étrangères" qui tentent de "subvertir la Chine par Internet".

Fin décembre, le Département de la sécurité publique de la province de Guangdong (sud de la Chine) organise un Salon sur le développement d'Internet et la sécurité du Réseau qui vise à évaluer l'influence d'Internet sur la "stabilité et l'ordre public", selon le chef de la police de la province. Luan Guangsheng, responsable de la police d'Internet dans cette province, affirme à un journaliste du quotidien South China Morning Post de Hong Kong, qu'il faut "contrôler de façon stricte le réseau" et que "les internautes doivent assumer leur responsabilité dans la diffusion des informations dangereuses". Luan Guangsheng a en revanche refusé de préciser le nombre de cyberpoliciers dans la province de Guangdong, mais a reconnu que ses effectifs sont en "augmentation".

La répression s'abat sur les cyberdissidents

Les autorités chinoises n'ont pas mis en place ce cadre juridique particulièrement rigide et liberticide dans le seul but de dissuader les cyberdissidents. La répression s'abat sur ceux qui usent du Net pour tenter de s'exprimer, de s'informer librement ou de critiquer le gouvernement et le Parti communiste. Au moins vingt-six cyberdissidents sont emprisonnés en Chine. Seize d'entre eux ont été condamnés à des peines de prison ferme.

Au cours du printemps 2001, Liu Weifang, commerçant, est condamné par un tribunal de la province de Xinjiang (Nord-Ouest), à trois ans de prison pour "subversion". Il est accusé d'avoir publié sur des forums de discussion, en 2000 et 2001, plusieurs articles très critiques envers le Parti communiste chinois et sur les réformes économiques entreprises par le gouvernement. Malgré l'utilisation d'un pseudonyme, Lgwf, la police est parvenue à l'identifier.

Le 11 mars, Lu Xinhua est interpellé à Wuhan (centre du pays). Selon le Centre d'information pour les droits de l'homme et de la démocratie, il a été formellement arrêté le 20 avril et accusé de "subversion". Lors de son arrestation, le 11 mars, la police a mis à sac son domicile et confisqué son ordinateur. Lu Xinhua est l'auteur de nombreux articles, parus sur des sites Internet étrangers, faisant état de violations des droits de l'homme à Wuhan et critiquant ouvertement le président chinois Jiang Zemin. En décembre, Lu Xinhua, membre du Parti démocrate chinois (PDC, illégal et dont les principaux leaders sont derrière les barreaux), est condamné à quatre ans de prison par la Cour intermédiaire de Wuhan à l'issue d'un procès tenu à huis clos.

Le 13 mars, Yang Zili, fondateur du site Internet lib126.com, est arrêté à Pékin alors qu'il sort de chez lui. Le même jour, sa femme est interpellée puis libérée 48 heures plus tard après avoir été obligée de s'engager par écrit à ne pas révéler l'affaire. Yang Zili, 30 ans, diplômé de la prestigieuse Université de Pékin, est l'auteur d'une série

d'articles théoriques diffusés sur son site, dans lesquels il prend position pour le libéralisme politique, critique la répression contre le mouvement spirituel Falungong et dénonce les difficultés des paysans. Dans un poème, il appelle à "asséner un coup fatal" au "spectre du communisme". La police a refusé de révéler les raisons et le lieu de l'incarcération de Yang Zili. Le même jour, trois autres animateurs du site lib.126.com, Jin Haike, ingénieur en géologie, Xu Wei, journaliste du *Quotidien du consommateur* et Zhang Honghai, journaliste free lance, sont arrêtés à Pékin par la police. Le 28 septembre 2001, les quatre cyberdissidents comparaissent devant la Cour populaire intermédiaire de Pékin. Alors que le procès devait être ouvert au public, la cour décide de n'accorder que trois accès individuels. Trois des quatre accusés sont représentés par un avocat. Seul Zhang Honghai choisit de se défendre lui-même. L'avocat de Jin Haike, Liu Dongbin, souligne que les témoignages des personnes citées par l'accusation sont discutables, car ils ont déjà été cités plusieurs fois dans des affaires similaires. Yang Zili établit que les chefs d'accusation "n'impliquent en aucun cas l'idée de subversion du pouvoir d'Etat. Quand nous parlons de liberté et de libéralisation, nous pensons que cela arrivera par des réformes. Est-ce que les vingt dernières années de réforme et d'ouverture ne peuvent pas être considérées comme une voie de libéralisation de la Chine ?" Les quatre dissidents rejettent également l'accusation selon laquelle ils bâtitaient des ramifications de leur groupe dans tout le pays par la publication d'articles sur Internet et la création de sites web. Selon Zhang Honghai, "rien dans le réquisitoire du procureur ne démontre que nous planifions de renverser le pouvoir. Nous ne possédions même pas les 300 yuans nécessaires à l'ouverture du site. Comment cela pourrait-il constituer une atteinte à l'autorité de l'Etat ?"

Dans son réquisitoire, le procureur affirme que les articles publiés sur Internet, notamment "Devenir un nouveau citoyen, réformer la Chine" et "Ce qui doit être fait", sont subversifs car ils accusent la Chine de "pratiquer une fausse forme de démocratie", demandent la "fin d'un système désuet" et affirment leur intention d'établir "une nouvelle Chine". Après une audition de quatre heures, la cour se retire sans avoir prononcé de verdict.

Le 17 avril, Chi Shouzhu, ouvrier et ancien prisonnier politique, est arrêté par la police dans la gare de Changchun (nord-est du pays). Il venait d'imprimer chez un ami des documents d'un site Internet dissident basé à l'étranger. Chi Shouzhu, âgé de 41 ans, a déjà passé dix ans en prison pour avoir participé au printemps de Pékin de juin 1989. Originaire de Jilin (Nord-Est), il s'était rendu à Changchun pour soigner des maladies contractées en prison. Cette arrestation, révélée par le Centre d'information sur les droits de l'homme et la démocratie, n'est pas confirmée par les autorités.

Le 18 avril, Leng Wanbao, un dissident de la province de Jilin (nord-est du pays), est interrogé pendant plus de deux heures par la police qui lui reproche la parution "d'articles subversifs" sur Internet.

Wang Sen, membre du Parti démocratique chinois, est arrêté le 30 avril à Dachuan, (province du Sichuan, sud-ouest du pays). Il aurait accusé dans un texte diffusé sur

Internet un centre médical public d'avoir vendu des médicaments contre la tuberculose donnés par la Croix-Rouge. Le 30 mai 2002, Wang Sen est condamné à dix ans de prison par la Cour intermédiaire populaire de Dazhou pour "tentative de renversement du pouvoir". La justice lui reproche également d'avoir organisé une manifestation d'ouvriers dans une usine de fer et d'acier de Dazhou.

Le 9 mai, Wang Jinbo est arrêté par la police de Junan (province du Shandong, est du pays). Selon l'*Agence France-Presse*, les policiers ont déclaré au père de Wang Jinbo que ce dernier faisait l'objet d'une mesure de détention de quinze jours pour "avoir diffamé la police locale sur Internet". Wang Jinbo, âgé de 29 ans et membre du Parti démocratique chinois, a déjà été arrêté à plusieurs reprises pour ses activités politiques. Le 13 décembre, il est reconnu coupable de "subversion" par le tribunal intermédiaire de Linyi (province du Shandong) et condamné à quatre ans de prison pour avoir envoyé par courrier électronique des articles critiquant l'attitude des autorités face au mouvement démocratique de 1989. Le procès s'était déroulé en novembre. Selon un juge siégeant à la cour, le dissident compte faire appel. Wang Jinbo a cessé de s'alimenter le 28 février 2003 à l'occasion de l'ouverture de l'Assemblée nationale populaire à Pékin. "Il entend ainsi exprimer son mécontentement par rapport à sa condamnation", a expliqué Ren Wanding, un ancien prisonnier politique, à des médias internationaux basés à Pékin. Le cyberdissident arrête sa grève de la faim une semaine plus tard. Selon ses proches, son état de santé s'est dégradé en 2003.

Le 18 mai, Hu Dalin, homme d'affaires et webmaster, est arrêté par la police de Shaoyang (Sud-Ouest) pour avoir publié en ligne des articles anti-américains écrits par son père. Aucune charge concrète n'ayant été retenue contre lui, la police a notifié à sa famille qu'il avait été interpellé pour "activités subversives sur Internet". Au cours des premiers mois de sa détention, ni ses parents ni sa fiancée n'ont été autorisés à lui rendre visite.

A la même période, Guo Quinghai, employé de banque âgé de 36 ans, est condamné à quatre ans de prison par le tribunal de Cangzhou (sud de Pékin) pour "subversion". Sa famille n'a pas été informée de la date de l'audience. Il serait détenu dans la prison de Cangxian, près de Cangzhou. Il avait été interpellé en septembre 2000 pour avoir publié sur des sites Internet étrangers des articles en faveur de la réforme politique et de la libération du cyberdissident Qi Yanchen. Bien qu'utilisant un pseudonyme, la police l'avait identifié.

Courant juin, Li Hongmin est arrêté à Canton (sud de la Chine) pour avoir divulgué par e-mail la version chinoise 2001 des "Archives de Tiananmen". Le texte évoque les responsabilités de certains hauts responsables chinois dans le massacre de la place Tiananmen en juin 1989. Selon le site dissident VIP Reference, basé aux Etats-Unis, Li Hongmin a été libéré quelques semaines après son arrestation mais a perdu son travail suite aux pressions des autorités.

Fin juin, les autorités annoncent que le procès de Huang Qi, fondateur du site 6-4tianwang arrêté un an auparavant pour avoir diffusé des informations "subversives"

sur son site Internet, est de nouveau reporté sine die par le tribunal intermédiaire de Chengdu (sud-ouest du pays). Un porte-parole a justifié cette décision en raison de la célébration du 80e anniversaire de la création du Parti communiste chinois. Mais selon de nombreux observateurs, il s'agit, pour le régime de Pékin, d'éviter d'attirer l'attention de l'opinion publique internationale avant la décision de Moscou concernant l'attribution des Jeux olympiques de 2008. Déjà, le 13 février 2001, les juges avaient suspendu le procès en raison de l'état de santé de Huang Qi. Sa femme, Zeng Li, déclare alors que son mari a été frappé en prison et porte une cicatrice au front. Il a également perdu une dent à la suite des coups qui lui ont été infligés. Cette dernière n'a pas été autorisée à lui rendre visite et son avocat ne l'a vu qu'une seule fois en sept mois. Mi-août, Fang Jung, l'avocat de Huang Qi, révèle que le procès "s'est tenu à huis clos et dans le plus grand secret". Il s'est achevé après seulement deux heures d'audience. Le verdict n'a pas été rendu public. Aucun membre de la famille du cyberdissident n'a été autorisé à assister aux audiences. L'épouse de Huang Qi s'est vu confisquer son appareil photo pour avoir pris un cliché de son mari conduit dans la salle du tribunal. Le procès de Huang Qi est le premier intenté à un créateur d'un site Internet pour avoir diffusé des informations "subversives".

Le 11 juillet, au lendemain de l'attribution des Jeux Olympiques d'été de 2008 à Pékin, Yan Peng, un dissident âgé de 38 ans et vendeur de matériel informatique, est arrêté dans la province du Guangxi (sud du pays). Selon le Centre d'information sur les droits de l'homme et la démocratie, il revenait d'un voyage organisé au Viêt-nam. Il est accusé d'avoir violé les lois sur l'émigration. Son ordinateur lui a été confisqué. Le 16 juillet, trois dissidents de Qingdao, dont Mu Chuanheng, tentent d'intervenir en faveur de la libération de Yan Peng, mais la police refuse de les recevoir. Le dissident est connu pour être l'un des premiers à avoir utilisé Internet pour lutter contre la dictature du Parti communiste chinois. Il a été incarcéré à plusieurs reprises depuis 1989. En septembre 2002, Yan Peng est condamné à dix-huit mois de prison par une cour de Qingdao.

Mi-août, Mu Chuanheng, avocat mais dans l'interdiction d'exercer sa profession depuis quinze ans, est interpellé à Qingdao (est du pays) pour avoir réclamé publiquement la libération de son ami Yan Peng (voir plus haut). L'ordinateur de Mu Chuanheng ainsi que plusieurs de ses écrits sont saisis à son domicile par une douzaine de policiers. Le dissident a notamment participé au premier "Printemps de Pékin" en 1979. Il a largement contribué au site culturel xinwenming.net, interdit en août 2000 par le ministère de la Sécurité d'Etat. En septembre 2002, Mu Chuanheng est condamné à trois ans de prison par une cour de Qingdao.

En septembre, Zhu Ruixiang, avocat, cofondateur et ancien rédacteur en chef de la radio Shaoyang, est reconnu coupable de "subversion" par le tribunal de Shaoyang (province du Hunan, sud-est de la Chine), pour avoir fait parvenir à douze de ses amis des articles du quotidien prodémocratique en ligne *VIP Reference* (www.bignews.org) critiquant le gouvernement. Il est condamné en première instance à neuf mois de prison, mais les autorités chinoises demandent aux magistrats d'être plus sévères. Le cyberdissident écope finalement d'une peine de trois ans de

prison. Lors de son arrestation le 8 mai, tous ses biens, dont son ordinateur, lui ont été confisqués par la police de Shaoyang.

Le 27 avril 2002, Yang Jianli, rédacteur en chef de la revue électronique dissidente *Yibao* (www.chinaeweekly.com) basée aux Etats-unis, est interpellé à l'aéroport de Kuming (province du Yunnan, sud du pays). Il est formellement arrêté le 2 juin 2002. Il revenait pour la première fois en Chine depuis son expulsion en 1989, avec un passeport emprunté à un ami après que les autorités chinoises avaient refusé de renouveler le sien. Inscrit sur liste noire depuis plusieurs années par les autorités de Pékin, Yang Jianli, né en 1963, est entré clandestinement en Chine afin d'enquêter sur des grèves ouvrières dans le nord-est du pays. Il serait détenu dans une prison de Pékin. Son frère, Yang Jianjun, s'est lui-même rendu à Pékin en juin et s'est heurté au refus de la police de dévoiler tout renseignement concernant la captivité de Yang Jianli. Marié à Fu Xiang et père de deux enfants, il réside à Brooklyn, dans le Massachusetts.

Le 24 juin, Li Dawei est condamné à onze ans de prison par un tribunal de la province du Gansu (nord-ouest du pays). Selon le Centre d'information sur les droits de l'homme et la démocratie, il est reconnu coupable d'avoir tenté de "subvertir le pouvoir d'Etat". Cet ancien policier est accusé d'avoir téléchargé plus de cinq cents textes sur des sites de démocrates chinois basés à l'étranger. Il les aurait ensuite édités en différents livres. Li Dawei aurait par ailleurs été en contact avec des organisations "réactionnaires" basées à l'étranger. Li Dawei, âgé de quarante ans, avait été arrêté en avril 2002 et son procès avait débuté en mai dernier. Son avocat, Dou Peixin, a affirmé que la plus haute cour provinciale avait accepté son appel.

En août, Chen Shaowen est interpellé par la police de Lianyuan, dans la province du Hunan (centre du pays). Il est formellement arrêté en septembre. Il serait emprisonné pour avoir publié sur le Net "de nombreux articles et essais réactionnaires", a déclaré un officiel à l'agence *Associated Press*. Le journaliste est un collaborateur régulier de plusieurs sites en langue chinoise basés à l'étranger, pour lesquels il avait écrit des articles concernant entre autres les inégalités sociales, le chômage et les écueils du système judiciaire.

Le 24 août, Wan Yanhai, fondateur de l'association Aizhi Action Project et du site aizhi.org qui œuvrent depuis 1994 contre la discrimination à l'encontre des victimes du sida et pour la liberté d'information sur Internet, est détenu au secret pendant près d'un mois par des agents du ministère de la Sécurité publique à Pékin. L'association Aizhi Action Project a contribué à faire connaître le scandale du sang contaminé dans la province du Henan (centre du pays), en publiant notamment sur son site les noms de paysans de la province morts du sida après avoir vendu leur sang. Le site, toujours accessible, comporte également des témoignages accablants sur la situation des séropositifs chinois. En juillet dernier, l'université qui hébergeait Aizhi Action Project a fermé les locaux de l'association qui a ensuite été interdite. Le 17 juillet, Wan Yanhai avait cosigné la "Déclaration des droits des internautes chinois", appelant à la liberté d'expression sur Internet. Début août, Wan Yanhai

réaffirmait sa volonté de continuer à informer sur le sida grâce à Internet alors que venait d'entrer en vigueur une loi interdisant la diffusion d'informations sur le sujet. Malgré certaines récentes ouvertures, le sida, notamment dans la province du Henan, est un sujet tabou en Chine.

Début novembre, Li Yibin, âgé de vingt-huit ans et diplômé en science informatique, est arrêté par la police de Pékin. Selon l'organisation de défense des droits de l'homme Human Rights in China, son arrestation fait suite à la publication du journal *Démocratie et liberté*, qu'il avait mis en ligne sous les pseudonymes "Printemps" ou "Neige de printemps".

Le 7 novembre, à la veille de l'inauguration du seizième Congrès du Parti communiste chinois, Liu Di, une étudiante en psychologie âgée de vingt-deux ans, est arrêtée sur le campus de l'université de Pékin. Sa famille n'a été informée de son arrestation que lorsque la police est venue procéder à une fouille de son domicile, saisissant ses notes, ses livres et son ordinateur. Ses proches, qui se sont déplacés au poste de police pour lui apporter des vêtements de rechange, n'ont pas été autorisés à voir la jeune femme. Les autorités n'ont pas confirmé sa détention, mais la police a affirmé à un professeur de Liu Di qu'elle était emprisonnée en raison de ses liens avec une "organisation illégale". Cependant, le père de l'étudiante affirme que son arrestation serait due à ses écrits diffusés sur Internet. Sous le pseudonyme "La souris inoxydable", Liu Di a encouragé les internautes à "ignorer la propagande du régime chinois" et à "vivre en toute liberté". Elle a également critiqué l'arrestation de Huang Qi, le créateur d'un site Internet, détenu depuis le 3 juin 2000 pour avoir mis en ligne des articles considérés comme subversifs par les autorités.

Le 4 décembre, la police de Chengdu (capitale de la province du Sichuan au sud-ouest de la Chine) arrête Ouyang Yi, responsable d'un site Internet, enseignant et membre du Parti démocrate (interdit). Selon l'organisation dissidente China Labor Watch qui a révélé cette arrestation, sa femme a été informée de l'arrestation de son époux par la police locale qui a perquisitionné le domicile familial à Suining, à près de 200 kilomètres de Chengdu, sur ordre de la police de la capitale provinciale. Ouyang Yi, âgé de trente-quatre ans, est un dissident bien connu des autorités. Il est l'un des 192 signataires d'une lettre ouverte adressée au seizième Congrès du Parti communiste chinois en novembre dernier appelant le Parti à revenir sur sa condamnation des protestations de la place Tiananmen de 1989. Dans ses articles diffusés sur Internet, il écrit sur le second Printemps de Pékin de 1989, l'échec des politiques économiques chinoises ou les nécessaires réformes de l'appareil d'Etat communiste. En raison de ses activités militantes, Ouyang Yi a déjà été interpellé par la police en 1996, 1998, 1999, et dans le courant 2002. Jusqu'à présent, ses détentions n'avaient pas excédé quarante-huit heures.

Le 18 décembre au matin, Liao Yiwu est arrêté par la police à son domicile de Chengdu, dans la province du Sichuan, au sud-ouest du pays. Il est relâché quelques heures plus tard, mais son domicile a été fouillé. Ecrivain et poète, âgé de quarante-deux ans, Liao Yiwu a commencé à diffuser des articles sur Internet dès lors que ses

écrits ont été interdits de publication par les autorités chinoises. Son engagement lui a valu un harcèlement régulier de la part des autorités.

Début mars 2003, Reporters sans frontières apprend que Qi Yanchen, détenu à la prison N°4 de Shijiazhuang, dans la province du Hebei (au sud de Pékin), est dans un état de santé préoccupant. Souffrant de troubles chroniques, notamment de colite, Qi Yanchen ne reçoit de médicaments que par l'intermédiaire de sa femme, Mi Hongwu, autorisée à lui rendre visite seulement une fois tous les deux mois. Lors de sa dernière visite, mi-janvier, Mi Hongwu a trouvé son mari "très affaibli". Qi Yanchen a été condamné, en septembre 2000, à quatre ans d'emprisonnement suite à la publication sur Internet de larges extraits de son livre "L'effondrement de la Chine" qualifié de "subversif" par le procureur en charge du procès.

Le 12 mars, Zhang Yuxiang est arrêté à son domicile de Nanjing (province de Jiangsu, est de la Chine) et conduit au Bureau de la sécurité publique où il est longuement interrogé par la police au sujet d'articles qu'il a diffusés sur Internet. Les policiers tenteraient de lui faire avouer ses contacts avec d'autres cyberdissidents toujours en liberté. Selon l'organisation Human Rights in China, il aurait été placé en résidence surveillée dans un bâtiment public du district de Siyang, mais cette information n'a pas été confirmée par les autorités locales. L'épouse de Zhang Yuxiang est sans nouvelles de lui depuis son arrestation et n'a par ailleurs reçu aucun document officiel concernant sa détention. Zhang Yuxiang, ancien cadre du Département de la propagande des Forces aériennes de Nanjing, a déjà passé deux ans en prison pour avoir aidé au développement de la Fédération chinoise démocratique, une organisation dissidente. Depuis sa libération, M. Zhang continue à diffuser régulièrement des articles politiques sur Internet et à signer des pétitions.

Le 25 mars, un officier du Bureau de la sécurité publique de Pékin a confirmé l'arrestation et l'inculpation du cyberdissident Jiang Lijun. Il avait disparu depuis le 6 novembre 2002. Son épouse Yan Lina était sans nouvelles de lui depuis cette date. La police l'avait secrètement incarcéré dans la prison de Qincheng (près de Pékin), réputée pour avoir été le lieu de détention des plus importants prisonniers politiques. Il aurait été inculpé, le 14 décembre, d'"incitation au renversement du pouvoir de l'Etat". Mais la police n'a fourni aucun document officiel à Yan Lina. La police considérerait Jiang Lijun comme le chef d'un petit groupe de cyberdissidents. Sa femme a fait appel aux services d'un avocat de Pékin, Mo Shaoping, connu pour avoir défendu plusieurs dissidents.

Blocage de l'accès aux sites "subversifs"

Outre les arrestations et condamnations à de lourdes peines des cyberdissidents, le pouvoir chinois bloque également l'accès aux sites dont il juge le contenu "dangereux ou subversif." Cela vaut non seulement pour les rares sites qui tentent, au sein même de la République populaire, de véhiculer des discours ou idées progressistes, mais également pour les sites d'information étrangers. Aujourd'hui, la Chine a acquis avec la collaboration d'entreprises occidentales telles que Cisco, Nortel ou Sun, une

technologie très sophistiquée pour censurer l'accès à Internet. Par ailleurs, les sites implantés en Chine, notamment Yahoo!, ont appliqué, sans résistance, les consignes chinoises sur la censure du contenu. Yahoo! a ainsi signé en 2002 une Charte chinoise pour éliminer les informations "subversives".

Selon une étude du Centre Berkam de l'université d'Harvard, menée de mai à novembre 2002, sur 204 000 sites visités par le biais des moteurs de recherche Google ou Yahoo!, plus de 50 000 ont été inaccessibles au moins une fois, depuis au moins un endroit en Chine. Hormis les sites à caractère explicitement pornographique, ceux dont le contenu traite du Tibet, de Taïwan ou de démocratie, comptent parmi les plus censurés par les autorités chinoises. Ainsi, plus de 60 % des sites "Tibet" et plus de 47 % des sites "Taïwan" recensés sur Google sont bloqués.

Les sites sur la démocratie et les droits de l'homme, tels que ceux d'Amnesty International, Human Rights Watch, ou encore Hong Kong Voice of Democracy, constituent une cible privilégiée pour les censeurs. Le domaine de l'éducation est également sous strict contrôle : plusieurs sites d'universités américaines sont ainsi rendus inaccessibles, comme ceux de l'université de Columbia ou du Massachusetts Institut of Technology (MIT), parce que ces écoles hébergent des groupes prodémocratiques. Les sites sur la religion ou la santé en Chine sont également la cible de la censure.

Les versions en ligne de 923 médias, *BBC*, *CNN* ou *Time Magazine* par exemple, ont été recensées comme étant régulièrement bloquées. De même, des sites gouvernementaux, comme celui de Taïwan, ne sont pas accessibles depuis la Chine.

Et les restrictions n'en finissent pas de tomber. Ainsi, fin mars 2001, les utilisateurs d'ordinateurs de la région de Shanghai sont informés qu'il est interdit de diffuser des programmes radios ou télévisés sur le Net sans l'accord officiel du gouvernement. Un mois plus tôt, le ministère de la Sécurité publique a annoncé le lancement de nouveaux logiciels connus sous le nom d'"Internet police 110", spécialement créés pour empêcher l'accès à des sites ayant des contenus religieux, sexuel ou violent. Début mai 2001, l'entreprise publique de télécommunications Xinjiang Telecommunications annonce que, dorénavant, les portails Internet non officiellement enregistrés seront automatiquement fermés.

Le 18 juin, le magazine en ligne *Hot Topic* est suspendu après quatre ans d'activité. Ce magazine a notamment publié des articles critiquant le gouvernement. Il compte 235 000 abonnés.

En juin, le site du ministère des Affaires étrangères australien (www.dfat.gov.au), inaccessible pour les internautes chinois depuis plus d'un an, reparait brièvement le temps de la visite à Pékin du ministre de la Communication australien, Richard Alston. Le porte-parole du gouvernement chinois écarte toute volonté de censure et invoque des incidents techniques à l'origine de ce blocage. Mais, selon les observateurs, les informations diffusées sur le site, notamment en matière de droits de l'homme et de risques de conflit dans certaines régions de Chine, en sont la cause véritable. En

juillet, le site est à nouveau accessible. Son rétablissement fait suite à l'appel lancé par le ministre australien des Affaires étrangères au chargé d'affaires chinois en poste à Canberra, Xie Xiaoyan.

Depuis le début du mois de juillet et pendant plusieurs semaines, les pages en mandarin du site Web de *Radio France Internationale (RFI)* sont inaccessibles aux internautes. La direction de RFI a demandé des explications au gouvernement chinois.

En août, ce sont les sites pourtant proches du Parti communiste, *China Bulletin*, magazine politique d'information en ligne, et *Tianya Zongheng*, un forum Internet basé à Haikou (province du Hainan), qui sont fermés. Les autorités leur reprochent d'avoir publié des articles critiquant le président Jiang Zemin et plus précisément, sa volonté d'ouverture économique.

Le 4 septembre, les sites de la chaîne de télévision américaine *CNN*, du quotidien *International Herald Tribune*, de la radio française *RFI*, de la radio britannique *BBC*, du site de la section américaine d'Amnesty International et des liens vers des organisations humanitaires (Médecins sans frontières par exemple) sur des portails chinois, sont bloqués par les autorités chinoises à la veille d'une visite du président Jiang Zemin en Corée du Nord. Motif : ces médias contiennent des informations sur la famine et la répression dans ce pays allié de Pékin.

Le 6 septembre, le bulletin en ligne *Baiyun Huanghe* (bbs.whnet.edu.cn) de l'université de Science et de Technologie de Huazong (centre du pays) est fermé sur ordre du Conseil d'Etat, suite à la diffusion par des étudiants d'articles sur le massacre de la Place Tiananmen en 1989. *Baiyun Huanghe* a été créé voilà cinq ans et compte trente mille abonnés. Le bulletin en ligne s'intéresse de très près à la politique et particulièrement aux affaires de corruption. Jusqu'en 2001, les étudiants pouvaient librement échanger sur le forum leurs opinions à propos de sujets tabous comme le Printemps de Pékin. L'accentuation du contrôle de l'information par le Parti a finalement eu raison de cet espace de dialogue jugé "subversif" par les autorités.

En octobre, les sites suivants sont toujours interdits aux internautes chinois : hrichina.org (site de Human Rights Watch en Chine), hrw.org (site de Human Rights Watch), amnesty.org, amnesty.org.uk, amnestyusa.org (sites d'Amnesty International), freetibet.org (site de l'organisation Freetibet), tibet.com (site du gouvernement tibétain en exil), cnn.com (site de la chaîne d'information américaine *CNN*), bbc.co.uk (site de la *BBC*), washingtonpost.com (site du quotidien *Washington Post*), 6-4tianwang.com (site du cyberdissident Huang Qi) et bignews.com (site du journal dissident en ligne *VIP Reference*).

Le 16 octobre, le forum de discussion Zhejiang, réservé aux journalistes chinois sur le site Xici.net, est fermé par les autorités. Le site est accusé de "diffusion d'informations subversives", de "diffamation à l'encontre d'hommes d'Etat et de corps constitués". Sous la pression des autorités, le webmaster du forum est licencié et les responsables du site doivent renforcer leur contrôle sur les autres forums. Les autorités ont refusé de

répondre aux questions de la presse étrangère sur la fermeture de Zhejiang qui intervient lors de la tenue du sommet de l'APEC à Shanghai.

Le 29 octobre, à l'issue de la visite officielle à Shanghai du président Georges Bush, les autorités bloquent de nouveau l'accès aux sites de plusieurs médias américains dont ceux de *CNN* et du *Washington Post*. Le 16 octobre, elles avaient pourtant débloqué l'accès aux sites du *New York Times* et du *Washington Post*, à l'occasion de l'ouverture du Forum de coopération économique Asie Pacifique (APEC) de Shanghai.

Le 16 mars 2002, l'Association chinoise de l'Internet, l'organe national en charge d'Internet, lance un "pacte d'autodiscipline" qui interdit à ses signataires de produire ou de relayer des informations "nuisibles à la sécurité nationale et à la stabilité sociale". En juillet, l'agence officielle *Chine nouvelle* annonce que les principaux sites web chinois, notamment Yahoo!, et fournisseurs d'accès à Internet ont signé un "pacte d'autodiscipline", par lequel ils s'engagent à pratiquer l'autocensure du contenu mis en ligne.

En avril, le webmaster du site Internet du service en chinois de la radio *Voice of America*, basée à Washington, constate une attaque électronique venant de Chine populaire. Des e-mails contenant des virus et des tentatives de piratage s'abattent sur le site. "Nous pensons que ces virus ont été spécialement créés pour cette attaque organisée en Chine", affirme le webmaster. Les responsables de sites dissidents chinois, de Falungong et d'organisations pro-tibétaines sont également attaqués. Certains ont pu tracer l'origine de ces attaques jusqu'à des comptes appartenant à des bureaux en province de la compagnie publique China Telecom.

Le 23 avril, la chaîne de télévision australienne *ABC* annonce que l'accès à son site Internet est bloqué par les autorités chinoises. La direction de la chaîne publique a déposé une plainte auprès du ministre des Affaires étrangères chinois et contre le Département de sécurité publique. Un responsable de l'ambassade d'Australie a déclaré que le barrage aurait été installé après des discussions au sein des plus hautes sphères de l'Etat, ce qui a aussitôt été démenti par un porte-parole du gouvernement. La visite du dalaï-lama en Australie en mai pourrait expliquer cette mesure de répression.

Le 16 mai, des journalistes basés à Pékin et à Shanghai constatent que les sites Internet de médias internationaux, notamment ceux de l'agence *Reuters*, de la chaîne de télévision *CNN* et du quotidien *Washington Post*, sont de nouveau accessibles aux internautes chinois. Les autorités n'ont pas confirmé la levée de cette censure. En revanche, les sites de la *BBC*, de *Time Magazine* et de *Voice of America* restent interdits aux Chinois. Selon un diplomate occidental basé à Pékin, cité par l'agence *Reuters* : "Les autorités chinoises ont peut-être réalisé qu'il était très facile de contourner leurs barrières. Il est alors plus efficace pour eux de laisser passer et ensuite de contrôler la consultation de ces sites."

Au début du mois de juin, trois sites, Tom.com, Sina.com et FM365.com, reçoivent une

“sanction administrative” par les autorités de Pékin pour avoir publié des “contenus inconvenants” sur la répression du printemps de Pékin de juin 1989. *Le Quotidien de Pékin* affirme que ces sanctions font suite à l’inspection par la police des bureaux de neuf des principaux portails chinois. *Le Quotidien de la jeunesse de Pékin* affirme pour sa part que la police va vérifier trois fois par semaine le contenu des 827 principaux portails chinois, et cela pendant trois mois. Ces mesures tentent de prévenir la publication d’informations “subversives” sur les événements de juin 1989.

Le 31 août 2002, Google.com est interdit aux internautes chinois. Le moteur de recherche est devenu très populaire en Chine, en raison de sa simplicité d’utilisation et de son efficacité à mener des recherches en langue chinoise. De nombreuses voix s’élèvent contre ce blocage dans les forums en ligne, les internautes soulignant qu’ils utilisaient Google.com pour faire de “la recherche et non de la politique”. Plus étonnant, les investisseurs étrangers et chinois, normalement très discrets sur la censure d’Internet, ont critiqué cette décision. “Ils se tirent dans le pied”, commente un Européen travaillant pour le gouvernement chinois, tandis que les responsables de Google.com négocient avec les autorités chinoises qui se refusent à tout commentaire. Les raisons du blocage restent mystérieuses. Certains évoquent le quatorzième résultat proposé par Google.com à la recherche “Jiang Zemin” : un jeu interactif baptisé “Abattez le vilain dictateur Jiang Zemin”. Un affront pour un Président sur le départ qui tente d’entrer dans le panthéon des leaders communistes chinois.

