DEFENDING FREEDOM
OF EXPRESSION AND INFORMATION

ARTICLE 19 Free Word Centre 60 Farringdon Road London EC1R 3GA
T +44 20 7324 2500 F +44 20 7490 0566
E info@article19.org W www.article19.org Tw @article19org facebook.com/article19org

ARTICLE 19

Liberté d'expression et TIC: aperçu des normes internationales

2013

Report

ARTICLE 19
Free Word Centre
60 Farringdon Road
London
EC1R 3GA
United Kingdom
T: +44 20 7324 2500
F: +44 20 7490 0566
E: info@article19.org
W: www.article19.org
Tw: @article19org
Fb: facebook.com/article19org

ISBN: 978-1-906586-61-4

This document has been published with support of the Adessium Foundation of The Netherlands, as part of their wider support for ARTICLE 19's work on freedom of expression and internet communications technology.

Table des matières

Remerciements

ARTICLE 19 est une organisation internationale des droits de l'homme fondée en 1986, qui défend et œuvre pour la promotion de la liberté d'expression et de la liberté d'information dans le monde entier. Elle tient son mandat de la Déclaration universelle des droits de l'homme, qui protège le droit à la liberté d'expression et d'information. Les nouvelles technologies de l'information et de la communication telles que l'Internet sont un moyen de plus en plus important de s'exprimer, de recevoir et répandre des informations. Par conséquent, ARTICLE 19 défend les libertés sur Internet depuis plus de 10 ans et agit pour l'évolution des politiques et des pratiques liées à la liberté d'expression sur Internet par le biais de notre réseau de partenaires, associés et contacts établis avec des experts. Nous avons également analysé diverses lois relatives à l'Internet, dont celles du Brésil, de la Bolivie, de la Russie, du Pakistan, de l'Iran, Irak, du Royaume-Uni, de la Tunisie et du Venezuela.

Ce rapport est publié avec le soutien de la Fondation Adessium des Pays-Bas, dans le cadre de son appui aux travaux d'ARTICLE 19 sur la liberté d'expression et les technologies de communication de l'Internet au Brésil, en Indonésie et en Tunisie.

Introduction

L'Internet et les nouvelles technologies de l'information et de la communication (TIC) font aujourd'hui partie intégrante de la vie quotidienne de nombreux individus dans le monde. Les TIC permettent à un nombre croissant de personnes de s'exprimer, améliorent la transparence et favorisent le débat public dans la société.

Cependant, les restrictions à la liberté d'expression en rapport avec les TIC se multiplient : de nombreuses signaux d'alerte montrent qu'un nombre croissant d'États tentent de resserrer leur emprise sur le flux croissant de l'information et la manière dont les personnes s'expriment en ligne.[1] De plus en plus, ce sont des acteurs du privé et des entreprises internationales qui sont les fournisseurs et les facilitateurs des nouvelles technologies de l'information et de la communication ; de ce fait, ils décident de la mesure dans laquelle les citoyens peuvent jouir du droit à la liberté d'expression.

Une question a émergé dans les nombreux débats autour de la protection de la liberté d'expression et des TIC : faut-il prévoir des lois et des traités spécifiques à l'Internet, spécialement conçus pour ce nouveau moyen de communication, ou les problèmes juridiques du Net doivent-ils être résolus dans le cadre de la législation et des normes internationales déjà existantes.

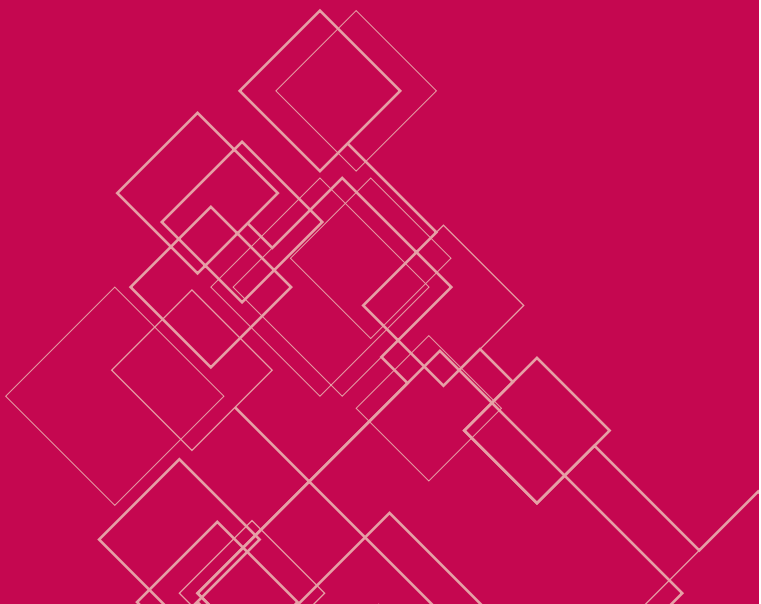
La première suggestion est fondée sur l'hypothèse que le flux mondial et décentralisé de l'information sur Internet et le cyberespace dans son ensemble ne peuvent être liés à une juridiction ou un État souverain précis. Il est également allégué que la mise en œuvre de lois existantes répond difficilement au volume du flux de données, à la recrudescence de la cybercriminalité et aux attaques contre l'infrastructure d'Internet. La seconde suggestion, soutenue par beaucoup d'organisations internationales des droits de l'homme, est fondée sur la présomption que l'Internet n'est qu'une plateforme de communication supplémentaire et non un monde virtuel distinct : par conséquent, ce sont les normes internationales existantes qui doivent être appliquées. Les règles juridiques existantes pour certains points comme le droit d'auteur, la diffamation et la protection de la vie privée, ont probablement besoin d'être revues pour respecter la nature et le rythme de l'ère numérique ; néanmoins, face à la peur suscitée par l'Internet chez certains gouvernements, de nouveaux standards internationaux risquent de diluer les normes des droits de l'homme existantes et de fragmenter et « nationaliser » l'Internet.

ARTICLE 19 soutient que le droit à la liberté d'expression n'était pas conçu pour être adapté à un média ou une technologie particulière. Qu'il soit exercé en ligne ou hors ligne, c'est un droit internationalement protégé que la quasi-totalité des pays se sont engagés à respecter.

Ce rapport présente un aperçu des principales normes internationales pertinentes en matière de protection du droit à la liberté d'expression en rapport avec les TIC. Il identifie les normes internationales et régionales relatives à la protection de sujets de préoccupation essentiels, comme l'accès à l'Internet et le contrôle de l'accès aux contenus en ligne, la réglementation des contenus, les droits des citoyens journalistes et des blogueurs, l'accès à l'information et les TIC et le cadre réglementaire de l'Internet.

Ce document a été conçu dans le but de mettre des ressources à disposition de toutes les personnes concernées par le libre exercice du droit à la liberté d'expression sur l'Internet, notamment les journalistes, fonctionnaires, juges, avocats et militants de la société civile.

Normes internationales relatives à la liberté d'expression et aux TIC



Principes fondamentaux de la liberté d'expression

L'Article 19 de la Déclaration universelle des droits de l'homme (DUDH)[2] garantit le droit à la liberté d'expression dans les termes suivants :

> Tout individu a droit à la liberté d'opinion et d'expression, ce qui implique le droit de ne pas être inquiété pour ses opinions et celui de chercher, de recevoir et de répandre, sans considérations de frontières, les informations et les idées par quelque moyen d'expression que ce soit.

En tant que résolution de l'Assemblée générale des Nations Unies, la DUDH n'est pas directement contraignante pour les États. Cependant, certaines dispositions, dont l'Article 19, sont généralement considérées comme ayant acquis une force juridique au titre du droit coutumier international depuis son adoption en 1948.[3]

Le Pacte international relatif aux droits civils et politiques (PIDCP) développe et donne une force juridique à un grand nombre de droits énoncés dans la DUDH.[4] Il garantit le droit à la liberté d'expression dans des termes similaires à ceux de l'Article 19 de la DUDH :

1 Nul ne peut être inquiété pour ses opinions.

2 Toute personne a droit à la liberté d'expression ; ce droit comprend la liberté de rechercher, de recevoir et de répandre des informations et des idées de toute espèce, sans considération de frontières, sous une forme orale, écrite, imprimée ou artistique ou par tout autre moyen de son choix.

