Organisation des Nations Unies
pour l'éducation, la science et la culture

Politique et société de l'information

# Limitation et restriction de la circulation globale de l'information

Publications de l'UNESCO pour la Politique et la société de l'information

UNESCO

# Politique et société de l'information : Limitation et restriction de la circulation globale de l'information

Gus Hosein

Février 2004

Publié en 2004
par l'Organisation des Nations Unies
pour l'éducation, la science et la culture
7, place de Fontenoy, 75352 Paris 07 SP

Composé et imprimé dans les ateliers de l'UNESCO



*Printed in France*
CI-2004/WS/6 cld/d /15795

# Sommaire

# Introduction

Le Sommet mondial sur la société de l'information, en décembre 2003, a été l'occasion de prononcer de beaux discours, de proclamer des déclarations et de rechercher de nouvelles possibilités. La date choisie venait à point nommé, compte tenu de tous les événements qui, au cours des dernières années, ont profondément modifié cette « société de l'information » qui apparaissait en rêve à tant de personnes, pour en faire ces réalités perçues par les milliers de participants au sommet.

Nous avions rêvé d'une société où l'abondance de l'information stimulerait la création du savoir et le renforcement des capacités de l'individu. Les frontières n'auraient plus aucun sens, le multiculturalisme prospérerait, la communication serait source d'enrichissement et la vérité serait libre. Si je ne suis pas tout à fait certain que nous ayons effectivement créé une « société de l'information », cette « société de l'information » garde naturellement en héritage tous les défis, les possibilités et les risques de la « société réelle ». Quelle que soit l'infrastructure que nous mettrons en place, il sera quasi impossible d'échapper aux jeux politiques de ceux qui la créeront et des citoyens du monde qui y résideront.

Le présent rapport illustre les jeux politiques de la société de l'information en examinant les ressorts de la liberté d'expression et de la vie privée. Les points litigieux de la société de l'information s'articulent en effet pour la plupart autour de la vie privée et de la liberté d'expression. Tous les discours sur la technologie et la vie politique dont le « droit de communiquer », « la liberté de participer », « les incitations à la création », l'accès et « la fracture numérique » ont en effet trait à la vie privée et à la liberté d'expression.

Ce n'est qu'en comprenant les ressorts politiques de la surveillance et de la censure que nous saurons déchiffrer les systèmes politiques et la gouvernance dans le contexte socio-technologique qui est le nôtre. Si nous considérons que les infrastructures de l'information et de la communication sont des composantes clefs de notre existence et des intérêts juridiques, politiques, économiques et sociaux, nous pourrons peut-être remonter jusqu'aux sources de la surveillance, des conflits et des défis qui se posent à nous.

À de nombreux égards, vie privée et liberté de parole sont comme l'endroit et le revers de la médaille. L'antagonisme est possible, notamment lors de reportages médiatiques sur la vie privée de tel ou tel, ou encore dans les réglementations

sur la calomnie et la diffamation, qui restreignent quelque peu la liberté d'expression. Nous nous attacherons plutôt dans notre rapport à mettre en relief les associations positives entre ces droits. Nous analyserons ici l'interdépendance de ces droits et les restrictions qu'ils subissent. De la surveillance peut découler la censure, de même que la mise en œuvre de certaines formes de censure peut déboucher sur la surveillance.

Les gouvernements et autres institutions agissent sur le droit à la liberté d'expression au moyen d'un vaste arsenal de régulations, tout en limitant la liberté de parole et l'interactivité en intensifiant la surveillance. La technologie joue un rôle majeur dans ces stratégies et ces mécanismes. Il s'agit pour nous de démonter ces mécanismes afin de comprendre comment notre cécité juridique, technologique et économique nous pousse à refermer les portes de la société ouverte.

# I.

# La régulation de la circulation transfrontalière de l'information

On peut faire remonter le concept de « société de l'information » aux années soixante, au moment où l'arrivée des ordinateurs coïncidait avec le déclin des secteurs agricoles et industriels dans de nombreuses économies. De la montée en puissance du secteur des services est issu le changement social. C'est au cours de cette période que les technologies de l'information ont été développées, acceptées et utilisées dans notre vie de tous les jours. Ce concept signifie pour nous aujourd'hui que les technologies très perfectionnées de l'information et de la communication occupent désormais une place prépondérante dans notre existence.

La « société de l'information » est désormais indissociable des moyens de communication tels qu'Internet, la téléphonie mobile avancée et autres procédés de communication interactive. C'est grâce aux infrastructures qu'utilisent ces moyens de communication partout dans le monde, tels que fils, câbles, fibres de verre et de plastique, satellites et antennes, qu'est possible la circulation transfrontalière de l'information. Au moyen de protocoles divers, les particuliers peuvent désormais, sans aucune difficulté, communiquer entre eux par delà les frontières. Les prestataires permettent aux individus d'avoir accès au courrier électronique, aux news-groups, de participer à des forum de discussion, d'héberger des sites Web, et de rechercher et de collecter des informations sur Internet par les procédés *PUSH* ou *PULL* en puisant dans des ressources ouvertes, où qu'elles soient.

Il est arrivé un moment où nous avons laissé le discours sur la « société de l'information » prendre le pas sur les mécanismes qui nous permettent de nous adapter aux nouvelles technologies. À présent, dans les programmes politiques, il est sans cesse question de l'avènement, de l'arrivée de la société de l'information et de la façon dont nous devons développer, entretenir et vendre cette nouvelle société. On la présente comme un lieu à part, distinct du vieux monde. En réalité, il ne s'agit là que d'un outil de rhétorique. Le vieux monde n'a pas cessé d'être ; il est aux prises avec les nouvelles technologies.

Internet et autres moyens de communication perfectionnés mirent en cause le fonctionnement du commerce, le développement des technologies et la conception de la politique. On pouvait désormais se servir d'Internet comme d'un marché global, échanger des idées et coder des applications. On affirmait que les nouvelles orientations politiques devraient tenir compte de l'augmentation du volume de l'information et de la difficulté à en contenir la circulation. En d'autres termes,

le droit applicable était redéfini chaque jour, c'est peut-être même l'individu qui en fixait le cadre – lorsqu'un Allemand achète un livre dans une librairie américaine ou qu'un programmateur australien collabore avec un Canadien à la réalisation d'une application logicielle mise au point en Norvège.

La compétence du gouvernement, en termes de loi et de pouvoir, ne s'étend habituellement qu'aux services et aux serveurs situés à l'intérieur des frontières de l'Etat. En outre, les prestataires ne sont normalement régis que par le droit de l'Etat dans lequel ils se trouvent physiquement. Si ni les serveurs ni les individus concernés ne se trouvent à l'intérieur des frontières de l'État, le gouvernement ne saurait édicter de réglementations ni sur ces librairies ni sur les codes en cours de réalisation. C'est du moins ainsi que nous imaginions les choses. Cette conception classique de la compétence a été remplacée par des interprétations plus problématiques d'un point de vue juridique et technologique.

Dans certains pays, une source d'information est considérée comme relevant de la juridiction nationale dès lors que les ressortissants y ont accès, quel que soit le lieu géographique où se situe le serveur. Ainsi, en France et en Australie, comme en témoignent certaines décisions de justice, on estime que les sites Internet américains entrent dans l'aire de compétence des tribunaux, et qu'ils doivent donc respecter la législation française ou australienne. Ainsi, partout dans le monde, les prestataires se retrouvent dans des situations juridiques épineuses, où ils sont censés respecter la législation d'un certain nombre d'États en plus des lois de leur propre pays.

L'éclatement des bulles économiques et l'importance donnée à la sécurité de la planète ont fait naître une certaine forme de scepticisme à l'égard de la liberté d'Internet et du renforcement des capacités que porte en elle la société de l'information. C'est maintenant chose courante que de rejeter l'optimisme technologique qui caractérisait jusqu'alors LA SOCIÉTÉ DE L'INFORMATION. Les affirmations du genre « sur Internet nul ne sait qui vous êtes ni où vous êtes » ou « les gouvernements n'ont pas le pouvoir de réguler les réseaux globaux » sont aujourd'hui souvent jugées irréalistes. On affirme actuellement qu'il est possible de réguler la circulation des données comme s'il ne s'agissait que d'une activité comme les autres. La vérité se situe sans doute quelque part entre ces deux positions.

## Droit et société de l'information

Les activités transnationales créeent des conflits entre les législations nationales et le contexte international. Un gouvernement est généralement habilité à légiférer et à faire appliquer la loi au sein de sa sphère de compétence nationale, et c'est, après tout, son droit le plus souverain. Le « principe de souveraineté » se définit sommairement comme le pouvoir exclusif exercé par le gouvernement à l'intérieur de ses propres frontières et pratiquement nulle part ailleurs.[1]

1. Jonathan W Leeds. 1998. United States International Law Enforcement Cooperation: "A Case Study in Thailand. Journal of International Law and Practice 7" (1):1-14.

Dans certaines circonstances toutefois, des conflits se produisent, le droit souverain est sujet à débat. C'est ce qui survient lorsqu'en cas de surabondance d'activités en provenance de l'étranger, l'autorité souveraine n'est plus en mesure de faire appliquer ses lois. Il y a conflit également lorsque la capacité de légiférer est affaiblie parce que le pouvoir n'est plus certain de sa capacité à faire appliquer les lois en raison du contexte de réglementation.

Ces problèmes ne sont pas typiques de la seule société de l'information. Prenons l'exemple d'un pays qui adopterait une loi afin d'interdire le développement d'un médicament. On peut douter de l'efficacité de cette loi dès lors qu'un autre pays s'abstient de se doter d'une loi de même teneur. À moins que le premier pays ait les moyens de protéger l'ensemble de ses frontières pour interdire le médicament sur son territoire, il sera possible de se le procurer, en violation de l'esprit de la loi. Il en va de même dans le domaine de la protection de l'environnement : quelle que soit la sévérité des mesures imposées par un État pour lutter contre la pollution atmosphérique, cela ne sert à rien si les États limitrophes ne prennent pas de mesures similaires, à défaut de quoi un débordement ne manquera pas de se produire. Dans tous les cas, les réglementations ont un coût disproportionné par rapport à leur efficacité.

Les conflits de ce type sont exacerbés dès lors qu'il s'agit de la circulation des données sur les réseaux numériques, ainsi que les produits et services qui y sont associés. Les individus peuvent en effet agir à distance sans pénétrer sur le territoire de l'État. En de telles circonstances, les contrôles aux frontières sont encore plus complexes sur le plan technologique et nuisent aux intérêts d'un grand nombre de pays, d'organisations non gouvernementales et d'industries.

Prenons la cryptographie, l'un des premiers problèmes sur lesquels ont achoppé les politiques gouvernementales. Bien que désireux de réglementer l'utilisation de certaines applications logicielles, dans les Etats démocratiques ouverts, les gouvernements n'ont pratiquement aucun moyen d'empêcher les individus de télécharger ces applications depuis un autre pays. Parmi les autres problèmes relatifs à la société de l'information et au commerce électronique, citons les impératifs liés au développement de nouveaux réseaux de communication et à la réduction des coûts d'accès, les obstacles à la bonne marche du commerce, au détriment des économies nationales, et enfin les conséquences sur les libertés civiles. À terme, les réglementations ont pour la plupart donné la preuve de leur inefficacité.

Les gouvernements ont depuis tiré les enseignements de ces échecs : la circulation transfrontalière de l'information représente un danger évident pour l'application de la politique nationale ; elle ne respecte pas les aires de compétence.

## Internet souverain

On pourrait envisager la situation autrement, en imaginant qu'Internet forme une aire de compétence à part entière et qu'il soit considéré comme tel. Conformément à la conception classique des notions de souveraineté et de compétence, les gouvernements s'appuient sur leurs frontières pour donner force à leur pouvoir, faire

appliquer leurs règles, donner une légitimité à leur action et s'adresser à leurs administrés. Citons un célèbre article signé par deux juristes spécialistes du droit et d'Internet, Johnson et Post,

> Le développement d'un réseau global d'ordinateurs est sur le point de briser les liens entre le lieu géographique et : (1) le pouvoir qu'ont les gouvernements nationaux d'exercer leur contrôle sur le comportement en ligne; (2) les effets du comportement en ligne sur les personnes ou les choses ; (3) la légimité des efforts d'un dirigeant local visant à appliquer ses règles à des phénomènes globaux ; et enfin (4) le fait que les règles applicables dépendent d'un lieu géographique.[2]

Internet et son « cyberespace » posent effectivement un défi à la souveraineté du gouvernement. Internet et la circulation transfrontalière de l'information produisent un effet de débordement en raison de la possibilité d'action à distance. En outre, poursuit-on, l'architecture d'Internet a créé un environnement qui résiste à l'action du gouvernement. Au moment même où les gouvernements s'efforçaient d'édicter des règles au niveau national, sur la cryptographie par exemple, Johnson et Post donnaient le conseil suivant :

> On pourrait résoudre la plupart des problèmes de droit et de fonds soulevés par la communication électronique transfrontalière au moyen d'un principe simple: il suffirait de considérer pour les besoins de l'analyse juridique que le « cyberespace» est un « lieu » à part, en reconnaissant l'existence d'une frontière juridiquement valide entre le cyberespace et le « monde réel » .

Ce n'est pas tant l'inutilité des actions et des politiques nationales qui est à craindre, mais leur caractère dangereux dans le contexte socio-technologique qui est le nôtre. Il est peut-être absurde de vouloir imposer une réglementation limitée par des frontières géographiques à un environnement dépourvu de frontières. Il faut surtout retenir que les réglementations nationales débordent du cadre des frontières en raison même de l'absence de frontières du cyberespace.

Plus simplement, imaginons que les États -Unis décident de réglementer une forme d'expression donnée ; Internet étant américain pour une très large part, cette décision aurait pour effet de réglementer cette forme d'expression dans d'autres pays du monde. Autre exemple, celui des tribunaux français qui mirent en cause Yahoo! pour avoir autorisé la vente aux enchères d'emblèmes nazis.[3] Yahoo ! fut enjoint d'empêcher les Français d'avoir accès aux sections de son site Web où étaient mis en vente des objets nazis. Toutefois, l'identification des internautes « français » pose des problèmes non négligeables. Yahoo ! a fini par interdire l'accès à ce site de vente aux enchères aux internautes du monde entier. Dans le premier cas, la règle américaine aurait eu des conséquences de fait dans le reste du monde; dans le second, la décision française déborde du cadre national et influence les autres États.