Le 6 septembre, AltaVista est le second moteur de recherche interdit de cité sur le Réseau chinois.

A partir du 7 septembre, les internautes chinois qui tentent de se connecter sur Google.com sont automatiquement dirigés vers des moteurs de recherche chinois, notamment Tianwang et Baidu.

Le 12 septembre, l’accès à Google depuis la Chine est restauré. Le moteur de recherche fait cependant l’objet d’une censure sélective. Selon les spécialistes, le tollé général qui avait accueilli la suspension et les pressions des milieux d’affaires sont à l’origine de ce revirement. “Le ministère n’a reçu aucune information sur le blocage de Google et nous ne savons rien non plus sur la levée d’un blocage”, a déclaré un responsable du ministère de l’Industrie de l’information. AltaVista, comme des dizaines d’autres sites, est toujours inaccessible.

En septembre, les internautes constatent la mise en place de nouveaux “logiciels renifleurs” qui bloquent l’accès à certaines pages des sites consultés. Ainsi, les articles sur la Chine - notamment sur la question du Tibet, de Taiwan ou des droits de l’homme - des sites des journaux étrangers sont bloqués. Les autres pages restent accessibles. Le 27 septembre, le journaliste Michael Jen-Siu du quotidien *South China Morning Post*, publié à Hong Kong, constate que cette censure sélective s’applique aux e-mails envoyés à partir de messageries telles que Hotmail, aux moteurs de recherche tels que Google.com et aux sites d’information étrangers tels que *CNN*. La majorité des pages répertoriées par Google à la recherche “Falungong” sont inaccessibles. Le message “Cette page ne peut être affichée” apparaît. Les autorités chinoises ont nié la mise en place de cette censure sélective.

En octobre, la division des crimes informatiques de la province de Jiangxi (sud-est du pays) ordonne à plus de trois mille cafés Internet de la province de vendre des cartes d'accès à leurs clients. Ces cartes doivent permettre à la police de vérifier les sites consultés par les internautes. L'un des responsables de ce projet affirme que ce système expérimental donne plus de pouvoir pour prévenir les crimes et identifier les criminels sur Internet.

Début janvier 2003, les autorités chinoises bloquent l'accès au site américain blogspot, spécialisé dans la mise en ligne de journaux intimes et utilisé par plus d'un million de personnes à travers le monde. Jason Shellen, directeur de cette start-up installée dans la Silicon Valley (Californie), assure qu'il ne s'agit pas de problèmes techniques mais bien d'un acte de censure, visant à empêcher les cybernautes chinois de consulter les divers services offerts par le site. Mais d'après l'une des utilisatrices chinoises de blogspot citée par l'agence de presse Reuters, le blocage de ce site n'aura pas les effets désirés : "Les 'bloggers' qui ont quelque chose à dire ne se laisseront pas dissuader par cette interdiction. Nous trouverons d'autres moyens."

Enfin, le 14 avril 2003, des internautes signalent que le site de Reporters sans frontières (www.rsf.org) est inaccessible depuis la Chine. Ce blocage pourrait être lié à la présence, en une du site, d'un communiqué sur l'emprisonnement prolongé de la jeune internaute Liu Di.

Filtres, nettoyage et surveillance sur les forums de discussion

Les principaux sites d'informations disposent de forums de discussion fréquentés par des centaines de milliers d'internautes et qui se veulent des "espaces d'expression libre". Mais par la volonté des autorités chinoises, ils sont également devenus de véritables pièges pour internautes. En effet, une dizaine de personnes ont été arrêtées par la police après avoir posté sur des forums des articles critiques du gouvernement.

Les forums de discussion chinois utilisent un système de filtres qui leur permet de trier les messages en deux catégories : ceux qui contiennent des mots interdits et les autres. Les premiers sont systématiquement détournés. Ils n'apparaissent pas sur le forum même si, de manière automatique, le gestionnaire du forum vous a annoncé : "Votre message a été accepté, mais il va être révisé par notre équipe. Quelques instants vont donc être nécessaires avant que votre message puisse être vu par les autres internautes" (message du site xinhuanet.com). Ces messages censurés sont censés être révisés par les webmasters des sites pour vérifier si leur contenu mérite réellement qu'ils soient interdits. Mais il est rare qu'un message "filtré" soit ensuite remis manuellement sur le forum. "Nous avons rarement le temps de le faire", a expliqué un responsable des forums de discussion de sina.com à Reporters sans frontières. On trouve néanmoins des messages "politiquement corrects" qui contiennent des mots interdits, comme Falungong, mais qui sont acceptés parce qu'ils sont critiqués par exemple du mouvement spirituel.

Le 11 mars 2003, un message contenant une liste approximative des mots censurés apparaît sur le forum de discussion de sina.com.cn. L'internaute a, bien entendu, pris la précaution de couper chacun des mots par un astérisque pour que la liste ne soit pas bloquée par les filtres. On y trouve "4 juin" (date du massacre de la place Tiananmen en 1989), "droits de l'homme", "indépendance de Taïwan", "pornographie", "sexe oral", "BBC" ou "Falungong". Le message a été retiré au bout de quelques minutes.

Les messages qui ne contiennent pas de mots interdits sont donc mis en ligne sur le forum. Ils apparaissent à la vue de tous les internautes connectés. Mais un groupe de "Ban Zhu" (webmaster du forum) sont chargés de vérifier leur contenu. En permanence, deux ou trois webmasters scrutent et animent en même temps les forums. Ils ne sont pas des policiers ou même des employés chargés d'épurer les sites. Il s'agit principalement de jeunes, parfois étudiants, et plus souvent volontaires, qui donnent de leur temps aux forums de discussion. Pourtant, ils gardent tout pouvoir de nettoyer les forums des messages jugés indésirables. Au-dessus des "Ban Zhu", on trouve des "Guan Li Yuan" (administrateur de forum) qui ont la responsabilité de garantir la bonne tenue des forums. Ils ont également le pouvoir de suspendre ou d'interdire les internautes jugés vulgaires ou politiquement incorrects. Un responsable de sina.com.cn nous a affirmé qu'il préfère d'abord avertir l'internaute avec un message électronique. Si son comportement ne s'améliore pas, celui-ci est suspendu pendant une semaine.

Dernier échelon de cette chaîne de contrôle : les services de surveillance d'Internet établis au sein des départements provinciaux de la sécurité publique. Il est très difficile d'obtenir des informations officielles sur le nombre de fonctionnaires, policiers ou informaticiens, employés par cette cyberpolice.

Lors d'une enquête menée par Reporters sans frontières en avril 2003, plus de 60 % de tous les messages envoyés ont été mis en ligne sur les forums de discussion. Ce pourcentage chute à 55 % quand il s'agit de messages au contenu polémique. Sur ces 55 %, plus de la moitié ont été retirés par les webmasters chargés de surveiller les sites. En résumé, seulement 30 % des messages polémiques ont été acceptés par les sites.

Les cybercafés dans le collimateur

Les cybercafés chinois semi-légaux, connus sous le nom de "wang ba" en mandarin, sont les nouvelles cibles du pouvoir. Une vaste campagne gouvernementale de vérification des cafés Internet a été lancée début 2001 par les autorités. Motif : seulement la moitié d'entre eux auraient installé les programmes capables de bloquer l'accès aux sites interdits aux internautes chinois. Ces logiciels de filtrage des contenus ont été rendus obligatoires par l'adoption en 2000 des lois sur l'Internet. Cette campagne s'est musclée à partir de juin 2002. La grande majorité des 200 000 cybercafés du pays

(statistique officielle) ont été inspectés et plus de cent mille ont été sanctionnés par les autorités. Le 26 décembre 2002, l'agence de presse officielle *Xinhua* annonce que les autorités ont fermé définitivement plus de 3 000 cybercafés et temporairement 12 000 autres, depuis le lancement de cette campagne.

Les lenteurs administratives et la corruption rendent très difficile l'obtention de licences d'exploitation de cafés Internet. La grande majorité des établissements sont donc semi-légaux. Ils ont pignon sur rue mais ne disposent pas de licence en bonne et due forme.

Le 14 avril, la Chine décide de suspendre pendant une durée de trois mois l'ouverture de nouveaux cybercafés pour mieux réglementer l'accès au réseau.

Le 29 avril, les autorités chinoises décident de fermer les cybercafés de la principale avenue de Pékin et dans un rayon de 200 mètres autour des bâtiments du Parti communiste chinois et des écoles de la capitale.

Le 2 juillet, des statistiques de la police chinoise font état de la fermeture d'au moins 8 014 cafés Internet au cours des deux mois précédents. 56 800 cybercafés ont également été inspectés durant cette période. Le 20 novembre, le journal chinois *Wen Hui Bao* affirme que plus de dix-sept mille cybercafés chinois ont été fermés pour avoir négligé de bloquer l'accès aux sites jugés "subversifs" ou "pornographiques".

Le 22 août, le journal officiel *Le Quotidien du Peuple* affirme que le ministère de la Culture a demandé aux autorités locales de lancer une campagne de "nettoyage spirituel" visant, entre autres, à supprimer les cybercafés clandestins. C'est au cours de la conférence sur le "contrôle de la propagation de la corruption et de la décadence" qui s'est tenue à Pékin le 20 août 2001 qu'il a également été demandé aux représentants de l'Etat dans les provinces de ne plus accorder de nouvelles licences et de sévir contre les activités illégales des cafés Internet.

Le 1er février 2002, la police de Chongqing (sud-ouest de la Chine) contraint les propriétaires de cybercafés à installer des logiciels filtrants sur leurs ordinateurs afin d'identifier et de bloquer les sites contraires à la "moralité publique".

Le 5 février 2002, le directeur adjoint de Feiyu, la plus grande chaîne de cafés Internet du pays avec plus de quatre cents établissements, annonce que les autorités ont sanctionné l'entreprise de trois mois de fermeture pour ne pas avoir respecté la législation en vigueur. Feiyu aurait omis de signaler aux services de sécurité la consultation par ses clients de sites, notamment pornographiques, jugés "dangereux" par les autorités. Cette sanction fait suite à une enquête de la police du district de Haidain, banlieue de Pékin, où Feiyu dispose de deux cafés Internet géants disposant de plus de huit cents ordinateurs chacun.

Entre fin avril et début mai, plus de deux cents établissements sont fermés à Shanghai, selon l'agence de presse officielle *Xinhua*. Selon les autorités, "ils ne

possédaient pas de licence” leur permettant d’exercer. Près de mille trois cents cybercafés de la capitale économique du sud du pays ont été inspectés. Ils ont pu rester ouverts lors de l’inspection.

Le 1er mai, le gouvernement a lancé “une campagne de remise en ordre visant à faire la chasse aux contenus nocifs sur la Toile”, notamment en contrôlant les cybercafés. Selon Luo Gan, l’un des principaux responsables du maintien de l’ordre en Chine, “les activités illégales en ligne sont en hausse”.

Le 3 juin, les autorités de Guangzhou (sud du pays) ferment neuf cafés Internet illégaux de la ville. Le matériel informatique est confisqué par la police.

Suite à un incident criminel, le 16 juin, dans un cybercafé illégal de Pékin qui cause la mort de vingt-quatre personnes, les autorités lancent une campagne nationale de vérification des licences des établissements. Des milliers de cafés Internet sont fermés et des milliers d’autres sont obligés de redemander une licence aux autorités. Cette campagne, initialement justifiée par la nécessité d’améliorer les conditions de sécurité dans les cybercafés, va se transformer en une vaste opération de répression qui a réduit les possibilités de millions d’internautes chinois de se connecter.

Quelques heures après l’incendie du cybercafé, dont les auteurs - deux jeunes internautes - seront condamnés à la prison à vie, Liu Qi, le maire de Pékin, ordonne la fermeture des deux mille quatre cents établissements de la ville. Pendant quelques semaines, aucun café Internet n’est ouvert au public. “Notre monde s’est rétréci”, commente un étudiant pékinois à un reporter de l’agence de presse Reuters. Pour justifier ces mesures radicales, le journal officiel *Le Quotidien du peuple* titre “Ne laissons pas les cafés Internet détruire les enfants”. De son côté, le journal *Nouvelles du soir de Pékin* demande à ses lecteurs de dénoncer aux autorités les cafés Internet et les salles de jeux vidéo illégaux. Il faut attendre le 17 juillet pour qu’une trentaine de cybercafés de Pékin soient autorisés à rouvrir leurs portes. Ils se sont engagés publiquement à ne pas accepter les jeunes de moins de 18 ans, à fermer entre minuit et huit heures du matin, et à bannir les paris et les jeux vidéo violents.

Le 17 juin, la municipalité de Tianjin (au sud de Pékin) entame une inspection de tous les cybercafés. Au même moment, les autorités de la province du Guangdong (sud du pays) suspendent l’attribution de nouvelles licences. A Shanghai cette fois, Wei Yixin, responsable du Bureau municipal de l’industrie et du commerce affirme au *Quotidien de Shanghai* que “des policiers vont agir pour fermer très rapidement des établissements qui n’ont pas de licence.”

Le 28 juin, le Centre d’information pour les droits de l’homme et la démocratie annonce que les autorités obligent désormais les propriétaires des cybercafés à installer dans tous les ordinateurs des logiciels capables de bloquer jusqu’à 500 000 sites et de “dénoncer” à la police la consultation des sites subversifs. Les autorités n’ont pas confirmé cette disposition mais, selon des experts basés à Pékin, il pourrait s’agir du logiciel “Filter King” conçu dans le cadre du programme “Bouclier doré”.

Le ministère de la Sécurité publique compterait installer ce logiciel, testé en 2001 dans la province du Xi'an (centre-est du pays), dans tout le pays.

Le 29 juin, un responsable du ministère de la Culture annonce que tous les cybercafés du pays devront se réenregistrer, avant le 1er octobre, auprès des autorités. "Les cafés Internet sans licence seront fermés et leurs propriétaires poursuivis", martèle ce responsable.

Le 10 juillet, les 528 cybercafés de la province du Hebei, au nord-est de la Chine, sont fermés sur ordre des autorités locales. Selon le *Beijing Morning Post*, des problèmes de sécurité seraient à l'origine de ces fermetures. 3 813 cybercafés auraient été inspectés par le gouvernement du Hebei depuis le 17 juin et 2 892 d'entre eux n'auraient pas respecté les consignes de sécurité, d'après le journal.

Le 12 août, les ministères de la Culture et de la Sécurité publique ainsi que le Département de l'industrie et du commerce ont interdit l'ouverture de tout nouveau cybercafé en Chine. Les spécialistes d'Internet considèrent cependant qu'une telle mesure sera difficile à appliquer indéfiniment.

Fin septembre, le Premier ministre Zhu Rongji signe une nouvelle loi sur l'exploitation des cybercafés. Les établissements sont interdits aux mineurs, ils sont non-fumeurs et fermés de minuit à huit heures du matin. Autre nouveauté, les propriétaires sont tenus pour responsables des pages consultées par leurs clients. Il est rappelé que "créer, télécharger, copier, envoyer, diffuser ou consulter des contenus considérés comme anticonstitutionnels, portant atteinte à l'unité nationale, à la souveraineté ou à l'intégrité territoriale de la Chine", sont des crimes au regard de la loi. Les propriétaires devront noter et garder pendant deux mois les noms de leurs clients et les sites qu'ils ont consultés. En cas d'infraction, les amendes s'élèveront jusqu'à 2 000 euros. La loi entre en vigueur le 15 novembre 2002.

Le 16 octobre, le journal *Wenhui Bao*, publié à Shanghai, annonce que 90 000 cybercafés ont été fermés dans le pays, depuis le début, en juin, de la campagne nationale d'inspection des licences et des conditions de sécurité. Le ministère de la Culture, cité par le quotidien, affirme que seuls 46 000 établissements sont enregistrés en bonne et due forme et que les inspections vont se poursuivre jusqu'à la fin de l'année.

Persécution des adeptes de Falungong

Les adeptes du mouvement spirituel Falungong subissent les foudres du pouvoir. Accusés par Jiang Zemin d'être membres d'une "secte satanique", ils ont bruyamment protesté, depuis 1999, contre l'interdiction de leur mouvement. La répression est d'une rare violence : des milliers de membres ont été arrêtés, torturés et rééduqués, notamment ceux qui ont utilisé Internet pour diffuser la parole du maître Li Hongzhi. De fait, les fidèles du mouvement se sont très bien organisés sur la Toile, à l'intérieur de la Chine comme à l'étranger. Au moins seize membres de Falungong sont détenus pour avoir diffusé ou consulté sur Internet de l'information concernant

leur mouvement. Deux autres adeptes sont morts de mauvais traitements au cours de leur détention.

Le 2 juin 2001, Wang Zhenyong professeur assistant en psychologie à l'Université Normale du Sud-Ouest, est arrêté pour avoir adressé par e-mail quatre articles sur le mouvement spirituel Falungong. Il avait téléchargé ces articles sur des sites étrangers en décembre 2000 avant de les envoyer à un collègue qui les avait ensuite diffusés sur Internet.

Le 27 juin, selon le Centre d'information sur les droits de l'homme et la démocratie, Li Changjun, un adepte du mouvement, décède après avoir été torturé au cours de sa garde à vue. Il avait été arrêté le 16 mai pour avoir téléchargé et imprimé des documents sur Falungong. Agé de 33 ans, Li Changjun travaillait au centre des impôts de Wuhan, dans la province de Hubei (centre-est du pays). Il avait déjà été arrêté à plusieurs reprises pour avoir maintenu son adhésion à "la secte malfaisante". Sa mère a déclaré que son fils était couvert de cicatrices et d'hématomes, que son cou et ses oreilles étaient violacés et qu'il était anormalement maigre.

Le 14 août, Chen Qiulan, âgé de 47 ans, membre du mouvement, meurt d'une crise cardiaque dans le centre de détention de Daging (province de Heilongjiang, nord-est du pays). Il avait été arrêté au mois de juillet pour avoir diffusé des informations sur Falungong sur Internet.

Le 13 décembre, six adeptes du mouvement sont condamnés pour "diffusion d'informations subversives sur Internet", à savoir des informations sur Falungong. Yao Yue, chercheuse en microélectronique à l'université de Tsinghua, est condamnée à une peine de douze ans de prison. Deux professeurs de l'université, Meng Jun et Wang Xin, sont condamnés à dix et neuf ans de détention. Dong Yanhong, une employée de l'université, et son époux, Liu Wenyu, sont condamnés à respectivement cinq et trois ans de détention. Wang Xuefei, étudiant à Shanghai, est condamné à une peine de onze ans de prison. Selon le Centre d'information sur les droits de l'homme et la démocratie, un officiel de la première Cour populaire intermédiaire de Pékin a confirmé ces condamnations.

Le 27 décembre, l'agence de presse officielle *Xinhua* annonce la condamnation à trois ans de prison de Quan Huicheng, adepte du mouvement spirituel, pour avoir téléchargé, photocopié et distribué des documents sur des sites Internet de Falungong basés à l'étranger. Quan Huicheng a été arrêté, en octobre, à proximité d'un cybercafé de la ville de Dongfang, sur la côte de l'île de Hainan (sud du pays).

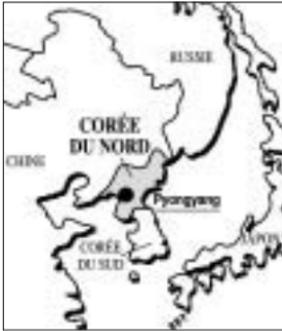
Le 18 février 2002, les autorités annoncent que le procès de Lin Yang, Ma Yan, Li Chunyang, Jiang Yuxia, Li Yanfang et Huang Kui, étudiants à l'université Tsinghua (dans la banlieue de Pékin), accusés d'avoir diffusé sur Internet des documents sur le mouvement, ne reprendra qu'après la visite du président Bush en Chine. Selon le Centre d'information sur les droits de l'homme et la démocratie, leur procès avait débuté en septembre 2001 devant la cour de Zhuhai (sud du pays).

Les cyberdissidents chinois détenus pour avoir diffusé des informations jugées “subversives” par les autorités :

- | | | |
|----------------|-------------------|-------------------|
| 1. Huang Qi | 10. Lu Xinhua | 19. Zhu Ruixiang |
| 2. Yan Pen | 11. Chi Shouzhu | 20. Li Dawei |
| 3. Qi Yanchen | 12. Yang Zili | 21. Chen Shaowen |
| 4. Yang Jianli | 13. Jin Haike | 22. Liu Di |
| 5. Liu Weifang | 14. Xu Wei | 23. Ouyang Yi |
| 6. Hu Dalin | 15. Zhang Honghai | 24. Li Yibin |
| 7. Wang Jinbo | 16. Jiang Shihua | 25. Jiang Lijun |
| 8. Wang Sen | 17. Wu Yilong | 26. Zhang Yuxiang |
| 9. Guo Qinghai | 18. Mu Chuanheng | |

LIENS :

- L'organisation Human Rights In China
<http://iso.hrichina.org/iso>
- L'agence de presse officielle *Xinhua*
www.xinhuanet.com
- Le site du webmaster emprisonné Huang Qi
<http://www.6-4tianwang.com>
- Les rapports de Human Rights Watch sur les droits de l'homme en Chine
www.hrw.org/asia/china.php
- Publication “You've Got Dissent! Chinese Dissident Use of the Internet and Beijing's Counter-Strategies”
www.rand.org/publications/MR/MR1543
- Informations sur la répression des cyberdissidents
dfn.org/focus/china/chinanetreport.htm
- Rapport sur le projet “Golden Shield”
www.ichrdd.ca/english/commdoc/publications/globalization/goldenShieldEng.html
- Le site d'informations du Falungong
www.faluninfo.net



Corée du Nord

POPULATION : 22 428 000

INTERNAUTES : STATISTIQUES NON DISPONIBLES

FOURNISSEURS D'ACCÈS PRIVÉS : NON

Officieusement, Internet est inexistant en Corée du Nord. Le pays le plus fermé au monde ne compte aucun fournisseur d'accès et pas d'internautes. Néanmoins, une poignée de privilégiés peuvent se connecter au Réseau via les communications internationales ou par satellite. Et le régime se sert de la Toile pour communiquer hors de ses frontières. Il a même créé, début 2002, Arirang, un site de promotion touristique du pays.

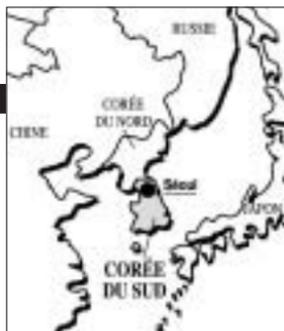
Le site progouvernemental DPRKorea Infobank (en coréen, en anglais, en japonais et en chinois), hébergé en Chine, vante les charmes de la Corée du Nord. Par ailleurs, une dizaine de sites officiels, dont celui de l'agence de presse nationale KCNA, sont hébergés au Japon ou en Chine. Le site de la KCNA se contente de reprendre des articles et des représentations du "cher leader" Kim Jong-il ou de travailleurs et paysans heureux. Aucun mot bien entendu sur la famine.

En 2000, une revue scientifique nord-coréenne *Le Monde de la Science* a publié un diagramme intitulé "Intranet" illustrant un projet de système de filtres installé entre Internet et l'Intranet nord-coréen, visant à sélectionner les informations circulant entre les deux réseaux.

Cette attitude ambiguë vis-à-vis du Net est dénoncée par les organisations de défense des droits de l'homme, qui utilisent quant à elles Internet pour combattre le régime répressif de Kim Jong-il. L'une des plus actives est l'Alliance citoyenne pour les droits de l'homme en Corée du Nord. Basée en Corée du Sud, elle dénonce toutes les facettes de l'oppression exercée par l'Etat nord-coréen sur sa population. Très investie dans l'aide aux transfuges qui parviennent à quitter la république communiste via la Chine ou la Russie, elle propose, sur son site, de nombreux témoignages.

LIENS :

- L'Alliance citoyenne pour les droits de l'homme en Corée du Nord
www.nkhumanrights.or.kr
- Site de promotion touristique : www.dprkorea.com
- L'agence de presse officielle KCNA : www.kcna.co.jp



Corée du Sud

POPULATION : 47 069 000

INTERNAUTES : 26 270 000

FOURNISSEURS D'ACCÈS PRIVÉS : OUI

La croissance du nombre d'internautes sud-coréens est soutenue et le pays possède l'un des plus grands nombres de connexions à haut débit. Mais la censure étatique des sites jugés "infâmes" existe toujours.

La Corée du Sud a bien saisi l'enjeu que représente Internet en termes de désenclavement et d'expansion économique. Au cours des quatre dernières années, le nombre de personnes connectées est passé, selon les statistiques, de trois à vingt-six millions. Ce succès est surtout à mettre au crédit du développement rapide du haut débit. Après les Etats-Unis, le pays est l'un de ceux qui possèdent le plus grand nombre de connexions de ce type au monde. Elles permettent des liaisons rapides et de grande qualité, séduisantes pour les internautes.

Une liste noire de 120 000 sites

Si Internet s'est fortement démocratisé en Corée du Sud, il est néanmoins réglementé. Le pays est l'un des premiers au monde à s'être doté, dès 1995, d'une loi contrôlant la diffusion et la consultation d'informations en ligne. Le Bureau sur l'éthique de l'information et de la communication (ICEC) surveille de très près les contenus des sites et des forums, et peut recommander le blocage de certains d'entre eux.

En juillet 2001, le ministère de l'Information et de la Communication (MIC) a ainsi appelé à bloquer l'accès à 120 000 sites dont les contenus ont été jugés "infâmes". Les sites visés ont été accusés de propager la pornographie, la violence, des informations sur le piratage informatique, des virus, la cybercriminalité ou d'inciter au suicide. Le gouvernement a dès lors réclamé l'installation de logiciels de filtrage sur les ordinateurs des cybercafés, des écoles, des bibliothèques publiques pour en empêcher la consultation. Il a également demandé aux fournisseurs d'accès d'en bloquer l'accès sous peine de sanctions pénales. Argument avancé : la nécessité de "protéger le jeune public en évitant qu'il ne soit exposé à des contenus dangereux".

Un argument fallacieux pour les militants de l'organisation Jinbonet qui œuvre pour la liberté d'expression sur Internet en Corée du Sud. "Il s'agit d'une attaque de plus contre la Toile. Déjà, en l'an 2000, le gouvernement avait tenté de mettre en place une censure du Web. Mais la levée de boucliers déclenchée par ce projet l'avait fait avorter. Cette nouvelle campagne n'est qu'une charge de plus", expliquent-ils.

“Le gouvernement n’a qu’un objectif : contrôler Internet et rétablir la censure.” Selon l’organisation, le ministère a mis en place des logiciels qui rapatrient automatiquement les sites jugés indésirables. Ensuite, des équipes de spécialistes d’Internet les décorrent et tentent de les bloquer.

En mai 2002, l’ICEC décide de fermer pendant deux mois le site non serviam qui milite contre le service militaire. L’organisme de contrôle affirme que le service s’impose à tous les hommes coréens et que les campagnes antimilitaristes ont suscité de nombreuses plaintes. Cette décision est prise en vertu de l’article 53 de la loi de 1995. En juin 2002, le Tribunal constitutionnel a jugé inconstitutionnels l’article 53 de la loi sur les activités relatives aux communications électroniques de 1995 et l’article 16 de l’ordonnance d’exécution de cette loi. Cette décision fait suite à des critiques des organisations Jinbonet et Avocats pour une société démocratique. En novembre 2002, l’Assemblée nationale a modifié le texte de l’article 53. La notion de “contenu dangereux” est remplacée par l’expression “contenu illégal”. En revanche, l’ICEC et le ministère de l’Information et de la Communication voient leurs pouvoirs de contrôle et de sanction maintenus.

Un militant politique arrêté

Le 25 juillet 2002, Kim Kang-pil, militant du Parti travailliste démocrate (DLP, extrême gauche sud-coréenne), est arrêté par la police pour avoir mis en ligne des articles relatifs à la Corée du Nord sur le site de son parti. Il est détenu en vertu de l’article 7 de la loi sur la sécurité nationale qui punit lourdement les Sud-Coréens coupables de sympathies pour le régime nord-coréen. Il est notamment accusé par le procureur d’avoir “agi en faveur de l’ennemi”. Il est condamné à un an de prison et un an d’interdiction de vote. A l’issue du procès, une association de lutte contre la censure sur Internet a déclaré : “Ce procès montre clairement que le gouvernement surveille les sites d’organisations politiques et sociales (...) Cette punition doit avoir d’autres motivations.” Kim Kang-pil est finalement libéré le 3 décembre 2002, après avoir été condamné à une peine avec sursis en appel.

Interdiction d’un site gay

Début janvier 2002, l’Alliance contre la discrimination en Corée des lesbiennes et des gays, un mouvement regroupant quinze associations de défense des droits des homosexuels a attaqué le gouvernement en justice pour s’opposer à l’interdiction du premier site gay du pays, exzone.com. Le collectif s’est appuyé sur la Constitution pour faire valoir ses droits. “En vertu de la Constitution, le gouvernement n’a pas le droit de déterminer les orientations sexuelles des gens”, ont affirmé ses porte-parole. Ces associations ont par ailleurs rappelé que l’interdiction de ce site était “contraire à la loi fondamentale du pays garantissant la liberté d’expression, de parole et de presse”.

Un comité gouvernemental de protection de l’enfance, qui dépend des services du Premier ministre, avait qualifié le site de “pornographique et nuisible à la moralité des jeunes” avant de prononcer son interdiction. Pourtant, quelques mois plus tôt, ce même comité avait utilisé Internet pour publier les identités d’une soixantaine de

délinquants sexuels, renseignements personnels et professionnels à l'appui. La nature explicite des délits commis par ces personnes, condamnées pour mauvais traitements sur des enfants de moins de treize ans, avait été mise en ligne en l'absence de tout filtrage.

Le haut débit, allié des hackers

Conséquence du succès du Web et du confort de connexion offert aux internautes sud-coréens par le haut débit : les pirates informatiques, les hackers, sont particulièrement actifs dans la péninsule. Selon une étude réalisée courant 2001 par le cabinet de consultants en sécurité Predictive Systems, 34 % des cyberattaques lancées dans le monde hors des Etats-Unis le sont depuis la Corée du Sud ou sont relayées dans le pays. "La Corée du Sud étant l'un des pays les mieux équipés en liaisons à haut débit derrière les Etats-Unis, il est facile de lancer des attaques d'ici, ou de se servir du pays comme tremplin", explique Richard Smith, auteur de l'étude.

Illustration concrète de ce phénomène : l'affaire de l'avion-espion américain qui a dû se poser en catastrophe sur le territoire chinois. En mai 2001, elle a déchaîné les passions des pirates informatiques américains et chinois. Et la Corée du Sud est devenue le champ de bataille de cette cyberguerre sino-américaine.

Plus d'une centaine d'attaques lancées par des pirates des deux pays ont pris pour cibles des sites d'universités, de sociétés et de centres de recherches sud-coréens. Pourquoi la Corée du Sud ? Parce que le pays, sorte d'interface entre La Chine et les Etats-Unis, possède de très nombreuses connexions avec les deux Etats. Les pirates des deux camps, qui ont souhaité dissimuler leurs identités, ont préféré asservir des sites sud-coréens pour livrer bataille, plutôt que de s'en prendre directement aux sites de "l'ennemi".

Campagne électorale sur Internet

Lors de l'élection présidentielle de décembre 2002, la bataille a fait rage entre les sites d'informations animés par de jeunes journalistes proches du candidat réformiste Roh Moo-hyun et les grands titres de la presse écrite tels que le quotidien conservateur *Chosun Ilbo*. La victoire du candidat libéral a notamment été rendue possible grâce au soutien de sites tels que Ohmynews qui a reçu vingt millions de visites par jour pendant la campagne électorale. Son fondateur, Oh Yeon-ho, affirme qu'il a reproduit sur Internet ses "combats de rue pour la démocratie des années 1980". Le site repose sur un réseau de 23 000 "reporters citoyens" dans tout le pays. Ohmynews a notamment révélé un scandale impliquant le groupe industriel Hyundai.

LIENS :

- Les organisations Jinbonet et Progressive Network Center : <http://english.jinbo.net>
- Le ministère de l'Information et de la Communication : www.mic.go.kr
- Le quotidien en ligne indépendant Ohmynews : www.ohmynews.com



Cuba

POPULATION : 11 237 000

INTERNAUTES : 120 000

FOURNISSEURS D'ACCÈS PRIVÉS : NON

Avec un accès soumis à autorisation et un rationnement des équipements nécessaires, Internet à Cuba apparaît comme un phénomène limité et sous haute surveillance.

Le développement du réseau informatique et des ressources d'Internet est présenté comme une priorité nationale à Cuba. Le ministre de l'Informatique et des Communications, Roberto Ignacio González Planas, a annoncé, en octobre 2002, dans le quotidien officiel *Granma International*, que le nombre des ordinateurs avait triplé en deux ans dans l'île, et que la fibre optique reliait La Havane à Camagüey (Centre), en attendant d'atteindre Santiago (Est).