En septembre 2011, le Comité des droits de l'homme des Nations Unies (CDH), organe de surveillance de l'application du PIDCP, a publié l'Observation générale N° 34 relative à l'Article 19 du PIDCP.[5] L'Observation générale N° 34 est une interprétation des normes minimales garanties par l'Article 19 du PIDCP, qui fait autorité. Elle est particulièrement instructive sur un grand nombre de problèmes liés à la liberté d'expression sur l'Internet.

Il est important de souligner que l'Observation générale N° 34 stipule que l'Article 19 du PIDCP protège toutes les formes d'expression et les moyens de sa dissémination, y compris toutes les formes d'expression électroniques et fondées sur l'Internet.[6] En d'autres termes, la protection de la liberté d'expression s'applique en ligne de la même manière qu'elle s'applique hors ligne.

Dans le même temps, l'Observation générale N° 34 impose aux Etats parties au PIDCP de considérer la mesure dans laquelle l'évolution des nouvelles technologies de l'information, notamment des systèmes électroniques de dissémination de l'information fondés sur la téléphonie mobile et Internet, a totalement transformé les pratiques de communication dans le monde.[7] En particulier, elle stipule que le cadre réglementaire des mass média doit tenir compte des différences entre les médias imprimés et audiovisuels et l'Internet, tout en notant la manière dont ils convergent.[8]

En juin 2012, le Conseil des droits de l'homme a adopté à l'unanimité la Résolution sur la promotion, la protection et l'exercice des droits de l'homme sur l'Internet, qui affirme que:

> Les droits dont les personnes jouissent hors ligne doivent être également protégés en ligne, en particulier le droit de toute personne à la liberté d'expression qui est applicable sans considération de frontières et par le moyen de son choix, conformément aux articles 19 de la Déclaration universelle des droits de l'homme et du Pacte international relatif aux droits civils et politiques.[9]

En mai 2011, dans son rapport au Conseil des droits de l'homme, le Rapporteur spécial de l'ONU pour la promotion et la protection du droit à la liberté d'opinion et d'expression Frank La Rue soulignait que :

> Le cadre du droit international relatif aux droits de l'homme, en particulier les dispositions relatives au droit à la liberté d'expression, demeure pertinent et continue de s'appliquer à l'Internet. De fait, les articles 19 de la Déclaration universelle des droits de l'homme et du Pacte international relatif aux droits civils et politique (…) ont été rédigés dans la perspective des innovations technologiques futures qui pourraient servir à l'exercice de ce droit et en tenant compte de cette éventualité.[10]

De même, dans leur Déclaration conjointe sur la liberté d'expression et l'Internet de juin 2011[11], les quatre mandataires spéciaux pour la protection de la liberté d'expression ont mis l'accent sur le fait que les approches réglementaires dans les secteurs des télécommunications et de l'audiovisuel ne pouvaient s'applier à l'Internet. En particulier, ils recommandent l'élaboration d'approches adéquates pour répondre aux contenus illégaux en ligne, et soulignent que des restrictions spécifiques aux contenus disséminés sur l'Internet ne sont pas nécessaires.[12] Ils promeuvent également l'usage de l'autoréglementation comme outil effectif dans les réparations prévues pour les discours diffamatoires.[13]

Restrictions du droit à la liberté d'expression

Bien que la liberté d'expression soit un droit fondamental, elle n'est pas garantie dans des termes absolus.

L'Article 19(3) du PIDCP permet de restreindre ce droit aux conditions suivantes :

> 3. L'exercice des libertés prévues au paragraphe 2 du présent article comporte des devoirs spéciaux et des responsabilités spéciales. Il peut en conséquence être soumis à certaines restrictions qui doivent toutefois être expressément fixées par la loi et qui sont nécessaires:
>
> (a) Au respect des droits ou de la réputation d'autrui;
>
> (b) À la sauvegarde de la sécurité nationale, de l'ordre public, de la santé ou de la moralité publiques.

Les restrictions du droit à la liberté d'expression doivent être définies de manière stricte et précise et ne doivent pas mettre en danger le droit lui-même. Pour savoir quand une restriction est définie de manière précise, il faut généralement appliquer un triple test. Ainsi, une restriction doit : (i) être fixée par la loi ; (ii) viser un objectif légitime ; et (iii) répondre aux tests stricts de nécessité et de proportionnalité.[14]

- Prévue par la loi : L'Article 19(3) du PIDCP exige que les restrictions du droit à la liberté d'expression soient fixées par la loi. En particulier, la loi doit être formulée avec suffisamment de précision pour permettre à un individu d'adapter sa conduite en conséquence.[15] Les restrictions ambiguës ou trop vastes ne sont donc pas autorisées en vertu de l'Article 19(3).
- Viser un objectif légitime : Les entraves au droit à la liberté d'expression doivent poursuivre un des objectifs légitimes énoncés à l'Article 19(3) (a) et (b) du PIDCP. Ainsi, il serait impossible d'interdire à des systèmes de diffusion de l'information de publier des contenus uniquement au motif qu'ils sont critiques à l'égard du gouvernement ou du système politique et social auquel adhère le gouvernement.[16] De même, une restriction à la liberté d'expression ne peut servir à protéger le gouvernement de l'embarras ou d'une dénonciation de conduites illicites, à dissimuler des informations sur le fonctionnement des institutions publiques ou à consolider une idéologie particulière.
- Répondre aux tests stricts de nécessité et de proportionnalité : Les Etats parties au PIDCP sont dans l'obligation d'assurer que toutes les restrictions légitimes au droit à la liberté d'expression sont nécessaires et proportionnées. Par nécessité, il faut entendre qu'il y a un besoin social pressant de la restreindre. La partie qui demande la restriction doit démontrer un lien direct et immédiat entre l'expression et l'intérêt protégé. Par proportionnalité, il faut entendre que la mesure la moins restrictive doit être appliquée si elle peut avoir le même effet qu'une mesure plus restrictive.

Les mêmes principes s'appliquent aux moyens électroniques de communication ou d'expression disséminées par le biais de l'Internet. En particulier, le Comité des droits de l'homme des Nations Unies a stipulé dans son Observation générale N° 34 que :

> 43. Toute restriction imposée au fonctionnement des sites Web, des blogs et de tout autre système de diffusion de l'information par le biais de l'Internet, de moyens électroniques ou autres, y compris les systèmes d'appui connexes à ces moyens de communication, comme les fournisseurs d'accès à Internet ou les moteurs de recherche, n'est licite que dans la mesure où elle est compatible avec le paragraphe 3. Les restrictions licites devraient d'une manière générale viser un contenu spécifique ; les interdictions générales de fonctionnement frappant certains sites et systèmes ne sont pas compatibles avec le paragraphe 3. Interdire à un site ou à un système de diffusion de l'information de publier un contenu uniquement au motif qu'il peut être critique à l'égard du gouvernement ou du système politique et social épousé par le gouvernement est tout aussi incompatible avec le paragraphe 3.[17]

Ces principes ont été approuvés par le Rapporteur spécial de l'ONU pour la promotion et la protection du droit à la liberté d'opinion et d'expression Frank La Rue dans son rapport 2011, où il clarifiait l'étendue des restrictions légitimes pour différents types d'expression en ligne.[18]

Normes régionales

De nombreux instruments régionaux protègent également le droit à la liberté d'expression et d'information.

L'Article 9 de la Charte africaine des droits de l'homme et des peuples (« Charte africaine »)[19] protège le droit à la liberté d'expression dans les termes suivants :

1 Toute personne a droit à l'information.

2 Toute personne a le droit d'exprimer et de diffuser ses opinions dans le cadre des lois et règlements.

La Commission africaine des droits de l'homme et des peuples (« Commission africaine ») a explicité l'Article 9 de la Charte africaine en octobre 2002 en adoptant la Déclaration de Principes sur la liberté d'expression en Afrique (« Déclaration africaine »).[20] Dans son Article 1, cette déclaration stipule que:

1 La liberté d'expression et d'information, y compris le droit de chercher, de recevoir et de communiquer des informations et idées de toute sorte, oralement, par écrit ou par impression, sous forme artistique ou sous toute autre forme de communication, y compris à travers les frontières, est un droit fondamental et inaliénable et un élément indispensable de la démocratie.