2. David R. Johnson et David G. Post, "Law and Borders--the Rise of Law in Cyberspace," Stanford Law Review (1996).
3. Pour une bonne synthèse de l'affaire, se reporter à Yaman Akdeniz, "Case Analysis of League against Racism and Antisemitism (Licra), French Union of Jewish Students, v. Yahoo! Inc. (USA), Yahoo France, Tribunal De Grande Instance De Paris, Interim Court Order, 20 November 2000.," Electronic Business Law Reports 1, no. 3 (2001).

## Internet n'est pas un cas à part

Pour aborder la question sous un angle différent, il conviendrait de considérer la « société de l'information », le « cyberespace » et Internet comme n'importe quelle autre forme d'activité transnationale. Les transactions dans le cyberespace ne sont pas si différentes d'autres types de transactions transnationales : les personnes concernées font partie de « l'espace réel » et sont réparties dans divers pays, les actions réalisées et les effets obtenus relèvent eux aussi du « monde réel ».

En ce sens, les transactions dans le cyberespace ne méritent aucune attention particulière de la part des législateurs nationaux.[4] Les choix politiques d'un pays auront toujours des conséquences sur les autres pays. Internet n'a rien inventé. Depuis que les technologies des transports et des communications ont commencé à évoluer, au cours de la première moitié du XX$^{e}$ siècle, l'activité multijuridictionnelle est devenue fréquente.

Au même moment, l'État régulateur s'est imposé et, nonobstant certaines difficultés liées à l'arbitrage juridictionnel, les conflits de compétence sont désormais bien compris. Même dans les cas où plusieurs juridictions sont saisies, les tribunaux appliquent un droit coutumier universel, qui ne dépend pas d'un pouvoir souverain en particulier, tel que le droit commercial coutumier, le droit de la mer ou le droit international public.[5]

Le droit international autorise dorénavant les États à appliquer leurs lois à une conduite extra-territoriale produisant des effets patents sur leur territoire. Selon le plus grand spécialiste juridique de cette question,

À l'époque actuelle, une transaction peut à bon droit être réglementée par la juridiction du lieu où la transaction est réalisée, par les juridictions des lieux où la transaction produit des effets patents ou encore par les juridictions des lieux d'où sont originaires les parties soumises aux réglementations.[6]

En réalité, les pays ont su réglementer la circulation de l'information. La directive publiée en 1995 par l'Union européenne pour harmoniser les pratiques en matière de protection des données contient deux articles qui réglementent la circulation transfrontalière de l'information.[7] Des pays aussi différents que l'Australie, la Chine et l'Arabie Saoudite appliquent diverses formes de censure afin de contrôler la nature des informations envoyées ou reçues, bien que l'on prétende que cela est impossible ou que la marge d'erreur est trop importante.

4. Jack. L Goldsmith, "Against Cyberanarchy," *University of Chicago Law Review* 65 (1998).
5. Jack. L Goldsmith, "Symposium on the Internet and Legal Theory: Regulation of the Internet: Three Persistent Fallacies," *Chicago-Kent Law Review* 73 (1998)."
6. Goldsmith, "Against Cyberanarchy."
7. Union européenne, "Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données " .

D'une certaine façon, toutes les nouvelles technologies bousculent les systèmes juridiques.

Ainsi le télégraphe a accru la rapidité et le volume des communications dans des proportions considérables, le temps de communication ne se comptant plus en mois et en semaines mais en heures et en minutes. De même, grâce au téléphone, les communications internationales sont devenues moins coûteuses et plus fréquentes tandis que leur confidentialité était améliorée.[8] À l'instar d'autres infrastructures du passé, Internet bouscule lui aussi les pratiques, mais d'une façon plus étonnante.

## Internet, un problème à part

Prétendre que rien n'a changé revient à faire preuve de cécité devant les transformations, les problèmes et les possibilités liés spécifiquement à l'expansion et à l'adoption de la société de l'information. Les gouvernements affirment souvent qu'ils se contentent de mettre leurs lois « à jour » afin de mieux les adapter à l'évolution du contexte technologique ; en présentant les grands changements politiques comme un fait naturel et non controversé, ils espèrent ainsi minimiser le débat.

Les conflits transfrontaliers ont souvent pu être résolus au moyen de l'harmonisation des législations. S'agissant d'Internet, un certain nombre d'initiatives en matière de mises à jour, de résolution des conflits et de disparités entre systèmes juridiques ont été prises par les Nations Unies, le Conseil de l'Europe, l'Organisation pour la sécurité et la coopération en Europe ainsi que le Groupe des huit pays les plus industrialisés. Plus récemment, le Sommet mondial sur la société de l'information peut être considéré comme un forum d'échanges sur les moyens de régir de façon efficace toute conduite économique, sociale ou criminelle transfrontalière.

Dans le contexte actuel des réseaux, il est impossible de considérer la circulation des données comme par le passé sans se heurter à des difficultés. On aura beau prétendre que les nouvelles et les anciennes technologies ne sont pas si différentes les unes des autres, des défis inédits se posent. Les nouvelles technologies exigent peut-être de nouveaux mécanismes juridiques qui seront peut-être en conflit avec les normes juridiques internationales. Enfin, il subsistera toujours des disparités entre les divers systèmes de gouvernement et, quel que soit le degré d'harmonisation, les droits de la personne ne seront jamais parfaitement protégés.

Revenons à notre discussion sur la « société de l'information » et les orientations politiques. La première façon d'envisager Internet et le pouvoir souverain révèle les risques de débordement des réglementations nationales. La seconde révèle les risques auxquels on s'expose à considérer Internet comme quelque chose de radicalement différent des autres types d'action transnationale. Quel est le rôle du gouvernement dans la « société de l'information » ? C'est ici que nous entrons dans l'univers de la politique en matière de technologie.

8. Goldsmith, "Against Cyberanarchy."

# II.

# La société de l'information et les défis de la réglementation

La « société de l'information » n'est guère qu'un outil de rhétorique, un instrument qui nous aide à comprendre et à distinguer ce qui est derrière nous de ce qui existe actuellement. Le « cyberespace » est lui aussi un outil de rhétorique. Ce que nous devons comprendre, c'est comment les structures juridiques et réglementaires et les pratiques du « monde réel » se trouvent modifiées par les technologies de l'information et de la communication, partie intégrante de cette « société de l'information ». Voilà, tout simplement, en quoi consistait le rêve d'une société nouvelle ; la réalité c'est que nous vivons dans des sociétés où coexistent les nouvelles technologies et tout un système de lois, de marchés, de pratiques et de normes.

Internet est un forum d'interactions et de communication, une multiplicité de protocoles de télécommunication et de technologies en constante évolution. Il constitue également un phénomène social, il n'y a qu'à considérer le nombre croissant d'internautes dans des pays toujours plus nombreux. C'est en même temps un marché interactif sur lequel sont effectuées toutes sortes de transactions électroniques, commerciales ou autres. C'est en outre la plus grande bibliothèque, le meilleur outil d'apprentissage et de communication... et le plus vaste réceptacle de pornographie et d'informations *obscènes et préjudiciables* jamais créé. Internet est un élément clef de notre vie quotidienne.

La société de l'information est-elle distincte de ce que nous avions connu jusqu'à présent ? À la fois oui, absolument, et non. Internet et les activités transnationales qui en découlent sont-ils différents du télégraphe et du téléphone ? Oui, bien qu'à de nombreux égards Internet soit moins spectaculaire. Enfin, les formes et les fonctions des gouvernements ont-elles été modifiées par les réseaux globaux de communication ? La réponse est oui, radicalement.

Les technologies modernes de l'information et de la communication posent certains défis aux gouvernements tout en leur offrant des possibilités. Nous avons déjà montré comment les questions de compétence compliquaient la tâche des gouvernements en matière de réglementation et que les réglementations nationales n'étaient pas sans poser problème – ces problèmes n'étant pas uniquement liés à l'aspect transnational, cependant. Il est tout aussi difficile de déterminer comment les infrastructures de la communication, comme Internet, peuvent être intégrées à un système de réglementation. Pour faire simple, devons-nous

considérer Internet à l'égal du téléphone, de la télévision, de la radio ou de la presse écrite ?

Les internautes sont-ils des télédiffuseurs en puissance ou simplement des individus utilisant des connexions point à point ? La réponse à cette question aura des répercussions sur la façon dont sont perçues les entités qui fournissent des services de communication par Internet.

Si les fournisseurs de services sur Internet sont soumis aux mêmes règles que les porteuses, à l'image des opérateurs téléphoniques, cela les déchargera d'une part de leurs responsabilités en matière de contrôle des contenus mais ils devront alors se plier à l'arsenal de réglementations sur les télécommunications. Si l'on conçoit Internet comme un moyen de diffusion tel que la télévision ou la radio, alors les fournisseurs de services sur Internet seront responsables du contenu des informations qui transitent par leurs réseaux. En fonction de leur modèle d'entreprise, les fournisseurs de services sur Internet assument parfois cette responsabilité par le biais des services proposés ; en règle générale cependant, c'est la loi qui fixe leurs responsabilités.

Toute réforme législative visant à réglementer Internet revient à déterminer ce qu'est Internet, un moyen de diffusion, un moyen de communication neutre du point de vue du contenu ou une porteuse. La responsabilité des entreprises varie en fonction des choix des gouvernements en matière de réglementation. Ainsi, selon le droit algérien, les fournisseurs de services sur Internet sont obligatoirement responsables du contenu des sites qu'ils hébergent ; selon le droit suisse, les prestataires ne sont responsables que si l'auteur ne peut être identifié ; en Hongrie, les fournisseurs d'espace gratuit sur Internet ne sont pas responsables des contenus sauf s'ils ont connaissance du caractère délictueux des sites qu'ils hébergent et qu'ils ne prennent aucune mesure pour y remédier ; au Royaume-Uni, le courant actuel de la pensée juridique veut que les fournisseurs de services sur Internet soient considérés comme des « éditeurs secondaires », comme les librairies ou les archives, plutôt que comme des porteuses.

## Définir Internet pour les besoins de la censure

Les gouvernements réglementent les secteurs de la diffusion. Rien de plus naturel, donc, que d'essayer d'appliquer ces règles à Internet.

Le cas de l'Australie illustre bien les problèmes qui se posent. Examinons ainsi la déclaration du vice-président de l'Australian Broadcasting Authority, partisan d'une réglementation par le gouvernement:

> Le secteur de la diffusion et, aujourd'hui, Internet, utilisent les biens publics, les ondes et les bandes passantes. La diffusion est un moyen de communication de masse qui se caractérise par un pouvoir d'intrusion considérable qu'Internet est clairement sur le point d'acquérir. (...)

> Il est indispensable que lorsqu'ils réviseront les règles actuelles et en élaboreront de nouvelles pour le secteur de la diffusion et Internet, les décideurs politiques et les législateurs réaffirment la cause de l'intérêt public qui, selon eux, devrait s'appliquer à ces secteurs d'activité et à leur système de gouvernance.[9]

Pour ce partisan de la réglementation, Internet est un « moyen de communication de masse » et en tant que tel, à l'instar de la télévision, il tombe sous le coup de l'autorité régulatrice de l'ABA. L'ABA, elle, agit selon ses propres lignes directrices pour contrôler les programmes au nom de l'intérêt public.

Cependant, Internet et la télévision sont deux choses bien distinctes. À cela, Roger Clarker, en désaccord avec la politique gouvernementale visant à censurer les contenus nationaux et à rendre les contenus internationaux inaccessibles, réplique:

> Ce qu'il y a de pitoyable dans cette déclaration, dans la politique du gouvernement et dans la législation adoptée par le sénat, favorable à l'opposition, et par la chambre des représentants, favorable au gouvernement, c'est qu'elles se distinguent par une ignorance aberrante de la nature de la technologie et donc de la conduite qu'elles prétendent régir. Non seulement les bénéficiaires visés n'en tireront aucun avantage mais tous ceux qui sont concernés auront à en pâtir.[10]

Son point de vue est partagé par de nombreuses personnes, dont beaucoup ne sont pas favorables à la censure. La communauté australienne des pirates informatiques[11] a fait connaître des positions analogues et donne des conseils aux internautes pour esquiver les contrôles grâce à des trouvailles technologiques telles que le cryptage, les connexions point à point, les connexions par proxy, etc.

Les partisans de la censure proposent souvent des innovations technologiques de leur cru. Tôt dans le débat politique, il a ainsi été suggéré d'appliquer à Internet des systèmes de classification des contenus comparables à ceux de la télévision ou du cinéma. Ce qui reviendrait à évaluer les dossiers et les sites Web en fonction de leur contenu. En réplique, l'American Civil Liberties Union a publié un rapport contre l'opinion de l'industrie du cinéma et de la télévision sur Internet : en raison même de la *culture, de l'économie et de la structure d'Internet,* tout système de classification se révèlerait inapplicable, notamment à cause des choix internationaux et parce que cela risquerait de faire supporter aux petites entreprises des charges trop lourdes.[12]

---

9. Australian Broadcasting Authority. 1999. "Broadcasting, co-regulation and the public good", NR 101/1999, 29 octobre 1999.
10. Roger Clarke, "Subject: Aba Demonstrates Its Ignorance to the World," *Forwarded to the Politech Mailing List, message titled FC: More on Australian official demanding Net-regulation -- demonstrating ignorance to the world,* 3 novembre 10:42:30 -0800 1999.
11. Dogcow, "Evading the Broadcasting Services Amendment (Online Services) Act 1999," (2600 Australia, 1999).
12. ACLU, "Fahrenheit 451.2: Is Cyberspace Burning? How Rating and Blocking Proposals May Torch Free Speech on the Internet," (American Civil Liberties Union, 1997).