Les restrictions matérielles restent néanmoins le principal obstacle à une expansion grand public du Réseau. D'une part, la densité téléphonique ne dépasse pas quatre lignes pour cent habitants. D'autre part, le coût prohibitif des communications téléphoniques internationales (deux dollars la minute vers les Etats-Unis) et la rareté des lignes internationales, accordées sur critères politiques et étroitement surveillées, empêchent toute connexion via un pourvoyeur d'accès situé à l'étranger. Luis Fernández, porte-parole de la Section des intérêts cubains à Washington, a mis en cause l'embargo pour justifier le rationnement des matériels : "Si nous ne devons pas y faire face, il y aurait des ordinateurs pour tout le monde."

Une explication qui passe sous silence le fait que les équipements nécessaires, y compris les plus récents, ne sont disponibles que dans les magasins d'Etat spécialisés, accessibles uniquement aux personnes autorisées. C'est oublier également qu'un arrêté du ministère du Commerce intérieur interdit, depuis janvier 2001, la vente aux particuliers dans les magasins d'Etat "d'ordinateurs, d'imprimantes, de machines à photocopier, photocopieuses et tous autres instruments d'impression de masse". Si un tel achat est considéré comme indispensable, une autorisation doit être sollicitée auprès du ministère du Commerce intérieur. Les modems étaient déjà avant cette date interdits à la vente au public. Internet à Cuba apparaît, dans ces conditions, comme un phénomène limité, alors que les entreprises informatiques cubaines démontrent une parfaite maîtrise de cette nouvelle technologie.

Priorité aux institutions

Le gouvernement a légiféré dès l'apparition d'Internet sur l'île. En juin 1996, le décret-loi 209, intitulé "Accès depuis la République de Cuba au réseau informatique global", précise que son utilisation ne peut se faire "en violation des principes moraux de la société cubaine ou des textes de loi du pays", et que les messages électroniques ne doivent pas "compromettre la sécurité nationale".

Les Cubains souhaitant disposer d'un accès à Internet ou utiliser les points d'accès ouverts au public doivent, pour obtenir l'accréditation obligatoire, fournir une "raison valable", et signer un contrat d'utilisation aux clauses restrictives. Selon le décret-loi 209, l'accès est accordé "en vertu de règlements donnant la priorité aux entités et institutions pouvant contribuer à la vie et au développement de la nation". Peuvent y prétendre à ce titre, en dehors des ambassades ou des sociétés étrangères, les personnalités politiques, les hauts fonctionnaires, les intellectuels, universitaires, chercheurs et journalistes officiels, les cadres des entreprises culturelles tournées vers l'exportation ou des entreprises d'informatique, ainsi que la hiérarchie catholique. Les sociétés cubaines exportatrices ont accès à la messagerie électronique nationale et à l'Intranet national.

Le 13 janvier 2000, un ministère de l'Informatique et des Communications a été créé pour "réguler, diriger, superviser et contrôler la politique cubaine en matière de technologies de la communication, l'informatique, les télécommunications, les réseaux informatiques, la radiodiffusion, le spectre radioélectrique, les services postaux et l'industrie électronique".

Dans *Granma internacional* du 18 juin 2001, Beatriz Alonso, directrice générale de Citmatel, l'un des deux serveurs de l'île, expliquait : "L'utilisation d'Internet par nos institutions est une possibilité d'accéder à l'information nécessaire dans le monde d'aujourd'hui. Il n'existe pas de sites de pornographie, de terrorisme et d'autres vices qui prolifèrent dans des nations capitalistes, et parmi lesquelles les Etats-Unis occupent une place de choix. L'usage d'Internet à Cuba s'est établi sur une base d'éthique et d'humanisme. Il existe un code d'éthique pour l'utilisation du Réseau des réseaux. Nous favorisons l'échange d'informations pour nos professionnels et techniciens, faisons connaître le développement atteint par Cuba, et fournissons des sources de connaissance à nos élèves et étudiants."

Les deux serveurs de l'île sont le Citmatel du CenaInternet, branche du ministère cubain de la Science, de la Technologie et de l'Environnement, et Infocom, branche de la société mixte italo-cubaine Etesca (Empresa de Telecomunicaciones de Cuba, S.A).

Les e-mails sous haute surveillance

Un marché noir d'adresses e-mails a vu le jour et profite aux rares Cubains disposant d'un ordinateur. Le 1er janvier 2001, une Agence de contrôle et de supervision (ACS) a été créée au sein du ministère de l'Informatique et des Communications, chargée

notamment de traquer ceux qui feraient "un usage indu des réseaux informatiques". Cité dans un article du quotidien Granma publié le 23 avril 2003, Carlos Martínez Albuérne, son directeur, rapporte qu'en 2002 des sanctions ont été prises contre trente et une personnes pour ce motif ou "pour avoir utilisé des messageries électroniques qui ne leur appartenaient pas". L'article ne précise pas les "sanctions" qui ont été infligées.

En matière de messagerie électronique, respecter la légalité revient à accepter d'être surveillé. Depuis septembre 2001, dans les points d'accès Etecsa, les Cubains peuvent accéder à un service de courrier électronique national sans se connecter sur le Web, après avoir obtenu une adresse e-mail personnelle. Une carte d'accès limité à ce service coûte cinq euros pour un usage de quatre heures (notons que le salaire moyen mensuel d'un Cubain tourne autour de dix euros). Les cartes sont nominatives. Leur acquéreur doit justifier de son identité, remplir un formulaire détaillé, et ses coordonnées sont enregistrées. Le pourvoyeur d'accès peut ainsi contrôler tout courrier reçu ou envoyé avant de l'émettre ou de le délivrer à son destinataire. Plusieurs usagers ont cru noter des retards, voire des "disparitions", dans leur correspondance, notamment avec l'étranger.

Vicenç Sanclemente, ancien correspondant à La Havane de la chaîne de télévision espagnole TVE, rapporte qu'en 1999, inquiet de ne plus recevoir de courriers électroniques sur l'ordinateur de son bureau alors qu'il attendait un message important de République dominicaine, il s'est adressé au technicien du ministère des Communications qui lui avait ouvert son compte Internet, croyant à un problème technique. Le préposé lui a répondu : "Mais c'est que cela fait plusieurs jours que tu n'as pas ouvert l'ordinateur que tu as à ton domicile. Et c'est là-bas que tu as trois messages de la République dominicaine, et aussi deux autres de Barcelone, un de Montse et un autre de Margaret."

L'accès aux cybercafés est également réduit pour les Cubains. Les étrangers de passage, sur présentation de leur passeport, peuvent accéder, à La Havane, à deux cybercafés, et la quasi-totalité des grands hôtels de la capitale est équipée d'un foyer Internet. Etecsa multiplie également, à La Havane et dans les métropoles provinciales, des points d'accès téléphone et Internet ouverts aux étrangers ainsi qu'aux Cubains titulaires des autorisations indispensables. Le surf sur le Web est libre à partir de ces points d'accès, y compris vers les sites étrangers, bien que les pourvoyeurs d'accès aient la possibilité technique, qu'ils exercent ponctuellement, de censurer l'accès à certains sites ou à certaines adresses.

Mais les tarifs sont prohibitifs : la connexion coûte au minimum deux euros le quart d'heure. A titre de comparaison, les cybercafés mexicains ou dominicains proposent leurs connexions (haut débit) à deux dollars l'heure. C'est pourquoi la fréquentation des points d'accès Internet est très réduite. Le confort des connexions, par modem téléphonique, est par ailleurs correct.

Les membres de l'Union nationale des écrivains et artistes (UNEAC) ont droit, à

l'Institut du Livre de la Havane, à leur propre cybercafé, El Aleph, avec accès à leur messagerie et à un réseau intranet national diffusant les sites Web officiels.

Le gouvernement poursuit à travers les organisations de jeunesse la création de 300 clubs Internet dans tout le pays, et il multiplie les cours de formation élémentaire et de perfectionnement. Quand ils sont connectés, les ordinateurs de ces centres ont un accès limité aux sites officiels.

Une fenêtre de liberté...

A Cuba, même sous très haut contrôle, Internet entrouvre une fenêtre de liberté. Ainsi, les journalistes indépendants exerçant dans le pays ont vu leurs débouchés s'élargir. La création à l'étranger (à Miami notamment) de sites Internet ou de pages Web accueillant les nouvelles qu'ils transmettent par téléphone ou par télécopieur a étendu le champ de diffusion d'informations qu'ils ne peuvent toujours pas publier dans leur propre pays. Leur production est désormais archivée et accessible dans le monde entier, alors qu'elle ne circulait auparavant que sur les ondes de *Radio Marti* (station fédérale américaine émettant à partir du territoire des Etats-Unis), peu audibles sur le territoire national et par essence éphémères.

Des événements tels l'arrestation d'un opposant, un mouvement d'humeur de la population ou une initiative d'organisation de la société civile, autrefois ignorés au moins un temps à l'étranger, sont ainsi immédiatement relayés en dehors du pays. Ces nouvelles en provenance des journalistes indépendants sont de plus en plus souvent reprises par les médias internationaux, un indice probant de leur crédibilité et de leur professionnalisme croissants.

Par ailleurs, la diffusion, même très restreinte, des nouvelles technologiques et des accès Internet a suscité un petit marché noir du Web, encore marginal mais déjà organisé.

Certains ayants droit louent notamment leurs login et mot de passe, pour une somme d'environ 60 dollars par mois (équivalent de six mois de salaire moyen). D'autres accueillent les surfeurs sur leur propre point d'accès, et facturent la connexion au temps écoulé.

Les personnels et les hôtes des points d'accès Etecsa, qui connaissent le mot de passe pour connecter touristes et ayants droit, accordent volontiers une séance de surf à leurs amis et relations, certains moyennant finance.

Enfin, la rumeur veut que des internautes aient pu introduire dans l'île des paraboles et des modems leur permettant de recourir au service de pourvoyeurs américains d'accès par satellite (tels Starband ou DirecPC), l'abonnement étant réglé par leurs relations aux Etats-Unis (de l'ordre de 500 dollars la mise en service, et de 100 dollars par mois).

... étroitement surveillée

Arrêté le 15 décembre 2000, José Orlando González Bridón, secrétaire général de la Confédération des travailleurs démocratiques de Cuba (Confederación de

Trabajadores Democráticos de Cuba – CTDC, illégale), est le premier membre de l'opposition à avoir été condamné à une peine de prison pour un article publié sur l'Internet. Dans ce dernier, publié le 5 août 2000 sur le site de Cuba Free Press (cuba-freepress.org) basé en Floride (Etats-Unis), il avait mis en cause la responsabilité de la police dans la mort de Joanna González Herrera, coordinatrice nationale de la CTDC. Il avait également communiqué cette information à une radio basée à Miami, qualifiée de "subversive" dans l'acte d'accusation.

José Orlando González Bridón a été libéré le 22 novembre 2001. Il a bénéficié d'une libération conditionnelle, trois semaines avant le terme de sa peine. Les autorités pénitentiaires lui ont expliqué qu'il était libéré pour "bonne conduite". Le syndicaliste a, quant à lui, attribué sa libération à la volonté des autorités de faire un geste alors que se tenait, les 23 et 24 novembre, le Sommet ibéro-américain à Lima (Pérou), où se réunissaient vingt-trois chefs d'Etat d'Amérique latine, d'Espagne et du Portugal. Sa libération est intervenue également une semaine avant une réunion prévue à La Havane pour relancer le dialogue politique entre l'Union européenne (UE) et Cuba. Depuis 1996, l'UE subordonne "une pleine coopération avec Cuba (...) à l'amélioration de la situation en matière de droits de l'homme et de libertés politiques". Cuba souhaitait alors adhérer aux Accords de Cotonou par lesquels les Quinze soutiennent les pays ACP (Afrique-Caraïbes-Pacifique).

Incarcéré à la prison de Combinado del Este, située dans la province de La Havane, le syndicaliste rapporte avoir été détenu de décembre 2000 à octobre 2001 dans une "cellule de punition" ("celda de castigo"), habituellement destinée aux prisonniers les plus durs pour des séjours n'excédant pas vingt et un jours. Pendant ces dix mois, il a été privé de contact avec tout autre détenu et ne disposait, pour seul meuble, que d'un lit qui lui était apporté à six heures du soir et lui était retiré à six heures du matin. María Esther Valdés, sa femme, était autorisée à lui rendre visite toutes les trois semaines seulement. Au cours de sa détention, les autorités ont refusé de lui fournir le régime alimentaire spécial que requièrent ses problèmes de pression artérielle. Le syndicaliste rapporte néanmoins se trouver dans un état de santé à peu près satisfaisant.

Il affirme avoir été témoin de scènes de mauvais traitements contre des prisonniers. Il dénonce également la corruption au sein de l'établissement. D'après le syndicaliste, des gardiens reçoivent de l'argent de détenus qui souhaitent obtenir une amélioration de leurs conditions de détention ou acheter de la drogue.

Le procès de José Orlando González Bridón s'était tenu le 24 mai 2001 après avoir été reporté à plusieurs reprises. Seule sa famille avait pu assister à l'audience, l'accès au tribunal ayant été interdit à la presse étrangère et aux opposants par un important dispositif de sécurité. D'après des proches du syndicaliste, les places disponibles pour le public étaient occupées par des membres des forces de l'ordre. Le 2 juin 2001, en première instance, José Orlando González Bridón avait été condamné à deux ans de prison pour "diffusion de fausses nouvelles compromettant le prestige et le crédit de l'Etat cubain" avec "l'intention manifeste de collaborer avec une puissance étrangère".

Le 21 août, en appel, le chef d'inculpation avait été requalifié en "diffamation des institutions, des organisations, et des héros et martyrs" et la peine avait été ramenée à un an de prison. D'après ses proches, l'article publié sur l'Internet a été utilisé comme un prétexte par les autorités pour punir l'ensemble de ses activités contre le gouvernement.

LIENS :

Sites publiant les articles des journalistes indépendants

- www.cubonet.org
- www.nuevaprensa.org (en espagnol)
- www.cubaencuentro.com (en espagnol)
- www.cartadecuba.org (en espagnol)

- Portail officiel "Internet et Institutions"
www.cubaweb.cu/esp/categorias/categories.asp?categoryID=60

- Portail de la presse officielle
www.cubaweb.cu/esp/categorias/categories.asp?categoryID=20



Danemark

POPULATION : 5 333 000

INTERNAUTES : 2 500 000

FOURNISSEURS D'ACCÈS PRIVÉS : OUI

Dès le mois d'octobre 2001, suite aux attentats du 11 septembre, le gouvernement danois a présenté un important projet de révision des principales lois nationales pour combattre plus activement le terrorisme. Sous l'intitulé générique de "batterie de mesures antiterroristes", les lois sur la justice, les affaires intérieures, l'économie et la fiscalité ont été amendées.

Le gouvernement a notamment demandé au ministère de la Justice de prendre de nouvelles dispositions pour légaliser la rétention des données relatives aux télécommunications, aux connexions au Réseau et aux e-mails, et de permettre à la police d'accéder plus rapidement et plus facilement à ces données personnelles. La loi antiterroriste du 31 mai 2002 porte à un an la rétention des données et permet aux services secrets, PET, et à la police de les consulter sur ordonnance judiciaire et dans le cas de crimes graves. La police peut également, dans les mêmes conditions, brancher sur les terminaux des opérateurs des systèmes d'enregistrement des frappes de clavier et d'interception des courriers électroniques, du même type que le logiciel américain Carnivore.

La présidence danoise de l'Union européenne semblait décidée à imposer des vues analogues aux autres Etats membres. Elle a soumis, le 24 juin 2002, une proposition de mesures intitulée "acte relatif aux technologies de l'information et mesures concernant les investigations et poursuites contre le crime organisé", stipulant 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".

En contrepartie de ces mesures restrictives, le gouvernement a créé, en septembre 2002, une commission chargée de garantir les droits des citoyens dans le domaine informatique, qui devrait proposer des mesures en juin 2003.

LIENS :

- L'organisation Digital Rights : www.digitalrights.dk
- L'agence danoise de protection des données Datatilsynet : www.datatilsynet.dk



Egypte

POPULATION : 69 080 000

INTERNAUTES : 600 000

FOURNISSEURS D'ACCÈS PRIVÉS : OUI

En 2002, les autorités égyptiennes ont renforcé leur contrôle sur Internet en créant un service spécial chargé des délits sur Internet.

L'Égypte est l'un des pays du Moyen-Orient où le Réseau connaît l'une des plus importantes croissances. Introduite en 1993, la Toile est accessible au grand public depuis 1995. Année après année, le nombre de fournisseurs d'accès et d'utilisateurs ne cesse d'augmenter. Le ministère des Communications et des Technologies de l'Information a renoncé au monopole de l'opérateur public Telecom Egypt et lancé, début 2002, une opération "Internet libre". Cette dernière consiste à permettre aux fournisseurs d'accès de fournir des numéros de téléphone spéciaux aux utilisateurs possédant un ordinateur et un modem. Ces derniers n'ont pas besoin de s'engager fermement avec un opérateur. Objectif : faire grimper le nombre des internautes et sensibiliser les Égyptiens aux nouvelles technologies.

Depuis son avènement, le Web a représenté un espace d'expression libre. Si la presse traditionnelle est très encadrée, Internet n'a fait l'objet d'aucune loi spécifique de régulation. Cependant, en septembre 2002, le ministère de l'Intérieur a mis en place un département chargé d'enquêter sur les délits sur Internet. A cette occasion, son directeur, Ahmed Essmat, déclarait au quotidien *Al-Ahram* que son département disposait de personnel pour observer la Toile tout au long de la journée.

Déjà fin 2001-début 2002, les internautes avaient été prévenus que les sujets sensibles, tabous (les relations entre coptes et musulmans ; la diffusion des doctrines terroristes ; la question des violations des droits de l'homme ; les critiques contre le président, sa famille, l'armée ; la présentation d'interprétations modernes de l'islam, etc.) ou l'esprit trop critique n'étaient pas les bienvenus dans le cyberspace.

Fin 2001, alors que cinquante-deux homosexuels étaient traduits devant la Cour de sûreté de l'Etat, les sites de la communauté gay avaient été particulièrement visés par la police. L'un d'entre eux n'avait d'ailleurs pas hésité à mettre cet avertissement sur sa page d'accueil : "Devinez qui nous regarde et nous surveille ? Les services de la sécurité de l'Etat !" En 2002, de véritables pièges ont été mis en place par la police. Ainsi, deux Égyptiens ont donné, via des sites gay, des rendez-vous à des internautes qui se sont révélés être des ... policiers. Les deux hommes ont été arrêtés.

Mi-décembre 2002, l'Egyptian Initiative for Personal Rights (EIPR) avait fait part de son inquiétude quant à un projet de loi sur la communication. L'EIPR avait notamment dénoncé la formulation très vague de l'article 65 qui permettait à l'Armée, à la Police et à la Sûreté nationale d'accéder à n'importe quel réseau de communications "pour satisfaire des besoins de sécurité intérieure". Suite à la campagne de cette association, des amendements positifs ont été introduits à ce texte, adopté fin décembre. L'article 65 mentionne désormais le droit des citoyens à la protection de leur vie privée et restreint, par ailleurs, le droit des agences de sécurité à s'immiscer dans des communications personnelles "sauf dans les limites prévues par la loi". Les agences de sécurité devront ainsi obtenir une autorisation judiciaire ad hoc de 30 jours maximum et uniquement dans le cadre d'une enquête sur un délit grave ou un méfait passible de plus de trois mois de prison.

Jugé pour la mise en ligne d'un poème vieux de trente ans

Le 30 juin 2002, Shohdy Surur, webmaster à l'hebdomadaire anglophone *Al-Ahram weekly*, a été condamné à une peine d'un an de prison en vertu de l'article 178 du code pénal qui punit "la possession de matériel immoral pour la vente et la distribution avec l'intention de corrompre la morale publique". Il est accusé d'avoir mis en ligne, sur le site wadada.net, consacré en partie à l'œuvre de Naguib Surur, son père, un de ses poèmes intitulé "Kuss Oummeyatt", qui contient "des phrases" portant "atteinte à la moralité publique". Ce poème, écrit dans un langage très populaire et émaillé de métaphores sexuelles, est surtout une critique de la société et de la culture égyptienne au lendemain de la défaite de l'Égypte en 1967. Dans ce texte, le poète et acteur Naguib Surur compare à plusieurs reprises l'Égypte à une prostituée. Aucune loi ne régissant l'usage d'Internet, la justice a dû se référer aux atteintes à la morale publique pour justifier les poursuites. Le poème figurait sur le site wadada.net (basé aux États-Unis) depuis trois ans déjà. Et Naguib Surur lui-même, décédé en 1978, n'avait lui-même pas été condamné pour ce texte. Le 22 novembre 2001, Shohdy Surur avait été arrêté à son domicile qui avait été fouillé. Son ordinateur lui avait été confisqué. Il avait été conduit au commissariat où il avait été interrogé pendant trois jours. Le 14 octobre 2002, la peine d'un an de prison a été confirmée par la cour d'appel. Détenteur de la double nationalité russo-égyptienne, le cyberdissident résidait en Russie au moment de cette condamnation.

En avril 2002, un étudiant de 19 ans, Andy Ibrahim Shoukri, a été interpellé, jugé et condamné à un mois de prison pour "diffusion de fausses informations." Il avait envoyé des e-mails d'alerte sur un tueur en série qui sévissait au Caire. "Des informations tronquées", selon la police.

LIENS :

- The Egyptian Organization for Human Rights
www.eohr.org.eg/



Emirats arabes unis

POPULATION : 2 654 000

INTERNAUTES : 1 175 600

FOURNISSEURS D'ACCÈS PRIVÉS : NON

L'ouverture, en janvier 2002, de Dubaï Media City, la zone franche dévolue aux médias et aux nouvelles technologies, n'a pas réellement changé la donne. Officiellement, seul l'accès aux sites "pornographiques" est bloqué. De fait, celui de bien d'autres est soumis au même filtrage.

L'Etat le plus féru d'Internet du golfe Persique n'est pas pour autant le plus tolérant. Certes, il n'a pas adopté de texte spécifique au contrôle de la Toile. Les seules références constitutionnelles en la matière, la loi sur les télécommunications de 1996, semblent même plutôt permissives puisqu'elles garantissent la liberté d'expression, quel que soit le support médiatique. Mieux encore : les Emirats arabes unis se sont dotés, en janvier 2002, d'une sorte de Silicon Valley du Golfe : la zone franche Dubaï Media City, dévolue aux entreprises des médias, de l'informatique et des nouvelles technologies. La chaîne de télévision satellitaire arabe *Middle East Broadcasting Center* (MBC), basée auparavant à Londres, s'y est par exemple installée. A terme, une centaine de compagnies, essentiellement étrangères, devraient y être représentées.

Mais il s'agit d'un esprit d'ouverture en trompe-l'œil. Un seul fournisseur d'accès, Etisalat, opérateur public de télécommunications, gère le monopole des connexions et services liés au réseau. Surtout, l'accès à Internet est toujours entravé par un dispositif de filtrage. Selon les autorités, ce dernier a pour unique vocation d'empêcher les internautes d'accéder aux sites "pornographiques". Reste que ce "fire wall" bloque également l'accès à de très nombreux autres sites.

Autant de garde-fous qui n'incitent pas les habitants des Emirats arabes unis à éprouver leur liberté d'expression sur le Net. L'autocensure reste de mise par peur de sanctions. On se garde ainsi d'évoquer des sujets touchant à la religion, à la morale, aux pays amis ou aux membres des familles régnantes.

LIENS :

• Emirates Internet & Multimedia
www.emirates.net.ae

• Le fournisseur d'accès officiel Etisalat
www.etisalat.co.ae

• Site d'informations
www.dubainews.com

• Le Press Club de Dubaï
www.dpc.org.ae

• Site d'informations sur les pays du Golfe (en arabe)
www.gulfissues.net

Espagne

POPULATION : 39 921 000

INTERNAUTES : 7 856 000

FOURNISSEURS D'ACCÈS PRIVÉS : OUI



Le 27 juin 2002, le Congrès des députés espagnols a définitivement adopté la LSSICE ou "Loi de l'Internet", qui vise à combattre la cybercriminalité et le terrorisme sur la Toile ibérique. Concoctée par le ministère des Sciences et Technologies, elle régit principalement l'obligation faite aux fournisseurs d'accès à Internet de conserver les données de connexion et de trafic de leurs clients pendant au moins un an. Un amendement, introduit par l'opposition à la majorité de José Maria Aznar, ne permet aux services de police ou de renseignements d'utiliser ces données qu'avec l'aval d'un magistrat.

Pour autant, les modalités pratiques de cette rétention généralisée des données de télécommunications n'ont pas été précisées. Pas plus que n'a été désignée l'autorité administrative habilitée à fermer des sites qui "attentent à une série de valeurs", sans qu'elle porte 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".

Par ailleurs, le secret des communications personnelles ordinaires est protégé en Espagne par l'article 18.3. Il précise que "le secret des communications, en particulier par voie postale, télégraphique ou téléphonique, est garanti, sauf ordre judiciaire". Un cadre législatif qui a poussé plusieurs organisations de défense de la vie privée, ainsi que des juristes éminents, à attaquer la loi en vertu de son caractère anticonstitutionnel.

LIENS :

- L'Agence de protection des données
www.agenciaprotecciondatos.org



Etats-Unis

POPULATION : 285 926 000

INTERNAUTES : 155 000 000

FOURNISSEURS D'ACCÈS PRIVÉS : OUI

Si les Etats-Unis sont à l'origine du réseau Internet, ils sont également les premiers à avoir mis en œuvre des technologies de surveillance des moyens de communication. Les attentats du 11 septembre n'ont fait que renforcer la volonté des autorités de contrôler la circulation de l'information sur la Toile.

Aux Etats-Unis, où plus d'un Américain sur deux est connecté à la Toile et où plus de 50 % des utilisateurs possèdent des connexions à haut débit, Internet est un indispensable outil de communication. Néanmoins, les attentats du 11 septembre 2001, ainsi que le recours supposé des terroristes à Internet pour communiquer entre eux et préparer leurs actions, ont sensiblement modifié l'approche du gouvernement américain vis-à-vis du Réseau.

Ainsi, quelques heures seulement après les attentats, 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 recueillir des informations sur d'éventuels échanges par e-mails 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 DCS 1000) sur les principaux serveurs informatiques des fournisseurs d'accès basés aux Etats-Unis. Selon les journalistes de *Wired*, "des agents du FBI se sont présentés afin d'installer leurs machines. Ils ont promis de prendre en charge tous les frais d'installation et d'exploitation." Le FBI aurait par ailleurs exigé de responsables de ces géants d'Internet - et obtenu - toutes les informations provenant de comptes dont l'adresse comportait le mot "Allah". Tous les grands fournisseurs d'accès auraient suivi l'exemple de Hotmail et pleinement collaboré avec les services de sécurité américains.

Assouplissement des procédures

Carnivore est un logiciel "d'écoute électronique" créé par le FBI. Il permet, après avoir été installé chez un fournisseur d'accès, d'enregistrer et de stocker toutes les données échangées par les utilisateurs. L'opération se fait par le biais de filtres d'analyse sémantique, sans faire de distinction entre les différents contenus interceptés, ce qui peut donc outrepasser le mandat d'une écoute classique. Combattu par les

défenseurs des libertés civiles aux Etats-Unis, ce système n'avait été utilisé jusqu'à présent qu'avec l'accord préalable d'un juge. Cependant, un texte intitulé "Combating terrorism act", voté en toute urgence après une demi-heure de débat par le Sénat le 13 septembre, soit à peine deux jours après les attentats, a exempté les services de sécurité américains de l'aval de la justice pour l'utilisation de Carnivore. Un enquêteur (prosecutor) pourra ainsi ordonner la surveillance électronique d'un individu pendant quarante-huit heures sans avoir à demander l'accord d'un juge.

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 du "USA-Patriot Act" (Provide Appropriate Tools Required to Intercept and Obstruct Terrorism). Cette loi, votée à une écrasante majorité, 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, dont les activités sont confidentielles, est nécessaire. Le texte allonge également la liste des informations que les enquêteurs peuvent exiger des fournisseurs d'accès sans l'aval d'un juge. Il autorise également ces derniers à remettre aux autorités, de leur propre initiative, des informations qui ne sont pas relatives au contenu, telle la navigation sur le web.

Une nouvelle étape a été franchie le 20 novembre 2002 avec l'approbation par le Sénat du Homeland Security Act, une loi qui instaure un superministère de l'Intérieur dont la mission est d'empêcher de nouvelles attaques terroristes. La nouvelle administration créée intégrera progressivement 170 000 fonctionnaires qui travaillaient jusqu'alors dans vingt-deux ministères et agences de l'Etat. La section 225 de cette loi sur la cybersécurité autorise les fournisseurs d'accès à révéler le contenu de communications électroniques à une administration, locale ou fédérale, s'ils pensent, "de bonne foi", que sa transmission aux autorités peut prévenir un danger de mort ou de blessure grave. L'organisation Electronic Frontier Foundation (EFF) souligne que, dans cette hypothèse, le fournisseur assume des responsabilités qui incombent normalement aux juges. Elle dénonce également que la révélation du contenu des communications se fasse dorénavant sur la base de la "bonne foi" du fournisseur d'accès et non plus sur celle d'"une croyance raisonnable". EFF souligne que la menace invoquée peut dès lors être très diffuse. La section 225 autorise également les agents de la loi à enregistrer, sans mandat, tout message envoyé ou reçu par un "ordinateur protégé" (tout ordinateur utilisé pour le commerce ou les communications entre Etats) qui fait l'objet d'une attaque. Elle porte également à vingt ans de prison la sanction d'un crime informatique provoquant des blessures graves, et à la prison à vie si le crime provoque la mort d'une personne.

La cryptographie au banc des accusés

Dans le même élan, de nombreux responsables américains s'en sont pris à 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. La cryptographie, utile notamment aux entreprises souhaitant échanger des données économiques sensibles, n'a jamais été interdite aux Etats-Unis. Son utilisation est néanmoins soumise à autorisation pour l'exportation, en application de l'Arrangement de Wassenaar qui exige le contrôle des marchandises à double usage, civil et militaire. L'après-11 septembre a relancé le débat entre les partisans de la cryptographie et ses opposants.

Déjà, en mars 2001, le directeur du FBI, s'était dit convaincu de l'utilisation de la cryptographie par les réseaux terroristes. Le 13 septembre, le sénateur républicain Judd Gregg a proposé, dans un discours prononcé devant le Congrès, l'interdiction globale des logiciels de cryptographie dont les diffuseurs n'auraient pas fourni à l'autorité publique la clé permettant de déchiffrer les messages.

Les autorités ont opportunément rappelé qu'après le premier attentat contre le World Trade Center, en 1993, le FBI avait découvert sur l'ordinateur portable du responsable reconnu de cette attaque des plans de détournement de onze avions de ligne américains. Le FBI avait alors mis dix mois à déchiffrer ces fichiers, dont la grande majorité avaient été cryptés à l'aide du logiciel PGP (Pretty Good Privacy). Le père de PGP, David Zimmerman, qui a failli connaître la prison aux Etats-Unis dans les années 1980 pour avoir diffusé largement son programme, a encore une fois défendu ses positions dans un entretien accordé au magazine *Futur(e)s* : " Que ce soit au Congrès, dans les tribunaux ou dans les colonnes des journaux, le pays a déjà débattu de cette question au cours de la dernière décennie. Et, tous ensemble, nous avons décidé que la société avait plus à gagner qu'à perdre d'une cryptographie forte. Il ne faut pas oublier que la cryptographie 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 sous les dictatures."

En outre, les logiciels de cryptographie sont mis à mal par le programme "Lanterne magique" ("Magic Lantern") du FBI. Envoyé par e-mail, ce virus, du type "cheval de Troie", enregistre à leur insu les touches sur lesquelles frappent les internautes. Il permettrait ainsi au FBI d'identifier les mots de passe et les clés des programmes de cryptage. Après les révélations de la presse à ce sujet, l'agence de renseignements américaine a démenti disposer d'un tel outil mais reconnaît travailler sur sa conception.

Contre la censure... mais pour le contrôle?

Si les autorités tentent de contrôler la circulation de l'information sur la Toile et surveiller ce qui s'y dit, 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* a révélé que le Bureau de l'influence stratégique (OSI, Office of Strategic Influence), un service du département d'Etat à la Défense, proposait de recourir à la diffusion de fausses informations auprès des médias étrangers, notamment en les diffusant sur de faux sites Internet, 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, a affirmé que M. Bush ignorait tout du projet de l'OSI et a ordonné la fermeture de ce bureau au motif, selon Donald Rumsfeld, que "le Pentagone ne ment pas au peuple américain" ni "aux audiences étrangères".