2 Tout individu doit avoir une chance égale pour exercer le droit à la liberté d'expression et à l'accès à l'information, sans discrimination aucune.

La Déclaration américaine des droits et devoirs de l'homme[21], adoptée par l'Organisation des Etats américains (OEA) en 1948, stipule dans son Article IV:

> Toute personne a droit à la liberté d'investigation, d'opinion, d'expression et de diffusion de la pensée par n'importe quel moyen.

L'Article 13 de la Convention américaine des droits de l'homme[22] va plus loin en prévoyant une obligation positive pour les Etats et en incluant une interdiction de la censure et de restrictions « indirectes »:

1 Toute personne a droit à la liberté de pensée et d'expression; ce droit comprend la liberté de rechercher, de recevoir et de répandre des informations et des idées de toute espèce, sans considération de frontières, que ce soit oralement ou par écrit, sous une forme imprimée ou artistique, ou par tout autre moyen de son choix.

2 L'exercice du droit prévu au paragraphe précédent ne peut être soumis à aucune censure préalable, mais il comporte des responsabilités ultérieures qui, expressément fixées par la loi, sont nécessaires:

   (a) Au respect des droits ou à la réputation d'autrui; ou

   (b) à la sauvegarde de la sécurité nationale, de l'ordre public, ou de la santé ou de la morale publiques.

3 La liberté d'expression ne peut être restreinte par des voies ou des moyens indirects, notamment par les monopoles d'Etat ou privés sur le papier journal, les fréquences radioélectriques, les outils ou le matériel de diffusion, ou par toute autre mesure visant à entraver la communication et la circulation des idées et des opinions.

La Déclaration interaméricaine de principes sur la liberté d'expression, un document de base pour interpréter l'Article 13 de la Convention américaine, fait clairement référence aux nouvelles technologies dans le langage et l'esprit du Principe 5:

> La censure préalable, l'interférence ou la pression directe ou indirecte sur toute forme d'expression, opinion ou information diffusée par tout moyen de communication oral, écrit, artistique, visuel ou électronique, doivent être interdits par la loi. Les restrictions à la libre circulation des idées et des opinions, ainsi que l'imposition arbitraire d'information et la création d'obstacles au libre flux de l'information, violent le droit à la liberté d'expression.[23]

En Asie, la Déclaration des droits de l'homme de l'ASEAN de novembre 2012, qui n'est pas juridiquement contraignante, reprend les termes de l'Article 23 du PIDCP, et stipule :

> Toute personne a droit à la liberté d'opinion et d'expression, y compris la liberté d'exprimer des opinions sans interférence et de chercher, recevoir et répandre des informations, que ce soit sous forme orale, sous forme écrite ou par tout autre moyen de son choix.[24]

Cependant, la Déclaration de l'ASEAN dans son ensemble reste en-deçà des normes internationales relatives aux droits de l'homme.

La Charte arabe des droits de l'homme (« Charte arabe »), adoptée par le Conseil de la Ligue des Etats arabes en 2004, vise à affirmer les principes de la DUDH et du PIDCP, ainsi que du Pacte international relatif aux droits économiques, sociaux et culturels, de la Charte des Nations Unies et de la Déclaration du Caire des droits de l'homme en Islam.[25]

Bien que la Charte arabe prévoie des protections moins solides de certains droits fondamentaux, l'Article 32 de la Charte arabe révisée protège la liberté d'expression dans les termes suivants :

1 La présente charte garantit le droit à l'information et la liberté d'opinion et d'expression, et le droit de rechercher, de recevoir et de répandre des informations par tout moyen, sans considération de frontières géographiques.

2 Ces droits et libertés sont exercés dans le cadre des principes fondamentaux de la société et sont soumis aux seules restrictions nécessaires au respect des droits et de la réputation d'autrui et à la sauvegarde de la sécurité nationale, de l'ordre public, de la santé publique ou de la moralité publique.

Il est important de noter que même ce texte controversé protège expressément le droit à la liberté d'expression et le droit à la liberté d'information.

L'Article 10 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales[26] stipule que :

1 Toute personne a droit à la liberté d'expression. Ce droit comprend la liberté d'opinion et la liberté de recevoir ou de communiquer des informations ou des idées sans qu'il puisse y avoir ingérence d'autorités publiques et sans considération de frontière. Le présent article n'empêche pas les Etats de soumettre les entreprises de radiodiffusion, de cinéma ou de télévision à un régime d'autorisations.

2 L'exercice de ces libertés comportant des devoirs et des responsabilités peut être soumis à certaines formalités, conditions, restrictions ou sanctions prévues par la loi, qui constituent des mesures nécessaires, dans une société démocratique, à la sécurité nationale, à l'intégrité territoriale ou à la sûreté publique, à la défense de l'ordre et à la prévention du crime, à la protection de la santé ou de la morale, à la protection de la réputation ou des droits d'autrui, pour empêcher la divulgation d'informations confidentielles ou pour garantir l'autorité et l'impartialité du pouvoir judiciaire.

Par ailleurs, l'Article 11 de la Charte des droits fondamentaux de l'Union européenne (« Charte européenne »)[27] s'inspire principalement de la formulation de l'Article 19 du PIDCP.

Il convient de souligner qu'au Conseil de l'Europe, le Comité des ministres a récemment adopté deux recommandations relative à la liberté sur l'Internet : la Recommandation sur une nouvelle conception des médias[28] et la Recommandation sur la protection et la promotion de l'universalité, de l'intégrité et de l'ouverture de l'Internet.[29]

La jurisprudence internationale et l'adoption d'instruments internationaux des droits de l'homme contraignants en rapport avec la liberté d'expression dans le contexte des TIC ont été relativement lents en comparaison du rythme auquel Internet s'est répandu et développé.[30] Toutefois, durant ces deux dernières années, plusieurs décisions importantes ont été prises par la Cour européenne des droits de l'homme et la Cour de justice de l'Union européenne.[31]

Accès à l'Internet

Accès universel à l'Internet

– L'accès à l'Internet est essentiel à l'exercice du droit à la liberté d'expression et d'autres droits à l'ère du numérique. On a observé qu'en l'absence de moyens de connexion ou sans connexion abordable, le droit à la liberté d'expression et la liberté des médias devenaient insignifiants dans l'univers en ligne.[32]

– Bien qu'il ne soit pas considéré comme un droit humain en soi par la législation internationale, le droit à l'accès universel à l'Internet a été mentionné ou évoqué dans plusieurs documents. Par exemple :

– La Déclaration de Principes du Sommet mondial 2003 sur la société de l'information (SMSI) stipule que la « communication est un processus social fondamental, un besoin essentiel de l'être humain et la base de toute organisation sociale. Elle est le pivot de la société de l'information. Toute personne, où que ce soit dans le monde, devrait avoir la possibilité de participer à la société de l'information et nul ne devrait être privé des avantages qu'elle offre ».[33]

– L'Observation générale N° 34 appelle les Etats parties à prendre toutes les mesures nécessaires pour favoriser l'indépendance des technologies de l'information et de la communication comme Internet et les systèmes de diffusion électronique de l'information utilisant la technologie mobile et de garantir l'accès des particuliers à ces derniers.[34]

– Le Rapport 2011 du Rapporteur spécial des Nations Unies pour la promotion et la protection de la liberté d'expression appelle les Etats parties à garantir que l'accès à l'Internet est maintenu en permanence, y compris durant des périodes d'agitation politique.[35] Le Rapporteur spécial a également distingué deux « dimensions » de ce thème : l'accès au contenu en ligne et l'accès à l'infrastructure et aux technologies de l'information et de la communication comme les câbles, modems, ordinateurs et logiciels, pour accéder à l'Internet en premier lieu.[36] Il a souligné que l'accès à l'infrastructure ainsi que la garantie d'un accès universel à l'Internet doivent être une priorité pour tous les Etats. Chaque pays doit ainsi élaborer une politique concrète et effective, en consultation avec des individus appartenant à tous les secteurs de la société, y compris le secteur privé et les ministères d'Etat pertinents, pour rendre l'Internet largement disponible, accessible et abordable pour toutes les fractions de la population.[37]