Dans le monde entier les partisans de la censure ont imaginé d'autres innovations technologiques, telles que des mécanismes de filtrage pour utilisateurs afin de bloquer l'accès aux « sites obscènes ». On n'est pas très loin de la décision américaine d'équiper tous les postes de télévision des 'puces anti-violence' (V-Chips) pour bloquer les programmes jugés indécents par les entreprises de télédiffusion. À cela près qu'il est beaucoup plus complexe de filtrer Internet. Nombre de rapports publiés par des universitaires et des organisations non-gouvernementales mettent en cause la capacité des systèmes de filtrage et montrent qu'en raison de la *nature d'Internet,* de son mode de distribution et de la difficulté d'instaurer un système de vérification automatisé efficace, les filtres bloquent également des contenus « qui n'ont rien d'obscène ». Sans compter que certains documents à caractère obscène passent au travers des mailles des filtres. Selon certains rapports, ces filtres manquent d'*objectivité,* dans la mesure où ils interdisent l'accès aux sites Web que leurs auteurs jugent contraires à leurs intérêts, comme les sites des organisations pour la protection de la liberté d'expression.[13]

Le tout premier procès sur la réglementation du contenu d'Internet aux Etats-Unis a permis de soulever quelques points intéressants. Dans les années 1990, le Congrès américain adoptait une loi rendant obligatoire la vérification de l'âge sur les sites Web à caractère « obscène ». À l'issue du procès *ACLU V. Reno,* la Communications Decency Act fut invalidée par les tribunaux, l'argument invoqué étant qu'il était trop difficile de définir ce qui constitue une information à caractère « obscène », et que toute restriction d'accès fondée sur l'âge de la majorité sexuelle serait à la fois difficile à mettre en place d'un point de vue technologique et onéreux. Le tribunal a ainsi indiqué que « toute réglementation d'Internet visant les contenus, l'intention fût-elle louable, risquait de mettre le feu au village global simplement pour faire rôtir un cochon », et ce « en raison de la nature d'Internet » et de la Constitution américaine.[14] Le tribunal reconnut qu'Internet différait de toutes les infrastructures de communication mises en place jusqu'alors et qu'il pouvait aider les individus à renforcer leurs capacités, en ajoutant que tout processus de réglementation devait faire preuve de la plus grande prudence. Ce qui n'était pas le cas de la CDA.

À l'instar du Congrès américain, de nombreux pays ont adopté leurs propres lois pour réglementer le contenu d'Internet. Parmi les stratégies et les mécanismes de réglementation, notons les initiatives sur la responsabilité des fournisseurs de services sur Internet ; l'obligation d'instaurer des autorisations pour les documents jugés obscènes; et la recommandation aux consommateurs d'utiliser des logiciels de filtrage. Toutefois, les erreurs et les dangers mis en évidence dès le début du débat sur la censure aux Etats-Unis restent d'actualité, ce qui n'a pas empêché les organisations gouvernementales internationales de préconiser des révisions législatives afin d'interdire la publication de documents obscènes ou préjudiciables.

13. Electronic Privacy Information Center, "Faulty Filters: How Content Filters Block Access to Kid-Friendly Information on the Internet," (1997).
14. "ACLU v. Reno" Court for the Eastern District of Pennsylvania, Etats-Unis, 1996.

## Définir Internet pour les besoins de la surveillance

Les gouvernements ont coutume d'élaborer des règles pour surveiller les communications. À partir des techniques d'interception du courrier, du télégraphe et de la télégraphie sans fil, au XX$^{e}$ siècle des lois autorisant l'interception des communications téléphoniques ont été adoptées. Aujourd'hui, les 'mises à jour' ont le plus souvent pour but d'étendre à Internet ces lois sur la surveillance des communications. Les gouvernements cherchent donc tout simplement à réglementer Internet comme s'il s'agissait d'un opérateur téléphonique.

En 2000, le Royaume-Uni a ainsi adopté la Regulation of Investigatory Powers Act, qui autorise l'État à intercepter les communications qui transitent par Internet. Au moment où la loi était adoptée, le gouvernement affirmait que ces nouvelles prérogatives n'avaient rien de nouveau : la loi s'applique à tous les prestataires de services dans le domaine des communications, de sorte que « ce sont les mêmes règles qui doivent être appliquées à l'ensemble du secteur, la loi ne faisant qu'incorporer le principe obligeant les prestataires à mettre en place un dispositif d'interception adapté »[15]. C'est donc dans un souci d'harmonisation des réglementations au sein du secteur des communications que les fournisseurs de services sur Internet sont régis comme de simples opérateurs téléphoniques.

À l'heure actuelle, les États-Unis imposent à tous les opérateurs téléphoniques de se munir d'une capacité de surveillance, bien que cette mesure n'ait pas encore été étendue aux fournisseurs de services sur Internet. Au moment où nous rédigeons ce rapport, des initiatives étaient lancées pour que la législation américaine sur l'obligation de se munir de dispositifs d'interception soit étendue au téléphone par Internet (VoIP–voix sur IP).

D'autres initiatives similaires ont déjà été prises par le gouvernement américain. En 1999, le département de la justice faisait appel à l'Internet Engineering Task Force (IETF) pour mettre au point un protocole permettant l'écoute des communications sur Internet. La « voix » de l'IETF est démocratique dans la mesure où chacun de ses adhérents a un droit de vote et où l'adhésion est ouverte à tous. Au terme d'un long débat, l'IETF s'est prononcé contre l'élaboration d'un tel protocole. Certains de ses membres, d'un avis contraire, affirmèrent que l'IETF pouvait (et devait) élaborer un protocole d'écoute *déterministe* qui puisse être utilisé dans le monde entier – au sens où, sur le plan technologique, un tel système rendrait nécessaire l'utilisation d'un système de garantie hautement sécurisé sur le plan technologique. D'aucuns estimèrent qu'on était passé à côté d'une occasion. Selon Stewart Baker, ancien *general counsel* de la NSA,

15. Chambre des Communes. 2000. "Second Reading of the Regulation of Investigatory Powers Bill", Jack Straw, Home Secretary. 6 mars 2000.

> Lorsque l'IETF (...) refusa de s'attaquer à ce problème, sa décision fut saluée comme une victoire pour les libertés civiles. En réalité, en raison de ce refus, il est probable que les systèmes d'écoute seront élaborés à l'issue de consultations discrètes avec le FBI, ce qui est plutôt ironique. Conclusion : dans les dix années qui viennent, l'idée qu'en raison de sa nature Internet oppose une résistance aux contrôles gouvernementaux pourrait être fort malmenée.[16]

Le débat a donc quitté la scène publique au moment même où l'on élaborait des techniques nouvelles. Les États-Unis ont ainsi déployé Carnivore, aujourd'hui rebaptisé DCS 1000, système informatique lié au réseau des fournisseurs de services sur Internet et capable d'enregistrer le trafic.

Considérer Internet comme un opérateur téléphonique, c'est laisser la porte ouverte à la surveillance des 'données relatives au trafic'. À l'époque du bon vieux téléphone, au terme d'un long débat juridique, on a jugé que les communications étaient de nature confidentielle et que la violation de la confidentialité des communications exigeait une autorisation légale. Ces 'autorisations légales' sont habituellement des mandats, des ordres judiciaires aux États-Unis ou encore des autorisations délivrées par les autorités politiques au Royaume-Uni.

Cette règle ne s'applique toutefois pas aux données relatives au trafic, qui comprennent les numéros appelés, les numéros d'appel et l'heure de l'appel. On jugea que la collecte et la divulgation des données relatives au trafic constituait une violation moins grave de la confidentialité et qu'en conséquence les garanties légales nécessaires étaient moins importantes. Conservées par les opérateurs téléphoniques, les données relatives au trafic peuvent être mises à la disposition des forces de l'ordre. Les conversations téléphoniques n'étant, elles, pas conservées par les opérateurs téléphoniques, en règle générale du moins, les contraintes légales pesant sur ces opérateurs s'en trouvent allégées ; les données relatives au trafic, moins délicates d'un point de vue juridique, sont ainsi accessibles aux gouvernements.

En classant Internet dans la même catégorie que les opérateurs téléphoniques, les gouvernements se sont donné les moyens d'accéder aux données relatives au trafic sur Internet, recueillies auprès des prestataires. Appliqué à Internet, toutefois, le terme juridique de « données relatives au trafic » prend un sens radicalement différent et désigne d'autres types d'information : toutes les adresses auxquelles les utilisateurs envoient des courriers électroniques, tous les serveurs auxquels ils se connectent, toutes les personnes avec qui ils conversent dans les groupes de discussion, éventuellement les sites Web sur lesquels ils se rendent, les pages qu'ils consultent et leurs thèmes de recherches. Comme le note le Conseil de l'Europe :

16. Stewart Baker, "Re: Metaswitch Embeds Police Spy Features in New Net-Phone Switch," (Politech Mailing List, 2003).

> La collecte de ces données peut, dans certaines situations, permettre d'établir une description des intérêts de la personne concernée, des personnes qui lui sont associées et du cadre social dans lequel elle évolue. Les Parties devraient en tenir compte au moment d'instaurer les sauvegardes appropriées et les conditions juridiques préalables à l'application de ces mesures.[17]

Quoi qu'il en soit, la loi autorise généralement les gouvernements à accéder facilement aux « données relatives au trafic », nonobstant leur caractère confidentiel et quelque différentes qu'elles soient des données relatives au trafic conservées par les opérateurs téléphoniques.

Aux États-Unis, les gouvernements successifs ont adopté une approche plus complexe. Le gouvernement de Clinton a d'abord fait part de son intention d'étendre aux connexions Internet par câble les pouvoirs légaux d'interception en proposant « des amendements [qui] mettront à jour les lois désuètes, si explicites s'agissant du matériel qu'elles en acquièrent une neutralité technologique »[18]. Cette formulation « désuète » fait référence à la Cable Act de 1984, qui protège les données relatives au trafic des communications par câble et les habitudes télévisuelles des téléspectateurs plus encore que le contenu des communications. Si le gouvernement Clinton n'est pas parvenu à réviser la législation sur le traitement des données relatives au trafic issues des connexions à Internet par câble, l'équipe de Bush a réussi, elle, à faire adopter la USA-PATRIOT Act en octobre 2001. La USA-PATRIOT Act modifie la Cable Act de la façon suivante : que le prestataire soit un câblo-opérateur ou un opérateur téléphonique, les données relatives au trafic sont soumises au même régime et doivent être rendues accessibles aux forces de l'ordre – les données du trafic des réseaux câblés sont donc nettement moins protégées. Cette mesure fut annoncée en grandes pompes par le ministre de la justice.

> Les agents de renseignement auront pour instruction de tirer parti des nouvelles normes caractérisées par leur neutralité technologique. (...) Les enquêteurs auront pour instruction de poursuivre sans relâche les terroristes sur Internet. Grâce aux pouvoirs plus étendus que garantit la loi, il est permis d'utiliser des appareils capables d'extraire les adresses des expéditeurs et des destinataires des communications transitant par Internet. [19]

La loi ouvre l'accès à quantité d'informations qui vont bien au-delà des simples habitudes télévisuelles. Ces informations comprennent les adresses de courriers électroniques, les numéros de téléphone, les sites Web consultés, éventuellement les termes utilisés dans les recherches faites par l'utilisateur et les fichiers téléchargés. Or, la loi protège ces données critiques comme si elles ne revêtaient qu'une importance mineure.

17. Conseil de l'Europe, *"Rapport explicatif à la Convention à la cyber-criminalité",* ETS n°185 (Strasbourg: 2001).
18. John Podesta, "Speech by the White House Chief of Staff on Cybersecurity," (Washington, D.C.: National Press Club, 2000).
19. Senate Committee on the Judiciary, *Testimony of the Attorney General,* 25 septembre 2001.

Ainsi, définit-on Internet comme un moyen de diffusion lorsque cela arrange les gouvernements en matière de censure, et comme une infrastructure de communications téléphoniques quand cela permet aux gouvernements d'instaurer des contrôles ne nécessitant qu'une autorisation légale minimale. Aucune de ces définitions ne correspond ni à ce qu'est véritablement la technologie ni à l'intrusion que représente la surveillance.

# III.

# Action et implications de la censure

L'expression « Internet considère la censure comme un désagrément à contourner » a pu être vraie à un moment donné. La situation a aujourd'hui bien changé. Les Etats-nations risquent gros à vouloir étendre leur compétence à la circulation globale des données. Quoi qu'il en soit, les gouvernements édictent des lois pour restreindre la liberté d'expression et surveiller les personnes. De la même façon, il peut s'avérer dangereux de définir Internet comme une infrastructure de communication comme les autres. Les gouvernements continuent pourtant à le faire afin de réglementer la circulation de l'information et d'exercer plus facilement leur contrôle sur les personnes.[20]

La censure utilise un certain nombre de mécanismes, mis en place en divers points de contrôle de l'architecture d'Internet : l'expéditeur de la communication, le prestataire source, le prestataire cible et le destinataire de la communication ou utilisateur final.[21] Les mécanismes mis en œuvre pour contrôler ces divers points comprennent entre autres :

- Les règles qui déterminent directement ce qui peut être exprimé et ce à quoi on peut accéder ;
- l'obligation d'installer des systèmes de filtrage ou autres procédés technologiques pour bloquer la circulation de l'information ;
- des systèmes d'autorisation relatifs à l'expression, à la transmission et à la réception ;
- des systèmes de responsabilité pour les utilisateurs et les fournisseurs de services sur Internet à l'origine de la communication ;
- des règles sur la calomnie et la diffamation ;
- des régimes de protection du droit d'auteur et de la propriété intellectuelle.

Ces systèmes sont utilisés ensemble ou séparément, selon le cas.

20. Les lois adoptées dans le monde entier pour censurer l'information ou restreindre la liberté d'expression ont été analysées par divers observateurs. Le rapport qui fait le plus autorité en ce domaine est celui qu'ont publié GreenNet Educational Trust et Privacy International. Voir GreenNet Educational Trust and Privacy International, "Silenced: An International Report on Censorship and Control of the Internet," (London: 2003).
21. Jonathan Zittrain, "Internet Points of Control," *Boston College Law Review* 43, no. 1 (2003).

Grâce à ces divers moyens, on contrôle la circulation de l'information au nom de la bienséance, de la sécurité et de la morale. On peut ainsi équiper les fournisseurs de services sur Internet destinataires de systèmes de filtrage afin d'empêcher les usagers d'accéder à des informations jugées préjudiciables. Les personnes peuvent être contraintes d'utiliser les mécanismes de filtrage installés sur leurs ordinateurs, dans les cybercafés ou les bibliothèques. Ceux qui souhaitent s'exprimer risquent de tomber sous le coup des lois sur la calomnie qui obligent les internautes à s'identifier et les fournisseurs de services sur Internet à obtenir une licence. Un tel système de licences risque de rendre les prestataires responsables du contenu des informations qu'ils acheminent. Enfin, les fournisseurs de services sur Internet peuvent être contraints de supprimer des contenus et de révéler des informations sur les auteurs des contenus en cause. La plupart de ces pouvoirs, sinon tous, peuvent être exercés en vertu du droit sur la propriété intellectuelle.