L'administration Bush pourrait d'ailleurs utiliser le Réseau pour briser le monopole de l'information qui sévit encore dans plusieurs Etats autoritaires. Le 2 octobre 2002, deux élus de la Chambre des représentants ont présenté un projet de loi visant à lutter contre la censure dans le monde. Le Global Internet Freedom Act ("Loi sur la liberté de l'Internet dans le monde") propose la création d'un Bureau fédéral de la liberté de l'Internet qui aura pour mission "de contrer les interférences et la censure sur Internet" imposées par des Etats autoritaires. Il soutiendra également les personnes persécutées pour leur usage d'Internet. Le Bureau serait rattaché à l'International Broadcasting Bureau, qui administre les stations de radio déjà existantes et qui visent à contourner la censure, telles que *Radio Free Europe* ou *Radio Free Asia*. Son budget serait de 50 millions de dollars pour les années 2003 et 2004.

Mais qu'est-ce que la censure ? Le Global Internet Freedom Act précise que les Etats-Unis ne prendront aucune mesure contre la censure imposée par les gouvernements afin de protéger les mineurs. En la matière, le procès qui oppose plusieurs organisations de défense des libertés individuelles et bibliothèques publiques à l'administration Bush sur le Children's Internet Protection Act (Loi de protection des mineurs à l'égard d'Internet) commence à prendre des proportions importantes. Le 12 novembre 2002, la Cour suprême a annoncé qu'elle statuera sur la constitutionnalité de cette loi, adoptée en 2000, qui oblige toute bibliothèque recevant des subventions fédérales pour s'équiper d'Internet à installer des filtres antipornographie. Ses détracteurs avaient dénoncé la loi au motif qu'elle viole le 1er amendement de la Constitution qui garantit la liberté d'expression. Ils soulignent également qu'en dehors des sites pornographiques, les logiciels de filtrage suppriment également l'accès à d'autres sites. En mai 2002, trois juges fédéraux de Philadelphie leur ont donné raison, considérant qu'en forçant les bibliothèques publiques à installer de tels filtres, la loi contraignait ces dernières à censurer des discours protégés par la Constitution. L'administration Bush a fait appel devant la Cour suprême au motif que le logiciel utilisé était le meilleur disponible pour empêcher l'argent des contribuables de subventionner l'expansion de sites obscènes ou de matériel inapproprié pour les enfants. 10 % des quelque 143 millions d'internautes aux Etats-Unis ont accès à Internet grâce aux bibliothèques publiques. 80 % d'entre elles ont reçu des aides fédérales pour s'équiper d'Internet.

Un avenir orwellien ?

Début novembre 2002, la presse américaine a annoncé l'ouverture au sein du Pentagone d'un nouveau bureau, baptisé Information Awareness Office (Bureau de veille de l'information). Ce bureau est chargé de développer de nouvelles technologies qui permettraient, par un tri d'informations relatives à la navigation sur Internet, telles que des achats par carte bleue ou des réservations de billets d'avions,

d'identifier des comportements de terroristes potentiels. Le projet, financé par le secrétariat d'Etat à la Défense, recevra 200 millions de dollars par an. Selon John Poindexter, directeur de ce nouveau bureau, les systèmes développés aideront les analystes à sélectionner les informations sur les voyages dans des zones jugées dangereuses, à identifier des e-mails douteux, à reconnaître des transferts de fonds douteux... Les informations seront récupérées grâce à des machines qui permettront aux agences de renseignements, avec la permission des gouvernements et des entreprises, d'extraire régulièrement de l'information. Un projet qualifié d'"orwellien" par ses détracteurs. Plusieurs organisations de défense des libertés individuelles s'accordent à dire que des informations relatives à des personnes sans rapport avec le terrorisme, et dont l'Etat n'a pas à avoir connaissance, seront forcément exfiltrées. Selon Marc Rotenberg, directeur de l'Electronic Privacy Information Center (EPIC), les autorités se retrouveront en possession d'informations jusqu'alors uniquement accessibles au pouvoir judiciaire dans le cadre d'enquêtes criminelles. Il dénonce le fait qu'il n'existera aucune entité chargée de contrôler les informations qui seront ainsi collectées.

Condamné en 1990 à six mois de prison pour avoir menti au Congrès dans le cadre de l'affaire Iran-Contras, John Poindexter a finalement vu sa peine annulée au motif que ses droits n'avaient pas été respectés.

LIENS :

Associations de défense des libertés civiles et de l'Internet

- American Civil Liberties Union
www.aclu.org
- The Center for Democracy and Technology
www.cdt.org
- The Digital Freedom Network
www.dfn.org
- The Electronic Frontier Foundation
[www.eff.org](http://www EFF.org)
- The Electronic Privacy Information Center
www.epic.org
- Peacefire
www.peacefire.org
- The Reporters Committee for Freedom of the Press
www.rcfp.org

Documents

- USA Patriot Act

www.eff.org/Privacy/Surveillance/Terrorism_militias/hr3162.php

- Homeland Security Act

www.whitehouse.gov/deptofhomeland/bill/index.html

- Global Internet Freedom Act

www.theorator.com/bills108/hr48.html

- Information Awareness Office

www.darpa.mil/iao

- Children's Internet Protection Act

www.ifea.net/cipa.html

Sur Carnivore

- www.fbi.gov/hq/lab/carnivore/carnivore2.htm

- www.epic.org/privacy/carnivore

Site d'informations spécialisé

- www.wired.com



EUROPE

France

POPULATION : 59 453 000

INTERNAUTES : 18 716 000

FOURNISSEURS D'ACCÈS PRIVÉS : OUI

Le nouvel arsenal législatif visant à lutter contre le terrorisme et contre la criminalité sur Internet met en cause la protection des informations et des sources.

Votée le 15 novembre 2001 en urgence, et quasiment à l'unanimité au terme d'un débat inexistant, la Loi sur la sécurité quotidienne (LSQ) a porté à un an la durée de conservation des archives de toutes les activités en ligne des clients et des données relatives aux envois et réceptions de e-mails par les fournisseurs d'accès à Internet. Elle autorise par ailleurs les juges à recourir aux "moyens de l'État soumis au secret de la Défense nationale" pour décrypter les messages. Elle oblige ainsi les fournisseurs de moyens de cryptographie à fournir aux autorités leurs protocoles de chiffrement. Les organisations de défense de la liberté d'expression 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.

Adoptée le 31 juillet 2002, la Loi d'orientation et de programmation pour la sécurité intérieure (LOPSI) autorise les officiers de police judiciaire, sur autorisation d'un magistrat, à "accéder directement à des fichiers informatiques et saisir à distance par la voie télématique ou informatique les renseignements qui paraîtraient nécessaires à la manifestation de la vérité".

Le projet de loi sur l'économie numérique (LEN), présenté par le gouvernement le 15 janvier 2003, a vocation à transposer en droit français la Directive européenne de 2000 sur le commerce électronique. La LEN introduit une clause sur la responsabilité civile et pénale des prestataires techniques, qui avait été annulée par le Conseil constitutionnel dans le projet de loi sur la société de l'information préparé en 2001 par le précédent gouvernement. L'article 2 dégage l'hébergeur de toute responsabilité civile et pénale à condition qu'il n'ait pas "eu effectivement connaissance d'une activité ou d'une information illicite" ou qu'il ait "agi promptement pour retirer les informations ou rendre l'accès à celles-ci impossible dès le moment où [il en a eu] de telles connaissances". Les hébergeurs sont également déchargés de toute responsabilité civile dès lors qu'ils "n'ont pas eu connaissance de faits ou de circonstances selon

lesquelles l'information ou l'activité illicite est apparente". Ce projet de loi a été adopté en première lecture par l'Assemblée nationale le 25 février 2003.

LIENS :

- L'association Iris (Imaginons un Réseau Internet Solidaire)

www.iris.sgdg.org

- Commission Nationale de l'Informatique et des Libertés (CNIL)

www.cnil.fr

- Textes officiels de référence

www.internet.gouv.fr



Inde

POPULATION : 1 025 096 000

INTERNAUTES : 16 580 000

FOURNISSEURS D'ACCÈS PRIVÉS : OUI

Prometteur, le développement d'Internet en Inde est entravé par un réseau téléphonique de médiocre qualité et les pressions exercées par le pouvoir. Deux lois, dont l'une votée suite aux attentats du 11 septembre, permettent de contrôler la Toile et de criminaliser un grand nombre d'agissements des internautes.

Dès le mois de mai 2000, le Parlement a adopté une loi sur la cybercriminalité, l'Information Technology Act. Elle définit comme un crime "l'accès sans autorisation à des informations électroniques". Le piratage est passible de peines allant jusqu'à trois ans de prison et de lourdes amendes. Les perquisitions de domiciles d'internautes et de cybercafés sont autorisées à tout moment et sans mandat, pour peu qu'on soupçonne des crimes informatiques. Enfin, toute personne responsable du lancement de site "anti-indien" risque cinq années d'emprisonnement.

En mars 2001, la presse a révélé que la police et des agences gouvernementales exercent des pressions régulières sur les fournisseurs d'accès et de services pour obtenir des informations personnelles sur les internautes. Le président de l'un des plus importants opérateurs du pays, Rediff.com, affirme qu'il est sollicité environ une fois par mois par la police et d'autres services d'Etat, mais "qu'il refuse de leur fournir des informations". Le patron de Satyam Infoway, l'un des principaux fournisseurs d'accès privés, confirme être soumis à des pressions quasi constantes.

Fichage des habitués des cybercafés

L'encadrement législatif strict de la Toile permet d'engager des poursuites contre quiconque déroge aux "règles morales et politiques" édictées par le pouvoir. Pour preuve, l'enquête ouverte en avril 2001 contre les élèves de l'une des plus grandes écoles de New Delhi. La police leur reprochait d'avoir créé "un site pornographique" mettant en scène leurs professeurs et camarades de classe. L'affaire a débuté lorsque le père d'une élève a porté plainte après avoir découvert le nom de sa fille sur le site. Régulièrement dénoncés par les autorités comme un fléau massivement répandu sur le Réseau, les sites pornographiques sont consultés abondamment dans les très

nombreux cybercafés qui ont poussé comme des champignons dans les grandes agglomérations. Pour montrer leur bonne volonté, ces établissements affichent des avertissements pour en éloigner le jeune public.

En mai 2001, la police de Mumbai a quant à elle annoncé que, pour se connecter à Internet depuis un cybercafé de la ville, il faut présenter une carte d'identité, un permis de conduire, une carte d'étudiant ou, pour les étrangers, un passeport ou des billets d'avion. A terme, chaque utilisateur d'Internet jugé "convenable" se voit délivrer une carte d'identité "spéciale client de cybercafé". Cette décision est loin de satisfaire les propriétaires de cafés Internet. Inflexibles, les représentants des autorités justifient cette mesure par le fait que, quotidiennement, une cinquantaine de plaintes sont déposées pour fraudes à la carte bancaire, piratage, activités terroristes supposées ou pornographie sur Internet.

Par ailleurs, en juin 2002, les services secrets indiens (Intelligence Bureau) auraient demandé au FBI américain de l'aider à développer des logiciels permettant de surveiller les téléphones portables et les e-mails des membres de groupes criminels et terroristes. Selon le site d'informations *rediff.com*, des négociations sont en cours pour mettre en place cette collaboration entre les deux agences de renseignements.

Le secret des sources journalistiques menacé

En novembre 2001, une loi, l'Ordonnance sur la prévention du terrorisme (POTO), a été promulguée dans la foulée des attentats du 11 septembre. Elle permet au gouvernement de surveiller tous types de communications, dont les communications électroniques telles que les e-mails. Et ce, sans contrôle judiciaire ou administratif. Les éléments recueillis au terme de ces interceptions de messages peuvent être utilisés à charge contre un suspect, devant une cour. Pour légitimer sa politique de lutte contre la cybercriminalité et le terrorisme, le gouvernement indien a décidé de partager ses informations avec les services spécialisés américains.

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 seraient passibles de cinq années d'emprisonnement. Suite aux critiques de l'opposition et des organisations de défense des droits de l'homme et de la liberté d'expression, les députés ont retiré l'article obligeant les journalistes à révéler leurs sources et éléments dans les dossiers terroristes. La loi a été votée pour une durée de trois ans, et non pour cinq ans comme prévu initialement.

***Thelka* harcelé par les autorités**

Cet encadrement du Net n'empêche pourtant pas les audacieux de se servir de la Toile comme d'un nouveau vecteur de liberté de la presse. Ainsi, en mars 2001, le site d'informations *Thelka*, qui signifie "faire sensation" en Hindi, a justifié son appellation. Vidéos à l'appui, ses journalistes d'investigation, qui se sont fait passer pour des

marchands d'armes, ont révélé que des hommes politiques, des fonctionnaires et des hauts gradés de l'armée avaient accepté des pots-de-vin et des relations avec des prostituées en échange de coups de pouce pour pénétrer les marchés publics, militaires notamment. Cette enquête sur la corruption en Inde a secoué la classe politique et menacé le gouvernement. George Fernandes, ministre de la Défense, et le président du Parti Bharatiya Janata (Parti du peuple indien), Bangaru Laxman, ont dû démissionner de leur poste.

Si cette affaire a cristallisé le nouveau rôle médiatique d'Internet, elle a aussi valu à ses instigateurs un sévère retour de bâton. Le rédacteur en chef de *Tehelka* s'est plaint des manœuvres des services du Premier ministre pour discréditer sa rédaction. *Tehelka* a notamment été accusé d'être financé par les services secrets pakistanais et le crime organisé. Les journalistes à l'origine du scoop ont été menacés physiquement et ont dû être placés sous étroite protection policière.

Ainsi, le 26 juin 2002, une vingtaine d'officiers du Bureau central d'investigation (CBI) perquisitionnent au siège de *Tehelka*, à New Delhi, ainsi qu'au domicile d'un de ses journalistes, Kumar Badal. Ce dernier est accusé par le CBI d'avoir engagé des braconniers pour tuer et filmer deux léopards appartenant à une espèce protégée dans la jungle de Saharanpur (Etat de l'Uttar Pradesh, nord du pays). Pourtant, selon des témoins, le CBI s'est révélé incapable de produire des documents, saisis dans les locaux du site, relatifs à cette affaire. Les officiers auraient en revanche confisqué des documents concernant la fondation du site, notamment des e-mails de Shankar Sharma, propriétaire de la compagnie First Global et financier initial du site, aujourd'hui en prison. En outre, la perquisition a été opérée quelques heures avant la déposition du rédacteur en chef du site, Tarun Tejpal, devant la Commission Venkataswami. Créée par le gouvernement, cette instance a pour mission d'enquêter sur une affaire de corruption révélée par le site en mars 2001. L'audition de Tarun Tejpal, prévue le même jour que celle de l'ancienne présidente du parti Samata, Jaya Jaitly - intermédiaire supposé entre des trafiquants d'armes et l'entourage de l'ancien ministre de la Défense -, a finalement été reportée. Selon l'avocat du site Internet, Kavin Gulati, l'enquête en était à un "moment crucial de l'interrogatoire croisé" des témoins, ce qui le laisse conclure que le choix de la date de perquisition était "absolument motivé". Le porte-parole du CBI a rétorqué qu'il s'agissait "d'une pure coïncidence".

Pour sa part, Kumar Badal, journaliste de *Tehelka* âgé de 29 ans, est arrêté le 3 juillet. Lors d'une grève de la faim, le journaliste en ligne déclare : "Toutes les souffrances que je dois endurer sont tout simplement dues au fait que je suis journaliste de *Tehelka* qui a pris fait et cause pour rendre compte de la corruption qui règne au plus haut niveau de l'Etat." Il est détenu en vertu de la Loi sur la protection de la nature. Le journaliste a reçu le soutien de sa rédaction et clame son innocence depuis le début de la procédure. Lors de sa détention, il a été l'objet de multiples brimades. Après six mois de détention, Kumar Badal a été libéré sous caution, le 13 janvier 2003, suite à une décision de la Cour suprême de New Delhi. Sa libération a été saluée par Tarun Tejpal, rédacteur en chef du site : "On a dit et redit que nous étions

victimes de représailles. Cette situation dure depuis deux ans. Nous sommes soulagés que notre reporter soit enfin libéré.” L’avocat du journaliste a dû verser une somme de cinquante mille roupies (près de 1 000 euros) pour la caution. La police fédérale a tenté le jour même de faire échouer cette libération prononcée par deux juges de la Cour suprême, sous le prétexte que l’enquête n’est pas finie. Bien qu’il soit désormais libre, Kumar Badal est assigné à résidence à New Delhi et devra se présenter dans les bureaux du Central Bureau Investigation tous les premiers lundis du mois. Il est également interdit d’entrée dans le district de Saharanpur (nord du pays) où la plainte a été déposée.

Le harcèlement à l’encontre de *Tehelka* explique en partie l’échec du site qui annonce, début 2003, son incapacité à maintenir son édition quotidienne. En une du site, Tarun Tejpal en donne les raisons : “Au cours des deux dernières années, *Tehelka* aura tout vu. Un travail acharné, une réputation incroyable, des accolades générales. Nous avons aussi fait face à une victimisation sans retenue de la part du puissant establishment à la suite de nos révélations sur la Défense. En deux ans, nous sommes passés de 120 personnes à trois (...), certains de nos employés ont été harcelés et arrêtés, et nos dettes se sont accumulées (...) nous espérons revenir pour construire des médias libres en Inde.”

Un journaliste emprisonné pour avoir téléchargé un document sur Internet

Le 7 septembre 2002, la police de New Delhi a inculpé d’espionnage le journaliste Iftikhar Gilani, chef du bureau du *Kashmir Times* à New Delhi, et correspondant du quotidien pakistanais *The Nation*, l’accusant d’avoir fourni au Pakistan des documents sur la position des troupes et des forces paramilitaires indiennes au Cachemire. L’acte d’accusation repose sur plusieurs articles de la Loi sur les secrets officiels, sur l’article 120-B (relatif à la conspiration criminelle) et sur l’article 292 (relatif à la pornographie) du code pénal indien. Après avoir successivement accusé Iftikhar Gilani de délit financier, d’espionnage et de pornographie, la police affirme avoir trouvé sur son ordinateur un document téléchargé sur un site Internet concernant le conflit armé au Cachemire. Ce document est accessible à tous les internautes. Mais la juge en charge de l’affaire a affirmé ne “pas avoir eu le temps de consulter” le site en question. Iftikhar Gilani, détenu depuis le 9 juin 2002 dans la prison de Tihar (proche de New Delhi), clame son innocence. Le journaliste a affirmé à Reporters sans frontières être “très déprimé”. Au début de sa détention, il a été frappé par des codétenus et il s’est vu refuser par les autorités l’accès à la bibliothèque de la prison. Au cours des mois de septembre, octobre et novembre, la cour a rejeté les demandes de libération sous caution déposées par l’avocat du journaliste. Le 23 décembre, un responsable des services secrets de l’armée indienne affirmait devant la juge qu’il n’y avait rien de secret dans les informations trouvées dans l’ordinateur de M. Gilani. Suite à ces déclarations, le gouvernement indien a été contraint d’abandonner la plainte et de demander à la cour, le 10 janvier 2003, de libérer le journaliste. Dans la soirée du 13 janvier, Iftikhar Gilani est libéré de prison. A sa sortie de prison, le journaliste déclare : “Il est temps que les personnes raisonnées, les journalistes et les hommes politiques abroge la loi sur les secrets d’Etat”.

LIENS :

- Le site d'informations *Tehelka*
<http://tehelka.com>
- Le département des Télécommunications
www.dotindia.com
- Le magazine indépendant *Frontline*
www.flonnet.com
- Le magazine informatique *Dataquest*
www.dqindia.com

Institutions européennes

Opposée à toute forme de “surveillance électronique généralisée ou exploratoire pratiquée à grande échelle”, l’Union européenne a revu sa position depuis les attentats du 11 septembre 2001. Le Conseil européen a gagné son bras de fer contre le Parlement pour imposer les vues des quinze Etats membres. A savoir : légiférer pour imposer la rétention généralisée des données de télécommunications et de connexion à Internet.

Jusqu’à la fin de l’été 2001, la politique officielle des Quinze en matière de régulation du cyberspace réfute toute idée de conservation généralisée des données de connexion et de surveillance d’Internet. Les attentats du 11 septembre relancent le débat.

Mi-octobre 2001, le président Bush écrit au Premier ministre belge, Guy Verhofstadt, alors président en exercice de l’Union, pour lui demander qu’un projet de directive européenne soit modifié pour tenir compte du contexte antiterroriste, afin que soit instituée la “rétention préventive” des données de connexion à Internet (logs de connexions). Dans son courrier, le président américain apporte son soutien au gouvernement britannique (qui, comme la France, a instauré cette rétention des données de connexion 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 communications électroniques.

Georges Bush précise au Premier ministre belge que les États-Unis s’opposent au principe de l’effacement automatique des données de connexion, 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.

Cette position va à l’encontre de celle de la Commission des libertés et des droits du citoyen du Parlement européen qui 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.

“Surveillance interdite”

Le rapport Cappato indique 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. 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”.

Néanmoins, sous la pression du Conseil européen, et malgré un lobbying actif de nombreuses ONG, les députés adoptent, le 30 mai 2002 la nouvelle directive. L’article 15.1 du nouveau texte impose désormais aux gouvernements européens qui ne se sont pas encore dotés d’arsenal législatif en la matière, de légiférer (dans un délai de quinze mois) 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 Quinze, dévoilé le 15 octobre 2001, expliquait pourtant que les gouvernements de l’Union avaient déjà les pouvoirs nécessaires pour intercepter les télécommunications en vue de combattre le terrorisme.

Convention contre la cybercriminalité

Après quatre années d’élaboration par le Conseil de l’Europe, la première Convention internationale contre la cybercriminalité a été signée à Budapest (Hongrie), le 26 novembre 2001. Premier traité international sur les infractions pénales commises via l’Internet et d’autres réseaux informatiques, la Convention contient une série de pouvoirs de procédures, comme la perquisition des réseaux informatiques et l’interception. Elle entrera en vigueur dès qu’elle aura été ratifiée par cinq pays, dont au moins trois membres du Conseil de l’Europe. A ce stade, la Convention a été signée par trente-quatre pays, dont les Etats-Unis, le Canada, le Japon et l’Afrique du Sud, mais seuls deux Etats l’ont ratifiée, l’Albanie et la Croatie.

Cette Convention est dénoncée par les défenseurs des libertés, les fournisseurs d’accès à Internet et, plus généralement, les professionnels du cyberspace qui la qualifient de dispositif “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 qui recèlent des informations intéressant 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’infor-

mations 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 citoyens européens”

Et ce n'est qu'un début. La présidence danoise de l'Union européenne a soumis, le 24 juin 2002, une proposition de mesures qui pourrait être portée 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". La proposition vise par ailleurs à harmoniser les législations de tous les pays européens, y compris les pays candidats qui rejoindront sous peu l'Union européenne.

LIENS :

- Le Parlement européen

www.europarl.eu.int

- Le Conseil de l'Europe

www.coe.int



Irak

POPULATION : 23 584 000

La chute du régime dictatorial de Saddam Hussein en avril 2003, suite à l'intervention militaire anglo-américaine, est porteuse de nombreux espoirs de changements pour les médias en général et Internet en particulier. Pour mémoire, la situation en 2002 était la suivante.

En Irak, l'information était placée sous le contrôle des autorités et les médias étaient censurés en conséquence. De même, le monopole était de mise en matière de fourniture d'accès à Internet. Le seul opérateur, Uruklink, dépendait directement du ministère de la Culture et de l'Information. Et les Irakiens ne pouvaient surfer que dans l'un des vingt-six "Centres Internet" ouverts sur le territoire. Il était impossible de disposer d'une connexion privée, à son domicile par exemple. Pour les experts étrangers, la raison en était simple : les autorités ne maîtrisaient pas encore l'utilisation des logiciels et dispositifs de filtrage et de blocage généralisé de sites.

Selon le témoignage d'un journaliste de la *BBC*, les employés des "Centres Internet" vous prévenaient, si vous étiez étranger, de ne pas chercher à vous connecter à votre compte mail personnel. Le site Hotmail, ainsi qu'un très grand nombre de sites et portails étrangers, étaient inaccessibles. Et chercher une parade relevait du challenge. Les ordinateurs étaient placés face aux murs et les hommes du Département Internet du gouvernement menaient des rondes dans les salles. Si vous étiez pris en train de vous connecter à un site étranger prohibé, ou si vous cherchiez à le faire, ils intervenaient pour couper la connexion et vous demander de quitter les lieux. Mais l'arme la plus efficace du régime pour contrôler le Net restait indubitablement la situation économique du pays. Une heure de connexion dans un "Centre Internet" coûtait un dollar alors que le salaire mensuel d'un fonctionnaire (l'administration est le premier employeur du pays) était de cinq dollars.

Au Kurdistan irakien, la situation était très différente : la marge de liberté des médias était beaucoup plus importante qu'en Irak et Internet nettement plus présent et plus libre.

LIENS :

- Agence de presse indépendante : www.iraqpress.org

Iran

POPULATION : 71 369 000

INTERNAUTES : 1 005 000

FOURNISSEURS D'ACCÈS PRIVÉS : OUI



Avec la fermeture de près d'une centaine de journaux depuis avril 2000, Internet est devenu le média grâce auquel les journalistes peuvent s'exprimer librement et appeler à davantage de libertés et de réformes. Agacés par ce nouveau procédé, les conservateurs, comme les réformateurs, ont renforcé leur contrôle de la Toile. Depuis janvier 2003, plusieurs animateurs de site et internautes ont été arrêtés.

Les fournisseurs d'accès privés à Internet ont commencé à se développer timidement en Iran dès 1994, à l'ombre du puissant opérateur public, Data Communication Company of Iran (DCI), placé sous l'autorité directe du ministère des Renseignements. L'arrivée au pouvoir, en 1997, du président réformateur Mohammad Khatami a fait souffler un vent d'espoir sur la Toile nationale. Puis, suite à la fermeture de près de cent journaux depuis avril 2000, les réformateurs ont créé des sites d'informations comme Emrooz, Rouydad ou Alliran. Des sites féminins ont également vu le jour comme Zanan Iran ou Zan. En 2002, les Iraniens, et tout particulièrement les jeunes et les femmes, ont été conquis par le weblog, le site personnel. Cet engouement pour Internet - on dénombre au moins 1 500 cybercafés dans la seule capitale - a rapidement fait peur au régime qui a mis en place des mesures pour le contrôler.

Les fournisseurs d'accès privés doivent, pour exercer leurs activités, obtenir un agrément des ministères des Renseignements et de l'Orientation islamique. Ils disposent par ailleurs d'un système de filtrage des sites et des courriers électroniques. En outre, chaque internaute qui ouvre une connexion au Web est tenu de signer un document stipulant qu'il s'engage à ne pas consulter des sites "non islamiques".

Les propriétaires de cybercafés, très fréquentés, notamment dans la capitale, par les jeunes, les étudiants et les intellectuels qui forment le gros du "bataillon" des internautes, demandent à ces derniers de se déconnecter s'ils les surprennent à surfer sur des sites qui contreviennent aux principes de l'islam. Les sites des mouvements d'opposition ou les sites critiques à l'égard du pouvoir sont, quant à eux, hébergés à l'étranger. Ils sont très visités par les Iraniens qui parviennent à contourner la censure.

Des mesures pour museler Internet

En mai 2001, le régime a renforcé son contrôle sur les cybercafés. Quatre cents d'entre eux ont été fermés à Téhéran. Depuis, une partie a rouvert. En novembre 2001, le Haut Conseil de la révolution culturelle, dirigé par le président Mohammad Khatami mais dominé par les conservateurs, a décrété que toutes les sociétés privées offrant un accès à Internet devaient démanteler leurs installations ou transférer leur matériel vers le secteur public. Ce décret est entré en application à la fin de l'année.

Le 2 janvier 2003, Ali Younessi, ministre des Renseignements, a dénoncé "la guerre larvée" menée à travers les sites Internet qui "diffusent des rumeurs et de la désinformation sur tous les responsables et les organes du pouvoir".

En janvier 2003, une commission a été créée pour recenser les sites d'informations jugés "illégaux". Cette commission qui regroupe des représentants des ministères de la Culture et des Renseignements, ainsi que de la radio et télévision d'Etat, fournit une liste des sites "illégaux" au ministère des Postes et Télécommunications qui la transmet auprès des fournisseurs d'accès, chargés d'en assurer le filtrage. Entre cent à trois cents sites, dont la majorité de sites d'informations, seraient inscrits sur cette fameuse liste noire.

Début mai, Abdolnabi Namazi, procureur général du pays, a annoncé la création d'une seconde commission chargée des délits commis sur Internet. Il a notamment affirmé que les auteurs d'écrits publiés sur des sites créés en Iran "devaient respecter le cadre de la Constitution et de la loi sur la presse, sinon ils encouraient une action légale". "Dans la mesure où nous n'avons pas encore de loi sur les délits commis sur Internet, les tribunaux peuvent se référer à la loi sur la presse", qui prévoit de lourdes peines de prison. Cette commission a pour rôle principal d'élaborer un projet de loi sur Internet.

En mai, le vice-ministre des Postes et Télécommunications, Massoud Davari-Nejad, a déclaré que son ministère avait pris des mesures pour bloquer l'accès "aux sites immoraux ainsi qu'aux sites politiques qui insultent les personnalités politiques et religieuses du pays". Ainsi, lorsque des internautes veulent accéder à un site illégal, ils sont avertis que "suite aux instructions du ministère des Postes et Télécommunications, la visite de ce site est interdite". Des mesures ont également été prises à l'encontre des fournisseurs d'accès. Début mai, dans la ville de Tabriz (nord de l'Iran), cinq fournisseurs d'accès privés ont été fermés parce qu'ils n'avaient pas mis en place un système de filtrage pour les sites interdits. La majorité de ceux qui restent autorisés sont... gouvernementaux. A Téhéran, durant la même période, au moins sept fournisseurs d'accès privés ont été fermés pour les mêmes raisons.

Ce contrôle croissant d'Internet est apparu, au fil du temps, comme n'étant plus l'apanage des seuls conservateurs. En mai, en effet, Abdollah Ramezanzadeh, porte-parole du gouvernement, et Ahmad Motamedi, ministre des Postes et des Télécommunications (tous deux réformateurs) ont mis en garde les propriétaires des

fournisseurs d'accès sur la non-application des nouvelles consignes et assuré que le système des filtrages était bel et bien légal.

Arrestation de webmasters et d'internautes

Le 16 janvier 2003, Javad Tavaf, rédacteur du site *Rangin Kaman*, a été arrêté à son domicile par des agents du ministère de la Justice. Son site d'informations, qui n'hésitait pas à critiquer le guide de la Révolution, l'ayatollah Khamenei, était, depuis un an, très visité. Il a été relâché le 18 janvier.

Le 18 février 2003, Mohamed Mohsen Sazegara, directeur du site d'informations *Alliran*, a été arrêté à son domicile par des membres des services de sécurité en civil. Son domicile, puis son bureau, ont été fouillés. De nombreux documents ont été confisqués. La semaine précédente, le journaliste avait diffusé, sur son site, un article dans lequel il appelait à une réforme de la Constitution. Il écrivait également que la volonté du peuple iranien était "prise en otage par six religieux du Conseil des gardiens" (instance, dominée par les conservateurs, dont les membres sont nommés par le Guide qui supervise les élections et ratifie les lois). Il a été libéré quelques jours plus tard.

En mars, près de soixante-dix jeunes filles et garçons ont été arrêtés à Téhéran pour avoir utilisé Internet pour organiser des rencontres et avoir des relations sexuelles interdites. Ils ont été libérés quelques jours plus tard.

Le 20 avril, Sina Motallebi, journaliste de *Hayat-é-No* et animateur du site *Rooznegar* a été arrêté après avoir été convoqué, la veille, par Adareh Amaken, une section de la police téhéranaise habituellement chargée des délits à caractère "moral" et considérée comme proche des services de renseignements. Après la fermeture, en janvier 2003, du quotidien réformateur *Hayat-é-No*, Sina Motallebi avait activé le site *Rooznegar* sur lequel il avait notamment pris la défense de Alireza Eshraghi, un journaliste de *Hayat-é-No*, arrêté le 11 janvier. Ce site, qui défendait notamment les journalistes emprisonnés, s'était attiré les foudres de certains réformateurs - qui y avaient été critiqués pour leur silence sur les arrestations de journalistes - et de la justice iranienne. Il a été libéré le 12 mai.

Internet utilisé aussi comme outil de propagande

La méfiance des conservateurs à l'égard du Net n'empêche pas son utilisation à des fins de propagande. Ainsi, des sites d'informations comme *Daricheh.org* ou *Jebhe.com* ont été mis en place et véhiculent les idées des durs du régime. L'université théologique de la ville sainte de Qom forme, par ailleurs, plusieurs milliers d'étudiants en informatique et de spécialistes d'Internet chaque année, afin que, selon un mollah de Qom, ils fassent "de leur savoir une utilisation à même de servir le pays et l'islam".

LIENS :

Sites d'informations

- www.daricheh.org
- www.jebhe.com (en persan)
- www.emrooz.org (en persan)
- www.rouydad.com (en persan)
- www.alliran.net (en persan)
- www.ranginkamaan.blogspot.com (en persan)

Sites féminins

- [www.womeniniran.com/ english.htm](http://www.womeniniran.com/english.htm)
- www.zan.org



Italie

POPULATION : 57 503 000

INTERNAUTES : 17 000 000

FOURNISSEURS D'ACCÈS PRIVÉS : OUI

Suite aux attentats du 11 septembre 2001, l'Italie a engagé une réforme de ses services de renseignements et une politique de lutte contre la criminalité sur Internet qui se sont traduites par un important renforcement de la surveillance de la Toile.