– La Déclaration conjointe 2011 des quatre mandataires spéciaux sur la liberté d'expression a souligné que les Etats ont l'obligation positive de faciliter l'accès universel à l'Internet et que la réalisation du droit à la liberté d'expression impose aux Etats l'obligation de promouvoir un accès universel à l'Internet.[38]

– Certaines législations nationales considèrent l'accès à l'Internet comme un droit humain fondamental ou comme une partie intégrante du droit fondamental à la liberté d'expression.[39] Les Etats qui garantissent le droit d'accès à l'Internet dans le cadre de leur législation nationale incluent la Grèce,[40] l'Estonie,[41] la France,[42] la Finlande,[43] l'Espagne[44] et le Costa Rica.[45]

Neutralité du Net

Le principe de « neutralité du réseau » ou « neutralité du Net » est un composant important du droit d'accès à l'Internet. Il protège le droit d'accès au contenu, aux applications, services et équipements d'Internet selon son choix individuel. Il oblige les FAI et les gouvernements à traiter tout le trafic et les données d'Internet sur un pied d'égalité, sans discrimination, et quelle que soit la nature de l'expéditeur, de l'utilisateur, du type de donnée, de contenu et de plateforme. Il est également interdit aux FAI et aux gouvernements d'accorder la priorité à la transmission de données, de bloquer des contenus sur Internet, ou de ralentir l'accès à certaines applications ou certains services.

La « neutralité de la plateforme » est une sous-catégorie de la neutralité du Net qui permet aux utilisateurs d'avoir un accès complet à toutes les caractéristiques et tous les sites Internet sous la même forme, quel que soit l'équipement utilisé pour se connecter au web.

Les défenseurs de la neutralité du Net soutiennent qu'elle est cruciale pour garantir le droit à la liberté d'expression, la préservation de la libre circulation de l'information et des idées et pour éviter la création d'une pénurie artificielle. En revanche, ses détracteurs considèrent qu'elle a un impact négatif sur la qualité des services dans la mesure où des prestations différentes requièrent un traitement différent de leur transmission.

Un débat approfondi a eu lieu sur la pertinence de la neutralité du Net et la manière dont elle doit être imposée par la législation, sachant que des approches fondées sur l'autorégulation se sont révélées inexploitables.[46] Il a été également allégué que la plupart des législations nationales étaient incapables de mettre un frein à des discriminations contre certains types de contenus sur l'Internet.[47]

La neutralité du Net n'est pas encore une norme consacrée par la législation internationale. Cependant, la Déclaration conjointe 2011 sur la liberté d'expression et l'Internet des quatre rapporteurs spéciaux recommandait que :

> Doit être interdite toute discrimination dans le traitement des données et le trafic sur Internet fondée sur un terminal, contenu, auteur, origine et/ou destination du contenu, un service ou une application.
>
> Les intermédiaires d'Internet sont tenus de garantir la transparence dans la gestion du trafic ou de l'information, et des informations pertinentes sur cette gestion doivent être mises à disposition des parties prenantes sous une forme accessible.[48]

En Europe, il y a eu quelques tentatives limitées de garantir à tous les utilisateurs un accès égal à l'Internet, notamment :

- Les conclusions du Conseil de l'Europe sur l'ouverture et la neutralité du Net en Europe, qui invitent les Etats membres à « favoriser l'application du principe de la neutralité du Net ».[49]
- Des résolutions non législatives votées par le Parlement européen où ce dernier appelle à une gestion transparente du trafic sur l'Internet. Il demande également à la Commission européenne de veiller à ce que des fournisseurs de services Internet

ne puissent bloquer, défavoriser, affecter ou affaiblir la capacité de chacun à utiliser un service en vue d'accéder à tout contenu, application ou service mis à disposition via Internet, de l'utiliser, de le transmettre, de le poster, de le recevoir ou de le proposer, quelle qu'en soit la source ou la cible;[50] de proposer des lois pour garantir la neutralité d'Internet[51] et de codifier de principe de neutralité de l'Internet par le biais d'une réglementation appropriée.[52]

En outre, plusieurs Etats ont adopté une législation nationale sur la neutralité d'Internet, dont notamment le Chili,[53] les Pays-Bas,[54] la Slovénie[55] et les Etats-Unis.[56]

Protocoles des « trois coups » et déconnexion

Les « trois-coups » sont des protocoles ou lois adoptés dans plusieurs pays[57] en vue de réduire le téléchargement illicite. En règle générale, les utilisateurs reçoivent trois avertissements en cas d'infraction supposée au droit d'auteur. Les récidivistes risquent des sanctions telles que la réduction de leur débit, le blocage de protocoles, la suspension de compte ou la déconnexion pure et simple d'Internet.

La sanction la plus sévère – la déconnexion d'Internet – a été récemment considérée comme très disproportionnée dans la mesure où l'application du droit d'auteur prend le dessus sur l'exercice du droit fondamental à la liberté d'expresison et du droit à la protection de la vie privée. Sachant que les adresses IP ne peuvent pas toujours être attribuées à un utilisateur particulier ou peuvent être facilement manipulées, des mesures de ce type suscitent aussi des préoccupations sur leur proportionnalité et la présomption d'innocence. Par exemple :

– Dans son rapport de 2011, le Rapporteur spécial des Nations Unies a jugé que la suspension de l'accès à Internet, quel que soit le motif invoqué, y compris lorsqu'il y a violation des lois sur le droit à la propriété intellectuelle, était disproportionnée et constituait une violation du droit à la liberté d'expression. Il a exhorté les Etats à abroger ou amender les lois existantes sur la propriété intellectuelle qui permettent de couper l'accès des utilisateurs à l'Internet, et à s'abstenir d'adopter de telles lois."[58]

– Dans leur Déclaration conjointe 2011, les quatre rapporteurs spéciaux pour la liberté d'expression ont affirmé que « la sanction consistant à suspendre l'accès à Internet est une mesure extrême qui ne peut se justifier que si des mesures moins restrictives ne sont pas disponibles ou que la suspension a été ordonnée par un tribunal, en tenant compte de l'impact de cette mesure sur la jouissance des droits humains."[59]

Les mesures dites des « trois-coups » sont aussi problématiques sur le plan des droits de l'homme dans la mesure où elles imposent aux FAI de contrôler ou filtrer le comportement en ligne de leurs utilisateurs, et par conséquent de s'ingérer dans la vie privée. A cet égard, la Cour de justice européenne a jugé que le contrôle, le filtrage et le blocage de systèmes installés par les FAI ou les réseaux sociaux en vue d'empêcher des infractions à la propriété intellectuelle sont disproportionnés et contraires aux droits humains fondamentaux, en particulier les droits à la vie privée et à la liberté d'information.[60]

Contrôle de l’accès aux contenus en ligne

Blocage, filtrage et suppression de contenu

La décision de bloquer, filtrer ou suspendre un contenu constitue une forme grave de censure qui est largement utilisée par des gouvernements, des administrations nationales et des FAI pour gérer des contenus indésirables ou controversés.