## Qui décide, qui censure ?

Les obstacles qui entravent l'accès à Internet ne sont pas toujours directement le fait des gouvernements. Dans certains pays, en raison de coûts d'accès prohibitifs, seules les élites nationales peuvent utiliser Internet. Ailleurs, l'organisation du marché aggrave les problèmes ; ainsi, à Bahreïn, en Birmanie, au Bélarus, en Tunisie et au Libéria, des quasi-monopoles d'État ont pour double fonction de limiter l'accès au marché tout en veillant à ce que le gouvernement puisse exercer sa surveillance. La libre concurrence ne résout cependant pas tout. Au Bangladesh, le gouvernement a coupé les lignes de soixante prestataires sous prétexte qu'ils n'avaient pas renouvelé leurs licences ; les prestataires prétendent, eux, que cette mesure visait uniquement à les empêcher d'intervenir sur le marché de la téléphonie par Internet afin de protéger le monopole de l'État dans le domaine des télécommunications vocales.

À l'époque où le téléphone était affaire de monopole d'État et d'entreprises publiques, les instances de régulation étaient peu nombreuses et les réglementations directement appliquées par les gouvernements. De nos jours, les autorités chargées du processus de réglementation varient d'un pays à l'autre ; il peut s'agir de ministères, d'instances de régulation ou encore d'entités indépendantes. Ainsi c'est un ministère en Suisse (où la police écrit directement aux fournisseurs de services sur Internet pour bloquer les informations à caractère raciste), en Italie (Comité sur la sécurité nationale et ministère des communications), au Laos (un comité composé de plusieurs ministères et chargé d'établir les règles relatives aux internautes) et en Tunisie (l'Agence tunisienne sur Internet, englobée dans le ministère des communications). Des instances de régulation sont chargées de veiller au contenu des informations en Australie (l'Australian Broadcasting Authority peut ordonner aux fournisseurs de services sur Internet de supprimer des documents), en Inde (la Commission indienne des communications), en Corée du Sud (la Commission sur la morale dans le domaine de l'information et des communications a le pouvoir d'ordonner la suppression de certaines informations sans décision judiciaire) et en Hongrie (Conseil national de la radio et de la télévision).

Il arrive en outre que les instances de régulation soient constituées de membres du gouvernement et qu'elles soient placées sous l'influence du gouvernement. Cette situation est notamment illustrée par le cas du Royaume-Uni, où l'Internet Watch Foundation a d'abord été créée en opposition aux réglementations. En Hongrie également, l'Association des fournisseurs de contenus, dont les objectifs initiaux étaient comparables à ceux de l'IWF, a cependant aujourd'hui un rôle contestable dans la mesure où elle propose la mise en œuvre de mécanismes de filtrage anti-pornographie et la suppression de toute « expression de vulgarité ou de violence » ou de tout ce qui offense le « bon goût », tout en recommandant des mesures contre les atteintes éventuelles aux droits d'auteur. L'autorité de ces organismes, toutefois, reste circonscrite à l'intérieur des frontières.

## Pourquoi censurer ?

Les raisons pour lesquelles la liberté d'expression est placée sous surveillance ou limitée sont vastes et variées. On ne peut que s'alarmer devant le nombre de définitions plus ou moins complètes de ce qui constitue des propos « obscènes ». Nous citons ici quelques-unes des plus éloquentes.

Dans de nombreux pays la censure a pour objet de protéger la sécurité nationale mais il serait intéressant de connaître et de comparer le sens des expressions « raison de sécurité » en Côte d'Ivoire et « sécurité publique et harmonie nationale » à Singapour. Les censeurs du droit égyptien prétendent sauvegarder la « morale publique » et contenir les rumeurs fausses ou sans fondement ainsi que les propos visant à provoquer l'agitation s'ils ont pour but de troubler l'ordre public, d'instiller la peur ou de nuire à l'intérêt public. Les lois égyptiennes sont souvent invoquées.[22]

Au Pérou sont interdites les informations « contraires à la morale et aux bonnes mœurs » En vertu des lois marocaines, des directeurs de journaux ont été arrêtés pour insulte au roi ou pour avoir publié un communiqué émanant d'un groupe islamiste,[23] la liste des sujets tabous comprenant également les ambitions territoriales du Maroc sur le Sahara occidental. La Tunisie dissuade tout commentaire pouvant être interprété comme une critique à l'égard de la politique du gouvernement. Le Zimbabwe interdit tout ce qui est « susceptible de provoquer la peur ou le découragement » sous peine d'être emprisonné pendant une durée maximale de sept ans. En Australie, les contrôles visent ce qui n'est pas adapté aux mineurs.

La Chine censure les informations qui troublent l'ordre public, divulguent des secrets d'État ou nuisent à l'honneur du pays ; les sites pornographiques y sont filtrés. En Inde sont interdits les documents à caractère « lascif » ou qui « tentent l'appétit de luxure ». Les sites Web sont rendus inaccessibles s'ils contiennent des

22. Glenn Frankel. 2004. "Egypt Muzzles Calls for Democracy". Washington Post, 6 janvier 2004, A01.
23. Comité pour la protection des journalistes, " CPJ Delegation Meets with Moroccan Ambassador: Calls for Immediate Release of Jailed Editors," (New York: 2003).

incitations à la haine, à la calomnie, à la diffamation, au jeu, au racisme, à la violence, au terrorisme ou encore s'ils concernent la pornographie y compris la pornographie faisant intervenir des enfants ainsi que les pratiques sado-masochistes. Outre tout ce qui a trait à l'inceste, à la pédophilie, à la bestialité et à la nécrophilie, Singapour interdit l'incitation à l'homosexualité et au lesbianisme. En Corée du Sud, une affaire en cours a pour objet d'examiner la constitutionnalité de l'interdiction de toute référence au lesbianisme et à l'homosexualité.

Dans de nombreux pays d'Europe, l'incitation au racisme et à la xénophobie est interdite. Dans un souci d'harmonisation, le Conseil de l'Europe préconise l'adoption d'une mesure qui garantirait que tous les Etats membres fassent de l'expression de ce type de discours un crime. Il encourage également les États membres à supprimer toute incitation au racisme et à la xénophobie dans les sites Web hébergés dans leurs pays respectifs. Ces mêmes Etats se sont également munis d'un régime précurseur en matière de calomnie et de diffamation.

Bien qu'en matière de limitation de la liberté d'expression, le gouvernement américain ait davantage les mains liées par la Constitution américaine et la jurisprudence, la censure prend d'autres formes. Ainsi les consommateurs sont-ils soumis aux Conditions des fournisseurs de services qui, en réalité, enfreignent les droits garantis par la Constitution : certaines formes d'expression et d'activité sont autorisées, tandis que d'autres, pourtant légales, sont interdites. L'industrie et le secteur privé prennent donc une part active à la limitation de la circulation de l'information.[24]

### La censure au-delà des gouvernements I : la propriété intellectuelle

Quand on parle de censure, on a tendance à ne considérer que l'action gouvernementale. L'inquiétude qu'inspirent la censure et la restriction de la circulation de l'information devrait plutôt attirer notre attention sur l'origine même de la surveillance. Le secteur industriel peut être une formidable machine à censurer, surtout lorsqu'il s'allie aux gouvernements. C'est en effet au nom de la protection du droit d'auteur et de la propriété intellectuelle que sont adoptées des lois et des pratiques effroyables.

Certaines de ces pratiques masquent en réalité des conflits d'intérêt entre divers secteurs industriels. Ainsi le Canada a-t-il interdit de visualiser des vidéos en continu, parce que ce programme enfreignait les réglementations relatives à la diffusion. Au Danemark comme en Hongrie on notera le cadre juridique contestable du 'deep linking', qui interdit aux portails de créer des liens vers certains articles afin d'obliger les internautes à se rendre sur les pages d'accueil des sites d'informations qui hébergent les articles en question. Aux États-Unis, les fournisseurs de contenus et le secteur des communications se livrent une bataille juridique à propos de la divulgation des données personnelles relatives aux abonnés qui utilisent les réseaux peer-to-peer.

24. Sandra Braman et Stephanie Lynch, "Advantage ISP: Terms of Service as Media Law -- a Comparative Study," (University of Alabama, 2002).

Dans certaines situations cependant, ces intérêts ne sont pas antagonistes. Contrairement à ce qui se passe aux États-Unis, en 2000 la Belgique a mis en place une pratique innovante qui permet de dépister les utilisateurs d'outils peer-to-peer : en vertu d'un accord à l'amiable, les fournisseurs de services sur Internet remettent à l'industrie du disque le nom de leurs abonnés.

Aux États-Unis, les lois relatives au droit d'auteur vont encore plus loin. Ainsi, en vertu de la Digital Millennium Copyright Act (DMCA), adoptée en 1998, la publication d'informations sur les dispositifs visant à contourner les mesures de protection des droits d'auteur peut entraîner des poursuites. C'est un délit, même si les personnes qui ont publié les informations en cause ne résident pas aux États-Unis. Ainsi, en 2001, Dmitry Sklyarov, programmateur russe auteur d'un logiciel permettant de contourner le système de protection des droits d'auteur d'Adobe eBooks, fut interpellé lors d'une réunion de pirates informatiques à Las Vegas, où il avait donné une conférence sur ses travaux. S'il ne fut pas poursuivi à titre personnel, la société moscovite qui l'employait, Elcomsoft, elle, le fut.

En fin de compte, Elcomsoft fut acquittée par le jury, en partie parce que la réalisation d'un tel logiciel n'est pas illicite en Russie. Dans une autre affaire, un étudiant norvégien de 16 ans, Jon Johansson, créa le logiciel DeCSS, permettant de contourner le système de protection des DVD à usage commercial. Il fut accusé par la Motion Picture Association of America, toujours en vertu de la DMCA. La MPAA n'en resta pas là, bien au contraire : elle attaqua en justice quiconque créait un lien avec le logiciel ; ce fut le cas d'Eric Corley, rédacteur de 2600 : the Hacker Quarterly qui (comme de nombreux internautes du monde entier) établit des liens avec DeCSS à partir du site Web du magazine.

Dans le domaine de la propriété intellectuelle, de plus en plus, le reste du monde emboîte le pas aux États-Unis. L'Europe est ainsi en passe d'élaborer un système de réglementions comparable à la DMCA des États-Unis ce qui, ajouté aux systèmes de surveillance européens, aura des conséquences catastrophiques pour le droit d'expression. Quant à l'Australie et au Canada, ils semblent sur le point d'adopter à la fois le régime de la propriété intellectuelle des États-Unis et les pratiques de surveillance de l'Europe.

### La censure au-delà des gouvernements II : calomnie et diffamation

Les personnes et les groupes ont eux aussi le pouvoir de censurer les agissements d'autrui en s'appuyant sur la calomnie et la diffamation.

Selon une étude menée au Royaume-Uni, la Commission des lois [25] a découvert que tous les ans certains fournisseurs de services sur Internet recevaient plus d'une centaine de plaintes émanant d'avocats ou de particuliers au sujet de textes

25. Commission des lois, "Law Commission Report on Defamation and the Internet: A Preliminary Investigation," (London: Law Commission of England and Wales, 2002).

diffamatoires qu'ils hébergent ou auxquels ils donnent accès. Il semble que dans leur grande majorité ces lettres proviennent d'avocats protestant contre des sites Web créés par des consommateurs mécontents. La Commission a malheureusement admis que la meilleure solution pour les destinataires des lettres consistait à supprimer les textes incriminés « sans trop se préoccuper ni de l'intérêt public ni de la vérité ». Cette réaction s'explique par le caractère discutable du statut légal des fournisseurs de services sur Internet au Royaume-Uni. La Commission des lois s'inquiète de ce que les groupes militants soient les premiers visés et l'objet principal de ce type de lettres. De telles pratiques juridiques frôlent dangereusement le muselage politique.

Tant que les fournisseurs de services sur Internet seront considérés comme des 'éditeurs secondaires', responsables en quelque sorte du contenu des informations hébergées par leurs services, leur responsabilité pénale sera engagée. Pour la Commission des lois, la situation serait peut-être réglée si ces prestataires étaient dégagés de toute responsabilité, comme c'est le cas aux États-Unis. À défaut, le statut des fournisseurs de services sur Internet devrait être clarifié : éditeurs, archivistes, simples canalisations ou porteuses...

Il importe également d'accorder une attention accrue aux conflits de compétence qui se posent dans les affaires de calomnie et de diffamation. Dans les pays du monde entier, les fournisseurs de services sur Internet et les fournisseurs de contenus se voient de plus en plus exposés aux lois sur la calomnie et la diffamation. C'est ce qui s'est produit en Australie, lorsqu'un tribunal australien s'est déclaré compétent pour juger une affaire de diffamation contre le Dow Jones, établi à New York. Plus récemment, un tribunal canadien a rendu une décision similaire en se référant à l'affaire australienne. Selon la décision, un article écrit par le Washington Post à propos d'une personne résidant et travaillant au Kenya pouvait faire l'objet de poursuites plusieurs années plus tard : le journal aurait dû « s'attendre à ce que l'histoire suive le plaignant où qu'il réside ».[26] L'Union européenne, qui s'attache à résoudre les conflits de lois dans les affaires de diffamation, détermine que quiconque installe des informations sur Internet est soumis aux lois sur la diffamation des États membres de l'UE.[27] Au Canada, un autre tribunal décidait récemment qu'en raison de l'anonymat « le risque que l'on prête foi aux propos diffamatoires était accru » et qu'en conséquence les auteurs de propos diffamatoires sur Internet devaient verser des dommages-intérêts plus élevés.[28]

Faute de s'attacher à résoudre ce problème, nous pourrions nous acheminer vers une forme de censure par intimidation juridique : intimidation des fournisseurs de services sur Internet ou des personnes, qui voient leur droit de parole bafoué.

26. Se reporter à l'article consacré à cette affaire par Michael Geist, "Web Decision extends long arm of Ontario law", The Toronto Star, 16 février 2004.
27. Article 19, communiqué de presse: "ARTICLE 19 concerned that proposed Rome II Regulations pose threat to Internet publishers' freedom of expression", 14 janvier 2004.
28. Patrick Brethour, "Net Libel Open to Higher Damages: Judge says anonymous Web postings can magnify impact of defamatory comments", Globe and Mail, 11 février 2004.

Les gouvernements ont eux aussi recours aux lois sur la diffamation. Dans certains pays, la diffamation constitue une infraction pénale. Le gouvernement de Singapour a ainsi engagé des poursuites à l'encontre d'opposants pour propos diffamatoires. De même, en Géorgie, le gouvernement utilise la loi sur la diffamation pour se protéger des media, qui s'exposent à la fois à des sanctions civiles et pénales, et a proposé que soit allongée la durée des peines prévue en cas de diffamation de fonctionnaires ou membres du gouvernement.[29] Selon Article 19, la Campagne mondiale pour la liberté d'expression :

- la diffamation ne devrait plus être considérée comme une infraction pénale;
- il devrait être interdit aux organismes publics, y compris à tout organisme représentant les pouvoirs législatifs, exécutifs ou judiciaires du gouvernement, d'engager des poursuites pour diffamation ;
- l'expression d'une opinion, contrairement à une accusation réelle, ne devrait pas être passible de poursuites;
- Les fournisseurs de services sur Internet et tout autre organisme remplissant des fonctions similaires devraient être dégagés de toute responsabilité ;
- la publication raisonnable devrait être protégée;
- Les dommages-intérêts alloués devraient être proportionnels aux préjudices subis et un montant maximum fixe devrait être déterminé en cas de dommage moral.