Pour lutter contre le terrorisme, le gouvernement italien a fait voter, fin 2001, une loi de réforme de ses services de renseignements. Ainsi, les agents des services secrets civils (SISDE) et militaires (SISMI), ainsi que les commandants des carabinieri et de la police nationale, sont désormais autorisés à procéder à des écoutes téléphoniques et électroniques sur simple autorisation du procureur de la République. Même si la nature secrète des activités au sein de ces services spéciaux empêche de savoir quels types d'écoutes sont à présent pratiqués, cette mesure a été vivement critiquée par les organisations de défense de la vie privée et de la confidentialité.

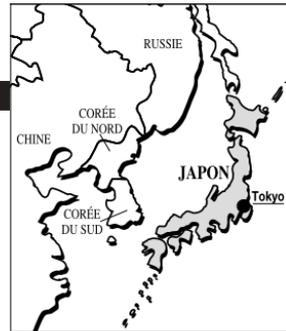
L'Italie, qui assurait la présidence du G8 au moment des attentats du 11 septembre, a également posé la première pierre, dans une déclaration officielle du 19 septembre 2001, d'une politique de "lutte contre la criminalité sur Internet et dans le domaine de la haute technologie". Cette politique s'est 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 crimes liés 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'Etat et de gouvernement, fin juin 2002.

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 ont particulièrement réagi à la révision de la Directive sur la protection des données de télécommunications (voir chapitre Institutions européennes). Ce texte, très controversé, voté le 30 mai 2002, modifie le régime européen en donnant la possibilité aux Etats membres de prévoir des mesures de rétention des données de télécommunications et de connexions à Internet (logs de connexions).

LIENS :

- L'Association pour la liberté dans la communication électronique interactive
ALCEI-EFI Electronic Frontiers Italy
www.alcei.it



Japon

POPULATION : 127 335 000

INTERNAUTES : 57 200 000

FOURNISSEURS D'ACCÈS PRIVÉS : OUI

Le succès populaire d'Internet au Japon, notamment sur les téléphones cellulaires, a été entaché par des révélations sur la participation de l'archipel au réseau d'espionnage électronique américain Echelon et sur la création d'un logiciel d'interception des courriers électroniques.

Féru de communication, de gadgets et de technologies numériques, les Japonais se sont naturellement, massivement et précocement intéressés à Internet. Sur l'archipel, outre les abonnements aux fournisseurs d'accès, les internautes fréquentent assidûment les cybercafés et l'avènement du "i-mode" lancé par DoCoMo, filiale de téléphonie mobile du géant nippon NTT, a ouvert une nouvelle voie dans la façon de surfer.

L'"i-mode", c'est le premier mariage réussi d'Internet et du téléphone cellulaire, qui permet de passer des coups de fil, mais aussi de regarder des vidéos de bonne qualité, d'écouter de la musique au format MP3 et, surtout, d'accéder à une kyrielle de services offerts par le Web. Entre quinze et vingt millions de personnes, essentiellement des jeunes gens de la tranche 15-34 ans, sont accros au "i-mode".

Paradoxalement, le pays accusait un retard par rapport à d'autres pays industrialisés en matière de connexions domestiques rapides et d'équipement de l'administration, de l'Education nationale notamment. En mars 2001, le gouvernement a lancé un plan destiné à combler ce retard. Baptisé "e-Japan strategy", il doit permettre de créer une infrastructure qui connectera trente millions de foyers nippons à l'Internet à grande vitesse et dix millions de foyers au Net à très grande vitesse d'ici à 2006.

Complice et victime d'espionnage

En 2001, le Japon a été fortement secoué par la révélation de sa participation au réseau espion d'écoute et d'interception des communications électroniques Echelon, créé par l'agence nord-américaine de sécurité nationale, la National Security Agency. Grâce à ses infrastructures (antennes paraboliques géantes, centres d'écoutes et d'interception, etc.) installées en des points stratégiques du globe (Etats-Unis, Grande-Bretagne, Nouvelle-Zélande, Japon et certainement ailleurs encore), ce

dispositif est capable d'intercepter, de trier, de classer et d'analyser les communications véhiculées par des signaux électriques et électroniques : téléphone, téléphone cellulaire, liaisons satellites, connexions par fibre optique, micro-onde, etc.

Le scandale a éclaté le 20 juin 2001, lorsqu'une délégation de plusieurs organisations non gouvernementales, emmenées par NaST (Networkers against Surveillance Taskforce), qui milite depuis 1997 contre la surveillance généralisée des nouveaux moyens de communication, a déposé devant le Parlement une motion réclamant que la lumière soit faite sur le rôle du Japon dans le dossier Echelon. S'il en ressort que le Japon a bien autorisé les Etats-Unis à installer une station d'écoute sur sa base de Misawa, au nord de l'île de Honshu, une autre question se pose : le Japon est-il lui-même victime de ce dispositif d'écoute, comme l'ont affirmé à maintes reprises de hauts fonctionnaires du ministère des Finances et du ministère du Commerce extérieur ?

Le quotidien *Mainichi Shimbun* a apporté quelques éléments de réponse. Selon une enquête publiée le 26 juin 2001, la Nouvelle-Zélande serait le "bras armé" des activités d'espionnage nord-américaines via Echelon contre les intérêts nippons. Une thèse étayée par Duncan Campbell, l'un des experts qui ont participé à l'enquête sur le réseau espion diligentée par le Parlement européen. Il a notamment révélé des cas concrets d'espionnage américain lors de négociations commerciales menées avec le Japon.

Les autorités de l'archipel ont été d'autant plus embarrassées par ces révélations qu'elles ont elles-mêmes été mises en accusation. Outre leur participation active à Echelon, elles ont développé leurs propres capacités d'écoutes. Le magazine *ZDNet*, citant une source militaire japonaise, a révélé que le Japon s'était en effet doté d'une flotte de cinq avions EP-3 "truffés de systèmes d'interception et d'écoutes électroniques". Des capacités technologiques d'espionnage utilisées à des fins nationales. Les informations recueillies sont, selon la même source, traitées à Tokyo au quartier général de l'Agence japonaise de la défense.

Par ailleurs, un budget de plus d'un million de dollars a été voté par le Parlement, en mars 2001, pour la conception d'un logiciel d'espionnage du courrier électronique "Kari-no-mail". La première version du logiciel a été achevée fin 2001, et il serait en cours d'installation chez les fournisseurs d'accès à Internet japonais. Mais les services de sécurité japonais n'ont jamais rendu explicitement compte de l'avancée du dossier auprès des élus. Les organisations de défense de la liberté d'expression et de défense des libertés civiles exigent la transparence dans cette affaire et réclament la suspension du logiciel espion.

LIENS :

- Site sur le programme Echelon
www.echelonwatch.org

- L'organisation Networkers against Surveillance Taskforce (en japonais)
www.jca.ax.apc.org/privacy

- L'opérateur DoCoMo, créateur du "i-mode"
www.nttdocomo.com/top.html

- Présentation du plan "e-Japan strategy"
www.kantei.go.jp/foreign/it/network/0122full_e.html

- Edition asiatique de *ZDnet*
www.zdnetasia.com



MOYEN-ORIENT

Jordanie

POPULATION : 5 051 000

INTERNAUTES : 234 000

FOURNISSEURS D'ACCÈS PRIVÉS : OUI

La Toile fait partie intégrante du quotidien des Jordaniens. Surtout dans la capitale et dans les grandes villes du royaume. Pour preuve la tentative, en janvier 2001, de la rue Chafic Rcheidat, à Irbid (nord du pays), d'entrer dans le livre Guinness des records pour ses cent cinq cybercafés implantés sur une longueur de moins d'un kilomètre...

Jusqu'en 2001, le web ne faisait l'objet d'aucune censure ou de contrôle. La situation a nettement évolué. La crainte de voir la seconde Intifada "contaminer" le royaume, conjuguée aux conséquences des attentats du 11 septembre 2001, ont incité les autorités à "mettre en garde toute partie quelle qu'elle soit contre toute tentative visant à nuire à la sécurité et à la stabilité du royaume".

Début octobre 2001, des mesures restrictives ont été adoptées contre la presse. Ces mesures prévoient la fermeture "provisoire ou permanente" des journaux en cas de publication d'informations "diffamatoires, fausses, nuisant à l'unité nationale, à la réputation de l'Etat, incitant à des grèves, des réunions publiques illégales ou troublant l'ordre public". De même, les peines pour "atteinte au couple royal" et "au prince héritier" ont été durcies. Ces délits sont désormais passibles d'une peine de prison de un à trois ans, alors qu'auparavant ils étaient sanctionnés par une amende. Des mesures qui concernent indistinctement la presse papier et la presse en ligne.

En décembre 2001, le monarque a formé le Conseil suprême de l'information et l'a chargé de mettre au point la politique d'information du pays, en remplacement du ministère. Les conséquences pour Internet de cette politique ne se sont malheureusement pas fait attendre. L'ancienne journaliste de la télévision et première femme députée, Toujane el-Fayçal, a été condamnée, le 16 mai 2002, à Amman, à un an et demi de prison par la Cour de sûreté de l'Etat pour "propagation à l'étranger d'informations portant atteinte à la réputation de l'Etat et à ses responsables". Dans une lettre ouverte publiée le 6 mars sur le site Internet du journal *Arab Times* (www.arabtimes.com), basé à Houston - Texas, Toujane el-Fayçal avait accusé le Premier ministre, Ali Abou Ragheb, de "profiter financièrement" de la décision de doubler les tarifs d'assurance des voitures. Toujane el-Fayçal était également accusée d'avoir diffamé l'autorité judiciaire en dénonçant, lors d'une interview sur la chaîne de

télévision qatarie *Al-Jazira*, la corruption de la justice jordanienne. "La cour a constaté que l'accusée a fait des déclarations et publié des articles (...) visant à déformer l'image de la Jordanie et à inciter des troubles dans le royaume", a déclaré le président de la cour avant de prononcer le verdict. Le roi Abdallah II a gracié la cyberdissidente en juin 2002.

LIENS :

- Le quotidien anglophone *Jordan Times*
www.jordantimes.com
- L'agence de presse officielle *Petra*
www.petra.gov.jo
- Journal indépendant spécialisé sur les médias *Al Mashreq Al I'lami* (en arabe)
www.al-mashreq.org
- Center for defending freedom of journalists (en arabe)
www.cdfj.org



Kazakhstan

POPULATION : 16 095 000

INTERNAUTES : 150 000

FOURNISSEURS D'ACCÈS PRIVÉS : OUI

Dans ce pays d'Asie centrale où la presse d'opposition en ligne est peut-être la plus active, les fournisseurs d'accès sont surveillés par les services de renseignements et les sites d'opposition régulièrement bloqués.

Au Kazakhstan, la loi assimile Internet aux médias et n'oblige donc pas les sites à se faire enregistrer auprès des autorités. Depuis 1999, un organisme étatique est chargé de contrôler l'ensemble des réseaux de télécommunications. Les fournisseurs d'accès doivent s'enregistrer auprès des autorités gouvernementales et leurs lignes sont surveillées par les services de renseignements. Les sites d'opposition sont régulièrement bloqués par la plupart des providers du pays. Pour éviter la censure, les internautes peuvent passer par des serveurs proxys, basés à l'étranger, moyennant un allongement du délai de connexion.

Dès sa création en septembre 2001, le site *Kub*, proche du mouvement d'opposition "Choix Démocratique du Kazakhstan", reçoit des menaces anonymes, interdisant la publication de toute information relative au président Noursultan Nazarbaïev, qui fait l'objet d'une enquête judiciaire à l'étranger pour détournement de fonds. L'accès au site est bloqué par les fournisseurs Kazakhtelecom, Nursat et Arna-Sprint au cours du premier trimestre 2002. Sergueï Douvanov, auteur d'un article dénonçant les fraudes du chef d'Etat, publié en ligne le 6 mai, est interrogé par les services secrets et poursuivi pour atteinte à l'honneur et à la dignité du président Nazarbaïev. Le 28 août, le journaliste est violemment agressé par des inconnus. Le lendemain, le site *club.kz*, qui a repris les propos de Sergueï Douvanov, est également bloqué. Le 11 mars 2003, Sergueï Douvanov est condamné en appel à trois ans et demi de prison pour le viol présumé d'une mineure. Les nombreuses irrégularités qui ont entaché l'enquête et le procès, ainsi que la répression dont est victime le journaliste, laissent supposer que cette accusation revêt un caractère politique.

L'accès au site *Respublika* est bloqué par Kazakhtelecom et Nursat de mars à mai 2002, puis à différentes reprises au cours de l'année. Le site diffusait des informations sur les procédures à l'encontre des deux principaux leaders de "Choix Démocratique du Kazakhstan".

Sous des prétextes techniques et administratifs, l'accès au site du journal indépendant *Navigator* est bloqué le 20 mai après la publication d'une interview de l'ancien procureur de Genève, Bernard Bertossa, qui confirmait l'existence de comptes bancaires en Suisse au nom de plusieurs hauts responsables kazakhs, dont le président Noursultan Nazarbaïev.

Le 4 septembre, l'accès au site zhakiyanov.info, site officiel du leader de "Choix Démocratique du Kazakhstan", Galymzhan Zhakiyanov, condamné à sept ans de prison, est bloqué par Nursat dans certaines régions du pays.

En avril 2003, Yuri Mizinov, responsable éditorial du journal électronique *Navigator*, fait appel à des experts qui concluent que tous les clients de Kazakhtelecom, le principal fournisseur d'accès Internet (public), sont empêchés d'accéder à son site Internet.

LIENS :

- Service kazakh de *Radio Free Europe/Radio Liberty*
www.rferl.org/bd/ka/index.html
- Le site d'informations *Eurasianet*
www.eurasianet.org/
- La Fondation internationale pour la protection de la liberté d'expression Adil soz www.adilsoz.kz/english/index.htm
- L'organisation de défense des droits de l'homme Kazakhstan International Bureau for Human Rights and Rule of Law
www.bureau.kz/index_eng.shtml
- Le site d'informations *Kub.kz*
www.kub.kz/hot.php



AFRIQUE

Kenya

POPULATION : 31 293 000

INTERNAUTES : 500 000

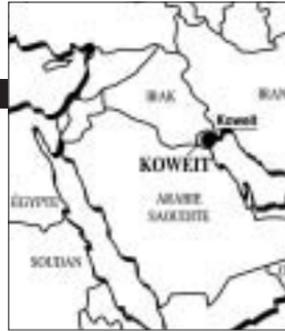
FOURNISSEURS D'ACCÈS PRIVÉS : OUI

Le Kenya est l'un des Etats d'Afrique subsaharienne le plus avancé, en matière de connexion au Réseau. La Toile est accessible depuis 1995 et aucun texte de loi n'en régent l'utilisation. Le nombre d'internautes, majoritairement issus des classes sociales élevées de la société, augmente massivement tous les ans.

Bien qu'Internet ne soit régi par aucune loi spécifique, le pouvoir, dont les rapports avec la presse sont toujours tendus, surveille de près l'utilisation du Réseau. Fin août et début septembre 2001, la police a perquisitionné deux cybercafés de Nairobi et interpellé plusieurs ressortissants étrangers accusés d'avoir diffusé des documents classés secret défense.

LIENS :

- "The future of the Internet in Kenya", article de l'*East African Standard*, quotidien régional
<http://allafrica.com/stories/200303040359.html>



Koweït

POPULATION : 1 971 000

INTERNAUTES : 200 000

FOURNISSEURS D'ACCÈS PRIVÉS : OUI

Les Koweïtiens font un usage quotidien de la Toile. Les cafés Internet sont nombreux (plus de trois cents) dans la petite mais riche monarchie et les ordinateurs pullulent dans les foyers. Mais le Koweït est encore sous le joug des islamistes. Ces derniers n'apprécient que modérément l'omniprésence du Réseau.

Fin décembre 2000, un membre du Parlement, issu de la ligne islamiste dure, a proposé de censurer les sites à caractère pornographique et d'exiger des fournisseurs d'accès au Net qu'ils "empêchent l'accès des internautes aux sites proposant des contenus à caractère pornographique ou immoral". Ainsi, en mai 2002, les autorités ont fermé provisoirement une cinquantaine de cybercafés dans le cadre d'une campagne destinée à lutter contre la pornographie. Les permis d'exercer délivrés à ces établissements ont été suspendus par le ministère des Communications. Une campagne d'inspection a été lancée suite à des dénonciations ou des plaintes rapportant que ces cafés Internet avaient permis à leurs clients de consulter librement des sites pornographiques. Le ministère en a profité pour annoncer que de nouvelles réglementations obligeront prochainement ces Web bars à adhérer à un système de contrôle plus strict sur ces questions. Depuis, les établissements ont rouvert. Les nouvelles réglementations font toujours l'objet de vives discussions, sous la pression notamment des députés islamistes.

LIENS :

- Site d'informations
www.kuwaitonline.com
- Le quotidien anglophone *Kuwait Times*
www.kuwaittimes.net
- L'agence de presse officielle *Kuwait News Agency*
www.kuna.net.kw
- Le quotidien arabophone *Al-Watan*
www.alwatan.com.kw
- Site d'informations sur les pays du Golfe (en arabe)
www.gulfissues.net



Laos

POPULATION : 5 403 000

INTERNAUTES : 15 000

FOURNISSEURS D'ACCÈS PRIVÉS : OUI

Le régime laotien ne tolère pas la liberté de la presse. Il ne tolère pas plus que les nouvelles technologies de l'information puissent devenir un vecteur d'expression démocratique.

Depuis qu'il s'est doté, en 1996, d'un accès à la Toile et a autorisé des fournisseurs d'accès (qu'il contrôle) à proposer leurs produits et services, le Réseau s'implante très lentement. Les connexions sont chères et les Laotiens redoutent d'utiliser un média qu'ils savent strictement contrôlé par le gouvernement et ses services.

On ne recense dans le pays que quelque quinze mille internautes et une cinquantaine de cybercafés ouverts dans la capitale, Vientiane. Les Laotiens recourent essentiellement à Internet pour envoyer et recevoir des courriers électroniques. Ils ne sont autorisés à accéder qu'aux sites accrédités par le pouvoir. Ainsi, les autorités ont bloqué l'accès au site d'opposition *Vientianetimes*, hébergé aux Etats-Unis et bête noire du gouvernement (à ne pas confondre avec le journal gouvernemental dont les créateurs du site ont détourné le nom). Tout internaute qui tente de s'y connecter reçoit un message l'avertissant que sa requête a été "enregistrée".

En 2000, l'Etat a mis en place l'Internet Committee of Lao qui regroupe les ministères de l'Information et de la Culture, des Postes et Télécommunications, et celui des Transports et des Sciences. Ce comité a édicté un règlement à l'attention des internautes du pays. Il interdit aux nationaux, résidents du pays ou expatriés, de publier en ligne tout contenu susceptible de "nuire à l'unité et à l'intégrité du pays".

L'agence de presse officielle KPL a précisé en octobre 2000 que les internautes qui utiliseraient Internet d'une "mauvaise manière" en mentant ou en persuadant le peuple de protester contre le gouvernement" pourraient être traduits en justice ou expulsés du pays. Concernant la presse en ligne, le principal fournisseur d'accès, Lao Telecommunications, affirme qu'un journaliste a le droit de publier des informations s'il a reçu le feu vert du comité et de son ministère de tutelle.

L'usage des courriers électroniques n'est pas plus libre. Nombreux sont ceux qui

affirment que des e-mails adressés au Laos n'arrivent jamais. Et s'ils parviennent à leurs destinataires, le pouvoir a eu préalablement tout loisir d'en violer le contenu. Les abonnés au mail doivent en effet communiquer leurs mots de passe lorsqu'ils s'abonnent auprès du fournisseur d'accès national.

LIENS :

- L'opérateur Lao Telecommunications
www.laotel.com
- Site dissident d'informations (hébergé aux Etats-Unis)
www.vientianetimes.com/Headlines.html



Liberia

POPULATION : 3 108 000

INTERNAUTES : PAS DE STATISTIQUES DISPONIBLES

FOURNISSEURS D'ACCÈS PRIVÉS : NON

Mis à terre par des années terribles de guerre civile, le Liberia tente difficilement de reconstruire ses infrastructures les plus vitales. Dans ces conditions, Internet est loin d'être une priorité. Le Réseau est quasi inexistant. Il est pratiquement impossible d'estimer le nombre d'internautes : ils seraient tout au plus quelques milliers.

Cela n'empêche pourtant pas le président Charles Taylor de prendre la Toile pour cible, de la même façon qu'il s'attaque à la presse d'opposition. Ce dernier dénonce la "cyberguerre" que lui font les journalistes exilés. Ils se servent en effet du Réseau pour diffuser leurs informations.

Data Tech, l'unique fournisseur d'accès du pays, est, pour sa part, accusé de couper volontairement l'accès au Web lorsque les sites de la diaspora libérienne diffusent trop d'informations critiques envers le gouvernement. Le pouvoir a lancé, courant 2001, un site d'informations baptisé *allaboutliberia.com*, pour contre-attaquer.

LIENS :

- Site gouvernemental d'informations
www.allaboutliberia.com
- Site d'informations d'opposition
www.theperspective.org



Malaisie

POPULATION : 22 633 000

INTERNAUTES : 6 500 000

FOURNISSEURS D'ACCÈS PRIVÉS : OUI

INTERNAUTES ET CYBERDISSIDENTS EMPRISONNÉS : 1

Bien que la Malaisie mise énormément sur Internet et les nouvelles technologies pour dynamiser son économie, le pouvoir harcèle la presse indépendante en ligne et soumet les sites de l'opposition à une forte pression.

Comme tous les grands pays d'Asie du Sud-Est, la Malaisie est très perméable à l'évolution des nouvelles technologies de l'information et Internet s'y développe donc rapidement. D'autant plus que, pour enrayer le déclin de l'économie traditionnelle, le Premier ministre Mahathir Mohamad (au pouvoir depuis 1981) a lancé, en 1996, un concept de révolution industrielle basée sur ces nouvelles technologies, baptisé "Super Corridor Multimedia" (MSC). A cette époque, le Premier ministre avait promis, pour protéger les droits des internautes, que son gouvernement ne censurerait pas Internet.

Cette appellation fait référence à une zone de quinze kilomètres de large sur cinquante kilomètres de long, qui englobera à terme le futur aéroport international de Kuala Lumpur et la nouvelle capitale administrative de la Malaisie, actuellement en construction, Putra Jaya. L'objectif est d'attirer dans ce périmètre les sièges et les laboratoires de recherche et de développement des plus grandes multinationales de l'informatique et du multimédia.

Harcèlement contre le quotidien en ligne *Malaysiakini*

Si le gouvernement croit aux vertus économiques d'Internet, il redoute néanmoins que ce nouveau média ne batte en brèche son strict contrôle des médias. Après s'être engagé à ne pas exercer de censure sur le Réseau, le pouvoir a pourtant pris pour cible *Malaysiakini*, le seul quotidien en ligne indépendant et critique. Ses journalistes n'ont pas droit à la carte de presse et subissent régulièrement les foudres du gouvernement, qui remet en cause la fiabilité des informations diffusées par le site et l'accuse de vouloir entacher sa crédibilité. L'intimidation verbale ne s'étant pas avérée suffisante, les reporters ont été directement inquiétés. Le 3 avril 2002, les journalistes de *Malaysiakini* sont autorisés par la sécurité du Parlement à assister à la séance de l'Assemblée, mais à la condition de ne pas poser de questions pendant les

conférences de presse, ni de s'approcher des élus du parti au pouvoir. Selon l'officier de la sécurité, le statut professionnel des journalistes de la publication Internet indépendante n'est pas clair. Depuis deux ans, le ministère de l'Information leur refuse une accréditation de presse. Deux autres sites d'information, RadiqRadio et Agendadaily, se sont également vu refuser ces accréditations.

En octobre 2002, *Malaysiakini*, qui revendique cent mille visiteurs par jour, a été contraint de faire payer l'accès à ses articles. Le manque de revenus publicitaires a, selon le rédacteur en chef, Steven Gan, motivé cette décision. En effet, les nombreuses attaques verbales des autorités, notamment du Premier ministre Mahathir Mohamad, ont découragé beaucoup d'investisseurs malaisiens et étrangers d'acheter de l'espace publicitaire sur les sites indépendants.

Le 20 janvier 2003, la police a saisi une vingtaine d'ordinateurs ainsi que plusieurs fichiers au siège de *Malaysiakini* suite à une plainte pour "sédition" et "incitation à la haine raciale" du mouvement de la jeunesse de l'UMNO (Organisation nationale unifiée malaise - parti au pouvoir). "C'est une tentative pour fermer *Malaysiakini*", a déclaré Steven Gan. Les autorités ont exigé de la rédaction qu'elle révèle l'identité de l'auteur d'une lettre publiée le 9 janvier sur le site de façon anonyme. L'auteur critiquait ouvertement la décision du gouvernement d'accorder des droits spéciaux à la majorité malaise. Elle comparait également l'UMNO, au mouvement américain du Ku Klux Klan. Steven Gan a refusé de révéler l'identité de l'auteur. "Nous resterons conformes à nos principes journalistiques", a-t-il expliqué. Le 22 janvier, le site a reçu l'ordre d'évacuer les bureaux occupés par la rédaction avant la fin de février. Cette injonction est prononcée par le propriétaire des lieux, la société PC Suria, détenue par l'entreprise d'Etat NASCOM. Comme le confirme son rédacteur en chef, Steven Gan : "Il s'agit d'une nouvelle tentative destinée à fermer *Malaysiakini*. Nous pensons que les autorités ont exercé une pression sur PC Suria afin de nous évincer." Premesh Chandran, directeur exécutif du site, a fait remarquer que la recherche de nouveaux locaux pourrait faire perdre environ 100 000 ringgits (26 000 euros) au journal et entraîner une cessation de ses activités d'au moins deux semaines. "Cela signifiera aussi une perte au niveau de nos abonnements et une perte de confiance auprès de nos lecteurs", a-t-il ajouté. La rédaction de *Malaysiakini* a refusé, le 5 février, d'obtempérer à l'ordre d'expulsion. "D'après le contrat initial, *Malaysiakini* peut rester dans ses locaux actuels jusqu'en décembre 2004." Gan a par ailleurs adressé une lettre à l'avocat de PC Suria, dans laquelle il affirme n'avoir violé aucune loi, tout en réitérant sa volonté de ne pas quitter les lieux. Suite aux protestations nationales et internationales, la pression sur le quotidien en ligne faiblit.

L'opposition, qui utilise Internet comme une tribune, est aussi régulièrement inquiétée. En mars 2001, les ordinateurs du site de l'organisation d'opposition National Justice Party ont été saisis. La police a perquisitionné le domicile du rédacteur en chef de ce site, Raja Petra Kamaruddin, en affirmant que le contenu éditorial était "séditieux". Le responsable de la rédaction du site a dû le faire héberger et gérer à l'étranger pour qu'il subsiste.

Un cyberjournaliste emprisonné

Le 10 avril 2002, Hishamuddin Rais, collaborateur du journal en ligne *Malaysiakini* et réalisateur de documentaires, détenu dans la prison de Kamunting à Taiping, dans l'État de Perak (nord du pays), entame une grève de la faim en compagnie de cinq autres dissidents détenus depuis un an en vertu de la loi sur la sécurité intérieure (Internal Security Act). Il est accusé avec ses cinq compagnons, membres de mouvements d'opposition, d'avoir "tenté de renverser" le gouvernement. Ils ont été condamnés, sans procès, à deux ans de prison. Selon leurs proches, leur santé se détériore rapidement. Hishamuddin Rais et Badrulamin Bahron sont admis le 16 avril à l'hôpital de la prison. Placés sous perfusion, ils refusent toujours de s'alimenter. Après huit jours de grève de la faim, ils reçoivent le soutien de militants des droits de l'homme, d'opposants et de l'ancien vice-Premier ministre, Anwar Ibrahim, également emprisonné, qui a cessé de s'alimenter pendant quelques jours, en signe de solidarité. En revanche, aucun média public ou proche du pouvoir n'évoque cette grève de la faim. Les six détenus y mettent fin après onze jours.

Un code du contenu des sites en projet

Le 30 mai 2001, le ministère de l'Énergie, des Communications et du Multimédia a annoncé le projet de création d'un Comité national de surveillance d'Internet (National Internet Advisory Committee), dont la mission serait de coordonner et de superviser l'usage du Réseau dans le pays, et d'établir une législation dans ce domaine.

Le même jour, le secrétaire parlementaire du ministère, Chia Kwang Chye, a rappelé qu'en l'absence d'une loi spécifique au Web, ses utilisateurs doivent se conformer aux termes de la loi sur la communication et le multimédia (Communication and Multimedia Act), qui "permet de poursuivre et de requérir un an de prison et de fortes amendes à l'encontre de toute personne qui disséminerait des articles faux ou diffamatoires sur Internet".

Fortement combattu par les quelques publications en ligne et l'opposition, un nouveau projet de loi spécifique au multimédia a avorté. En mars 2002, le pouvoir a annoncé qu'il abandonnait cette idée. Pourtant, en février 2002, Steven Gan, rédacteur en chef de *Malaysiakini*, a révélé que le gouvernement souhaite "introduire un code du contenu des sites qui permettra de trier les informations pouvant être mises en ligne". En outre, le ministère préparerait une réforme du système gouvernemental d'attribution des licences. Pour Steven Gan, "l'objectif est clairement de pouvoir contrôler a priori ce qui peut être diffusé, et d'écarter toutes les informations critiques ou les propos des opposants". Ces textes n'ont toujours pas été adoptés.

LIENS :

- Le quotidien en ligne *Malysiakini*
www.malysiakini.com.my
- L'organisation de défense des droits de l'homme Aliran
www.aliran.com
- Le site d'un parti d'opposition
dapmalaysia.org/english
- La Malaysian Communications and Multimedia Commission
www.mcmc.gov.my/mcmc
- Le ministère de l'Energie, des Communications et du Multimédia
www.ktkm.gov.my



Maldives

POPULATION : 300 000

INTERNAUTES : 15 000

FOURNISSEURS D'ACCÈS PRIVÉS : NON

INTERNAUTES ET CYBERDISSIDENTS EMPRISONNÉS : 4

Le président Maumoon Abdul Gayoom, au pouvoir depuis 1978, refuse aux personnalités critiques de l'île le droit de se servir d'Internet pour contester son pouvoir. Il l'a rappélé violemment en 2002 en faisant condamner à de très lourdes peines de prison les auteurs d'une lettre d'information électronique. En revanche, son gouvernement tente de promouvoir une vision paradisiaque des Maldives à travers de nombreux sites dédiés au tourisme.

La liberté d'expression, notamment sur Internet, est limitée par plusieurs lois. Ainsi, un texte législatif de 1968 interdit les discours et les articles "hostiles à l'islam", "contraires à la sécurité nationale" ou "injurieux". Cependant, au moins deux journaux privés des Maldives publient des critiques à l'encontre du gouvernement.

Mohamed Nasheed, député d'opposition et journaliste indépendant, est arrêté le 8 octobre 2001 après avoir publié plusieurs articles sur Internet. Il a également signé en février 2001 une pétition demandant l'autorisation de créer un parti d'opposition. Après un mois de détention au secret à Malé, il est condamné, à l'issue d'un procès expéditif, à deux ans et demi de baigne sur l'atoll isolé de Raat pour "vol". Le 13 mars, son appel est entendu par la Haute Cour des Maldives sans qu'il ait droit à un avocat. Les juges décident de ne pas le renvoyer au baigne mais de le placer en résidence surveillée à Malé. Il est par ailleurs exclu du Parlement.

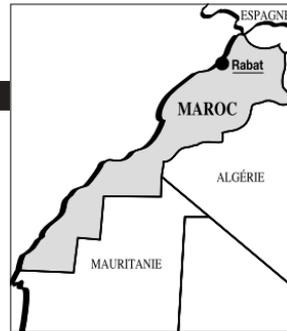
En janvier 2002, les hommes d'affaires Mohamed Zaki, Ibrahim Luthfee et Ahmad Didi, ainsi que Fathimath Nisreen, assistante d'Ibrahim Luthfee, sont arrêtés par la police pour avoir diffusé des articles critiques du gouvernement sur leur bulletin d'information électronique *Sandhaanu*. Selon Amnesty International, le bulletin en divehi (langue des Maldives) ne comportait aucun appel à la violence. Détenus au secret pendant deux semaines par la police de Malé (capitale), ils sont transférés au centre de détention de l'île de Dhoonidhoo. En mai, ils sont inculpés de "diffamation" et d'avoir "tenté de renverser le gouvernement" en publiant des informations sur *Sandhaanu*. Les autorités leur refusent le droit de consulter un avocat et de recevoir des visites de leurs familles. En juin, ils sont transférés sur l'île de Mafushi où ils sont

détenus dans de petites cellules. Le 7 juillet 2002, Mohamed Zaki, Ibrahim Luthfee et Ahmad Didi sont condamnés à la prison à vie. Fathimath Nisreen, âgée de 21 ans, est quant à elle condamnée à dix ans de prison ferme pour avoir notamment exprimé son "mécontentement à l'encontre de la politique du gouvernement" et soutenu les auteurs des articles de *Sandhaanu*. Les autorités ont refusé aux accusés de se pourvoir en appel. Lors du procès, Ibrahim Luthfee, 37 ans, et Ahmad Didi, 50 ans, ont reconnu être les auteurs de ce bulletin d'information électronique, tandis que Mohamed Zaki, 50 ans et résidant en Malaisie, était chargé de l'envoyer aux internautes qui le demandaient. Ibrahim Luthfee a affirmé aux juges qu'il était prêt à prouver point par point les accusations qu'il avait lancées contre le président Gayoom.