Ces mesures reposent souvent sur une base discutable en l'absence de législation nationale. La décision de bloquer, filtrer ou supprimer un contenu résulte rarement d'une procédure régulière et n'est pas nécessairement prise par des tribunaux indépendants ou des organes juridictionnels.[61] Ces mesures sont également faciles à imposer dans la mesure où de nombreux Etats considèrent les prestataires intermédiaires comme responsables. Par ailleurs, on a observé que les politiques de blocage étaient inefficaces, compte tenu de la réapparition rapide et du contournement facile de contenus bloqués ou filtrés, ainsi que de la charge financière que représentent les systèmes de blocage pour les FAI et les consommateurs.[62]

Compatibilité avec le droit à la liberté d'expression

Le caractère problématique de ces mesures a été souligné par les quatre rapporteurs spéciaux dans leur Déclaration conjointe de 2011 où ils affirmaient que :

- Le blocage obligatoire de sites entiers, adresses IP, ports, protocoles réseaux ou types d'usage (comme les réseaux sociaux) est une mesure extrême – analogue à l'interdiction d'un journal ou d'un radiodiffuseur – qui ne peut être justifiée que si elle est conforme aux normes internationales, par exemple si elle est nécessaire pour protéger les enfants des abus sexuels.
- Les systèmes de filtrage de contenus imposés par un gouvernement ou un fournisseur de service commercial qui ne sont pas contrôlés par les utilisateurs finaux constituent une forme de censure préalable et ne peuvent justifier une restriction de la liberté d'expression.
- Les produits conçus pour faciliter le filtrage de données par les utilisateurs finaux doivent être accompagnés d'informations claires sur leur fonctionnement et leurs écueils potentiels en termes de filtrage abusif.[63]

A l'échelon régional, plusieurs organes européens ont pris position sur la compatibilité de ces mesures avec les normes relatives aux droits de l'homme. En 2012, la Cour européenne des droits de l'homme[64] a affirmé que le blocage était compatible avec la Convention européenne uniquement lorsqu'un cadre juridique strict était en place, qui réglementait son étendue et offrait la garantie d'un examen judiciaire pour empêcher d'éventuels abus. La Cour européenne a également souligné que la protection du droit à la liberté d'expression s'appliquait non seulement au contenu d'une expression mais aussi aux moyens de sa diffusion et que le droit à la liberté d'expression s'appliquait « sans considération de frontières ».

Procédure régulière

Le non-respect des normes de procédure régulière semble être l'un des problèmes majeurs des mesures de blocage et de filtrage. En particulier, il a été souligné que les gouvernements et les FAI prenaient des décisions de manière non transparente et que des mécanismes de réparation efficaces, opportuns et indépendants étaient largement indisponibles.

Le Rapporteur spécial des Nations Unies pour la promotion de la liberté d'expression a insisté sur le fait que :

> Toute demande soumise à des prestataires intermédiaires pour empêcher l'accès à certains contenus, ou divulguer des informations personnelles dans un but strictement limité tel que l'administration de la justice pénale, doit être faite sous forme d'un ordre prononcé par un tribunal ou un organe compétent indépendant de toute pression politique, commerciale ou de toute autre influence injustifiée.[65]

Au niveau régional, deux Recommandations sur la protection des droits de l'homme dans le contexte des moteurs de recherche et dans le cadre des services de réseaux sociaux comprennent des dispositions sur le droit à une procédure régulière, notamment dans le contexte de mécanismes d'autorégulation. Dans ces recommandations, le Comité des ministres demande aux Etats parties de :

> Assurer la promotion de mécanismes d'autorégulation et de co-régulation transparents pour les moteurs de recherche, notamment en ce qui concerne l'accessibilité des contenus déclarés illicites par un tribunal ou une autorité compétente, et de ceux qui sont préjudiciables, en tenant compte des normes du Conseil de l'Europe en matière de protection de la liberté d'expression et de droits à une procédure régulière.
>
> Veiller à ce que toute loi, règle ou demande individuelle relative à la désindexation ou au filtrage de contenus respecte pleinement les dispositions juridiques pertinentes, le droit à la liberté d'expression et le droit de rechercher, de recevoir et de communiquer des informations. Les principes du droit à une procédure régulière et de l'accès à des mécanismes de réparation indépendants, ainsi qu'à des mécanismes prévoyant l'obligation de rendre compte devraient également être respectés dans ce contexte.[66]

Il a également affirmé que:

> Il est important que ces mécanismes respectent les garanties procédurales, conformément au droit à être entendu et au droit de contester ou faire appel des décisions rendues, y compris lorsque cela s'avère nécessaire, au droit à un procès équitable, dans un délai raisonnable, à commencer par la présomption d'innocence.[67]

Saisie de noms de domaine ou suspension

La saisie de noms de domaine ou la suspension d'un site est une autre mesure extrême qui s'avère problématique sur le plan des droits de l'homme. Si les conséquences du blocage d'un nom de domaine sont restreintes à une juridiction et un Etat particulier, la saisie d'un nom de domaine affecte les contenus respectifs dans le monde entier. Les principales préoccupations concernant la compatibilité de ces mesures avec les normes des droits de l'homme comprennent la nature disproportionnée de ces sanctions : si la saisie d'un nom de domaine peut viser un objectif légitime, par exemple protéger les enfants et les mineurs, elle conduit souvent au blocage de contenus licites.[68]

De plus, des mesures sont appliquées en l'absence de garantie de procédure régulière, avec peu ou aucun contrôle judiciaire. Il a été observé que les injonctions des tribunaux autorisant la saisie de noms de domaine reposent sur des déclarations sous serment ex parte, signifiant que seul le gouvernement présente des preuves et les opérateurs Internet n'ont aucune possibilité d'être entendus ou de répondre à des allégations jusqu'à ce que leurs sites soient fermés.[69]

Responsabilité des intermédiaires/responsabilité du contenu provenant d'un tiers

Les prestataires intermédiaires d'Internet – tels que les fournisseurs de services Internet, les moteurs de recherche et les plateformes de réseaux sociaux – jouent un rôle crucial en permettant à des personnes du monde entier de communiquer entre elles. En raison de leurs capacités techniques, les prestataires intermédiaires d'Internet font l'objet d'une pression croissante de la part des gouvernements et des groupes d'intérêts pour contrôler les contenus en ligne.

Usant de méthodes variées,[70] un nombre croissant de gouvernements a commencé à recourir à des intermédiaires – et dans certains cas à les forcer – pour supprimer ou bloquer l'accès des citoyens à des contenus qu'ils jugent illégaux ou « préjudiciables ».[71] Si certaines de ces restrictions sont appliquées directement par une autorité de régulation étatique,[72] beaucoup d'Etats ont adopté des régimes juridiques de responsabilité civile qui ont forcé efficacement des intermédiaires à surveiller des aspects d'Internet pour le compte de l'Etat.[73]

Le fait de soumettre les FAI à une obligation de responsabilité en tant qu'intermédiaires pose problème du point de vue de la liberté d'expression. Fondamentalement, cela confère aux prestataires intermédiaires un pouvoir quasi judiciaire de juger de la légalité d'un contenu. Toutefois, les fournisseurs de services sont non seulement mal équipés et manquent de légitimité pour jouer un tel rôle, mais ils ne sont pas non plus soumis aux garanties de procédure régulière, et tenus de prendre des décisions transparentes ou d'offrir des mécanismes de réparation indépendants.

Dans son rapport 2011, le Rapporteur spécial pour la liberté d'expression a critiqué ces systèmes de responsabilité des intermédiaires, et souligné l'absence de mécanismes de réparation, le risque d'autocensure des intermédiaires et le fait que des organismes privés sont mal placés pour maintenir un équilibre entre les différents droit humains fondamentaux lorsqu'une décision de suppression de contenu est prise :

> 42. Alors que le système de notification et retrait est un moyen d'empêcher des prestataires intermédiaires de se livrer activement à des pratiques illicites sur leurs services ou de les encourager, il peut faire l'objet d'abus à la fois de la part des Etats et des acteurs privés. Les utilisateurs qui se voient notifier par un fournisseur de services que leur contenu a été signalé comme illicite disposent souvent de faibles recours ou de ressources insuffisantes pour s'opposer au retrait. Par ailleurs, étant donné que les intermédiaires peuvent encore être tenus responsables financièrement, et dans certains cas pénalement, du non-retrait d'un contenu après réception de la notification par les utilisateurs, ils restent prudents et tendent à privilégier la sécurité en censurant exagérément des contenus potentiellement illicites. Le manque de transparence qui prévaut dans le processus de prise de décision des intermédiaires masque souvent des pratiques discriminatoires ou des pressions politiques qui affectent les décisions prises par les sociétés. Par ailleurs, en tant qu'entités privées, les intermédiaires ne sont pas le mieux placés pour déterminer si un contenu particulier est illicite ou non, car cela requiert un équilibre adéquat entre des intérêts divergents et un examen des défenses.[74]

Le Rapporteur spécial des Nations Unies a donc recommandé d'appliquer les mesures suivantes pour remédier à ces problèmes.