Il n'est pas nécessaire que la censure soit encadrée par des lois; le simple fait que les recueils de lois puissent être perçus par le profane comme une indication de faute ou d'erreur peut conduire à la censure.

## La politique du filtrage et du blocage

Internet est sans doute l'application la plus simple à censurer dans la mesure où un site Web est généralement créé par un individu identifiable, et hébergé par un service commercial. De nombreuses options s'offrent donc au prétendu censeur : il peut contacter les fournisseurs de services sur Internet qui hébergent le site et leur demander de le supprimer ; faire arrêter l'auteur du site ou l'attaquer en justice ; ou encore, ajouter l'adresse du site Web à une base de données répertoriant les sites non autorisés à l'adresse des citoyens ou des consommateurs. Toutes ces méthodes ont été mises en pratique. Les deux premières d'entre elles comportent un risque, celui de faire du site Web supprimé une « *cause célèbre* » (NdT en français dans le texte) : en guise de protestation, les internautes résidant dans les pays hors de la portée du censeur peuvent créer des sites miroirs pour dupliquer le site originel.

Le recours à des mécanismes de blocage est fréquent mais pour que ces mesures soient efficaces les dispositifs doivent être fiables. Le risque est que les utilisateurs découvrent le moyen de contourner ces dispositifs, par exemple en utilisant des sites

29. Article 19, "Harsh Georgian Defamation Laws Must Be Amended," (London: The Global Campaign for Free Expression, 2004).

Web les rendant anonymes (proxy) ou en se connectant par proxy, telle que l'option « cache » du moteur de recherche Google. Il s'agit dans les deux cas d'intermédiaires qui reçoivent le site Web et l'affichent pour l'utilisateur. Cela reviendrait à envoyer un assistant inconnu acheter un livre interdit dans une librairie.

La technologie et les techniques du blocage et de la surveillance sont développées sur décision politique pour la réalisation de tâches précises ; elles sont elles-mêmes limitées par des contraintes techniques. Le blocage peut être effectué à la source, auprès des fournisseurs de services sur Internet ou au niveau de l'utilisateur final.

### Mécanismes de filtrage installés auprès des prestataires cibles

Il est possible de bloquer les sites Web sélectionnés au niveau national mais c'est dans les pays où le nombre des fournisseurs de services est le plus restreint que le blocage est le plus efficace. En effet, dans ces cas précis, on n'accède pas à Internet selon un mode décentralisé mais via une société d'État chargée de contrôler et de bloquer l'accès.

La Chine a ainsi mis en place le célèbre « bouclier d'or » qui empêche les ressortissants chinois d'accéder aux informations fournies par des serveurs situés hors de Chine. Selon les analyses du Harvard University Berkman Center for Internet & Society, des dispositifs de filtrage au niveau des paquets sont intégrés à des routeurs aux frontières. Sont également utilisés les dispositifs de filtrage par détection de mots-clefs, grâce à quoi des fichiers téléchargés à partir d'un serveur sur lequel n'a été installé aucun mécanisme de filtrage sont rendus inaccessibles. Les chercheurs ont découvert au travers de cette étude que les recherches effectuées par Google en Chine à partir des mots « justice Chine » ou « dissident Chine » ne provoquaient le blocage que de moins de la moitié des résultats. Parallèlement, les serveurs de la BBC, de CNN, du Time, de PBS et autres grands sites de l'information étaient bloqués. Le blocage n'est pas toujours logique, toutefois ; les chercheurs ont ainsi pu constater que Reuters, de même que le Washington Post, avaient été bloqués pendant un certain temps, puis débloqués.[30]

Les chercheurs du Berkman Center ont réalisé une étude semblable sur le blocage en Arabie Saoudite.[31] Dans ce pays, tout ce qui circule par Internet transite par l'Unité des services Internet du gouvernement, qui passe les informations au crible des « valeurs islamiques ». Sont ainsi bloquées toute référence claire à la sexualité et les pages relatives à la drogue, aux bombes, à l'alcool, au jeu ou encore celles qui insultent l'islam. Les chercheurs se sont également aperçu qu'étaient censurés certains sites consacrés aux religions, à l'humour, à la musique, au cinéma, ainsi que des références à l'homosexualité. D'autre part, des pages sur la santé ou présentant un caractère éducatif, comme la rubrique de l'Encyclopedia Universalis

30. Jonathan Zittrain et Benjamin Edelman, "Internet Filtering in China," *IEEE Internet Computing,* mars-avril (2003).
31. Jonathan Zittrain et Benjamin Edelman, "Documentation of Internet Filtering in Saudi Arabia," (Berkman Center for Internet and Society, 2002).

en ligne sur les femmes dans l'histoire américaine, la maison d'Anne Frank, ou encore des sites sur la politique du Moyen-Orient étaient eux aussi bloqués.

Pour conclure sur les systèmes de filtrage installés au niveau des fournisseurs de services sur Internet, nous prendrons l'exemple de la Pennsylvanie. En vertu d'une loi de cet état, les prestataires ont l'obligation de bloquer des sites Web répertoriés relatifs à la pornographie infantile. Pour les chercheurs du Berkman Center,[32] cette mesure pose problème parce que 87,3% des sites Web actifs .com, .net et .org partagent les mêmes adresses IP. En d'autres termes, si une adresse IP est bloquée en raison d'un site particulier visé par la loi de Pennsylvanie, d'autres sites sans aucun lien avec le site incriminé se retrouveront eux aussi bloqués. Autre problème, les prestataires américains qui desservent la Pennsylvanie ne peuvent en aucun cas distinguer les habitants de cet état des habitants du reste du pays, de sorte que les effets de l'interdiction se manifestent bien au-delà des frontières de la Pennsylvanie. En septembre 2002, WorldCom annonçait que l'accès aux adresses répertoriées serait bloqué pour tous ses abonnés d'Amérique du Nord, afin de respecter la loi de Pennsylvanie.[33]

### L'installation de mécanismes de filtrage par l'utilisateur final

On peut se procurer dans le commerce des logiciels de filtrage à installer par l'utilisateur final. Dans un certain nombre de pays, ces applications logicielles sont destinées aux parents inquiets de voir leurs enfants accéder à des informations en ligne dont ils jugent qu'elles ne leur conviennent pas et aux sociétés et autres organisations qui souhaitent empêcher leurs employés de profiter de leurs connexions Internet pour fréquenter des sites pornographiques.

L'installation de mécanismes de filtrage est souvent rendue obligatoire par la loi. En vertu de la loi américaine, l'allocation de subventions aux bibliothèques et aux écoles est conditionnelle à l'utilisation de logiciels de filtrage. En vertu de la loi australienne et de décisions politiques en Chine et en Argentine, il est obligatoire de s'équiper de mécanismes de filtrage. Ailleurs, comme au Danemark, en Corée du Sud et en Afghanistan, les écoles, les bibliothèques et les cybercafés sont tenus d'utiliser des logiciels de filtrage afin de garantir aux enfants un accès protégé. Ce sont les personnes les plus désavantagées qui subissent ces mesures de censure le plus durement car pour accéder à Internet elles n'ont d'autre possibilité que de se rendre dans ce type d'établissement.

En général les logiciels de blocage utilisent une base de données interne recensant les sites mis à l'index. Il s'y ajoute parfois des systèmes de détection de mots ou de phrases : l'accès aux sites sur lesquels ils apparaissent est bloqué. Dans les deux cas, il s'avère que ces systèmes bloquent souvent des sites non répertoriés ou qu'ils préser-

32. Benjamin Edelman, "Web Sites Sharing IP Addresses: Prevalence and Significance," (Berkman Center for Internet and Society, 2003).
33. Lisa Bowman et Declan McCullagh. 2002. "WorldCom blocks access to child porn". CNet News.com, 23 septembre 2002.

vent au contraire l'accès à des sites répertoriés. Les sociétés commerciales qui produisent de tels logiciels observent généralement une grande discrétion sur le contenu exact de leurs bases de données. Les gouvernements adoptent la même attitude. Ainsi, sommée au nom des lois sur la liberté de l'information de divulguer le nom des sites mis à l'index, l'Australian Broadcasting Association refusa d'obtempérer. Ces deux exemples portent à croire que les sites censurés ne correspondent pas aux classements.

Lorsqu'on tente de censurer Internet en supprimant l'accès à certains sites au moyen de mots-clefs, on risque de bloquer également, peut-être involontairement, des sites qui n'ont rien à voir avec ce que l'on cherche à interdire. AOL, par exemple, a dû prier les habitants de Scunthorpe, en Angleterre, de bien vouloir épeler autrement le nom de leur ville parce que celui-ci était détecté par le système de censure intégré à son logiciel en raison de quatre lettres qui y figurent. De la même façon, les tentatives visant à bloquer les discussions sur le sexe en utilisant des mots-clefs comme « sein » suppriment l'accès aux sites des groupes de soutien aux patientes souffrant d'un cancer du sein. En 2003, les membres du Parlement du Royaume-Uni n'ont pu échanger de courriers électroniques pour discuter du projet de loi sur les délits sexuels (Sexual Offences Bill) à cause de la mise en place par le Parlement d'un système de filtrage des courriers électroniques non sollicités présentant un caractère pornographique.

Les logiciels de filtrage commercialisés posent des problèmes d'ordre moins technique. Il arrive que les éditeurs de logiciels bloquent les articles et les commentaires critiques à l'égard de leur produit ou encore que les systèmes de filtrage reflètent les prises de position de leurs fabricants et qu'ils ciblent les sites pour la promotion des pratiques sexuelles sans risques, l'avortement ou même les droits de l'homme, bien que ces sites n'enfreignent en rien la loi des pays dans lesquels ils sont accessibles.

Afin que l'on prenne conscience des problèmes posés par les systèmes de filtrage, des chercheurs ont passé beaucoup de temps à analyser les listes de sites bloqués. Ils ont ainsi démontré que de nombreux sites, bien que ne contenant rien d'immoral, étaient interdits d'accès – il s'agit du surblocage. Ils ont également découvert qu'un assez grand nombre de sites qui auraient dû être filtrés ne l'étaient pas – le sous-blocage.[34]

Prenons pour exemple le moteur de recherche Google. Le filtre Google SafeSearch exclut des résultats de ses recherches les documents manifestement pornographiques ou indésirables. Les résultats sont scannés automatiquement pour filtrer les sites pornographiques ou ayant des références sexuellement explicites afin, notamment, de protéger les enfants. Or, comme le révèle une étude du Berkman Center for Internet & Society, un certain nombre de résultats sont classés de façon inappropriée.[35]

34. Benjamin Edelman, *Sites Blocked by Internet Filtering Programs: Edelman Expert Report for Multnomah County Public Library Et Al., Vs. United States of America, Et Al.* (2003 [cité le 24 février 2004]); accessible sur le site http://cyber.law.harvard.edu/people/edelman/mul-v-us/.

35. Benjamin Edelman, *Empirical Analysis of Google Safesearch* (Berkman Center for Internet & Society, 14 avril 2003 [cité le 12 février 2004]); accessible sur le site http://cyber.law.harvard.edu/people/edelman/google-safesearch/.

Parmi les pages rejetées figurent certains sites du gouvernement américain (congress.gov, thomas.loc.gov, shuttle.nasa.gov), des sites créés par d'autres gouvernements (le ministère de la justice de Hong Kong, le ministre de la justice des Territoires du Nord-Ouest au Canada, le bureau du Premier ministre en Israël, le Conseil national de la formation professionnelle en Malaisie), des sites concernant la vie politique (le parti républicain du Vermont, les démocrates d'Austin, au Texas), des articles d'actualité (dont des articles du New York Times sur les blogs, la déflation et la stratégie militaire des États-Unis, des articles de la BBC, de c/net news.com, du Washington Post et de Wired), les sites à vocation éducative (un cours de chimie du Middlebury College, des documents sur la guerre du Vietnam de Berkeley, des sites de de la faculté de droit de l'université Baltimore et de l'université Northeastern), ainsi que des sites religieux (Biblical Studies Foundation, Modern Literal Bible, Kosher for Passover). Parmi les sites qui ne présentent rien de sexuellement explicite, certains ont été bloqués en raison de mots équivoques apparaissant dans leur titre (comme Hardcore Visual Basic Programming) mais pour la plupart la raison de leur exclusion demeure incompréhensible.

Parmi les sites censurés certains étaient destinés aux enfants et présentaient une utilité pour eux, comme celui de l'Encyclopédie Grolier. Ont également été rendus inaccessibles des sites d'information sur la sexualité ou sur la répression des drogues. Dans le même temps, des sites clairement pornographiques continuaient, eux, à être accessibles.

D'autres études sur les principales applications de filtrage mettent en évidence d'étranges résultats. Ainsi, selon une étude de la National Coalition Against Censorship, les plus grands distributeurs de logiciels de filtrage pratiquent régulièrement le surblocage.[36] Parmi les sites bloqués par une ou plusieurs applications logicielles, les cas les plus litigieux comprennent :

- Les pages d'accueil de la Traditional Values Coalition et d'un membre du Congrès américain.
- La League for Programming Freedom du MIT, une partie du site de la ville d'Hiroshima, les sites consacrés à Georgia O'Keeffe et à Vincent Van Gogh, ainsi que celui de la Society for the Promotion of Unconditional Relationships, qui promeut la monogamie.
- La plupart des sites des homosexuels et lesbiennes et, après avoir détecté les mots « 21 au moins » (« least 21 »), un article publié sur le site d'Amnesty International (la phrase incriminée était: « les rapports faisant état de fusillades à Irian Jaya portent à 21 au moins le nombre de personnes tuées ou blessées en Indonésie et au Timor Oriental. »)
- Un essai sur « L'Obscénité sur Internet: les enseignements du monde de

36. Marjorie Heins et Christina Cho, "Internet Filters: A Public Policy Report," (Free Expression Policy Project, National Coalition Against Censorship, 2001).

l'art » (« Indecency on the Internet: Lessons from the Art World »), le rapport des Nations Unies intitulé « VIH / AIDS: L'épidémie globale » (« HIV/AIDS: The Global Epidemic ») et les pages d'accueil de quatre galeries de photographie.