Ils sont toujours incarcérés sur l'île de Mafushi dans des conditions de détention difficiles. Les autorités les ont placés dans le Bloc C habituellement réservé aux drogués et aux voleurs. Leurs cellules ne sont pas ventilées et ils ne disposent que de cinq litres d'eau par jour pour boire et se laver. Leurs familles ne sont autorisées à leur rendre visite qu'une fois par mois.

LIENS :

- Site d'informations basé à l'étranger
www.maldivesculture.com/main.html
- Site d'un quotidien publié à Malé
www.haveeru.com.mv/english
- Site d'opposition sur les droits de l'homme
www.geocities.com/CapitolHill/Lobby/2311
- Le site de la présidence des Maldives
www.presidencymaldives.gov.mv/v3
- Le site du seul fournisseur d'accès
www.dhivehinet.net.mv



Maroc

POPULATION : 30 430 000

INTERNAUTES : 500 000

FOURNISSEURS D'ACCÈS PRIVÉS : OUI

Jusqu'à l'année 2003, le Net marocain a été l'un des plus libres du Maghreb. Le gouvernement n'a imposé aucune restriction particulière et n'a pas entravé l'accès à des sites particuliers. Pour exemple, les sites proches du Front Polisario sont accessibles depuis le pays. En outre, le pouvoir n'a pas légiféré pour encadrer le développement du Réseau.

La presse marocaine s'est accaparée le Réseau pour en faire une arme anticensure. Ainsi, en décembre 2000, trois hebdomadaires avaient été définitivement interdits pour avoir relaté une affaire mettant en cause le Premier ministre d'alors, Abderrahmane Youssoufi. En guise de réponse, les dirigeants des trois magazines avaient diffusé en ligne les articles censurés, sur des sites français notamment.

En 2002, le site de l'hebdomadaire *Rissalat Al Foutouwa*, organe de la section étudiante de l'association islamiste Al-Adl Wal Ihsane (justice et spiritualité), est à nouveau consultable depuis le Maroc. Celui-ci avait été bloqué en avril 2001 par les autorités.

LIENS :

- Le site Maghreb des droits de l'homme
www.maghreb-ddh.org



MAURITANIE

Mauritanie

POPULATION : 2 747 000

INTERNUTES : 10 000

FOURNISSEURS D'ACCÈS PRIVÉS : OUI

C'est en 1997 que la Mauritanie a été reliée au Réseau. Les cafés Internet sont les lieux dans lesquels les Mauritaniens surfent le plus sur la Toile. Le prix élevé des ordinateurs et le coût des abonnements (environ trente euros par mois) et des connexions freinent le développement des connexions personnelles à domicile.

Bien qu'encore faiblement démocratisé, le Web est toutefois encadré et contrôlé par le pouvoir. La majorité des fournisseurs d'accès privés est détenue par des hommes d'affaires proches du pouvoir. Les dirigeants de cybercafés sont contraints, si on le leur demande, de transmettre à la direction de la Sûreté de l'Etat une copie des e-mails reçus ou envoyés depuis leurs établissements.

LIENS :

- Le site Maghreb des droits de l'homme
www.maghreb-ddh.org



Mozambique

POPULATION 18 644 000

INTERNAUTES : 30 000

FOURNISSEURS D'ACCÈS PRIVÉS : OUI

Le Web se développe dans le pays malgré la faiblesse du réseau téléphonique. L'année 2002 a été marquée par le procès des assassins présumés du journaliste Carlos Cardoso, directeur du quotidien *Metical*, diffusé uniquement par courrier électronique ou par fax.

Lentement mais sûrement, Internet se développe au Mozambique. Les habitants s'intéressent de plus en plus aux nouvelles technologies de l'information, qu'ils utilisent essentiellement dans les cybercafés. Les principales villes du Mozambique disposent d'un bon réseau Internet. Dans l'ensemble, les sites ne sont pas menacés de fermeture, de censure, ou de contrôle. Le gouvernement cherche même à étendre l'accès à Internet et a créé à cette fin la Commission pour les politiques des technologies de l'information, placée sous la responsabilité du Premier ministre Pascoal Mocumbi.

A l'instar de la presse, le gouvernement ne soumet la Toile à aucune pression politique. Pourtant, la jeune histoire d'Internet au Mozambique a été élaboussée par une affaire grave : l'assassinat, dans la soirée du 22 novembre 2000, de Carlos Cardoso, directeur de *Metical*, un quotidien alors diffusé uniquement par courrier électronique ou par fax. Le journaliste était dans son véhicule avec son chauffeur, sur l'avenue Martires de Machava à Maputo, quand deux hommes leur ont bloqué la route et ont ouvert le feu. Carlos Cardoso, touché à plusieurs reprises à la tête, est mort sur le coup. Son chauffeur a été grièvement blessé. Le journaliste venait de quitter le siège du journal et rentrait à son domicile. Avant son assassinat, Carlos Cardoso enquêtait sur la disparition de 144 milliards de meticaïs (un peu plus de 7 millions d'euros) à la Banque commerciale du Mozambique (BCM). *Metical* avait suivi de près cette affaire en s'étonnant de l'absence d'enquête et avait notamment cité les noms des frères Satar et de Vicente Ramaya - trois hommes d'affaires importants et influents dans le pays - dans des articles.

Une enquête gênante sur la Toile

Le dossier revient sur le devant de la scène début 2001. Le 28 février, le ministre de l'Intérieur annonce l'arrestation de suspects en relation avec l'assassinat de Carlos

Cardoso et, quelques jours plus tard, la police interpelle les frères Momade Abdul Satar et Ayob Abdul Satar ainsi que Vicente Ramaya, ancien directeur du bureau de Maputo de la BCM. Fin mai, six personnes, au total, sont inculpées dans le cadre de cette affaire.

Dans la nuit du 1er septembre 2002, Anibal Antonio dos Santos Junior, plus connu sous le surnom Anibalzinho, l'un des six suspects, s'évade de la prison de haute sécurité de Maputo. La police ne donne aucune explication. Des organisations s'étaient récemment inquiétées des dysfonctionnements du système pénitentiaire mozambicain. En août, Momade Abdul Satar, l'un des commanditaires présumés dans cette affaire, avait été placé en "cellule d'isolement" après qu'on avait trouvé un téléphone portable en sa possession. Le 3 septembre, les autorités judiciaires annoncent l'arrestation des trois responsables des services de police qui opèrent à l'intérieur de la prison. Selon la version officielle, Anibalzinho se serait évadé par la porte de sa cellule. Or, celle-ci était fermée par trois serrures qui ne pouvaient être ouvertes que par les responsables de ces trois services de police. Quelques jours plus tard, huit autres policiers sont arrêtés.

Le 8 septembre, l'hebdomadaire progouvernemental *Domingo* appelle à la démission du ministre de l'Intérieur, Almerino Manhenje. A la fin du mois, l'hebdomadaire indépendant *Mediafax* accuse le ministre de l'Intérieur de complicité dans l'évasion d'Anibalzinho. Un éditorial affirme que le ministre contrôlait directement la sécurité de la prison.

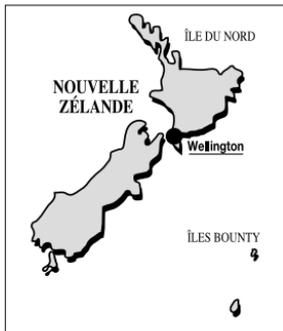
Le 18 novembre, deux ans après les faits, le procès des assassins présumés de Carlos Cardoso débute à Maputo. Après l'évasion d'Anibalzinho, cinq prévenus figurent sur le banc des accusés. Une salle d'audience spéciale est mise en place à l'intérieur même de la prison de haute sécurité par crainte de "troubles à l'ordre public". Des mesures spéciales sont également prises pour assurer la sécurité du juge Augusto Paulino. Les journalistes sont autorisés à assister aux débats.

Dès le lendemain, Manuel Fernandes, l'un des suspects, accuse Nyimpine Chissano, le fils du président de la République, d'avoir ordonné l'assassinat de Carlos Cardoso. Le chef de l'Etat, Joaquim Chissano, annonce publiquement que la justice doit être rendue dans son pays et que le "procès doit continuer", même si le nom de son fils a été mentionné. Le 20 novembre, l'un des hommes d'affaires impliqués dans cette affaire, Momade Abdul Satar, affirme avoir payé Anibalzinho, sur l'ordre de Nyimpine Chissano, pour assassiner le journaliste. Le 25, Carlos Rachid Cassamo, soupçonné d'être celui qui a tiré sur Carlos Cardoso, accuse à son tour le fils du chef de l'Etat d'être le commanditaire principal dans cette affaire.

Le 5 décembre, Nyimpine Chissano, appelé à témoigner devant la cour, nie toute implication dans l'assassinat de Carlos Cardoso. Le 31 janvier 2003, les six prévenus sont condamnés à des peines comprises entre vingt-trois et vingt-huit ans de prison. Parallèlement, le procureur de la République annonce qu'une enquête est en cours pour déterminer l'éventuelle implication de Nyimpine Chissano dans l'assassinat du journaliste.

LIENS :

- Commission pour les politiques des technologies de l'information (en portugais)
www.infopol.gov.mz
- Le quotidien en ligne *Metical* (sur abonnement, en portugais)
www.tropical.co.mz/~metical
- Site de l'hebdomadaire indépendant *Mediafax* (en portugais)
www.mediacoop.odline.com



Nouvelle-Zélande

POPULATION : 3 808 000

INTERNAUTES : 1 908 000

FOURNISSEURS D'ACCÈS PRIVÉS : OUI

Pour lutter contre la criminalité et le terrorisme, la Nouvelle-Zélande s'est dotée d'outils judiciaires qui lui permettent de contrôler les ordinateurs et les courriers électroniques privés.

En mars 2001, le gouvernement a dévoilé les contours d'un projet de loi destiné à lutter contre la cybercriminalité et, selon lui, à améliorer la protection de la vie privée des Néo-Zélandais.

Bruce Slane, rapporteur sur les questions de protection de la vie privée, s'est immédiatement attaqué "à la pratique pernicieuse qui permettrait à la police de pirater les ordinateurs personnels des citoyens dans le cadre d'enquêtes". Une disposition d'autant plus controversée que, selon cette nouvelle loi, les enquêteurs n'auraient besoin que d'un avis de recherche pour déclencher une procédure de contrôle des ordinateurs individuels et des courriers électroniques privés. Selon Bruce Slane, "ce seul avis n'est pas adapté à une mesure qui permet de mener des investigations secrètes et une surveillance furtive des citoyens". Le ministre des Technologies de l'Information de l'époque, Paul Swain, a défendu son projet en expliquant que "les agences gouvernementales (police, services de renseignements) ont besoin de ces dispositions pour lutter contre le crime et le terrorisme" qui ont investi Internet.

Au mois de juillet 2001, la loi a été vigoureusement dénoncée par les élus du Parti Vert. Ils ont regretté que le comité gouvernemental pour la Loi et l'Ordre ait ignoré les inquiétudes de la population quant à la possible violation de leurs communications électroniques par la police, d'autant que cette dernière n'a pas su justifier de tels besoins.

Dans la foulée des mesures antiterroristes préconisées en novembre 2001 par le gouvernement, suite aux attentats du 11 septembre, des dispositions spécifiques ont été recommandées pour mieux contrôler encore les ordinateurs personnels et les communications via Internet. Dévoilée en décembre 2001, une mesure demande ainsi à tous les utilisateurs d'ordinateurs et aux internautes de coopérer avec la police dans le cadre d'enquêtes, si celle-ci en fait la demande. Il a également été demandé aux fournisseurs d'accès à Internet de collaborer étroitement avec la police,

le GCSB, l'agence de renseignements gouvernementale spécialisée dans l'espionnage électronique, et le SIS, le service d'espionnage national. En mars 2002, le gouvernement a débloqué un million cinq cent mille euros pour financer ces mesures d'écoutes des conversations téléphoniques et des e-mails. Une nouvelle loi oblige également les opérateurs de téléphonie et les fournisseurs d'accès et de services à Internet à se doter de moyens d'interception des communications de leurs clients.

En novembre 2002, le gouvernement prend une nouvelle initiative pour renforcer les pouvoirs de la police, du GCSB et du SIS, en matière de surveillance des courriers électroniques. La Telecommunications (Interception Capability) Bill exige des opérateurs Internet qu'ils se dotent de système de surveillance et d'interception de messages cryptés. Ce projet de loi, préparé après la publication d'un rapport de la Commission de réforme du droit (Law Reform Commission), prévoit des amendes s'élevant jusqu'à 25 000 euros en cas de refus de respecter ces dispositions. Encore une fois, les organisations de défense de la liberté d'expression, le Parti Vert, notamment le député Keith Locke, et certains opérateurs Internet dénoncent les graves implications de cette loi en termes de protection des communications électroniques privées. En avril 2003, la loi n'a toujours pas été adoptée.

Toutes ces initiatives du gouvernement visent à obliger les opérateurs Internet, notamment les fournisseurs d'accès, à surveiller, si nécessaire, le contenu des communications des internautes. Grâce à ces législations, la police et les services secrets disposent, par ailleurs, de pouvoirs qui échappent largement au contrôle de la justice ou du Parlement.

A la pointe du réseau Echelon d'espionnage électronique

Fin juin 2001, la presse a révélé que la Nouvelle-Zélande participait au réseau espion Echelon d'écoutes électroniques créé par les Américains. Nicky Hager, journaliste néo-zélandais et spécialiste du réseau Echelon, a affirmé que "les moyens d'interception de communications, électroniques notamment, de la NSA (National Security Agency, l'agence américaine d'espionnage technologique qui gère Echelon) ont été utilisés, au moins jusqu'à la fin des années 80, pour des missions d'espionnage industriel contre le Japon, au bénéfice des Etats-Unis". L'Amérique surveille, selon lui, "la manière dont la seconde économie mondiale peut influencer les Etats du Pacifique Sud".

Le reporter a ajouté que le GCSB a espionné le Japon depuis sa base de Wellington jusqu'en 1989 et a contribué à analyser les données sur ce même pays fournies par les autres bases du réseau Echelon. Après 1990, le GCSB a créé une base à Waihopai, près de la ville de Blenheim pour renforcer son dispositif. Un système sophistiqué de recueil de données a été mis sur pied afin d'espionner les transmissions des ambassades et consulats japonais. Parmi les documents secrets figuraient des rapports et des télégrammes diplomatiques des missions et ambassades japonaises en Océanie, ainsi que des informations confidentielles sur le

commerce, la pêche, les négociations commerciales, les négociations sur le prix du charbon ou le soutien aux pays en voie de développement et les questions d'immigration.

LIENS :

- La Société Internet de Nouvelle-Zélande
www.internetnz.net.nz/index.html
- The Government Communications Security Bureau
www.gcsb.govt.nz
- La Fondation Electronic Frontier
www.eff.org
- Informations sur la loi de lutte contre le terrorisme
www.arena.org.nz/davesub.htm
- Site du Commissaire à la vie privée
www.privacy.org.nz/top.html
- Le quotidien *The New Zealand Herald*
www.nzherald.co.nz



Oman

POPULATION : 2 622 000

INTERNAUTES : 120 000

FOURNISSEURS D'ACCÈS PRIVÉS : NON

Bien qu'il s'en défende, l'Etat contrôle le contenu des sites Internet, via l'Organisation générale des Télécommunications (GTO), l'unique fournisseur d'accès créé en 1997. GTO bloque ainsi l'accès à un grand nombre de sites, étrangers notamment, considérés comme moralement non conformes à l'islam, pour protéger ses ressortissants de "la contamination occidentale". L'Etat utilise néanmoins le Réseau pour diffuser l'information officielle, en particulier grâce au site de l'agence de presse nationale *Oman News Agency*.

LIENS :

- Site d'informations
www.omanobserver.com
- Site d'informations sur les pays du Golfe (en arabe)
www.gulfissues.net



Ouzbékistan

POPULATION : 25 257 000

FOURNISSEURS D'ACCÈS PRIVÉS : OUI

INTERNAUTES : 275 000

Même si le nombre d'internautes a doublé entre 2001 et fin 2002, des coûts de connexion élevés limitent l'accès du plus grand nombre à Internet. Et les rares privilégiés soupçonnent l'Etat de surveiller leurs communications.

Plusieurs cybercafés ont fait leur apparition dans la capitale, Tachkent. Mais, selon l'organisation américaine Internews, leurs clients doivent s'engager par écrit à ne pas diffuser de messages à "caractère politique et religieux". L'autocensure reste donc de rigueur dans un pays où aucune information indépendante n'est tolérée. On recense plusieurs fournisseurs d'accès à Internet, dont deux entreprises privées. Selon le quotidien russe *Vedomosti*, les autorités ont levé, en octobre 2002, le monopole d'accès jusque-là exercé par l'entreprise étatique Uzpak. Selon OpenNet Initiative (ONI), qui répertorie les sites censurés, les autorités bloquent systématiquement les sites d'opposition tels ceux du parti Birlik et du parti islamique interdit Hizb ut-Tahrir. Elles censurent par intermittence des sites d'informations qui diffusent des articles polémiques sur le président Karimov.

En février 2003, la loi sur les principes et les garanties de la liberté d'information, qui impose une série de restrictions à la diffusion des informations par tous types de médias, dont Internet, est entrée en application. L'article 4 de cette nouvelle loi stipule notamment que "la liberté d'informer" peut être limitée au nom de la protection (...) des valeurs morales de la communauté, de même que de la sécurité nationale et du potentiel spirituel, culturel et scientifique du pays". La formulation floue de ces principes laisse une large place à l'interprétation et donc à la censure. Comme pour d'autres articles restrictifs, qui invoquent la "préservation des valeurs culturelles et historiques", la "prévention de l'influence psychologique et de la manipulation de la conscience publique" ou la "stabilité sociale".

LIENS :

- Le service ouzbek de *Radio Free Europe/Radio Liberty* : www.rferl.org/bd/uz/index.html
- Le site d'informations *Eurasianet* : www.eurasianet.org
- Le site censuré du parti d'opposition Mouvement populaire d'Ouzbékistan Birlik www.birlik.net/engl.html



Pakistan

POPULATION : 144 971 000

INTERNAUTES : 500 000

FOURNISSEURS D'ACCÈS PRIVÉS : OUI

Encore limité, le Réseau, essentiellement utilisé dans les cybercafés, ne semble pas soumis à une censure particulière. L'affaire Daniel Pearl prouve en revanche qu'Internet peut être pris en otage par les groupes les plus extrémistes. Enfin, le régime militaire a tout fait pour museler un site de journalisme d'investigation, basé aux Etats-Unis.

Avec seulement un demi-million d'utilisateurs d'Internet, le Pakistan accuse un retard certain en matière de développement des nouvelles technologies d'information. Il s'explique essentiellement par la taille du pays et l'état de son développement économique. Difficile, en effet, de démocratiser Internet dans un Etat pauvre, qui ne compte que quelques millions seulement de lignes téléphoniques privées, essentiellement dans les grandes agglomérations.

Le gouvernement du général Pervez Musharraf semble néanmoins œuvrer dans le sens du développement de la Toile. Même si en juillet 2002, la Pakistan Telecommunication Authority (PTA) a tenté d'imposer aux cybercafés de contrôler l'identité de leurs clients. Pervez Musharraf affirme que l'Etat a déjà déboursé plus de cent millions d'euros d'investissements et fortement baissé le coût des communications et des services depuis 1999. Au début des années 2000, le Pakistan s'est lancé dans une course au développement des technologies numériques, dans le cadre du programme "Information Technology & Telecom Policy", une politique en faveur des technologies de l'information et des télécommunications.

Un développement lent et difficile

Dans le cadre de la "Information Technology & Telecom Policy", le gouvernement a baissé le coût d'accès à Internet et investi dans le développement des infrastructures de télécommunications. Dans le même temps, Internet a été placé sous l'autorité directe de la PTA. Le monopole d'Etat dans ce secteur a pris fin en décembre 2001. Problème : les grands opérateurs comme AOL renâclent à investir dans un pays qui offre des perspectives de faible rentabilité.

Pour l'heure, les Pakistanais se ruent dans les cybercafés, qui pullulent dans les villes. A Peshawar, par exemple, un nouveau café Internet ouvre quasiment chaque jour.

L'instrumentalisation de la Toile dans l'affaire Daniel Pearl

Reste que l'affaire Daniel Pearl a mis en lumière le fait qu'Internet peut être un point de cristallisation des tensions qui se sont exacerbées au Pakistan depuis le 11 septembre 2001. Soutien des taliban afghans jusqu'aux attentats du 11 septembre, le régime de Pervez Musharraf doit composer avec une population traversée par certains courants islamistes extrémistes.

Internet, soulignent les observateurs pakistanais, peut également être "pris en otage par ces mêmes groupes radicaux". L'enlèvement, le 23 janvier 2002, à Karachi, du journaliste américain du *Wall Street Journal*, Daniel Pearl, et son assassinat par un groupe islamiste pakistanais, en a été l'illustration. Les ravisseurs du reporter ont en effet abondamment utilisé Internet, depuis leurs ordinateurs personnels mais aussi dans les cybercafés, pour annoncer ce kidnapping, faire passer leurs messages politiques et médiatiser leur forfait. Une affaire et un constat qui pourraient freiner le développement du Web au Pakistan. Les Américains ne se plaignent-ils pas, régulièrement, du fait que les membres d'Al-Qaida "se servent du Net, souvent depuis le Pakistan, pour faire passer leurs messages, se regrouper ou lancer des opérations" ?

Quoi qu'il en soit, en janvier 2003, l'Agence fédérale d'investigation (FIA) se voit chargée de combattre le cyberterrorisme et la cybercriminalité. Avec le soutien financier et humain des Etats-Unis, le Pakistan met en place un service de surveillance du Réseau. Avant cette date, la police pakistanaise disposait seulement de trois officiers formés à la traque de la cybercriminalité. Les autorités n'ont pas précisé si des logiciels de surveillance des courriers électroniques seraient utilisés par la FIA.

Cabale du régime militaire contre le site *South Asia Tribune*

Le 2 novembre 2002, le ministère de l'Information fait savoir par une annonce spéciale publiée dans les principaux journaux pakistanais que ceux qui reproduiraient des articles émanant du site *South Asia Tribune*, basé à Washington, s'exposent à des poursuites en vertu de l'Ordonnance sur la diffamation promulguée le 1^{er} octobre 2002. Selon la loi, les journalistes convaincus de diffamation peuvent encourir jusqu'à trois mois d'emprisonnement, assortis d'une amende de près de cinquante mille roupies (huit cent cinquante euros) et de l'obligation de publier des excuses.

Le *South Asia Tribune* a été créé en juillet 2002 par Shaheen Sehbaï, ancien responsable de la rédaction du quotidien *The News*, exilé aux Etats-Unis depuis mars 2002. Shaheen Sehbaï a déjà exposé sur son site plusieurs scandales relatifs à la corruption et aux atteintes aux droits de l'homme du gouvernement militaire pakistanais. Il revendique une moyenne de cent mille consultations par mois. Des journalistes pakistanais ont repris certaines informations du *South Asia Tribune*. L'annonce du ministère de l'Information ne mentionne pas explicitement le nom de Shaheen Sehbaï et de son journal d'investigation en ligne, mais fait référence à un "journaliste pakistanais auto-exilé (...) qui a lancé une campagne de diffamation contre le gouvernement du Pakistan et ses fonctionnaires".

Depuis son départ en exil, Shaheen Sehbai est victime d'une véritable cabale. Une plainte pour un "cambriolage" qu'il aurait commis en février 2001 a été déposée contre lui, en août, par un employé de l'armée. Deux de ses proches ont été arrêtés et détenus pendant plusieurs semaines à Islamabad pour leur supposée "complicité" dans le "cambriolage". Des journalistes favorables à Shaheen Sehbai ont été menacés par les services secrets (ISI) pour avoir publiquement pris la défense de l'ancien responsable de *The News*.

Tentatives de contrôle de la Toile

En novembre 2002, le site *South Asia Tribune* révèle que la PTA a ordonné en juillet aux fournisseurs d'accès et aux propriétaires des cybercafés de relever l'identité, le temps de connexion, le numéro d'appel et les adresses IP de leurs clients. Autant d'informations que, à la demande des services de sécurité, les opérateurs devront être capables de fournir. Selon une note signée par le colonel Nayyar Hassan, haut responsable de la PTA, la montée de la cybercriminalité justifie que les fournisseurs d'accès gardent la trace, pendant un mois, des connexions de leurs clients. De même, les propriétaires de cybercafés doivent enregistrer pendant quinze jours les activités de leurs clients. Documents à l'appui, le site d'investigation révèle que la PTA a envoyé un rappel, début août, pour l'application de ces mesures. Selon le même colonel Nayyar Hassan de la PTA, les opérateurs n'ont pas coopéré.

Le 2 avril 2003, la compagnie de télécommunications du Pakistan (PTCL) annonce que 400 nouveaux sites au contenu "indécents" ont été ajoutés à une première liste de 110 adresses Internet interdites. Les opérateurs pakistanais ont été priés de prendre les mesures nécessaires pour bloquer l'accès à ces sites pornographiques. Selon le quotidien *The News*, des fournisseurs d'accès ont souligné que cette décision allait ralentir l'accès à Internet. Le 6 avril, Zahir Khan, un haut responsable de la PTCL, annonce que près de 1 800 sites pornographiques ont été interdits d'accès aux internautes pakistanais. Il affirme que l'entreprise publique envisage d'importer de nouveaux logiciels qui permettront de bloquer plus facilement ces sites. Dans la ligne de mire de la PTCL, on trouve également les sites "anti-islamiques" et "blasphématoires". La PTCL a reconnu que ces mesures ralentissent l'utilisation d'Internet, mais que ce problème temporaire est rendu nécessaire par la "grande menace sociale" que représentent ces sites pornographiques. Un leader du parti fondamentaliste Jamaat-e-Islami, Mairajul Huda, s'est félicité de ces décisions, tout en précisant qu'il était encore nécessaire de "réformer les médias électroniques dans le sens de notre culture et religion afin que notre jeunesse ne soit pas tentée par ces démons."

Cyberguerre entre l'Inde et le Pakistan

En mai 2003, le gouvernement pakistanais crée un comité interministériel spécial pour contrer les attaques de hackers indiens contre les sites officiels pakistanais. De plus en plus fréquemment, des sites pakistanais sont rendus inaccessibles en raison de piratages. Le ministre de la Technologie de l'information, Awais Ahmad Khan Leghari, affirme que "si ces agresseurs sont identifiés, le gouvernement du Pakistan

portera cette question devant les organisations internationales compétentes puisqu'il existe des cyberlois pour contrôler ces crimes." En avril, le même ministre avait annoncé que le gouvernement envisageait de recruter des hackers pour contrer ces attaques. Selon *The News*, le groupe de travail sur la sécurité du Réseau, mis en place par le gouvernement, a la responsabilité de "protéger la cybersécurité du pays".

LIENS :

- Le *South Asia Tribune*, basé aux Etats-Unis
www.satribune.com
- Le fournisseur d'accès étatique Paknet
www.paknet.com.pk
- La Fondation Pakistan Press
www.oneworld.org/ppf
- Le quotidien Dawn
www.dawn.com
- Le quotidien libéral *Daily Times*
www.dailytimes.com.pk

Philippines

POPULATION : 77 131 000

FOURNISSEURS D'ACCÈS PRIVÉS : OUI

INTERNAUTES : 2 000 000



Le développement d'Internet bénéficie d'un contexte globalement favorable à la liberté d'expression. Mais la lutte contre les organisations séparatistes, qualifiées de "terroristes", tend à justifier l'adoption de législations qui permettraient une surveillance d'Internet.

Les Philippines est l'un des rares pays au monde à avoir concocté des lois couvrant dix différents types de cybercriminalité, répartis en quatre catégories : crimes liés aux données, avec notamment l'interception, la modification et le vol ; crimes liés aux Réseaux, comprenant l'interférence et le sabotage ; crimes liés aux accès, incluant le piratage et la propagation de virus ; et crimes informatiques en association, particulièrement la complicité avec des criminels du Net, la fraude informatique et la contrefaçon.

Mais il n'existe pas actuellement de contrôle, par filtrage ou blocage, du contenu d'Internet imposé par l'Etat et chacun peut créer son site sans aucune demande formelle. Des initiatives du secteur privé ont cependant visé à contrôler le contenu du Net, notamment les sites pornographiques.

En avril 2000, la Conférence des évêques catholiques des Philippines (Catholic Bishops Conference of the Philippines - CBCP) a lancé CBCPnet.com, son propre fournisseur d'accès à Internet muni d'un pare-feu bloquant l'accès aux sites pornographiques et ainsi garanti "sans danger pour les enfants".

En juin 2001, le projet de loi 471 ou Loi de protection des étudiants contre l'Internet de 2001 est déposé. La loi obligerait les bibliothèques des institutions d'enseignement privées et publiques ayant accès à Internet à installer des logiciels de blocage des sites aux contenus "obscènes et violents". Le texte n'a toujours pas été promulgué.

Antiterrorisme et menaces sur la confidentialité et la sécurité

Les projets de nouvelles lois antiterroristes, et notamment l'article 10 de la House Bill 3802, élaborés après les attentats du 11 septembre, donnent toute latitude au gouvernement de "mettre sur écoute toute ligne, tout câble ou tout moyen de trans-

mettre toutes formes de communications, écrites ou orales, conversations, débats, informations ou données, et d'intercepter secrètement, d'écouter ou de surprendre et d'enregistrer les communications, écrites ou orales, les conversations, les débats, les informations ou les données". Cette autorité s'étend clairement à la surveillance de l'Internet et des communications par e-mail.

De plus, dans ces projets de loi, la définition du terrorisme est suffisamment floue pour être appliquée à toutes sortes de critiques légitimes du gouvernement. Bien que la Constitution garantisse très clairement la liberté d'expression, ces nouvelles mesures, présentées par le gouvernement de Gloria Arroyo dans un contexte de guerre ouverte contre les séparatistes musulmans sur l'île de Mindanao, sonnent comme un avertissement aux groupes qui s'opposent radicalement aux décisions de Manille.

Même si certaines dispositions de l'avant-projet visent à empêcher d'éventuels abus de la loi, les organisations de défense des droits de l'homme craignent toujours que cette dernière soit facilement détournée aux dépens des droits civils et politiques. Un collectif conduit par la députée Liza Maza la qualifie, en mai 2002, de "mère de toute loi répressive." D'autres considèrent que ces projets de lois antiterroristes remettent en vigueur la loi antisubversive qui était utilisée par l'ancien dictateur Ferdinand Marcos contre les groupes d'opposition et les individus pendant la dictature et qui avait été abrogée.

LIENS :

- Article sur les lois antiterroristes
www.cyberdyaryo.com/features/f2002_0513_02.htm
- Site sur la liberté d'expression aux Philippines
www.cmfr.com.ph/index.html
- Le quotidien *Inquirer*
www.inq7.net
- Archives d'Amnesty International sur les droits de l'homme aux Philippines
web.amnesty.org/library/eng-phl/index

Royaume-Uni

POPULATION : 59 542 000

INTERNAUTES : 24 000 000

FOURNISSEURS D'ACCÈS PRIVÉS : OUI



Le gouvernement de Tony Blair a adopté, au lendemain du 11 septembre, de nouvelles mesures de surveillance à l'encontre d'Internet.

Le "Terrorism Act", la loi antiterroriste votée 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 ostensiblement les e-mails privés". En vertu de la nouvelle loi, la police est dispensée de demander l'autorisation 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 annoncé qu'ils envisageaient la délocalisation de leurs serveurs hors de Grande-Bretagne.

Mi-juin 2002, David Blunkett, ministre de l'Intérieur, a par ailleurs présenté un projet de révision d'une loi très controversée adoptée en juin 2000, le "Rip Act" (Regulation of Investigatory Powers Act). Dans le but de lutter contre la criminalité informatique, ce texte permet le contrôle de tout le trafic du réseau (courriers électroniques et sites) par les services secrets. Le projet de David Blunkett préconisait, quant à lui, d'autoriser les administrations locales (impôts, Sécurité sociale, services municipaux, etc.) à accéder aux données relatives aux connexions des citoyens au Réseau et à leurs envois et réceptions de e-mails. Il a provoqué une telle levée de boucliers, tant dans la presse qu'au niveau des groupes de défense des libertés civiles, que le gouvernement a décidé, début juillet 2002, de reporter sine die cette révision législative.