- Les mesures de censure ne doivent jamais être déléguées à des entités privées, et les prestataires intermédiaires ne doivent pas être tenus responsables du fait qu'ils ne prennent pas de mesures qui portent atteinte aux droits humains des individus.
- Toute demande soumise à des prestataires intermédiaires pour empêcher l'accès à certains contenus, ou pour divulguer des informations personnelles dans un but strictement limité tel que l'administration de la justice pénale, doit être faite par ordonnance d'un tribunal ou d'un organe compétent indépendant de toute pression politique, commerciale ou autre influence injustifiée.
- Les entreprises doivent agir avec diligence afin d'éviter les infractions aux droits des individus.
- Les entreprises doivent mettre en place des conditions générales d'utilisation claires dénuées d'ambiguïté, conformément aux normes et aux principes des droits de l'homme, et doivent examiner en permanence l'impact de leurs services et technologies sur le droit à la liberté d'expression de leurs utilisateurs, ainsi que sur les problèmes potentiels susceptibles de se poser quand ils font l'objet d'abus.
- Les prestataires intermédiaires ne doivent mettre en place des restrictions aux droits fondamentaux qu'à la suite d'une intervention judiciaire, et doivent être transparents pour l'utilisateur concerné – et le cas échéant pour le grand public – sur les mesures prises.
- Les prestataires intermédiaires doivent avertir les utilisateurs avant de mettre en place des mesures de restriction, et doivent limiter l'impact des restrictions au seul contenu concerné.
- Les fournisseurs de services doivent divulguer des informations détaillées sur les demandes de suppression de contenus et l'accessibilité à des sites.
- Des réparations efficaces doivent être mises à disposition des utilisateurs touchés, notamment la possibilité de faire appel par le biais de procédures prévues par le prestataire de services et par une autorité judiciaire compétente.[75]

Dans leur Déclaration conjointe 2005, les quatre Rapporteurs spéciaux pour la liberté d'expression ont affirmé que :

> Nul ne doit être tenu responsable de contenus sur Internet dont il n'est pas l'auteur, sauf s'il y adhère ou refuse d'obtempérer à une injonction des tribunaux ordonnant le retrait des contenus incriminés.[76]

La Déclaration conjointe 2011 réitère cette position et inclut une recommandation sur le non-contrôle :

(a) Les simples fournisseurs de services comme l'accès, la recherche, la transmission ou le stockage automatique, intermédiaire et temporaire de l'information (caching) ne doivent pas être tenus responsables de contenus produits par des tiers et disséminés par le biais de leurs services, à moins qu'ils ne soient intervenus dans le contenu concerné ou qu'ils aient refusé d'obéir à une injonction de retrait d'un tribunal, quand ils ont la capacité de le faire (« principe du simple transport »).

(b) Il convient d'envisager d'exempter d'autres prestataires intermédiaires, y compris ceux mentionnés dans le préambule, de toute responsabilité pour des contenus produits par des tiers dans les mêmes conditions qu'au paragraphe 2(a). Au minimum, les prestataires intermédiaires ne doivent pas être tenus de contrôler les contenus créés par les internautes ni être soumis à des règles extrajudiciaires de suppression de contenus qui ne garantissent pas une protection suffisante de la liberté d'expression (ce qui est le cas de nombreux systèmes de « notification et retrait » actuellement en place).[77]

Au niveau régional, la Déclaration sur la liberté de communication sur l'Internet [78] du Conseil de l'Europe, conforme à la Directive européenne sur le commerce électronique,[79] exempte généralement les prestataires intermédiaires de responsabilité et appelle les Etats parties à « ne pas imposer aux fournisseurs de services l'obligation générale de surveiller les contenus diffusés sur l'Internet auxquels ils donnent accès, qu'ils transmettent ou qu'ils stockent, ni celle de rechercher activement des faits ou des circonstances révélant des activités illicites » dans la mesure où cela pourrait avoir un impact sur le droit à la liberté d'expression des utilisateurs. Toutefois, la Directive sur le commerce électronique et les Principes du Conseil de l'Europe établissent une distinction entre les différentes fonctions et les différents rôles des fournisseurs d'accès, de services, d'hébergement et de contenu. De ce fait, le degré de responsabilité dépend de la capacité des fournisseurs en ligne à contrôler des contenus. Par ailleurs, l'exclusion d'une obligation « générale » de contrôle n'empêche pas les Etats parties d'imposer des obligations de surveillance aux prestataires de services dans certains cas, notamment dans les enquêtes pénales. Seuls les fournisseurs de services qui ne procurent qu'un « simple transport » ou accès à la communication sont totalement exemptés de responsabilité.[80] Les fournisseurs de services peuvent être tenus responsables des contenus qu'ils hébergent uniquement dans la mesure où ils ont une « connaissance réelle » de son caractère illicite et qu'ils ne le suppriment pas dans les « meilleurs délais » (procédure de « notification et suppression ») ou s'ils mettent à disposition un contenu illicite (principe de « l'hébergement » (safe harbour)).[81] Ni la Directive sur le commerce électronique ni les Principes du Conseil de l'Europe ne prévoient des protections contre les abus de « notification ».

Responsabilité en matière d'hyperliens

La responsabilité des créateurs de liens hypertextes qui renvoient vers d'autres sites ou blogs, forums de discussions ou autres plateformes constitue un autre sujet de préoccupation. Plusieurs tribunaux nationaux ont reconnu une responsabilité en matière d'hyperliens renvoyant à des contenus illicites ou considérés comme diffamatoires, avec, dans la plupart des affaires jugées, des liens vers des sites ou plateformes contenant des informations protégées par un droit d'auteur.[82]

Cette question est problématique pour plusieurs raisons. Dans la mesure où le contenu du site auquel renvoie le lien peut changer par la suite, le prestataire est tenu responsable d'un contenu sur lequel il n'exerce aucun contrôle. En fait, cela sous-entend que les individus devraient surveiller constamment tous les hyperliens qu'ils ont créés pour s'assurer que ces derniers n'ont pas été modifiés. De plus, sachant que les personnes créent des liens vers des sites qui dépendent de diverses juridictions, cela sous-entend que les utilisateurs doivent connaître la législation précise de chaque juridiction et qu'ils peuvent déterminer la légalité ou l'illégalité du site auquel ils renvoient (une question à laquelle de nombreux tribunaux n'ont pas pu répondre).

Agir ainsi peut avoir pour conséquence de dissuader les internautes de créer des liens par crainte de voir leur responsabilité juridique mise en cause, ce qui peut gravement entraver un aspect essentiel du sens et de l'objectif d'Internet, à savoir connecter des individus en eux et à l'information.

En 2012, la Cour européenne des droits de l'homme a traité de la responsabilité en matière d'hyperliens :

> L'Internet étant un espace public par excellence, l'Etat dispose d'une marge d'appréciation étroite s'agissant des informations diffusées par ce biais. Cela est encore plus vrai des hyperliens vers des pages Internet et qui ne sont pas, de facto ou de jure, sous le contrôle du créateur de l'hyperlien. Dans ce cas, la faible marge d'appréciation de l'Etat est déterminée par le principe voulant que le créateur de l'hyperlien ne peut être tenu pour responsable du contenu illégal des pages Internet accessibles par l'hyperlien, sauf lorsqu'il a de facto ou de jure le contrôle de la page auquel l'hyperlien renvoie ou a souscrit au contenu illégal de cette page. La création d'un lien ne saurait en elle-même être comprise comme une forme tacite d'approbation, car il faut d'autres éléments pour mettre en évidence la mens rea intentionnelle de la personne qui créé l'hyperlien.[83]

A titre de comparaison, il convient de se référer à une décision prise par la Cour suprême canadienne en 2009 qui a déclaré :