- En raison du mot « dick » détecté, le site officiel de Richard « Dick » Armey, alors chef de la majorité de la Chambre des représentants.
- Les pages d'accueil de la Civil Liberties Union du Wisconsin et de la National Coalition Against Censorship.
- La Déclaration d'indépendance des États-Unis, les œuvres théâtrales complètes de Shakespeare, Moby Dick et 'Marijuana: Facts for Teens', brochure publiée par le National Institute on Drug Abuse (département du National Institutes of Health).
- Des sites relatifs aux droits de l'homme tels que le site du Commissaire du Conseil des Etats de la Baltique, celui d'Algeria Watch, ainsi que celui de la bibliothèque médicale Archie R. Dykes de l'Université du Kansas (après détection du mot 'dykes').
- Une page de Jewish Teens ainsi que le site consacré au projet sur la génétique moléculaire canine de l'université de l'état du Michigan.
- Le National Journal of Sexual Orientation Law, la page sur les livres interdits de l'université Carnegie Mellon, le site d'un traiteur appelé « Let's Have an Affair » et, grâce à la fonction de détection « mots grossiers », les recherches sur Bastard Out of Carolina et « The Owl and the Pussy Cat ».

Les systèmes de filtrage bloquent également l'accès aux 'sites failles', dont les services confèrent l'anonymat aux internautes, protègent la confidentialité de leurs transactions, traduisent des documents, présentent des textes connus sous une version humoristique ou encore, offrent des dispositifs de test des pages Web, etc. Comme l'indique un expert :

> Pour que la censure mène à bien la tâche qu'on attend d'elle (le contrôle de l'information), il ne doit pas y avoir de moyens d'échapper à ce contrôle. Elle doit donc interdire tout site qui permettrait à une personne de recevoir des informations mises à l'index par le programme de censure. Par conséquent, les sites qui confèrent l'anonymat, protègent la confidentialité ou encore, proposent des services de traduction devraient être interdits.[37]

Par voie de conséquence, les mécanismes de filtrage empêchent forcément les utilisateurs d'avoir recours à des services qui protègent la confidentialité de leurs transactions. La raison en est simple : la confidentialité permet la liberté d'expression et l'accès à l'information. Le contrôle et la restriction de la confidentialité rendent possible la censure et la renforcent.

37. Seth Finkelstein, "*Bess's Secret Loophole (Censorware Vs. Privacy* & *Anonymity),"* (Anticensorware Investigations, 2002).

# IV.

# Vie privée et surveillance

Liberté d'expression et vie privée sont étroitement liées. De même, censure et surveillance sont interdépendantes. Dans le chapitre qui suit, nous verrons comment les efforts visant à renforcer la surveillance se répercutent sur la censure en limitant la liberté d'expression. De même, les efforts visant à renforcer la censure s'appuient de plus en plus sur les mécanismes de surveillance.

Dans la célèbre décision qui invalidait la Communications Decency Act, la District Court américain déclarait que le défaut majeur que présentait cette loi était de supposer que la vérification en ligne de l'identité et de l'âge des utilisateurs était possible.

> Il n'existe pas de méthode efficace pour vérifier l'identité ou l'âge d'un utilisateur qui accède à des données par courrier électronique, diffuseurs de messages, groupes ou forums de discussion. Une adresse électronique ne contient pas d'informations fiables à propos de la personne qui l'emploie et qui est susceptible d'avoir recours à un « alias » électronique ou à un système de réexpédition anonyme. Il n'existe pas de répertoire universel ou fiable de toutes les adresses électroniques et des noms ou numéros de téléphone correspondant ; un tel répertoire serait d'ailleurs incomplet ou vite obsolète. Ce sont les raisons pour lesquelles, dans la plupart des cas, un expéditeur ne peut savoir avec certitude si le destinataire de son message est un adulte ou un mineur. La vérification de l'âge dans les courriers électroniques est plus difficile encore dans le cas des diffuseurs de messages tels que les listservs, qui envoient automatiquement des messages à toutes les adresses électroniques figurant sur le répertoire de l'expéditeur. Les experts gouvernementaux [...] s'accordent à reconnaître qu'à l'heure actuelle la technologie ne permet pas à un expéditeur de savoir avec certitude si la liste d'un diffuseur de messages ne contient que les adresses de personnes adultes.[38]

Les lois qui tentent de limiter l'accès de certains groupes de personnes à des informations données posent des difficultés semblables. Les débordements sont inévitables. Et les adultes risquent de ne plus avoir accès aux informations auxquelles ils sont en droit d'accéder. Parce qu'il est impossible d'identifier un internaute de Pennsylvanie, l'ensemble des clients d'un prestataire d'Amérique du Nord

38. Chief Juage suprême Sloviter. 1996. *American Civil Liberties Union et al. v. Janet Reno, Attorney General of the United States:* United States District Court for the Eastern District of Pennsylvania.

ne pourra plus accéder à certains sites. Et les décisions judiciaires françaises auront des conséquences pour tous ceux qui se rendent sur les sites de ventes aux enchères de Yahoo !

Il n'existe pas de procédés simples permettant d'identifier les internautes en ligne. Même si on en découvrait, la solution idéale n'existe pas. En dépit de ses nombreux détracteurs, le droit des personnes de communiquer de façon anonyme est très prisé par la société, il est inscrit dans la législation.

## Le droit de ne pas se présenter

La protection de l'expression sous condition d'anonymat est le fruit d'une longue tradition dans les démocraties participatives. En 1776, Thomas Paine publiait Common Sense qu'il signait « écrit par un Anglais ». Les Federalist Papers, qui figurent parmi les œuvres les plus admirées de l'histoire des Etats-Unis, ont été écrits sous pseudonyme en 1787-88. L'auteur, désigné sous le nom de « Publius », entendait ainsi convaincre les habitants de New-York de ratifier le projet de constitution.

Aux États-Unis, le droit de participer sous couvert d'anonymat est garanti par le Premier Amendement, qui protège la liberté de parole. Le Premier Amendement à la Constitution américaine dispose :

> Le Congrès ne fera aucune loi qui touche l'établissement ou interdise le libre exercice d'une religion, ni qui restreigne la liberté de la parole ou de la presse, ou le droit qu'a le peuple de s'assembler pacifiquement et d'adresser des pétitions au Gouvernement.

Toute tentative gouvernementale de limiter la liberté de parole peut être déclarée illégale parce que contraire à la Constitution. La restriction de la liberté d'expression peut être illégale pour les motifs suivants: une trop grande imprécision conduisant à une restriction de la liberté d'expression; une portée trop large des lois qui interdisent les libertés d'expression garanties ou non garanties; une restriction d'emblée de la liberté de parole; une réglementation sur le fonds de ce qui est exprimé, à moins que l'on soit en présence d'intérêts gouvernementaux bien précis et qu'il ne soit pas possible d'atténuer la restriction ; quant à l'obligation de parole, elle n'est pas reconnue. L'interdiction de l'obligation de parole a été utilisée pour abroger des lois contraignant les personnes à révéler leur identité.[39]

Aux États-Unis, l'une des affaires les plus anciennes portées devant les tribunaux et concernant l'anonymat date d'avant même la Constitution. Lors du procès Zenger, en 1735, John Peter Zenger, un imprimeur, refusa de révéler l'identité des auteurs anonymes qui avaient fait paraître des critiques à l'encontre

39. Electronic Privacy Information Center, "Free Speech" (EPIC, 8 avril 2002 [cité en février 2004]); disponible sur http://www.epic.org/free_speech/.

du gouverneur royal de New York. Par la suite, le gouverneur et son conseil intentèrent des poursuites contre Zenger pour écrits diffamatoires incitant à la sédition. D'aucuns estiment que c'est en réaction à ces événements que fut rédigé le Premier Amendement à la Constitution des États-Unis.

Le droit de participer à la vie politique de façon anonyme fut réaffirmé par la Cour suprême des États-Unis au XX$^{e}$ siècle. Dans l'affaire *Lovell v. Griffin,* en 1938, la Cour suprême invalida une ordonnance qui interdisait strictement toute distribution d'œuvres écrites en tout lieu et à toute heure à Griffin, en Géorgie, sans autorisation préalable. L'arrêt précisait que les pamphlets et les libelles « ont, au cours de l'histoire, été des armes pour la défense de la liberté » et que l'application de l'ordonnance Griffin « restaurerait le système d'autorisations et de censure dans sa forme la plus dure ». Il existait à l'époque aux États-Unis de nombreuses ordonnances de ce type. Bien qu'on entendît également par là prévenir la fraude, le désordre et le dépôt d'ordures, la Cour se refusa à retenir ces motifs, indiquant qu'il existait « d'autres moyens d'atteindre ces objectifs légitimes sans restreindre la liberté de parole et la liberté de la presse ».

En 1958, la Cour suprême confirma les droits de la NAACP de refuser de remettre la liste de ses adhérents au gouvernement de l'état de l'Alabama, qui ne la voyait pas d'un bon œil.[40] À la même époque, dans l'affaire *Talley v. California,* la Cour suprême réaffirma le droit de s'exprimer de façon anonyme. Cette affaire concernait une ordonnance prise par la ville de Los Angeles pour limiter la distribution de prospectus en exigeant l'identification de la personne qui avait écrit, imprimé et distribué le prospectus. Le requérant, Talley, fut arrêté et jugé pour avoir enfreint cette ordonnance en distribuant des prospectus dans lesquels il incitait les lecteurs à soutenir le boycott mené par la National Consumers Mobilization contre un certain nombre de commerçants et de négociants nommément désignés, sous prétexte que ces derniers vendaient des produits « provenant de fabricants qui refusaient le principe de l'égalité des chances devant l'emploi aux 'Nègres, aux Mexicains et aux Orientaux'».

Dans la décision concernant l'affaire *Talley v. California,*[41] les juges déclarèrent:

> Les pamphlets, les prospectus, les brochures et même les livres anonymes ont contribué de façon importante aux progrès de l'humanité. À différentes époques de l'histoire, des groupes ou des sectes persécutés ont ainsi pu critiquer, sous couvert d'anonymat, des pratiques et des lois tyranniques. La loi intolérable sur l'autorisation de parution de la presse en Angleterre, également appliquée dans les Colonies, a notamment été adoptée parce qu'il est notoire que l'identification des imprimeurs, des auteurs et des dis-

40. *NAACP v. Alabama* ex rel. Patterson, 357 US 449 (1958) and upheld in *NAACP v Alabama,* 377 US 228 (1964).

41. *Talley V. California: Cour suprême des États-Unis,* 362 U.S. 60, décision du 7 mars 1960.

> tributeurs restreint la circulation d'écrits condamnant le gouvernement. Les vieilles affaires de diffamation incitant à la sédition en Angleterre nous montrent jusqu'où les autorités sont allées pour découvrir les auteurs des livres qui les attaquaient. John Lilburne fut fouetté, mis au pilori et soumis à l'amende pour avoir refusé de répondre à des questions qui n'avaient d'autre but que de rassembler des preuves afin de le condamner, lui-même ou d'autres personnes, pour avoir distribué des livres sous le manteau en Angleterre. Deux pasteurs puritains, John Penry et John Udal, furent condamnés à mort après avoir été accusés d'avoir écrit, imprimé ou publié des livres. Avant la guerre d'Indépendance, les patriotes coloniaux devaient souvent cacher qu'ils avaient écrit ou distribué des textes sous peine d'être poursuivis par les tribunaux anglais. C'est à peu près à cette époque que furent rédigées les Lettres de Junius: l'identité de leurs auteurs reste inconnue à ce jour. Les Federalist Papers, en faveur de l'adoption de notre Constitution, furent eux aussi publiés sous pseudonymes. Il est clair qu'on peut avoir recours à l'anonymat en vue de la réalisation des objectifs les plus positifs.

Selon l'opinion exprimée par la Cour suprême, les Lettres de Junius comprenaient notamment une lettre rédigée le 28 mai 1770 dans laquelle l'auteur s'interrogeait à propos de la taxe sur le thé imposée aux États-Unis: « Qu'est-ce d'autre donc que la manifestation odieuse et inutile d'un pouvoir spéculatif, l'imposition de la marque de l'esclavage aux Américains, sans que leurs maîtres en tirent aucun profit ? ». Toujours selon la Cour suprême, c'est « une question qu'il n'aurait pas pu poser sans le couvert de l'anonymat ».

L'affaire *McIntyre v. Ohio Elections Committee* est emblématique du droit de s'exprimer sous couvert d'anonymat. Cette affaire contestait le Code de l'Ohio qui interdisait la distribution de prospectus anonymes à caractère politique. Il était obligatoire, en vertu du Code, que les documents écrits mentionnent le nom et l'adresse de l'auteur ou des responsables des revendications.

En 1988, Margaret McIntyre (décédée au moment où fut rendue la décision), distribua des brochures aux personnes présentes lors d'une réunion publique dans une école de l'Ohio. Une partie de ces brochures étaient signées de son nom, les autres portaient la mention « Des parents et des contribuables inquiets ». Un responsable de l'école porta plainte devant le Comité des élections de l'Ohio, qui infligea une amende de 100$ à Margaret McIntyre.

Dans cette affaire, la Cour suprême exprima l'opinion que rien ne permettait de supposer que le texte était faux, trompeur ou diffamatoire.[42]

42. *McIntyre V. Ohio Elections Commission: the Supreme Court of the United States,* No. 93-986, décision du 19 avril 1995.

> Il est indiscutable que la mise en circulation sur le marché des idées d'une œuvre écrite anonyme est beaucoup plus importante que toute exigence du public visant à ce que l'auteur dévoile son identité en guise de condition préalable. Par conséquent, si un auteur décide de conserver l'anonymat, cette décision, comme celle de retrancher des éléments du texte publié ou d'en ajouter, relève de la liberté d'expression garantie par le Premier Amendement.

En guise d'approbation, le juge Thomas prit une toute autre approche. Plutôt que de s'interroger sur la validité et la valeur historique du droit à la liberté d'expression sous couvert d'anonymat, « nous devrions nous demander si l'expression "liberté de parole, liberté de la presse", dans son acception première garantit la publication de brochures anonymes. Il me semble que c'est le cas. »

Par opposition, le juge Scalia, soutenu par le juge suprême, décréta que la publication anonyme de pamphlets constituait une pratique préjudiciable et frauduleuse.