Elizabeth France, commissaire à l'Information en Grande-Bretagne (cette autorité indépendante veille à ce que les droits des citoyens, en matière d'accès à leurs informations personnelles, ne soient pas violés par l'Etat, les administrations ou les services de sécurité), a taillé en pièces ce projet, dans un rapport rendu public en août 2002. Elle affirme que la rétention des données et le projet de révision du "Rip Act" peuvent porter gravement atteinte aux libertés fondamentales des Britanniques et faire reculer le droit (garanti) à la protection de la vie privée. Elle considère même que des points de la loi et du nouveau projet de loi sont anticonstitutionnels.

LIENS :

- Site officiel du gouvernement
www.hms0.gov.uk

- L'association Cyber-Rights & Cyber-Liberties
www.cyber-rights.org

- Association des fournisseurs d'accès du Royaume-Uni
www.ispa.org.uk



Russie

POPULATION : 144 664 000

INTERNAUTES : 6 000 000

FOURNISSEURS D'ACCÈS PRIVÉS : OUI

Internet est devenu un moyen très utilisé de diffusion de l'information. Mais la liberté d'expression des voix dissidentes sur le Net est mise à mal par des lois dites "antiterroristes".

À la demande du président russe Vladimir Poutine, la Douma, principale chambre du Parlement, a voté, fin juin 2002, un projet de loi relatif à l'interdiction des "activités extrémistes sous toutes ses formes" sur Internet. Ce nouveau dispositif législatif inquiète les défenseurs de la liberté d'expression en ligne. Ils voient en lui un accroissement préjudiciable des pouvoirs de la police. L'opposition politique au président Poutine craint, quant à elle, que le pouvoir n'utilise régulièrement cette loi pour s'en prendre à des partis minoritaires. Il lui suffirait en effet d'accuser ces formations politiques ou ces opposants d'encourager ou de supporter des activités extrémistes sur Internet pour pouvoir les poursuivre en justice et faire fermer leurs sites.

"Il est vrai qu'il y a aujourd'hui en Russie des extrémistes, des nationalistes. Mais le véritable objectif de cette loi n'est pas celui déclaré de les éradiquer", a affirmé Sergei Kovalev, l'un des 450 députés de l'Assemblée russe et membre du parti libéral Union des forces de droite, le SPS. "Le texte permet d'interdire des activités en ligne sans aucun motif sérieux", souligne le député. Il s'inquiète par ailleurs d'un article prévoyant une sanction qui pourrait "prendre en considération" les lois russes sur la criminalité.

Mais les critiques les plus sévères portent sur la définition en onze points de ce qu'est une activité extrémiste. Elle fait écho aux textes interdisant le terrorisme et toute tentative visant à renverser un gouvernement ou inciter à l'émeute ou au conflit racial. Le texte bannit également toute activité ou publication qui menacerait la "sécurité" de la Russie. Les défenseurs de la liberté d'expression et des droits de l'homme sont convaincus que cette trop large définition de l'extrémisme mettra en danger des activités tout à fait légitimes, tels les sites Web qui militent contre la guerre en Tchétchénie.

Fin octobre 2002, le ministère de l'Information a menacé de fermer le site Internet de

la radio *Ekho Moskvyy* parce qu'elle avait diffusé une interview de preneurs d'otages tchéchènes qui retenaient plusieurs centaines de personnes dans un théâtre moscovite. Cet événement a donné l'occasion aux autorités de proposer une loi antiterroriste qui permet au pouvoir de poursuivre n'importe quel journaliste couvrant des sujets liés au terrorisme ou à la guerre en Tchétchénie. Au dernier moment, Vladimir Poutine a mis son veto à loi et demandé aux parlementaires de la reformuler.

Les sites d'informations tchéchènes sont par ailleurs méthodiquement bloqués, comme chechen.ru, fermé par le FSB (ex-KGB) le 5 novembre 2002. Début décembre, Dmitri Chepchugov, chef du département de lutte contre la cybercriminalité du ministère de l'Intérieur, a déclaré que tous les sites Internet liés aux combattants tchéchènes avaient été identifiés, et qu'un nombre indéterminé de sites avaient été fermés. Bien que basés à l'étranger, ces derniers vont jusqu'à être interdits d'accès par les providers du pays d'accueil. Ainsi, l'accès du site [kavkazt-senter](http://kavkazt-senter.com), basé en Estonie, a été rendu impossible fin avril 2003, après des pressions des autorités russes.

LIENS :

- La Fondation pour la défense de la glasnost
www.gdf.ru
- Le site de *Radio Free Europe/Radio Liberty*
rferl.org
- Agence de presse pour les droits de l'homme *Prima-News*
www.prima-news.ru/eng



Singapour

POPULATION : 4 108 000

INTERNAUTES : 2 247 000

FOURNISSEURS D'ACCÈS PRIVÉS : OUI

L'Etat-Cité est l'un des pays les mieux connectés d'Asie, mais le gouvernement n'accorde qu'un espace très réduit aux opposants qui utilisent Internet pour s'exprimer. Les autorités tentent également d'imposer une utilisation "responsable" de l'Internet.

Ouvert au grand public en 1995, Internet a connu depuis un développement fulgurant. Près de 70 % des foyers sont équipés d'un ordinateur. Alors que huit cent mille internautes étaient recensés en 1999, ils sont désormais plus de deux millions. Quant au nombre de sites domiciliés dans l'Etat (enregistrés avec le suffixe ".sg"), il est passé de neuf cents en 1996 à plus de dix-sept mille aujourd'hui.

Néanmoins, l'Etat n'apprécie guère la critique et l'opposition, et, même s'il s'en défend, pratique une censure relativement discrète mais efficace. Il a placé Internet, dès la fin des années 90, sous le contrôle de l'autorité audiovisuelle de Singapour (SBA) qui contrôle l'accès aux sites et les contenus, et appelle au respect d'une charte définissant une utilisation "responsable" d'Internet. La SBA demande aux opérateurs de bloquer l'accès aux sites proposant des contenus "portant atteinte à la sécurité publique, à la défense nationale, à l'harmonie raciale et religieuse et à la morale publique". Elle aurait déjà fait bloquer plus cent sites dont le contenu a été jugé pornographique par l'autorité de régulation. Cette même autorité a également imposé un Code pratique à l'usage des fournisseurs d'accès. Ces derniers voient leurs activités soumises à l'obtention d'une licence. Ils doivent par ailleurs accepter l'installation au sein de leurs infrastructures de systèmes de filtrage au travers desquels doivent passer les connexions Internet locales.

Les sites Internet politiques et religieux doivent être enregistrés auprès de l'Autorité de développement des médias (MDA). Cet organisme public demande également aux fournisseurs d'accès de bloquer une centaine de sites jugés indésirables. Certains opérateurs Internet incitent également leurs clients à installer des filtres, notamment CyberPatrol et Smart Filter, sur leurs ordinateurs. Mais cela concerne essentiellement les sites pornographiques.

En 2001, des amendements ont été votés, en marge des élections législatives, pour

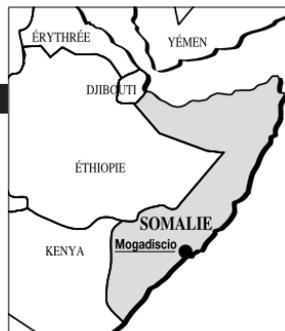
restreindre l'utilisation des sites politiques. Les opposants, les contestataires ou les journalistes soucieux d'exercer leur esprit critique se heurtent par ailleurs à deux écueils. D'une part, la loi sur la sécurité intérieure, qui permet de détenir quiconque porte atteinte à la notion très vague de "sécurité de l'Etat". D'autre part, le montant élevé des amendes à régler dans le cas de condamnations pour diffamation.

En juillet 2002, Zulfikar Mohamad Shariff, opposant et auteur de nombreux articles sur Internet, est contraint de s'exiler après que la police eut perquisitionné son domicile et menacé de l'arrêter. Son ordinateur est saisi. Il est accusé d'avoir diffamé la belle-fille d'un ministre. Il risque deux ans de prison. Réfugié en Australie, il a appris récemment que des accusations de sédition et de menace à l'harmonie raciale pèseront contre lui s'il rentre à Singapour.

En mars 2003, le gouvernement met en place une Cyber Wellness ("cyber bon comportement") Task Force censée apprendre à la population de Singapour comment bien se comporter sur Internet. Parmi les objectifs de cet organisme public : empêcher que les millions d'internautes singapouriens n'envoient des "e-mails inutiles" ou du spam, ne se connectent à des sites pornographiques ou n'utilisent des pseudonymes sur les forums de discussion. Michael Yap, le directeur de cette Task Force, prévoit des campagnes d'information, la création de sites Internet et des ateliers de formation.

LIENS :

- L'organisation de défense de la liberté d'expression en Asie du Sud-Est Think Centre
www.thinkcentre.org
- Le site de James Gomez, spécialiste des questions de liberté d'expression à Singapour
www.jamesgomeznews.com
- La Media Development Authority, autorité de régulation des médias et d'Internet
www.mda.gov.sg



Somalie

POPULATION : 9 157 000

INTERNAUTES : STATISTIQUES NON DISPONIBLES

FOURNISSEURS D'ACCÈS PRIVÉS : OUI

Raccordée à la Toile depuis 1999, la Somalie est très en retard en matière de développement des nouvelles technologies de l'information. Quelques centaines d'Internautes seulement surfent sur Internet dans la quarantaine de Call Shops (centres d'appel) et de Web bars de la capitale, Mogadiscio. A cela, deux raisons : on ne recense pas plus de deux mille lignes téléphoniques dans le pays, et le coût des communications, même s'il a baissé en 2002, reste onéreux pour l'une des populations les plus pauvres d'Afrique.

Fait rare dans le monde et dans l'histoire récente d'Internet : 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. Ainsi, durant deux mois, les Somaliens ont été isolés du reste du monde numérique. Courant janvier 2002, un nouvel opérateur, NetXchange, a réinvesti le marché. Il propose des services en matière de fourniture d'accès à la Toile et de Télécommunications. Il a, de fait, englobé les activités des deux défunctes compagnies.

LIENS :

- "Internet Returns to Mogadishu", article de *AllAfrica.com*, 23 janvier 2002
<http://allafrica.com/stories/200201230295.html>



Sri Lanka

POPULATION : 19 104 000

INTERNAUTES : 200 000

FOURNISSEURS D'ACCÈS PRIVÉS : OUI

Bien que différents fournisseurs d'accès proposent leurs services et que plus d'une centaine de cybercafés aient ouvert leurs portes dans les grandes villes, le nombre d'internautes peine à dépasser la barre des deux cent mille. Ces derniers utilisent essentiellement le Réseau pour envoyer et recevoir des courriers électroniques.

Aucune loi spécifique ne régit Internet au Sri Lanka. L'autorité de régulation des télécommunications donne son agrément technique aux fournisseurs d'accès tandis que les éditeurs et responsables de sites doivent s'enregistrer auprès du Council for Information Technology (Cintec), carte d'identité ou registre commercial à l'appui. Ils sont donc aisément identifiables par les autorités. Pour autant, aucun site n'a été censuré.

Lent, le développement d'Internet joue néanmoins un rôle particulier dans la vie politique sri lankaise. Depuis vingt ans, la guerre fait rage entre le pouvoir et les rebelles du Liberation Tigers Tamil Ealam, les Tigres tamouls. Un affrontement qui se prolonge jusque sur la Toile.

Accusé par la presse progouvernementale, en juin 2001, d'être un espion des Tigres tamouls, Dharmaratnam Sivaram, directeur du site d'informations *Tamilnet*, a été frappé par des inconnus à son bureau, le 26 décembre 2001. Une blessure qui lui a été infligée à la tête a nécessité six points de suture. *Tamilnet* est le plus connu des sites sur la situation politique et militaire dans les zones ravagées par la guerre entre l'armée et les Tigres tamouls.

Dans la nuit du 7 janvier 2002, c'est au tour du domicile de Senathirajah Jeyanandamoorthy, correspondant de *Tamilnet* et du *Tamil Daily Virakesari* à Batticaloa (est de l'île), d'être attaqué à la grenade. Les assaillants ont également tenté d'incendier la maison. Le journaliste et sa famille ont réussi à échapper aux flammes. Selon l'Association des journalistes de l'Est, le journaliste a reçu des menaces de mort, notamment d'organisations extrémistes musulmanes. M. Jeyanandamoorthy est l'auteur de plusieurs articles portant sur les activités des extrémistes musulmans dans cette région du pays. Par ailleurs, ses articles sur les

rebelles Tigres tamouls lui ont également attiré les critiques des nationalistes cinghalais.

Le développement d'Internet devrait bénéficier de l'apaisement de la situation. Un cessez-le-feu est observé par les belligérants depuis le 22 février 2002, et des négociations ont débuté en mai.

LIENS :

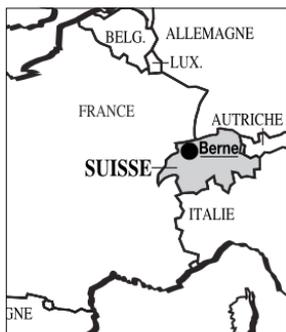
• Site d'informations indépendant
www.theacademic.org

• Le site d'informations *Tamilnet*
www.tamilnet.com

• Site favorable au LTTE
www.eelamweb.com

• Le Council for Information Technology
www.cintec.lk

• L'armée sri lankaise
www.slarmy.org



EUROPE

Suisse

POPULATION : 7 170 000

INTERNAUTES : 2 375 000

FOURNISSEURS D'ACCÈS PRIVÉS : OUI

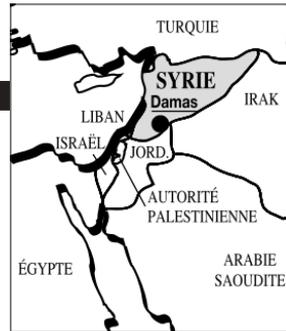
L'article 322-bis du code pénal suisse, entré en vigueur le 1^{er} avril 1998, permet de poursuivre celui qui, délibérément ou par négligence, ne se sera pas opposé à la publication de contenus illicites. Ce système de responsabilité en cascade, applicable en presse écrite, vaut également pour Internet. Ainsi, à défaut d'en trouver l'auteur ou de pouvoir le traduire devant un tribunal suisse, on pourrait imputer la responsabilité du contenu d'un site à son éditeur, à son hébergeur, voire au fournisseur d'accès.

La loi fédérale sur la surveillance de la correspondance par poste et télécommunication, entrée en vigueur le 1^{er} janvier 2002, oblige les fournisseurs à conserver pendant six mois les données et les communications de leurs utilisateurs et à les transmettre, sur ordonnance judiciaire et si possible en temps réel, au service chargé de la surveillance.

Par ailleurs, la police fédérale estime, dans un avis écrit publié au printemps 2000, que l'hébergeur a le devoir de vérifier la légalité des données hébergées en cas de plainte. La police peut également être amenée à demander à un fournisseur de bloquer l'accès à un site Web, et à un hébergeur de rendre inaccessible ou de supprimer un site donné. Le tout à leurs frais et sans dédommagement. L'étendue précise des obligations de surveillance et de comportement à charge des hébergeurs et des fournisseurs d'accès est toutefois discutée en doctrine, et aucun tribunal suisse ne s'est encore penché directement sur ces questions de responsabilité.

LIENS :

- Préposé fédéral à la protection des données
www.edsb.ch
- Droit des technologies de l'information
www.juriscom.net
- L'association des utilisateurs d'Internet SIUG
www.saug.ch



Syrie

POPULATION : 16 610 000

INTERNAUTES : 60 000

FOURNISSEURS D'ACCÈS PRIVÉS : NON

La Syrie est l'un des Etats qui surveillent le plus étroitement Internet. L'accès au Réseau est réservé aux administrations et à certaines entreprises privilégiées. Le reste de la population ne peut surfer que dans les quelques rares cybercafés officiels soumis à un contrôle strict, ou dans des cafés Internet clandestins.

Le Syrian Telecommunications Establishment (STE, gouvernemental) verrouille la Toile. L'accès à tous les contenus jugés "offensants", tels les sites pornographiques ou pro-israéliens, sont bloqués. Les e-mails sont contrôlés. L'envoi de courriers électroniques à des étrangers, sans autorisation des autorités, est passible d'une peine de prison. Quand un particulier souhaite bénéficier d'une connexion à son domicile, les techniciens d'Etat viennent installer le matériel chez lui ainsi que les logiciels nécessaires et choisissent eux-mêmes son mot de passe.

LIENS :

- Le quotidien arabophone gouvernemental *Teshreen*. Ce site en arabe permet d'accéder au site du journal gouvernemental anglophone *Syria Times*.
www.teshreen.com

- Site d'informations sur les pays arabes
www.arabnews.com



Thaïlande

POPULATION : 63 584 000

INTERNAUTES : 4 800 000

FOURNISSEURS D'ACCÈS PRIVÉS : OUI

Le Réseau thaïlandais est placé sous l'autorité de quatre organismes de tutelle : le National Information Technology Committee (NITC), le National Electronics and Computer Technology (NECTEC), la Telephone Organisation of Thailand (TOT) et la Communications Authority of Thailand. La multiplication de ces organismes a freiné le développement de la Toile plus qu'elle ne l'a soutenu. D'autant que la Communications Authority of Thailand détient, du fait d'une disposition légale, au moins 32 % du capital de chacun des fournisseurs d'accès, tous privés.

Les médias, très présents sur la Toile, ne dénoncent pas de cas de censure de leurs sites, même si les relations restent tendues entre les médias indépendants et le Premier ministre populiste Thaksin Shinawatra. En revanche, la NITC a dévoilé, en juillet 2001, son intention de traquer les "contenus inappropriés" sur le Réseau. Ce plan contraint les fournisseurs d'accès à conserver pendant au moins trois mois les données de connexion des internautes. Ces mesures doivent permettre, selon les autorités, de repérer et faire bloquer l'accès aux sites indésirables, et de poursuivre les internautes qui s'y connecteraient. Le Département royal de la police doit coopérer étroitement avec la NITC. Cette dernière est principalement chargée, en étroite collaboration avec des experts techniques et juridiques, de surveiller Internet pour identifier les sites visés ainsi que les nombreux cybercafés.

Le 19 décembre 2002, Surapong Suebwonglee, ministre de l'Information et des Technologies de la communication a annoncé qu'il avait sollicité la collaboration des opérateurs Internet, notamment la vingtaine de fournisseurs d'accès du pays, pour empêcher les internautes d'accéder aux sites à caractère "obscène" et "subversif". Selon le quotidien *The Nation*, le ministre a défini les sites subversifs comme étant ceux qui mettent en danger la sécurité nationale et la monarchie. Surapong Suebwonglee veut faire d'Internet en Thaïlande un "endroit plaisant".

LIENS :

- The Communications Authority of Thailand : www.cat.or.th/eng
- Le groupe de presse The Nation : www.nationmultimedia.com



Tunisie

POPULATION : 9 562 000

INTERNAUTES : 505 500

FOURNISSEURS D'ACCÈS PRIVÉS : OUI

CYBERDISSIDENT EMPRISONNÉ : 1

En Tunisie, le discours officiel prône le développement rapide et une démocratisation exemplaire d'Internet. Cependant, les services de sécurité opèrent une surveillance implacable du cyberspace. Censure des sites, interception des e-mails, contrôle des cybercafés, arrestations et condamnations arbitraires sont le lot quotidien des internautes. Arrêté en 2002, un cyberdissident a été condamné à deux ans de prison.

Raccordée à la Toile depuis le milieu des années 90, la Tunisie est le pays du Maghreb le plus avancé en matière d'expansion d'Internet. Une expansion qu'il faut imputer à la volonté politique du pouvoir d'encourager le Web, dans lequel il place beaucoup d'espoirs économiques. L'ATI, l'Agence tunisienne d'Internet, dépend directement du ministère des Télécommunications. Elle gère le Réseau au plan national. L'infrastructure téléphonique étant globalement de qualité, les autorités ont encouragé l'expansion du secteur des fournisseurs d'accès. Il en existe douze : six publics et six privés. Le gouvernement a créé trois cents Publinets (cybercafés publics) sur l'ensemble du territoire et revendique un taux d'équipement et des connexions des établissements scolaires enviable : "100 % des universités et établissements secondaires, par exemple". Un chiffre qu'il faut relativiser : à la faculté de droit de Tunis, il existerait une quinzaine d'ordinateurs pour 17 000 étudiants.

Comme la liberté de la presse n'existe pas en Tunisie, les internautes ont massivement investi la Toile pour exploiter cet espace d'expression. C'est le cas de la journaliste Sihem Bensedrine qui, n'ayant pas obtenu d'agrément pour publier son journal, a créé un webmagazine, *Kalima*. Mais c'était sans compter sur la puissance de l'appareil policier et la détermination du président Ben Ali à faire taire la cyberdissidence. L'Etat tunisien est l'un de ceux qui ont déployé la plus vaste panoplie de censure au monde à l'encontre d'Internet. Les seuls fournisseurs d'accès autorisés à desservir le grand public appartiennent à des proches du Président, dont sa propre fille. L'ATI veille à ce que le marché soit rigoureusement encadré et contrôlé par les autorités : pour exercer, les fournisseurs d'accès doivent signer un contrat stipulant que l'usage d'Internet doit se limiter "à des fins scientifiques, technologiques,

commerciales, strictement en rapport avec les activités des clients”.

Le cyberspace tunisien est régi par le code de la presse de 2001, un texte qui organise la censure. Certains sites d'informations tunisiens (*Kalima*, *TUNeZINE*), mais aussi d'ONG ou de médias étrangers diffusant des informations critiques contre le gouvernement, voient régulièrement leurs accès bloqués en Tunisie.

Les pouvoirs de la “cyberpolice”

Les gérants des Publinets ont le droit de surveiller les écrans des ordinateurs pour voir sur quels sites surfent les clients. Ils peuvent même les contraindre à se déconnecter à tout moment. De nombreux témoignages prouvent que ces cybercafés sont étroitement surveillés par la machine policière de Zine el-Abidine Ben Ali. Régulièrement, des policiers en civil viennent relever les historiques des navigations effectuées depuis les machines. Par recoupements, ils peuvent ainsi savoir qui a surfé et sur quels sites.

En 2002, le contrôle des moyens de communication, dont Internet, a encore été renforcé. Une véritable police du cyberspace sévit. Ses activités : traquer les sites “subversifs” pour pouvoir en bloquer l'accès ; intercepter les requêtes vers des sites ou les courriers à contenus “politiques ou critiques” ; rechercher le maximum d'adresses de “proxys”, ces serveurs relais qui permettent aux internautes d'accéder aux sites interdits en contournant les systèmes de blocage, et les rendre inopérants ; pister et interpeller les internautes trop actifs, les cyberdissidents.

Le 5 février 2003, un groupe d'une vingtaine de jeunes hommes sont arrêtés, à leur domicile, dans la ville de Zarzis (500 km au sud du pays). En avril, sept d'entre eux, dont un mineur, sont détenus à la prison civile de Tunis. Ils sont accusés “d'association de malfaiteurs, de vol et acquisition de produits pour la fabrication d'explosifs” pour avoir consulté des sites “terroristes”. Selon leur avocat qui a pu leur rendre visite en prison, ils ont été torturés.

Le 22 avril, le quotidien *La Presse* rapporte que le gouvernement a gelé l'octroi d'autorisations pour les cybercafés privés et annoncé son intention de limiter l'accès à Internet à des “centres de services publics” contrôlés par l'Etat.

“Ettounsi” condamné à deux ans de prison

Le 4 juin 2002, Zouhair Yahyaoui a été arrêté à Tunis par des policiers en civil dans une société informatique où il tenait une permanence. Le jeune homme a ensuite été conduit à son domicile, où les policiers ont effectué une fouille de sa chambre et saisi son matériel informatique personnel.

Durant la période d'interrogatoire, le cyberdissident a subi trois séances de “suspension”, méthode de torture qui consiste à suspendre la personne par les bras, avec les pieds touchant à peine le sol. C'est à l'issue de la dernière séance que le cyberdissi-

dent a fini par révéler le mot de passe d'accès à son site qui a permis aux autorités de le bloquer.

Zouhair Yahyaoui écrivait sous le pseudonyme "Ettounsi" qui signifie le "Tunisien" en arabe. Il avait fondé le site *TUNeZINE* en juillet 2001, pour diffuser des informations sur la lutte en faveur de la démocratie et des libertés en Tunisie, et publier en ligne des documents de l'opposition. Il avait écrit de nombreuses chroniques et pamphlets et avait été le premier à diffuser la lettre dénonçant le système judiciaire du pays, adressée au président de la République par le juge Mokhtar Yahyaoui, dont Zouhair est le neveu. Par ailleurs, *almizen.com*, le site du juge, que gérait également Zouhair Yahyaoui, a été totalement effacé.

TUNeZINE avait été censuré par les autorités dès sa création. Mais les fans du journal en ligne recevaient chaque semaine une liste d'adresses de "proxys", des serveurs relais permettant d'accéder au journal en dépit du blocage.

Le 10 juillet 2002, Zouhair Yahyaoui a été condamné, en appel, à une année de prison pour "propagation de fausses nouvelles dans le but de faire croire à un attentat contre les personnes ou contre les biens" (article 306 ter du code pénal), et à une autre année et quatre mois pour "vol par utilisation frauduleuse de moyens de communication" à savoir la connexion à Internet aux dépens du gérant du cybercafé dont il était l'employé (article 84 du code des communications). Incarcéré dans des conditions très difficiles, le cyberdissident a fait deux grèves de la faim au cours du premier semestre 2003 pour demander sa libération.

LIENS :

- Le magazine d'informations en ligne *Kalima*
www.kalima-tunisie.com
- Le site *TUNeZINE*
www.tunezine.com
- Le site Maghreb des droits de l'homme
www.maghreb-ddh.org



ASIE CENTRALE

Turkménistan

POPULATION : 4 835 000

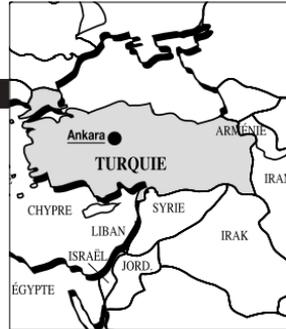
INTERNAUTES : 8 000

FOURNISSEURS D'ACCÈS PRIVÉS : NON

Le régime du président Separmourad Nyazov exerce un contrôle total sur les médias. Internet, pourtant quasiment inexistant dans le pays, n'échappe pas à cette mainmise. Seul l'opérateur étatique Turkmen Telecom est habilité à en fournir l'accès. Le site de *Radio Free Europe/Radio Liberty*, une radio financée par le Congrès américain et basée à Prague, est l'une des rares sources d'informations indépendantes disponibles au Turkménistan.

LIENS :

- Le service turkmène de *Radio Free Europe/Radio Liberty*
www.rferl.org/bd/tu
- Le site d'informations *Eurasianet*
www.eurasianet.org



Turquie

POPULATION : 67 632 000

INTERNAUTES : 4 900 000

FOURNISSEURS D'ACCÈS PRIVÉS : OUI

Le gouvernement d'Ankara sait se montrer aussi peu libéral envers Internet qu'envers la presse. Il censure ou traduit en justice les journalistes qui osent critiquer l'Etat et ses institutions.

Le Réseau a le vent en poupe, en Turquie. On estime à environ sept cent mille le nombre de personnes disposant d'une connexion à leurs domiciles. Les autres accros du Web surfent dans les cybercafés qui ouvrent à un rythme effréné, notamment dans les grandes agglomérations. Si l'opérateur public Turkish Telekom, via sa filiale TTnet, a pris les plus importantes parts du marché, d'autres opérateurs, privés, se développent sans problème majeur.

Néanmoins, les propriétaires de cybercafés doivent s'engager par écrit, avant d'ouvrir leur commerce, à "interdire tout accès à des sites séparatistes, intégristes, islamistes ou pornographiques". Ils doivent également obtenir une autorisation auprès de la police. Cette dernière s'est dotée d'une "brigade électronique" dont la mission est de renforcer le contrôle d'Internet et des communications électroniques. Une Direction générale de l'Internet existe par ailleurs au sein de la police à Ankara, et des directions régionales ont vu le jour dans le reste du pays.

Le Réseau n'est encadré par aucun texte législatif spécifique mais la loi sur le Haut Conseil de l'audiovisuel (RTÜK), adoptée en mai 2002, impose des restrictions sévères à la liberté d'expression sur Internet, le contenu des pages Web devant être soumis aux autorités pour approbation avant publication. Les magistrats tendent à juger les affaires liées à Internet en se référant à la loi très restrictive régissant la presse. Ainsi, le 6 décembre 2001, la cour correctionnelle d'Istanbul a décrété la fermeture de *ideapolitika.com*, le site de la revue trimestrielle politique et culturelle *Idea Politika*, suite aux poursuites judiciaires dont elle était elle-même l'objet. Cette décision n'a pas pu entrer en vigueur, le site étant administré en France. Erol Ozkoray, ancien directeur de la revue, comparaitra le 11 juillet 2003 devant la cour pour la publication, le 11 septembre 2001, d'un article intitulé "A quoi sert l'armée?" sur le site de la revue. Poursuivi pour insulte à l'armée, le journaliste encourt une peine de trois ans de prison.

Le 23 mars 2000, Coskun Ak, coordinateur des activités interactives de la société Superonline, a été condamné à quarante mois de prison pour "moqueries et insultes envers la République, les forces armées, les forces de sécurité et la justice". Coskun Ak était accusé d'avoir laissé en ligne, en mai 1999, un texte sur les atteintes aux droits de l'homme dans le sud-est du pays, posté sur le forum du site par un internaute. La peine a été commuée en amende. Le 24 avril 2003, la cour d'assises d'Istanbul a acquitté Coskun Ak. Elle a estimé qu'il n'existait pas suffisamment d'éléments permettant de déterminer sa responsabilité vis-à-vis du contenu du texte incriminé contenant "des offenses et insultes graves à l'encontre des institutions de l'Etat".

LIENS :

- Site de la revue *Idea Politika*
www.ideapolitika.com
- L'organisation Cyber-Rights & Cyber-Liberties
www.cyber-rights.org
- L'Union européenne en ligne
www.europa.eu.int



Ukraine

POPULATION : 49 112 000

INTERNAUTES : 600 000

FOURNISSEURS D'ACCÈS PRIVÉS : OUI

Bien que peu avancé, le développement d'Internet en Ukraine a profité aux journalistes d'investigation et à leurs publications en ligne, seuls à même de publier des enquêtes non censurées. En retour, ces derniers sont régulièrement soumis à la pression des autorités.

L'Ukraine affiche un retard certain en matière de développement d'Internet. Le prix des ordinateurs et, surtout, les coûts de connexion au Réseau sont trop élevés pour une grande partie de la population. Quant au report régulier de la privatisation d'UkrNet, l'opérateur national de télécommunications, il constitue un obstacle à l'arrivée de nouveaux concurrents et donc à une baisse significative des prix. Pourtant, dans ce pays administré avec poigne par le président Leonid Koutchma, les journalistes audacieux ont recours à la Toile depuis la fin des années 90 pour publier une information indépendante. Une audace professionnelle qui peut leur coûter cher. L'affaire Gongadze est, à cet égard, tristement révélatrice.

Avancées dans l'enquête sur le meurtre de Géorgiy Gongadze

Fondé au printemps 2000, *Ukrainskaïa Pravda*, premier journal d'opposition publié uniquement sur Internet, s'impose rapidement auprès des internautes locaux par le style incisif de ses articles. "C'est une façon d'exercer librement notre métier même si dans l'Ukraine d'aujourd'hui cela est pratiquement impossible", écrivait Géorgiy Gongadze, son fondateur et rédacteur en chef. Durant les mois précédant sa disparition, le journaliste dénonce à plusieurs reprises les menaces dont il fait l'objet. En juillet 2000, il s'adresse même au procureur général d'Ukraine, Mihailo Potebenko, pour dénoncer les actions "d'intimidation préméditée pour lui faire peur, ou empêcher ses activités". Le 2 novembre 2000, le corps décapité du journaliste est retrouvé près de Tarachtcha, à 140 kilomètres de Kiev. Les révélations sur une probable implication de hauts responsables de l'Etat dans la disparition et le meurtre de Géorgiy Gongadze ébranlent le pouvoir du président Leonid Koutchma. Néanmoins, l'appareil d'Etat fait puissamment obstacle à la recherche de la vérité. Le parquet général et le ministère de l'Intérieur s'opposent à toute enquête sérieuse sur les conditions de la disparition et du meurtre du journaliste.