> Assujettir [les hyperliens] à la règle traditionnellement applicable en matière de diffusion aurait pour effet de gravement restreindre la circulation de l'information et, partant, la liberté d'expression. L'« effet paralysant » que cela serait susceptible d'avoir sur le fonctionnement de l'Internet pourrait être lourd de conséquences désastreuses, car il est peu probable que les auteurs d'articles de fond consentiraient à courir le risque d'engager leur responsabilité en incorporant dans leurs articles des liens menant à d'autres articles dont le contenu peut changer tout à fait indépendamment de leur volonté. Compte tenu de l'importance capitale du rôle des hyperliens dans l'Internet, nous risquerions de compromettre le fonctionnement de l'Internet dans son ensemble. L'application stricte de la règle en matière de diffusion dans ces circonstances reviendrait à s'efforcer de faire entrer une cheville carrée archaïque dans le trou hexagonal de la modernité.[84]

La Cour suprême canadienne a également maintenu un jugement antérieur de la Cour d'appel de Colombie-Britannique, et affirmé que:

> Un hyperlien s'apparente à une note de bas de page ou une référence à un site dans un contenu imprimé tel qu'une newsletter. La finalité de l'hyperlien est de diriger le lecteur vers un nouveau contenu provenant d'une source différente. La seule différence est la facilité avec laquelle un hyperlien permet au lecteur, par un simple clic de souris, d'accéder instantanément à un contenu supplémentaire.
>
> Bien qu'un hyperlien fournisse un accès immédiat à des contenus publiés sur un autre site, cela n'équivaut pas à une nouvelle publication du contenu du site d'origine. Cela est particulièrement vrai dans la mesure où un lecteur a la possibilité de suivre ou de ne pas suivre les hyperliens fournis.
>
> Les lecteurs d'une newsletter, qu'elle soit sous forme papier ou en ligne, qui prennent connaissance d'une référence au site d'un tiers peuvent se rendre sur ce site. J'en conclus que cela ne fait pas de celui qui a publié l'adresse du site un éditeur des contenus que trouvent les lecteurs quand ils y accèdent.[85]

Réglementation des contenus diffusés en ligne

Face au développement exponentiel d'Internet et du nombre de plus en plus croissant de ses usagers, les gouvernements sont de plus en plus préoccupés par la disponibilité d'une large gamme de contenus en ligne qu'ils sont incapables de contrôler. En effet, l'Internet permet aux utilisateurs d'accéder à des informations et des idées hors de leur territoire de résidence. Si de nombreux pays ont une vision différente du caractère illicite ou « diffamatoire » d'un contenu, fondée sur leurs traditions culturelles, morales ou religieuses, la réglementation des contenus en ligne est devenue un enjeu important pour les gouvernements du monde entier.

Dans l'ensemble, les Etats sont préoccupés par la propagande terroriste, les contenus racistes, les discours de haine, les contenus sexuellement explicites dont la pornographie infantile, les contenus blasphématoires, les expressions critiques à l'égard du gouvernement et de ses institutions et les contenus non autorisés par les détenteurs de droits d'auteur.

Toutefois, comme l'a justement remarqué le Rapporteur spécial des Nations Unies, ces différents types de contenus exigent des réponses juridiques et technologiques différentes.[86] Dans son rapport de 2011, le Rapporteur spécial des Nations Unies a identifié trois types d'expression en vue de la réglementation en ligne :

– L'expression qui constitue une infraction au regard du droit international et qui peut être passible de poursuites pénales ;

– L'expression qui n'est pas passible de poursuites pénales mais qui peut justifier une restriction et des poursuites au civil ; et

– L'expression qui n'est pas passible de sanctions pénales ou civiles mais qui reste néanmoins préoccupante en termes de tolérance, de civilité et de respect d'autrui.[87]

En particulier, le Rapporteur spécial a identifié les modes d'expression qui doivent être interdits par les Etats en vertu du droit international: (a) la pornographie mettant en scène des enfants; (b) l'incitation directe et publique à commettre un génocide; (c) l'apologie de la haine; et (d) l'incitation au terrorisme. Il a également précisé que la législation pénalisant ces modes types d'expression doit être suffisamment précise et prévoir des garanties suffisantes et réelles contre les excès ou les abus, y compris la surveillance et l'examen par un tribunal ou un organisme de réglementation indépendant et impartial.[88]

En d'autres termes, ces lois doivent également répondre aux critères du triple test énoncé ci-dessus. Par exemple, une législation interdisant la dissémination de la pornographie infantile sur les réseaux Internet au moyen de technologies de blocage et de filtrage est tenue de se soumettre à ces obligations.

De la même façon, les législations relatives au discours de haine visant l'expression en ligne ne doivent pas être ambiguës, et doivent poursuivre un objectif légitime et respecter les principes de nécessité et de proportionnalité. A cet égard, le Rapporteur spécial s'est inquiété du caractère excessivement vague d'un grand nombre de dispositions nationales visant à interdire le discours de haine, en violation des normes internationales relatives à la protection de la liberté d'expression. Cela comprend des expressions telles que la lutte contre « l'incitation aux tensions religieuses », « la promotion des dissensions entre croyants et non-croyants », « le dénigrement des religions », « l'incitation à la commission d'infractions », « l'instigation à la haine et au mépris du régime au pouvoir », « l'incitation à la subversion contre l'autorité de l'Etat » et « les infractions de nature à troubler l'ordre public ».

Le Rapporteur spécial a également précisé quelles restrictions en ligne ne sont pas, selon lui, autorisées par le droit international. Il a notamment recommandé aux Etats de fournir des détails précis sur la nécessité et la justification des mesures de blocage décidées à l'encontre d'un site donné, soulignant que « les critères utilisés pour déterminer les contenus devant être bloqués doivent être définis par une autorité judiciaire compétente ou par un organe indépendant de toute pression politique ou commerciale ou de toute autre influence injustifiée, afin d'éviter que le blocage ne soit utilisé comme moyen de censure ».[89]

Enfin, le Rapporteur spécial a précisé que tous les autres types d'expression tels que les commentaires diffamatoires ne devaient pas être passibles de sanctions. Au contraire, les Etats doivent promouvoir un usage plus large de l'expression pour combattre le discours offensant. A cet égard, il convient de mentionner qu'avec les nouveaux types d'application du Web 2.0, dont la zone de commentaires sur les sites de journaux, blogs et espaces de dialogue en ligne, etc., il est dorénavant possible de répondre instantanément et sans frais à des propos malveillants. De ce fait, le Rapporteur spécial a fait remarquer que les sanctions disponibles pour la diffamation hors ligne et des infractions similaires pourraient être inutiles et disproportionnées en ligne.[90]

Cybercriminalité

Des pays tentent de plus en plus fréquemment de réglementer les contenus d'Internet par le biais d'une supposée « législation de la cybercriminalité ». A ce jour, il n'existe pas de définition universelle du terme « cybercriminalité » :[91] ce mot est généralement utilisé pour décrire tout crime traditionnellement défini comme tel et commis à l'aide d'un réseau informatique ou d'Internet. En général, il recouvre un grand éventail d'infractions pénales, allant des activités terroristes et d'espionnage menées à l'aide d'Internet au piratage illégal de systèmes informatiques, à des attaques par des réseaux de robots (« boot net »)[92] dans le but de diffuser des spam et d'organiser des fraudes à la carte de crédit, du phishing, des vols et manipulations de données, et du harcèlement électronique, pour n'en citer que quelques-uns.