> Elle favorise l'iniquité en supprimant l'obligation de rendre compte de ses actes, ce qui est généralement le but de l'anonymat. Il existe bien entendu des exceptions, et lorsque l'anonymat est nécessaire pour se protéger des menaces, du harcèlement ou des représailles, le Premier Amendement exigera une exemption à la loi de l'Ohio. Mais à vouloir abroger la loi de l'Ohio dans son application générale ainsi que les lois de même teneur de 48 autres états de l'État fédéral sous prétexte que l'expression d'idées sous couvert d'anonymat est depuis toujours sacro-sainte dans notre société, cela me paraît être une déformation du passé qui ne peut mener qu'à un avenir anesthésié.

Les arguments pour et contre sont réitérés dans toutes les affaires relatives à l'anonymat et à sa contribution à une société libre et ouverte.

La décision judiciaire la plus récente concerne l'affaire *Watchtower Bible v. Stratton,* en juin 2002. Les conclusions du tribunal furent les suivantes :[43]

> L'anonymat constitue un bouclier contre la tyrannie de la majorité [...]. C'est une illustration des desseins poursuivis par la *Bill of Rights* et le Premier Amendement en particulier : protéger les empêcheurs de tourner en rond des représailles et éviter que leurs idées ne disparaissent dans une société intolérante.

Selon la décision rendue par le tribunal, il est inconstitutionnel d'exiger d'une personne qu'elle obtienne une autorisation faisant mention de son nom avant de faire du porte à porte pour promouvoir une cause politique.

Quant à Internet, les gouvernements ont, à de nombreuses reprises, tenté d'imposer que les personnes s'identifient avant de leur octroyer le droit de parole. En 1996, les législateurs de l'état de Géorgie adoptèrent une loi interdisant à quiconque

43. *Watchtower Bible & Tract Society of New York, Inc. et al. v. Village of Stratton et al.:* the Supreme Court of the United States, No. 00-1737, décision du 17 juin 2002.

de s'exprimer en ligne sous couvert d'anonymat ou d'un pseudonyme. L'American Civil Liberties Union (ACLU) émit une mise en garde sur le caractère inconstitutionnel de la loi, en ce qu'elle imposait des limitations fondées sur le contenu à la liberté d'expression sur les réseaux d'ordinateurs.[44] Les tribunaux acquiescèrent, jugeant que la loi, trop générale et trop vague, limitait et donc enfreignait la Constitution.

> [Les juristes de l'état de Géorgie] prétendent que la loi n'a d'autre but que de prévenir la fraude ce qui, comme l'admet le tribunal, représente un intérêt légitime de l'état. Cependant, la loi n'a pas été taillée sur mesure pour atteindre cet objectif, au lieu de quoi, elle abolit le droit d'expression licite et garanti par ailleurs. Plus précisément, en raison de son libellé, ses dispositions prohibitives sont applicables que l'auteur ait des intentions frauduleuses ou que la fraude ait lieu quoi qu'il en soit. Elles risquent donc de s'appliquer à de très nombreuses transmissions d'informations qui « identifient à tort » l'expéditeur mais qui ne sont pas « frauduleuses » en vertu du code pénal.[45]

Cette décision eut une grande importance car, à l'époque, un certain nombre d'états et de pays envisageaient d'adopter des dispositions similaires.

## Le droit d'accès sous condition d'anonymat: pour ou contre

Devant l'intensification des pressions, le Congrès américain adopta la Communications Decency Act en 1996 pour tenter de trouver une solution au problème des documents obscènes en ligne. Les opposants à la CDA prétendirent que la logique qui sous-tendait la décision McIntyre s'appliquait avec plus de force encore à Internet. Selon David Sobel, expert de premier plan en la matière :

> Que les millions de personnes qui visitent des sites Internet recherchent des informations sur les adolescentes enceintes, le SIDA et autres maladies sexuellement transmissibles, les œuvres littéraires classiques ou la poésie d'avant-garde, leur droit d'effectuer ces recherches de façon privée et anonyme est protégé par la Constitution. La CDA cherche à abolir ce droit.[46]

La décision du tribunal s'appuya sur des idées semblables.

> L'anonymat est important pour les internautes qui cherchent des informations d'une nature particulière, par exemple sur les sites du Critical Path AIDS Project, du Queer Resources Directory – qui s'adresse principalement aux jeunes homosexuels – ou du Stop Prisoner Rape (SPR). De nombreuses personnes inscrites sur la liste de diffusion du SPR exigent de conserver l'anonymat en raison de l'opprobre qui frappe les prisonniers victimes de viol.

44. ACLU, "Fahrenheit 451.2: Is Cyberspace Burning? How Rating and Blocking Proposals May Torch Free Speech on the Internet."
45. *American Civil Liberties Union of Georgia V. Miller,* 977 F. Supp. 1228 (1997).
46. Electronic Privacy Information Center, "Internet "Indecency" Legislation: An Unconstitutional Assault of Free Speech and Privacy Rights," (Washington DC: 1996).

La loi fut abolie au nom de la protection de l'identité, de l'anonymat et de la liberté d'expression.

L'anonymat des internautes s'arrête avec les fournisseurs de services sur Internet, cependant. Il n'est pas étonnant que le gouvernement moi du Kenya demande régulièrement aux prestataires de lui faire parvenir leurs listes d'abonnés, que les clients des cybercafés birmans aient l'obligation de s'inscrire et de présenter le numéro de leur carte d'identité et l'adresse de leur domicile, ou encore qu'en Corée du Sud le gouvernement ait fait une proposition de réglementation qui exigerait que toute personne souhaitant participer aux forums de discussion des organismes publics fournisse au préalable son numéro de carte d'identité nationale ; de même, en Italie, les clients des cybercafés sont arbitrairement contraints de montrer leur passeport ;[47] on notera encore que l'inquiétude monte dans une ville californienne, où un arrêté oblige les cybercafés à installer un système de vidéo-surveillance. En Inde, la police somme l'état du Maharashtra d'imposer aux cybercafés, comme condition à l'obtention d'une licence, qu'ils s'équipent de mécanismes de filtrage; ils ont de plus l'obligation de demander aux internautes de remplir de longs formulaires indiquant leur adresse, leur numéro de téléphone et autres coordonnées, et de fournir une photographie d'identité.[48] La recherche et la divulgation de l'identité des clients des prestataires prêtent de plus en plus à controverse.

L'affaire anon.penet.fi est sans doute la plus célèbre en matière de divulgation contrainte d'identité sur Internet. Anon.penet.fi, un service de réexpédition anonyme, était administré depuis la Finlande par Johan Helsingius. Au bout de trois ans d'activité, le système de réexpédition comptait 500.000 clients et traitait plus de 7.000 messages par jour quand il dut fermer boutique.[49] La police finlandaise se présenta à Helsingius munie d'un mandat de perquisition sur la base d'une allégation de l'église de scientologie selon laquelle anon.penet.fi avait été utilisé pour rendre publiques des informations d'ordre privé, extraites de l'ordinateur d'une église, en les affichant sur le groupe USENET alt.religion.scientology.

Le 22 août 1996, le tribunal de police d'Helsinki somma M. Helsingius de remettre à la police l'adresse électronique de l'expéditeur.[50] Le tribunal de police d'Helsinki fondait notamment sa décision sur le principe selon lequel un témoin ne peut s'abstenir de révéler des faits lors d'un procès, que les messages dont il était question avaient été envoyés à un groupe de discussion public et que les messages publics n'étaient nullement protégés par la loi. Helsingius, refusant de donner cours à cette requête, avança que le caractère confidentiel du courrier postal, des

47. Anita Ramasastry, "Can a City Require Surveillance Cameras in Cybercafes without Violating the First Amendment? A California Court Rules on the Issue," *Findlaw's Writ Legal Commentary, 19 février 2004.*
48. Zubair Ahmed, "Bombay Plans Cyber Cafe Controls," *BBC News Online,* 27 janvier 2004.
49. Daniel Akst, "Postcard from Cyberspace: The Helsinki Incident and the Right to Anonymity," *Los Angeles Times,* 22 février 1995.
50. Johan Helsingius, "Press Release: Johan Helsingius Gets Injunction in Scientology Case -- Privacy Protection of Anonymous Messages Still Unclear," (Penet.fi, 1996).

communications téléphoniques ou autres messages de nature privée est protégé par la Constitution finlandaise et ne saurait être violé lors d'une enquête préliminaire sur une allégation d'atteinte au droit d'auteur, qui constituait somme toute une infraction mineure. En raison de la décision du tribunal et après cinq perquisitions successives sur la base d'autres allégations d'atteinte au droit d'auteur et de plaintes portant sur des insultes à l'encontre de responsables politiques étrangers contenues dans des messages, Helsingius ferma son serveur de réexpédition.[51]

Cette décision fut sans doute en partie motivée par la crainte qu'inspire la criminalité. Selon le London Observer citant un conseiller du Federal Bureau of Investigation (FBI), jusqu'à 90% de la pornographie enfantine vue par ce conseiller sur Internet avait transité par le service de réexpédition d'Helsingius.[52] On sut au terme de l'enquête menée par la police finlandaise que cette allégation était sans fondement; un an avant la parution de l'article de l'Observer, la police avait d'ailleurs indiqué que le service de réexpédition était restreint de façon à ne pas pouvoir acheminer de photographies. Le service fut également accusé d'être fréquemment utilisé par la mafia russe.[53] En raison de toutes ces accusations, le serveur fut fermé, bien qu'il eût été utilisé par une association britannique de prévention du suicide qui venait en aide à des personnes dépressives préférant garder l'anonymat.[54]

## La restriction de la liberté d'expression par la surveillance de masse

La divulgation de l'identité des utilisateurs est une pratique de plus en plus fréquente. On relève dans le monde entier des affaires où les tribunaux exigent que soit rendue publique l'identité de simples utilisateurs et de personnes qui installent des documents sur Internet ou envoient des courriers électroniques. La législation sur le droit d'auteur, qui exige que soient rendues publiques les données à caractère personnel des abonnés soupçonnés de pratiquer des échanges de fichiers, ne contribue en rien au respect de la vie privée. On estime à 2.400 le nombre des citations à comparaître ordonnées à ce jour par l'industrie du disque et de la musique aux États-Unis.[55]

L'une des affaires en cours les plus importantes se déroule actuellement devant la District Court for the Eastern District of Pennsylvania, aux États-Unis, et oppose BMG Music à 203 individus anonymes et sans relations entre eux. Selon

51. Johan Helsingius, "Press Release: Johan Helsingius Closes His Internet Remailer," (Penet.fi, 1996).
52. CNET Staff, ""Remailer" Service Shut Down," *CNET News.com,* 31 août 1996, 2:00pm PT 1996.
53. Paul A. Strassman and William Marlow, "Risk Free Access into the Global Information Infrastructure Via Anonymous Re-Mailers" (article présenté au Symposium on Global Information Infrastructure: Information, Policy & International Infrastructure, Cambridge, MA, 28-30 janvier 1996).
54. CNET Staff, ""Remailer" Service Shut Down."
55. Electronic Frontier Foundation, *Subpoena Database Query Tool* (EFF, 1 décembre 2003 [cité en février 2004]).

l'entreprise, les défendeurs ont fait en sorte que des musiques pourtant protégées par le droit d'auteur puissent être téléchargées sur Internet à partir de leur propre ordinateur. Les défendeurs sont donc accusés d'expression illicite sur Internet. La difficulté vient de ce que le droit à l'expression sous couvert d'anonymat étant protégé par la Constitution, l'injonction de produire des données relatives aux abonnés entraîne une immunité relative. En déterminant l'identité de ces personnes, pourrait-on affirmer, on risque de porter un coup à liberté d'expression sous couvert d'anonymat : les internautes sauront qu'ils peuvent être identifiés sur la base de simples allégations de personnes qui n'ont pas forcément l'intention d'engager des poursuites.[56]

La divulgation des données personnelles pourrait, cependant, aboutir à un problème plus grave encore. On élabore des politiques visant à contraindre les prestataires à révéler aux forces de l'ordre l'identité des personnes qui utilisent leurs services de communication. Les informations fournies ne s'arrêtent pas à l'identité de l'abonné, elles comprennent également les données relatives au trafic.

L'accès aux données relatives au trafic pose problème du point de vue de la protection de la vie privée. Selon le Groupe d'experts de la Commission européenne sur la vie privée et la protection des données,[57] les données relatives au trafic et les infrastructures modernes de la communication sont de plus en plus problématiques du point de vue de la protection de la vie privée.

> Les réseaux de télécommunications et notamment l'Internet se caractérisent par leur capacité à générer un volume important de données dites transactionnelles (données créées pour assurer les bonnes connexions). La possibilité d'utiliser les réseaux de manière interactive (un trait caractéristique de nombreux services l'Internet) augmente encore le volume de ces données transactionnelles. En consultant un journal en ligne, l'utilisateur intervient en choisissant les pages qu'il souhaite lire. Ces choix exprimés par les clics de la souris génèrent un itinéraire constitué de données transactionnelles. Les médias et les services d'information traditionnels sont au contraire consommés de manière plus passive (la télévision, par exemple), leur caractère interactif étant limité au monde hors ligne des kiosques à journaux et des bibliothèques. Bien que dans certaines législations les données transactionnelles bénéficient d'un certain niveau de protection grâce aux règles protégeant la confidentialité de la correspondance, l'augmentation massive du volume des données de cette nature constitue un sujet de préoccupation légitime.

Le champ des données concernées est de plus en plus étendu en raison des nouvelles orientations politiques.

56. Public Citizen et al., "Memorandum in Response to Motion for Expedited Discovery in BMG Music, Et A., V. Does 1-203," (United States District Court for the Eastern District of Pennsylvania, 2004).
57. Article 29, Groupe de protection des personnes à l'égard du traitement des données à caractère personnel, "Recommandation 3/97: L'anonymat sur Internet," (Bruxelles: Commission européenne, 1997).

Dans les années 90, deux organisations internationales ont travaillé à la mise en œuvre d'accords de coopération internationale sur la criminalité « high-tech» ou cybercriminalité en matière de prévention et d'enquête. Depuis 1995, le Groupe des huit pays les plus industrialisés (G8) s'est réuni officiellement à intervalle régulier afin d'étudier les possibilités d'harmonisation et de coopération et de créer de nouvelles instances d'enquête. De même, le Conseil de l'Europe (CoE), organisation internationale d'élaboration de traités composée de 43 membres, a entrepris dès 1997 de rédiger une convention sur la cybercriminalité, achevée et ouverte à signature en novembre 2001. Les travaux de ces deux organisations ont eu des conséquences sur la divulgation des données personnelles par les fournisseurs de services.