Au cours de l'année 2002, l'enquête connaît cependant de véritables avancées. Le 19 juillet, le parquet général ordonne une nouvelle expertise des enregistrements impliquant le Président et accepte une nouvelle analyse du corps de Géorgiy Gongadze avec la participation de spécialistes européens. Le 5 août, le nouveau procureur général, Sviatoslav Piskoun, accorde à Robert Ménard, secrétaire général de Reporters sans frontières, la qualité de représentant légal des parties civiles. Le 3 septembre, le procureur général admet que des violations de la loi ont été commises au cours de l'enquête, reconnaît l'identité du corps et la mort du journaliste par décapitation. Le 10 septembre, le procureur général annonce la mise en examen du procureur de Tarachtcha, la ville où le corps du journaliste a été retrouvé, pour falsification du premier procès-verbal sur le corps de la victime et pour ne pas avoir procédé à l'identification du corps dès sa découverte. Sergiy Belinskiy, l'enquêteur de Tarachtcha, est également mis en examen pour falsification de documents. A l'occasion du deuxième anniversaire de la disparition de Gongadze, le 16 septembre, Reporters sans frontières demande la possibilité d'étudier, avec l'aide d'un expert indépendant de son choix, l'intégralité des résultats des expertises précédentes ainsi que les textes les ordonnant. L'organisation demande également au parquet de procéder à l'audition des quatre hommes identifiés qui auraient suivi la victime les semaines précédant sa disparition. Le même jour, avec le concours du réseau Damoclès et de l'Institut des Mass Medias, Myroslava Gongadze, la veuve de Géorgiy Gongadze, dépose une plainte à la Cour européenne des droits de l'homme, mettant en cause l'obstruction du parquet au cours de l'enquête. En octobre, le secrétaire général de Reporters sans frontières et un médecin légiste français examinent tous les documents relatifs aux expertises antérieures. Une expertise indépendante, menée en janvier 2003 à l'initiative de Reporters sans frontières et à la demande de la mère de Géorgiy Gongadze, permet d'identifier le corps du journaliste disparu. L'enquête, qui s'orienterait désormais vers d'anciens responsables du ministère de l'Intérieur, n'a encore donné aucun résultat.

Le contrôle s'intensifie

En janvier 2001, une Direction d'Internet est créée au sein du Comité d'Etat pour l'information. Sa mission est bien définie : "surveiller la fausse information en Ukraine."

Le 28 février, une directive du gouvernement place le Centre d'Etat de la sécurité d'information sous la direction du SBU, les services secrets ukrainiens, et de ce fait Internet sous le contrôle de ces derniers.

Le 1^{er} juin, est créée une ONG spécialisée dans l'administration des noms de domaines en ".ua" des sites ukrainiens. Parmi ses fondateurs figurent, outre le SBU, quelques fournisseurs d'accès, dont MM. Kokhmaniuk et Sviridov qui enregistraient les noms de domaines en ".ua" mais ont accepté de céder leurs droits à la nouvelle ONG. Cette dernière a initié, le 12 novembre, un projet de loi qui, sous couvert de lutte contre le terrorisme, le crime organisé ou la pornographie, permettrait de renforcer le contrôle du Réseau.

Le 26 juin, le journaliste d'investigation Oleg Yeltsov est convoqué pour un interrogatoire dans les bureaux du SBU (services secrets ukrainiens). Il est accusé de "violation de secret d'Etat" suite à la publication sur le site *Ukraina Kriminalna* (Ukraine criminelle) d'un article au sujet du train de vie de l'ancien chef des services secrets, Leonid Derkach, et de son fils, un oligarque ukrainien. L'appartement d'Oleg Yeltsov est perquisitionné pendant son interrogatoire.

Le 16 juillet, Volodymyr Radtchenko, chef du SBU, a déclaré lors d'une conférence de presse à Kiev : "En tant que SBU, nous désirons que tous les utilisateurs d'Internet soient enregistrés." Il a justifié cette volonté par le souhait de constituer un annuaire pour les internautes.

Le 23 août, le président Léonid Koutchma signe un décret sur la transparence de la télécommunication en Ukraine, qui donne un mois au gouvernement pour définir les mesures nécessaires à l'amélioration des méthodes de règlement par l'Etat de la circulation des informations.

Le 25 septembre, l'accès au site Internet du journal d'opposition *Antenna* à Tcherkassy est bloqué. La veille, le journal avait reçu la visite de responsables de la milice locale qui lui avaient proposé une "protection informatique" du site du journal.

En décembre 2001, les journalistes du journal en ligne *Forum* sont convoqués par le SBU pour divulgation de secret d'Etat suite à la publication sur leur site, le 15 juin 2001, d'un article citant le compte rendu de la vérification du département des réserves d'Etat par le service de contrôle d'Etat. L'assistance juridique de l'Institut des Mass Medias (IMM) permet aux journalistes d'échapper aux poursuites judiciaires.

Le 21 février 2002, les responsables du journal d'information politique en ligne *Obkom* portent plainte contre l'administration fiscale ukrainienne de Kiev. La veille, des fonctionnaires des services fiscaux se sont rendus dans les locaux du site pour le perquisitionner, alors que leur mandat concerne une banque de l'étage du dessous. Malgré les protestations du rédacteur en chef, Sergiy Soukhobok, et la présentation des différentes autorisations nécessaires à l'activité du journal sur la Toile, les fonctionnaires saisissent le matériel informatique et une partie de la documentation du titre. Bien que les services fiscaux aient reconnu avoir perquisitionné le journal "par hasard", ils n'ont jamais rendu les ordinateurs aux journalistes.

LIENS :

- L'organisation ukrainienne de défense de la liberté d'expression, Institut des Mass Medias : <http://fr.imi.org.ua>
- Le journal d'opposition *Antenna* : www.antenna.com.ua
- Le journal d'opposition en ligne *Ukrainskaïa Pravda* : www2.pravda.com.ua/en



Viêt-nam

POPULATION : 79 175 000

INTERNAUTES : 1 500 000

FOURNISSEURS D'ACCÈS PRIVÉS : OUI

INTERNAUTES ET CYBERDISSIDENTS EMPRISONNÉS : 5

Arrestations de cyberdissidents, blocage de l'accès aux sites jugés "politiquement ou culturellement incorrects", contrôle des courriers électroniques... bien que peu développé, le Réseau est toujours sous la coupe du Parti communiste. Le gouvernement d'Hanoi semble reproduire à la lettre le modèle chinois de contrôle du Réseau.

En avril 2001, l'arrivée à la tête du Parti communiste de Nong Duc Manh, le plus jeune dirigeant du tout-puissant Parti, a nourri l'espoir d'une plus grande liberté des médias et d'une accélération du développement d'Internet. Force est de constater que la situation n'a pas évolué en ce sens. Le Viêt-nam reste l'un des Etats de la planète les plus répressifs à l'encontre des cyberlibertés. L'un des principaux freins au développement du Réseau : les prix élevés des connexions et des communications. Cependant, les connexions à Internet sont de plus en plus nombreuses dans les universités, et le nombre de cybercafés croît très rapidement.

Mais le leader des cinq fournisseurs d'accès, publics ou semi-publics, Vietnam Data Communications (VDC), qui comptabilise près de 60 % du nombre total d'internautes, dépend de l'administration des Postes et Télécommunications, donc de l'Etat. Et ce dernier entend bien exercer un contrôle étroit des sites et des courriers électroniques. Ainsi, il bloque l'accès aux sites jugés politiquement ou moralement "dangereux", aux sites d'information étrangers et à ceux des organisations de défense des droits de l'homme créés par la diaspora vietnamienne. VDC contrôle, quant à lui, les sites visités par ses abonnés.

Selon des organisations d'opposition, le gouvernement communiste aurait même une politique active de piratage de sites indésirables. Le mouvement spirituel Hoahao affirme, par exemple, que les services de l'ambassade du Vietnam à Singapour envoient des virus aux adresses e-mails de ses adeptes, ainsi qu'aux opposants de la diaspora.

Pourtant, le Net sert désormais activement la propagande gouvernementale. Les tra-

vaux du neuvième congrès du PC, en avril 2001, ont été retransmis, dans plusieurs langues, sur le site de l'agence de presse officielle VNA. Des points d'accès à Internet avaient été mis en place dans le pays pour que la population suive le congrès sur la Toile. Et le Parti communiste vietnamien véhicule sa doctrine sur son propre site, ouvert en 2001.

En août 2001, le Premier ministre, reprenant à son compte certaines mesures proposées par le Département général des Postes et Télécommunications (DGPT), qui contrôle le développement des nouvelles technologies de l'information, a annoncé que le gouvernement allait autoriser l'arrivée sur le marché de nouveaux fournisseurs d'accès, y compris issus du secteur privé. Le gouvernement a par ailleurs interdit que l'usage d'Internet serve la contestation politique et permette de fomenter des actions hostiles contre le pays ou à même de déstabiliser la sécurité, de violer la morale, les lois et réglementations. Un message à destination des cyberdissidents.

Le 8 janvier 2002, Nguyen Khac Hai, vice-ministre de la Culture et de l'Information, promulgue un décret ordonnant à la police de saisir et de détruire toute publication non préalablement soumise au contrôle gouvernemental. Selon la radio BBC, les photocopies des pages d'informations du site Internet dissident Dialogue sont notamment visées par cette décision.

Le 5 août, le DGPT demande aux autorités des soixante et une provinces du pays de renforcer le contrôle et les inspections des cybercafés. Les autorités d'Hanoi recommandent de punir ceux qui se rendraient coupables d'une "utilisation nuisible" d'Internet. Deux jours plus tard, le ministère de la Culture et de l'Information suspend le site *TTVOnline* en raison d'une absence d'autorisation en bonne et due forme, et de la diffusion d'informations violant la loi sur la presse et "déformant la vérité". Le ministère se refuse à préciser la nature de ces informations. Selon d'autres sources officielles citées par l'*Agence France-Presse*, c'est le forum de discussion du site, où étaient abordés des thèmes tels que les concessions territoriales accordées en 1999 à la Chine, les réformes politiques et la corruption au sein du Parti communiste, qui aurait attiré les foudres du gouvernement. *TTVOnline* avait été élu, en 2001, meilleur site Internet pour les jeunes par la presse spécialisée.

Le 16 août, Phan An Sa, inspecteur en chef adjoint au ministère de la Culture et de l'Information, a appelé à faire barrage à la diffusion de matériaux subversifs ou pornographiques sur Internet. Il a stigmatisé cinq catégories d'utilisation du Net "portant préjudice à la sécurité nationale". Parmi elles, l'échange d'informations antigouvernementales et l'usage d'Internet pour frauder. Phan An Sa a ajouté que les autorités devraient imposer des amendes et mieux éduquer les jeunes quant à la façon d'utiliser le Réseau. La majorité des internautes vietnamiens a entre 14 et 24 ans. Début 2003, Phan An Sa annonce de nouveaux projets législatifs pour mieux contrôler le contenu diffusé sur Internet. Les sites hébergés au Viêt-nam devront disposer d'une licence et signaler aux autorités chaque modification de leur contenu. Par ailleurs, ce responsable souhaite que les opérateurs, notamment les fournisseurs d'accès et les propriétaires de cafés Internet, soient responsables du contenu diffusé

par leurs clients. Il explique ainsi, en janvier 2003, à un journaliste étranger que "les propriétaires de restaurant doivent garantir que la nourriture ne contient pas de substances dangereuses. C'est la même chose avec les propriétaires de cafés Internet. Ils ne sont pas autorisés à fournir à la jeunesse des substances empoisonnées".

Le 26 juin, le journal officiel *Thoi Bao Kinh te Vietnam* (Les Temps économiques du Viêt-nam) annonce que le gouvernement compte mettre en place un système national de contrôle des utilisateurs des cafés Internet. L'objectif du gouvernement est d'empêcher les Vietnamiens d'accéder à des sites Internet "politiquement et moralement dangereux". Cette décision a été prise suite à un rapport du ministère de la Culture et de l'Information qui a jugé "très nombreuses" les violations de la loi sur la diffusion d'informations subversives et de secrets d'Etat. Le même rapport a conduit le Premier ministre Pham Van Khai à ordonner, le 24 juin, à la police d'inspecter les quatre mille établissements Internet du pays.

Cinq cyberdissidents arrêtés en 13 mois

Le Chi Quang, un professeur d'informatique également diplômé de la Faculté de droit, est arrêté le 21 février 2002 dans un café Internet de Hanoi. Il est inculpé pour avoir diffusé à l'étranger des informations dangereuses. Les policiers ont saisi du matériel informatique et des documents à son domicile. Le Chi Quang, aujourd'hui âgé de 32 ans, est placé en détention dans le camp B14 de la province de Ha Dong (nord du pays). Son arrestation fait suite à la diffusion sur Internet d'un texte intitulé "Vigilance envers l'Empire du Nord". Dans ce document très détaillé, le dissident revenait sur les conditions dans lesquelles les autorités vietnamiennes ont signé des accords frontaliers avec le gouvernement de Pékin. Le texte a été très largement diffusé au sein de la communauté vietnamienne à l'étranger. Le 8 novembre, Le Chi Quang est condamné à quatre ans de prison ferme et trois ans de résidence surveillée pour "délit d'opposition à l'Etat de la République socialiste du Viêt-nam", en vertu de l'article 88 du code pénal qui interdit la distribution d'informations en opposition au gouvernement. Au cours du procès, qui n'a duré que trois heures, les droits de la défense n'ont pas été respectés. La presse étrangère n'a pas été autorisée à assister à l'audience. Seuls les parents de Le Chi Quang ont pu s'y rendre. Selon sa mère, "il a confirmé les faits dont on l'accuse, mais a rejeté l'accusation (...). Nous comptons faire appel de cette décision injuste." Lors du procès, le cyberdissident est apparu très affaibli et le visage enflé. Ses proches ont confirmé qu'il souffre d'une maladie des reins et que les autorités de la prison ont refusé de le soigner. Près d'une centaine de personnes, notamment des dissidents, s'étaient réunies devant le tribunal. L'un des manifestants aurait été interpellé par la police.

Le 8 mars, la police de Hô Chi Minh-Ville a perquisitionné le domicile de Tran Khue, professeur de littérature et fondateur d'une association de lutte contre la corruption. Les policiers ont saisi un ordinateur, une imprimante, un appareil photo, des téléphones portables et des documents appartenant au dissident. Le 10 mars, ce dernier a été placé en résidence surveillée en vertu de la directive administrative 31/ CP.

Cette décision fait suite à la diffusion sur Internet d'une lettre de Tran Khue adressée au président chinois Jiang Zemin, à la veille d'une visite officielle au Viêt-nam. Le dissident demandait au chef d'Etat de revoir certaines clauses des accords sino-vietnamiens. En août 2001, Tran Khue avait déjà été interpellé par la police et reconduit à son domicile alors qu'il enquêtait sur la situation dans les zones frontalières avec la Chine.

Le 25 mars, le colonel Le Van, membre de l'unité spéciale P4-A25 de la police, se rend au domicile de Son Hong Pham, médecin et représentant commercial pour une firme pharmaceutique, et lui ordonne de se présenter dans les locaux de son unité spéciale. Le dissident y est interrogé sur ses traductions d'articles publiés sur le site de l'ambassade américaine. Peu après, huit membres de cette unité ont perquisitionné son domicile à Hanoi. Ils ont saisi du matériel informatique ainsi que des documents personnels. Le 26 mars, Son Hong Pham est retourné au poste de police afin d'y réclamer, sans succès, ses effets personnels. Le lendemain, le dissident a diffusé sur Internet une lettre ouverte afin de protester contre la perquisition illégale et la saisie de ses effets personnels. Deux jours plus tard, sa famille annonce sa "disparition". Il faut attendre le 15 avril pour que sa mère soit autorisée à lui rendre visite en prison. Sa famille apprend que son arrestation ferait suite à la traduction et la diffusion sur Internet d'un article intitulé "Ce qu'est la démocratie", extrait des pages du site de l'ambassade des Etats-Unis au Viêt-nam. Le dissident est également l'auteur de nombreux articles, tels "La promotion de la démocratie : un élément clé pour un nouvel ordre mondial" ou encore "Souveraineté et droits de l'homme : la quête d'une réconciliation", parus sur les forums Internet Danchu.net et Ykien.net, tous deux consacrés à la promotion de la démocratie. Le 29 avril, on apprend que Son Hong Pham est détenu à la prison B14, près de Hanoi. Victime de pressions et de menaces, son épouse, Ha Thuy Vu, a dû quitter leur domicile en compagnie de ses deux fils. En juillet, le ministère de l'Intérieur se prononce pour le maintien en détention de Pham Hong Son.

Dans la soirée du 25 septembre, la police pénètre dans la maison de Nguyen Vu Binh afin de procéder à une fouille et à la saisie de ses effets personnels. Le journaliste est mis en état d'arrestation et incarcéré à la prison B 14, dans le district de Thanh Tri, à environ dix kilomètres de Hanoi. Collaborateur au *Tap Chi Cong San* (magazine du journal communiste), Nguyen Vu Binh a été renvoyé en janvier 2001 pour avoir essayé de fonder un parti indépendant. Il a écrit depuis des articles critiques sur la politique du gouvernement vietnamien. Le journaliste a déjà été brièvement interpellé le 19 juillet, pour avoir envoyé un témoignage écrit aux participants d'un congrès américain sur les droits de l'homme à Washington DC. Relâché le jour suivant, il est néanmoins placé en résidence surveillée, sous le contrôle étroit de la police, devant laquelle il est appelé à se présenter quotidiennement. En août, il a rejoint un groupe de vingt autres écrivains et dissidents pour signer une pétition adressée au gouvernement vietnamien, demandant des réformes juridiques et l'instauration d'un corps de lutte anticorruption indépendant. Les autorités ne se sont pas prononcées officiellement sur les raisons de l'arrestation de Nguyen Vu Binh. Elle pourrait être en relation avec la diffusion en ligne, en août, d'un de ses essais

critiques intitulé "Réflexion sur les accords frontaliers sino-vietnamiens" de décembre 1999.

Le 20 décembre, Nguyen Khac Toan est condamné à douze ans de prison par le tribunal populaire de Hanoi. Il est reconnu coupable d'espionnage pour avoir envoyé des informations par courrier électronique à des organisations de défense des droits de l'homme en exil jugées "réactionnaires" par le gouvernement vietnamien. C'est pour les autorités une violation de l'article 80 du code pénal. Les droits de Nguyen Khac Toan sont bafoués de bout en bout de la procédure. En total manquement à l'article 131 de la Constitution vietnamienne qui statue clairement sur la tenue d'un procès public, tout accès au tribunal est interdit, y compris aux membres de sa famille. L'audience ne dure que quelques heures. Le dissident ne peut rencontrer son avocat que deux fois, quelques jours avant la tenue de son procès, et n'a jamais pu s'entretenir avec lui en privé. Ancien officier de l'armée, Nguyen Khac Toan a été arrêté le 8 janvier 2002 dans un café Internet de Hanoi. Il est désormais détenu dans la prison B14, non loin de la capitale.

Le 17 mars 2003, la police vietnamienne arrête le Docteur Nguyen Dan Que, responsable de la publication clandestine *Tuong Lai* (L'Avenir) et auteur de nombreux articles publiés sur Internet. Quelques heures plus tard, la police revient à son domicile pour y saisir son ordinateur, son téléphone portable et de nombreux documents personnels. Son arrestation serait liée à la publication d'un communiqué sur Internet, dans lequel il dénonçait le manque de liberté de la presse dans son pays. Il réagissait ainsi aux propos de la porte-parole du ministère vietnamien des Affaires étrangères qui avait affirmé, le 12 mars, que la liberté d'information était garantie dans le pays. Nguyen Dan Que, qui a déjà passé près de vingt ans en prison, est détenu dans la maison d'arrêt municipale d'Hô Chi Minh-Ville. Diplômé de médecine à l'université de Saïgon, il avait été arrêté en 1978 et détenu pendant dix ans sans jugement. Relâché en 1988, il avait été une nouvelle fois arrêté en 1990 pour sa défense des libertés publiques, et condamné à vingt ans de travaux forcés et cinq ans d'emprisonnement. En 1998, une amnistie lui avait permis de recouvrer sa liberté. Cependant, il était toujours soumis à de fréquentes séances d'interrogatoires et à des fouilles répétées de son domicile, ainsi qu'à des campagnes de diffamation, orchestrées par le Département de la sécurité de Hô Chi Minh-Ville.

LIENS :

- Le ministère des Postes et télécommunications
www.vnpt.com.vn
- Informations d'Amnesty International sur le Viêt-nam
web.amnesty.org/library/eng-vnm/index
- Site d'informations officiel
www.vnn.vn
- *Radio Free Asia*
www.rfa.org/service/index.html?service=vie

Zimbabwe

POPULATION : 12 852 000

INTERNAUTES : 500 000

FOURNISSEURS D'ACCÈS PRIVÉS : OUI



Membre du peloton de tête des pays africains les plus connectés à Internet, le Zimbabwe s'est doté dès l'an 2000 d'une loi lui permettant de contrôler les courriers électroniques. La guerre ouverte entre le président Robert Mugabe et les médias indépendants et étrangers a débouché, en 2002, sur le vote d'une loi sur l'Accès à l'information et la protection de la vie privée, particulièrement dangereuse pour la liberté d'expression. Pour preuve, le procès intenté à un journaliste qui a diffusé un article "répréhensible" sur le site du journal britannique *The Guardian*.

Si de plus en plus de Zimbabwewéens se connectent à la Toile, notamment dans les dizaines de cybercafés ouverts dans la capitale, Harare, et dans les grandes villes du pays, ils n'auront peut-être bientôt plus le loisir de surfer sur des sites critiques à l'égard du pouvoir exercé sans partage par le président, Robert Mugabe.

En novembre 2000, le gouvernement a fait promulguer le "Posts and Telecommunications Act" qui régit les activités en ligne dans le pays. En vertu de ce texte, les services de sécurité peuvent contrôler les communications téléphoniques ainsi que les e-mails. La loi prévoit même l'étroite collaboration des fournisseurs d'accès et des opérateurs, membres de la Computer Society of Zimbabwe. Ces derniers ne peuvent refuser de donner les informations qui leur sont demandées ou de garantir l'accès à leurs serveurs aux officiers de police ou de renseignements.

L'année 2001 et le début de l'année 2002 ont été synonymes d'escalade vertigineuse en matière de censure et d'intimidation des journalistes et médias qui osent critiquer le président Mugabe. De nombreuses arrestations de reporters de la presse indépendante ou expulsions de correspondants de la presse internationale ont été au menu de cette campagne de tentative de mise au pas des médias.

Fin 2001 et courant 2002, le pouvoir a fait interdire la plupart des publications étrangères, britanniques notamment. Indisponibles dans le pays, leurs articles peuvent néanmoins être lus sur leurs sites Internet. C'est l'argument avancé en juin 2002 par les autorités pour traduire en justice le journaliste Andrew Meldrum, correspondant au Zimbabwe des journaux britanniques *The Guardian* et *The Economist*, et de *Radio France Internationale (RFI)*.

C'est la première fois qu'un journaliste est jugé en vertu de la nouvelle loi sur l'Accès à l'information et la protection de la vie privée. Andrew Meldrum est accusé "d'abus de privilèges journalistiques pour avoir publié des fausses informations".

Le reporter avait repris dans *The Guardian* une information publiée par le quotidien zimbabwéen *The Daily News* qui faisait état de la décapitation d'une femme par des militants de la ZANU-PF (Union nationale africaine du Zimbabwe - au pouvoir), dans un village du nord-ouest du pays. Quelques jours plus tard, *The Daily News* avait reconnu que cette information n'était pas authentifiée et avait publié ses excuses pour le préjudice subi par la ZANU-PF. Le 30 avril, Lloyd Mudiwa et Collin Chiwanza, journalistes du *Daily News*, avaient été arrêtés. Le lendemain, c'était au tour d'Andrew Meldrum de l'être.

Dans la mesure où *The Guardian* est interdit de diffusion dans le pays, les autorités reprochaient au titre d'avoir diffusé l'article en ligne sur son site, consultable par les Zimbabwéens.

Le 15 juillet, Andrew Meldrum a été reconnu non coupable des charges de "publication de fausses informations" et "d'abus de ses privilèges journalistiques" et acquitté par le tribunal d'Harare présidé par le juge Godfrey Macheyo.

LIENS :

• The Computer Society of Zimbabwe
www.csz.org.zw

• Site du quotidien *Daily News*
www.dailynews.co.zw

Les Nations unies contre la liberté d'expression

Par CLAUDE MOISY

Peut-on soupçonner l'Organisation des Nations unies, dépositaire de la Déclaration universelle des droits de l'homme, de prêter la main à un mauvais coup contre la liberté d'expression et la libre circulation de l'information ? La question se pose à propos du Sommet mondial pour la société de l'information, organisé à Genève en décembre 2003, et dont le but originel est de réduire le "fossé numérique" entre pays riches et pays pauvres.

Depuis deux ans, les travaux préparatoires de ce sommet ont vu émerger, de la part de nombreux États répressifs en matière de liberté d'expression, une tendance à en profiter pour soumettre Internet à des réglementations qui leur permettraient de faire obstacle à la libre circulation de l'information. Certaines de leurs propositions redonnent vie au défunt projet de "Nouvel ordre mondial de l'information et de la communication" (Nomic) qui a failli faire exploser l'Unesco, il y a une vingtaine d'années. On caricature à peine en disant que la philosophie sous-jacente à l'approche dirigiste en train de se manifester est que la liberté de l'information est moins un droit individuel qu'un droit collectif des peuples, ne pouvant être mieux exercé que par leurs gouvernements.

Le grand danger aujourd'hui, c'est que les conditions anarchiques dans lesquelles s'est répandu Internet fournissent aux États des prétextes parfois légitimes pour s'efforcer d'y mettre un peu d'ordre. Pour les uns, il s'agit de prévenir l'utilisation des réseaux par le terrorisme, la grande criminalité, le blanchiment d'argent ou la pédophilie. D'autres veulent que la propriété industrielle ou intellectuelle ne soit pas vidée de son sens par la liberté des échanges que permettent les nouvelles technologies. Pour d'autres encore, il s'agit d'empêcher que le développement des réseaux n'accroisse davantage l'hégémonie d'une langue et d'une culture. Les États de droit sont peut-être susceptibles d'adopter des systèmes de surveillance d'Internet qui respectent les droits fondamentaux de la personne humaine et la libre circulation de l'information. Mais on sait malheureusement trop bien avec quelle constance les États autoritaires détournent des dispositions légitimes pour soumettre l'expression et l'information à leur contrôle exclusif. Les récents rapports annuels de Reporters sans frontières et d'autres organisations similaires montrent d'évidence que les régimes qui ont refusé l'indépendance des médias traditionnels ont été les premiers à s'efforcer d'empêcher le libre accès de leur peuple aux réseaux.

La Déclaration de principes et le Plan d'action devant être adoptés au Sommet de Genève ont fait l'objet, en conférences intergouvernementales préparatoires, de projets déjà avancés dans lesquels on trouve, en ce qui concerne la circulation de l'information, des notions alarmantes. On y demande par exemple la reconnaissance qu'Internet "peut être utilisé dans des buts qui sont incompatibles avec la stabilité et la sécurité internationales et peut affecter négativement l'intégrité de l'infrastructure des États ... ainsi que le fonctionnement de l'économie". Ce n'est peut-être pas complètement faux, mais cela peut justifier toutes les censures de la part de régimes paranoïaques. Comme du temps du Nomic, on parle de "rééquilibrage des flux d'information" et de "respect de la souveraineté nationale" dans la diffusion des informations. Tout aussi inquiétant est un paragraphe parlant de "nouvelles façons de penser les droits de l'homme ... les libertés fondamentales, le progrès économique et la justice sociale". Cela ressemble au vieux dada de la Chine qui revendique toujours dans le domaine des droits de l'homme le respect des "spécificités nationales". En d'autres termes, chaque gouvernement est libre de décider ce qui est bon pour son peuple.

Les médias nationaux et internationaux, surtout ceux qui diffusent sur Internet, ont toutes les raisons de se méfier d'une nouvelle notion qui se présente, elle aussi, comme un progrès dans la reconnaissance des droits de l'homme. C'est le "droit de communiquer" considéré comme un droit humain fondamental ne pouvant être limité aux entreprises de communication. À première vue, cela peut sembler aller dans le sens de la liberté d'expression jusqu'à ce qu'on en réalise toutes les implications. Les

médias violeraient un droit de l'homme s'ils refusaient à tout un chacun de s'exprimer librement dans leurs colonnes, sur leurs ondes ou sur leur site, même s'il n'y avait jamais été mis en cause. On connaît les problèmes techniques posés aux médias par le droit de réponse. La reconnaissance du "droit de communiquer" rendrait leur gestion impossible.

De nombreuses organisations de défense de la liberté de la presse, dont Reporters sans frontières, ont présenté aux organisateurs de la conférence de Genève une déclaration revendicative qu'elles sont déterminées à défendre jusqu'au bout. Elles posent comme principe que les nouvelles technologies fournissent des moyens de communication comme les autres qui ne nécessitent pas de législations spécifiques. Pour elles, les médias doivent bénéficier, sur Internet et sur les réseaux satellitaires internationaux, des mêmes droits et libertés que sur les moyens de communication traditionnels. Elles insistent pour que la déclaration de Genève réaffirme, en matière d'expression et d'information, la priorité absolue de l'article 19 de la Déclaration universelle des droits de l'homme qui doit s'appliquer intégralement aux techniques nouvelles comme aux anciennes. Plusieurs autres réunions préparatoires sont prévues avant décembre 2003. Mais les gouvernements les plus répressifs en matière d'information ont montré jusqu'ici qu'ils n'étaient pas ouverts au dialogue avec "la société civile", même si l'UNESCO, partie prenante au Sommet, s'est montrée sensible aux positions des organisations de défense de la liberté de la presse.

Ces organisations ont bien conscience que leurs préoccupations ne sont qu'un des nombreux aspects d'un sommet mondial dont le principal objet est de mettre les nouvelles technologies de l'information au service des peuples les plus en retard afin d'accroître leurs chances de se développer. Mais elles refusent que ce louable but soit exploité par les ennemis de la liberté de la presse pour faire légitimer par les Nations unies de nouvelles entraves à l'indépendance de l'information.

Les craintes des défenseurs de la liberté ne peuvent qu'être avivées par le spectacle que donne depuis quelque temps la Commission des droits de l'homme des Nations unies, dont sont membres plusieurs des régimes les plus répressifs de la planète, et qui refuse maintenant de condamner des pays comme la Chine ou Cuba. De surcroît, la seconde session du Sommet de la société de l'information est prévue pour 2005... en Tunisie, dont le chef de l'État est constamment classé par Reporters sans frontières parmi les "prédateurs de la liberté de la presse" et qui a déjà fait condamner et emprisonner des internautes.

CLAUDE MOISY

ADMINISTRATEUR DE REPORTERS SANS FRONTIÈRES

TABLE DES MATIÈRES

LA LIBRE CIRCULATION DES INFORMATIONS A UN PRIX	5
<u>Afghanistan</u>	9
<u>Afrique du Sud</u>	11
<u>Algérie</u>	13
<u>Allemagne</u>	15
<u>Arabie Saoudite</u>	17
<u>Australie</u>	19
<u>Azerbaïdjan</u>	21
<u>Bahreïn</u>	22
<u>Bangladesh</u>	23
<u>Belarus</u>	25
<u>Belgique</u>	26
<u>Birmanie</u>	27
<u>Burundi</u>	30
<u>Canada</u>	31
<u>Chine</u>	33
<u>Corée du Nord</u>	53
<u>Corée du Sud</u>	54
<u>Cuba</u>	57
<u>Danemark</u>	63
<u>Egypte</u>	64

<u>Emirats Arabes Unis</u>	<u>66</u>	<u>Nouvelle-Zélande</u>	<u>115</u>
<u>Espagne</u>	<u>68</u>	<u>Oman</u>	<u>118</u>
<u>Etats-Unis</u>	<u>69</u>	<u>Ouzbékistan</u>	<u>119</u>
<u>France</u>	<u>75</u>	<u>Pakistan</u>	<u>120</u>
<u>Inde</u>	<u>77</u>	<u>Philippines</u>	<u>124</u>
<u>Institutions européennes</u>	<u>82</u>	<u>Royaume-Uni</u>	<u>126</u>
<u>Irak</u>	<u>85</u>	<u>Russie</u>	<u>128</u>
<u>Iran</u>	<u>86</u>	<u>Singapour</u>	<u>130</u>
<u>Italie</u>	<u>90</u>	<u>Somalie</u>	<u>132</u>
<u>Japon</u>	<u>92</u>	<u>Sri Lanka</u>	<u>133</u>
<u>Jordanie</u>	<u>95</u>	<u>Suisse</u>	<u>135</u>
<u>Kazakhstan</u>	<u>97</u>	<u>Syrie</u>	<u>136</u>
<u>Kenya</u>	<u>99</u>	<u>Thaïlande</u>	<u>137</u>
<u>Koweït</u>	<u>100</u>	<u>Tunisie</u>	<u>138</u>
<u>Laos</u>	<u>101</u>	<u>Turkménistan</u>	<u>141</u>
<u>Liberia</u>	<u>103</u>	<u>Turquie</u>	<u>142</u>
<u>Malaisie</u>	<u>104</u>	<u>Ukraine</u>	<u>144</u>
<u>Maldives</u>	<u>108</u>	<u>Viêt-nam</u>	<u>147</u>
<u>Maroc</u>	<u>110</u>	<u>Zimbabwe</u>	<u>152</u>
<u>Mauritanie</u>	<u>111</u>	LES NATIONS UNIES CONTRE LA LIBERTÉ D'EXPRESSION ?	<u>155</u>
<u>Mozambique</u>	<u>112</u>		

REPORTERS SANS FRONTIÈRES

Secrétariat international

5, rue Geoffroy-Marie 75009 Paris, France

Tél. : 33 . 1 . 44 . 83 . 84 . 84

Fax : 33 . 1 . 45 . 23 . 11 . 51

Site internet :

www.rsf.org