La Convention sur la cybercriminalité du Conseil de l'Europe exige des pays qui la ratifient qu'ils contraignent les fournisseurs de service à rendre publique l'identité de leurs abonnés et à conserver et à fournir, sur demande, les données relatives au trafic en cas d'enquête judiciaire. Grâce à ces nouveaux pouvoirs, les Etats peuvent désormais mettre en commun les données relatives à l'enquête: si un pays demande des informations à un autre pays, ce dernier doit accepter en exigeant des prestataires situés sur son territoire qu'ils lui remettent les informations concernées, ce qui soulève d'autres problèmes. Les pays sont soumis à des pressions en vue de l'adoption de la convention. Cette convention pourrait permettre aux intérêts américains en matière de droit d'auteur d'étendre leurs pouvoirs à l'ensemble du globe et d'avoir accès à l'identité des abonnés et autres données dans les pays étrangers, même dans les cas où ces informations n'ont pu être obtenues aux États-Unis.

L'accès aux données relatives au trafic pose des problèmes encore plus graves lorsque les fournisseurs d'accès sont contraints par la loi d'archiver ces données pendant d'assez longues périodes, ce qui va à l'encontre de l'esprit même des lois sur la protection de la vie privée. Depuis toujours, le G8 préconise la conservation des données relatives au trafic, position que l'on retrouve aux États-Unis dans les années 90. Selon le directeur du FBI de l'époque,

> Nous encourageons les fournisseurs de services sur Internet à conserver pendant une période déterminée les données relatives aux abonnés et aux communications ; actuellement, à l'inverse des opérateurs téléphoniques, ils les éliminent au bout d'un laps de temps très court. Certaines informations sont cruciales pour repérer les cas de [pornographie enfantine] ou même pour remonter des pistes. Ce serait donc très utile et nous espérons vivement que cela pourra être réalisé, ne serait-ce que sur la base du volontariat. La conservation des 'caller ID' par les fournisseurs de services sur Internet serait également une mesure très utile, et nous espérons là aussi que les fournisseurs s'engageront sur la base du volontariat ; nous avons entamé des discussions avec eux pour déterminer s'ils pouvaient nous fournir l'aide dont nous avons besoin.[58]

58. Louis Freeh, "Hearing of the Commerce, Justice, State and the Judiciary Committee -- Subject: FY '99 Appropriations for Proposal to Prevent Child Exploitation on the Internet," (Washington DC: Federal Bureau of Investigation, 1998).

Par la suite, les États-Unis engagèrent l'Union européenne et le G8 à adopter une position similaire. En octobre 2001, le président George W. Bush recommanda dans une lettre au président de la Commission européenne de modifier la politique européenne, « d'aborder le domaine de la protection des données dans le contexte de l'application du droit et de la nécessité impérieuse de lutter contre le terrorisme » et, par conséquent, « de [r]éviser les projets de directives sur la vie privée qui préconisent la destruction obligatoire de données cruciales afin que leur conservation pendant une période de temps raisonnable soit autorisée ».[59] Cette lettre faisait suite aux recommandations du ministère américain de la justice à la Commission européenne afin que « les modalités de protection des données lors de la mise en commun des informations relatives à l'application du droit soient élaborés de façon à ne pas nuire à la coopération internationale » : [60]

> Lors de l'élaboration des modalités de protection des données, il s'agit de trouver un juste équilibre entre la protection de la vie privée, le besoin légitime des fournisseurs de services de sécuriser leurs réseaux et d'empêcher la fraude, et le renforcement de la sécurité publique.[61]

On retrouve une formulation quasi identique dans les documents préparés à l'occasion de la réunion du G8 consacrée à la conservation des données en mai 2002 :

> Il s'agit de garantir que, dans son application, la législation sur la protection des données, prend en considération la sécurité publique et autres valeurs de la société, notamment en autorisant la conservation et la protection des données essentielles à la sécurisation des réseaux ou aux enquêtes et poursuites menées au nom du maintien de l'ordre, en particulier pour ce qui concerne Internet et autres nouvelles technologies.[62]

Sous prétexte que la conservation des données relatives au trafic revêt une importance capitale dans le cadre de la lutte contre le terrorisme, un certain nombre de pays ont adopté des positions favorables à la conservation des données. En décembre 2001, au Royaume-Uni, un projet de loi de lutte contre le terrorisme contenant une disposition sur la conservation des données fut présenté et adopté. La France et bien d'autres pays membres de l'Union européenne emboîtèrent le pas au Royaume-Uni, également suivi très rapidement par d'autres Etats tels que l'Afrique du Sud et l'Argentine. Dans l'ensemble de ces pays, les fournisseurs de services sur Internet (et les opérateurs téléphoniques) ont désormais l'obligation de

59. Président Bush, "Letter to President of the European Commission: Proposals for US-EU Counter-Terrorism Cooperation," (Bruxelles: 2001).
60. Gouvernement des États-Unis, "Comments of the United States Government on the European Commission Communication on Combating Computer Crime," (Bruxelles: 2001).
61. Gouvernement des États-Unis, "Prepared Statement of the United States of America, Presented at European Union Forum on Cybercrime," (Bruxelles: 2001).
62. Ministres de la justice et de l'intérieur du G8, "G8 Statement on Data Protection Regimes," (Mont-Tremblant: Sommet mondial sur la société de l'information, G8 2002).

conserver les données relatives au trafic pendant de longues périodes, dans l'éventualité où ces données seraient nécessaires à la poursuite d'une enquête judiciaire. L'Algérie a même proposé de conserver les nom et adresse des clients des fournisseurs de services sur Internet ainsi que l'adresse des sites sur lesquels ils se rendent, mais cette pratique a par la suite été abandonnée. Les États-Unis n'ont pas encore adopté de semblables mesures.

Grâce à ces nouvelles orientations politiques, les Etats ont désormais la possibilité d'organiser la surveillance de masse des individus et de mettre en commun les données à caractère personnel. Dans le cadre d'une enquête judiciaire, la France et les États-Unis peuvent désormais échanger des données Internet recueillies par téléphones mobiles. Les adresses IP en interaction avec un serveur situé au Royaume-Uni sont systématiquement conservées par le fournisseur de services et remises aux pouvoirs publics britanniques moyennant un minimum d'autorisations légales ; ces autorisations sont encore plus limitées lorsque les données sont transmises à des gouvernements étrangers.

Le public ne semble pas avoir pris conscience de ces systèmes de surveillance de masse. Cependant, lorsque éclateront les premières affaires d'atteinte au droit d'auteur et que les pratiques d'un individu sur Internet pendant plusieurs années seront rendues publiques devant un tribunal pour prouver que cet individu a mis une chanson à la disposition des internautes du monde entier, et que les données liées à l'enquête seront remises à des plaignants aux États-Unis, alors seulement nous prendrons la mesure de la gravité catastrophique de la situation.

Ce n'est qu'alors peut-être que nous commencerons à nous demander si Internet et la société de l'information ont réellement la capacité d'être libres. La liberté d'expression pourrait fort s'en ressentir: si nous savons que notre fournisseur de services sur Internet a l'obligation de conserver nos communications dans ses archives pendant une période de temps prescrite par le gouvernement et que ces données peuvent être remises aux pouvoirs publics du pays ou même à des pays étrangers, nous serons moins enclins à accéder à certaines informations. Nous serons moins enclins à publier des informations si cela peut amener un gouvernement étranger à exiger que notre fournisseur de services local lui transmette les données personnelles et autres détails nous concernant ou même à nous poursuivre en justice devant des tribunaux étrangers. Nous serons moins enclins à participer à la société de l'information à cause des politiques élaborées pour la « sauver » qui « mettent au goût du jour » de vieilles lois et en adoptent de nouvelles pour mener les guerres d'aujourd'hui et protéger les chasses gardées d'hier.

# V.

# Recommandations pour les politiques de demain et les prochains Sommets mondiaux sur la société de l'information

Notre monde regorge de diversité. Les différentes sociétés ne considèrent pas de la même façon la liberté de parole et la vie privée, elles les réglementent diversement selon des objectifs et des desseins variés, et pour des résultats divers. Sur les conséquences de ces politiques, la réflexion fait cruellement défaut. Le monde ne converge pas nécessairement sur la destruction de la liberté d'expression; mais Internet n'est pas nécessairement non plus le grand libérateur, le moteur de la résistance à la censure, contrairement à ce que nous avions pu croire. Au fil des années, la censure sur Internet a pris des formes étonnantes. Lorsque la censure est associée aux nouveaux systèmes de surveillance, toutefois, on ne s'étonne plus, on s'alarme.

La « société de l'information » en tant qu'instrument de rhétorique a montré ses limites. Nous employions cette expression pour évoquer notre espoir de bâtir un monde nouveau où les technologies de l'information perfectionnées, en nous permettant d'aller plus loin, augmenteraient nos connaissances et nous aideraient à participer davantage. Ce rêve n'était pas fait pour devenir réalité ; les anciennes institutions et les vieilles pratiques sont indissociables.

Ces institutions comprennent les gouvernements et les milieux industriels. Les pratiques font référence à la censure des informations « obscènes » et « préjudiciables », aux œuvres protégées par le droit d'auteur, aux accusations de calomnie et de diffamation. Grâce à ces mécanismes et à ces techniques nouvelles, ils ont réussi à transformer l'infrastructure de la communication qui avait su susciter notre enthousiasme.

De prime abord on nous avait averti qu'il était impossible de réglementer une infrastructure telle qu'Internet, que cela exigeait une compétence transnationale. Sans faire grand cas de cet avertissement, les gouvernements ont entrepris d'édicter des lois pour censurer la liberté d'expression au sein de leur propre aire de compétence. On nous a ensuite averti que les réglementations fixées dans une juridiction pouvaient déborder du cadre des frontières et avoir des effets préjudiciables dans d'autres juridictions, ce qui était funeste non seulement pour Internet mais aussi pour les droits démocratiques des citoyens. On ne prêta pas plus d'importance à cet avertissement-là. On affirma qu'après tout Internet n'était pas un cas à part, qu'il y avait toujours eu des activités transnationales et qu'elles avaient toujours fait l'objet de réglementations.

D'autres initiatives suivirent. Les gouvernements tentèrent de régir Internet comme s'il s'agissait d'un moyen de diffusion afin d'y appliquer les mesures de contrôle réservées jusque-là à la télévision, exigèrent l'utilisation de mécanismes de filtrage défectueux qui surbloquent l'expression d'opinions politiques et sous-bloquent les informations visées. Lorsque cela les arrange, ils régissent Internet comme s'il s'agissait d'un opérateur téléphonique afin de pouvoir y appliquer les règles plus anciennes relatives à l'obligation d'installer des dispositifs de surveillance. Ils ont en outre « révisé » la législation relative au droit d'auteur, à la calomnie et à la diffamation afin de l'étendre aux nouvelles infrastructures de communication.

Résultat, cette infrastructure qui devait servir de fondation à une nouvelle société globale s'est muée en un environnement réglementé à la hâte et excessivement contrôlé. Ces réglementations et ces contrôles varient d'une ville à l'autre, d'un état à l'autre, d'une province à l'autre, ils varient selon les gouvernements et selon les secteurs industriels concernés. Les contrôles s'exercent en tous points de l'infrastructure, là où le pouvoir peut contrôler la circulation de l'information. On installe des mécanismes de filtrage et on assigne des responsabilités.

Là où les contrôles ne peuvent être efficaces, c'est la surveillance qui prend le relais. Aujourd'hui, on peut échanger des dossiers et s'exprimer mais lorsque les comportements en ligne sont dévoilés et que sont divulguées des communications datant de plusieurs mois ou de plusieurs années, comme l'exigent les politiques anti-terroristes, on sera sans doute moins enclin à effectuer des transactions par Internet. S'ils sont obligés de montrer une pièce d'identité ou qu'ils sont filmés lorsqu'ils utilisent des ordinateurs publics ou fréquentent des cybercafés, les individus seront amenés à modifier leurs comportements. Ce qui avait été salué comme une infrastructure propre à favoriser la diversité fait désormais partie d'une société qui a les moyens de normaliser les comportements.

Les Sommets mondiaux sur la société de l'information devraient s'attacher à rectifier ces problèmes plutôt que de mettre à la disposition des chefs d'État un podium d'où ils pourront annoncer les initiatives qu'ils prennent pour établir et soutenir leurs « sociétés de l'information » nationales, pendant qu'ils se rendent à d'autres réunions internationales plus importantes pour mettre en place des systèmes de surveillance internationaux. Il faudra travailler dur pour rétablir la liberté dans le nouveau monde que nous édifions. On dépense de l'énergie sans compter pour combattre le terrorisme et protéger le droit d'auteur. Nous ne prenons pas nos propres droits au sérieux.

Il reste beaucoup à faire. Il faut contester les choix politiques, abroger des lois, détruire et reconstruire. Certes, ce Sommet, organisé par l'un des gouvernements les plus répressifs de la planète, n'est pas le lieu idéal pour faire progresser de telles idées. C'est dès maintenant, pourtant, que nous pouvons nous mettre au

travail, et peut-être pouvons-nous commencer là où la situation est la plus désastreuse. À nous de reconstruire la « société de l'information » pour qu'elle représente quelque chose d'optimiste et de bon, afin de remplacer l'image de cynisme qu'elle reflète à présent. Nous pouvons briser les frontières de la circulation de l'information et des responsabilités juridiques, défaire les liens qui entravent nos droits et nous libérer des contraintes anciennes afin de rêver tout notre soûl.

## À propos de l'auteur

Gus Hosein est professeur invité auprès de Privacy International, conseiller auprès de l'American Civil Liberties Union et professeur invité à la London School of Economics and Political Science. Titulaire d'un B.Math en mathématiques appliquées de l'université de Waterloo et d'un doctorat en systèmes d'information de la LSE, il mène actuellement des recherches sur la politique internationale, l'élaboration des politiques anti-terroristes, ainsi que la protection de la vie privée et des données. Pour plus d'informations, consulter : http://is.lse.ac.uk/staff/hosein.

## Remerciements

Je tiens à remercier mes collègues de Privacy International, et plus particulièrement David Banisar, Simon Davies et Wendy Grossman, ainsi que mes collègues de GreenNet Educational Trust, notamment Karen Banks et Heather Ford. Je voudrais également remercier l'Open Society Institute pour le soutien apporté à la phase de recherches ainsi que le Social Science Research Council, qui a a soutenu la mise en place des fondations intellectuelles du présent rapport. Et enfin, je tiens à exprimer ma gratitude à l'UNESCO pour la valeur qu'elle accorde aux rapports produits dans ce domaine... y compris au mien.