Un grand nombre de lois récemment adoptées restent pourtant vagues et trop larges, et par conséquent ouvertes à des interprétations arbitraires et subjectives, et menacent la protection du droit à la liberté d'expression. Par exemple, en 2011, le Rapporteur spécial des Nations unies pour la liberté d'expression s'est inquiété que :

> [L]'expression légitime sur Internet est pénalisée en violation des obligations internationales relatives au droits de l'homme des Etats, que ce soit par le biais de l'application de lois déjà existantes à l'expression en ligne, ou par la création de nouvelles lois spécifiquement conçues pour pénaliser l'expression sur Internet. De telles lois sont souvent justifiées sur la base de la protection de la réputation d'un individu, de la sécurité nationale, ou pour lutter contre le terrorisme, mais dans la pratique elles sont utilisées pour censurer des contenus que le gouvernement et d'autres entités puissantes n'aiment pas ou auxquels ils n'adhèrent pas.[93]

Toutefois, les normes internaitonales relatives à la cybercriminalité reconnaissent l'importance de préserver l'équilibre entre les impératifs de sécurité et la protection des droits fondamentaux, en particulier le droit à la liberté d'expression. La Résolution de l'Assemblée générale des Nations Unies portant sur la « création d'une culture mondiale de la cybersécurité » stipule que :

> La sécurité doit être assurée dans le respect des valeurs reconnues par les sociétés démocratiques, notamment la liberté d'échanger des pensées et des idées, la libre circulation de l'information, la confidentialité de l'information et des communications, la protection adéquate de l'information à caractère personnel, l'ouverture et la transparence.[94]

De la même manière, la Convention sur la cybercriminalité du Conseil de l'Europe (2001) confirme les obligations des Etats parties :

> Gardant à l'esprit la nécessité de garantir un équilibre adéquat entre les intérêts de l'action répressive et le respect des droits de l'homme fondamentaux... qui réaffirment le droit de ne pas être inquiété pour ses opinions, le droit à la liberté d'expression, y compris la liberté de rechercher, d'obtenir et de communiquer des informations et des idées de toute nature, sans considération de frontière, ainsi que le droit au respect de la vie privée.[95]

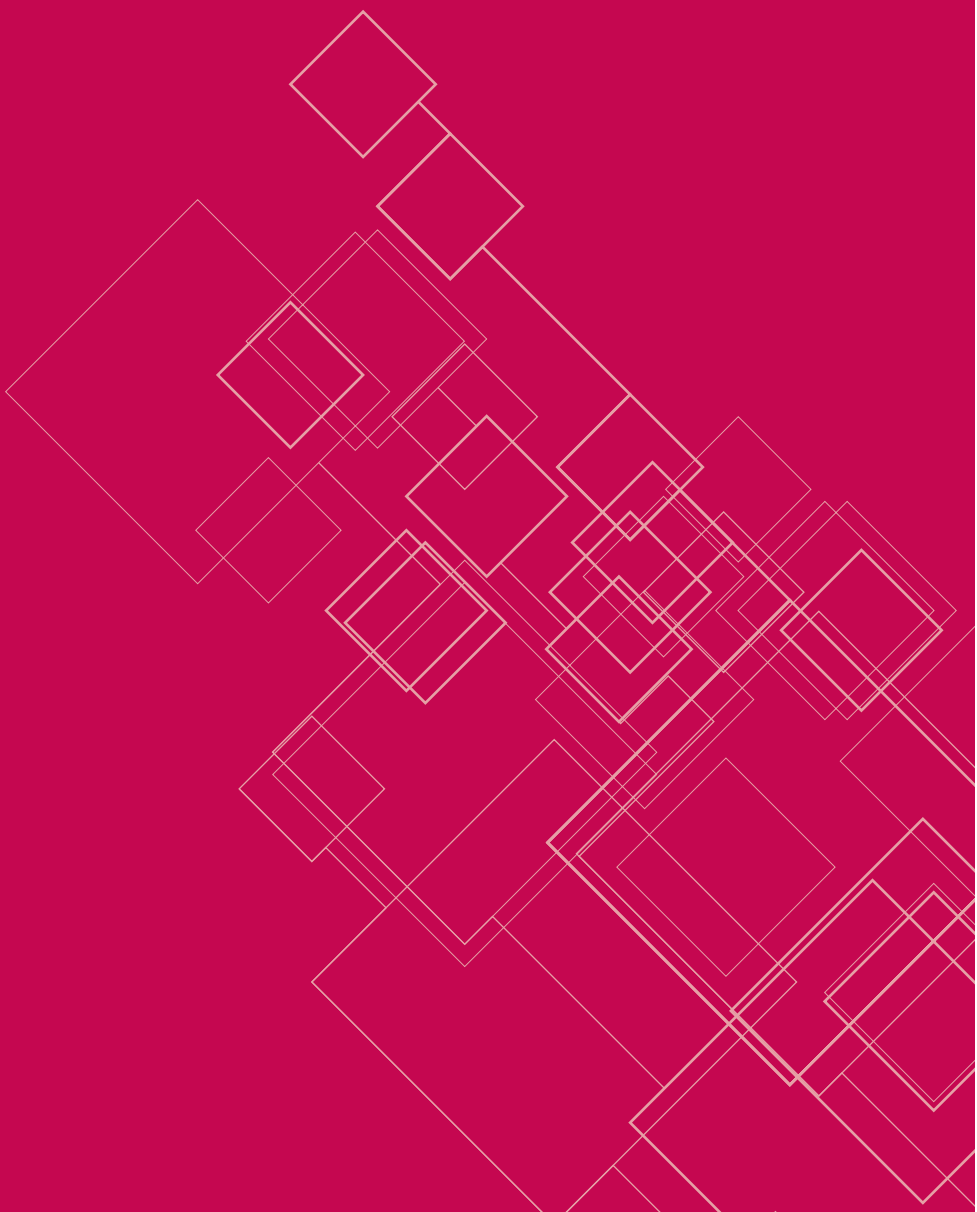
Il est notable que cette convention ne prévoit aucune restriction de contenu autre que celles relatives à la pornographie infantile. Il convient également de mentionner que la convention reconnaît la capacité des lois nationales sur la cybercriminalité à cibler la contestation politique et permet aux Etats de refuser toute demande d'entraide à d'autres Etats quand cette demande est susceptible d'être liée à des poursuites motivées par des considérations politiques.[96]

Sur la base des normes internationales, il est possible de conclure que la législation visant à lutter contre la cybercriminalité a besoin d'être conçue de manière à respecter la législation internationale des droits de l'homme et les normes internationales relatives à la liberté d'expression et ne doit pas être utilisée pour faire taire l'expression légitime ou pour poursuivre des citoyens critiques, des défenseurs des droits de l'homme, des blogueurs et des journalistes par le biais de médias électroniques. La législation sur la cybercriminalité doit respecter le principe de proportionnalité qui est essentiel à la protection des droits de l'homme ainsi que les critères suivants :

Toute législation doit fournir des définitions précises, claires et adéquates des termes juridiques et techniques déterminants couverts par l'infraction.

- La législation doit exiger des preuves sur la probabilité du préjudice découlant de l'activité criminelle, notamment en rapport aux infractions impliquant l'obtention ou la diffusion d'information classifiées.
- La législation doit demander que soit identifiée la nature du danger pour la sécurité nationale résultant d'une activité criminelle.
- La législation doit prévoir une défense de l'intérêt public en rapport avec l'obtention et la diffusion d'informations classées secrètes.
- La législation doit s'abstenir d'imposer des peines d'emprisonnement pour des infractions liées à l'expression, à l'exception de celles autorisées par les normes juridiques internationales et avec des protections adéquates contre les abus.[97]

Droits des citoyens journalistes et des blogueurs



L'avènement d'Internet signifie que chaque individu peut dorénavant publier lui-même ses opinions et ses idées sur un blog ou un réseau social, soulevant la question de la définition du journalisme et d'un « média » à l'ère du numérique. Se pose également la question de savoir comment des « citoyens journalistes » et des « blogueurs » doivent être réglementés.

En bref, il n'existe actuellement aucune définition reconnue du journalisme ou de ce qui constitue un « média » à l'ère du numérique au niveau international. Cependant, le Comité des droits de l'homme des Nations Unies et le Conseil de l'Europe ont fourni les éléments de réponse mentionnés ci-dessous. Concernant la réglementation, il semble évident que la législation internationale ne contraint pas les blogueurs et les citoyens journalistes à s'immatriculer, et encore moins à s'enregistrer sous leur véritable identité. Toutefois, il n'existe pas de normes précises sur les deux questions suivantes : premièrement, les citoyens journalistes et les blogueurs sont-ils tenus de respecter des normes professionnelles et, le cas échéant, lesquelles ; et deuxièmement, les citoyens journalistes et les blogueurs ont-ils le droit de bénéficier de la protection des sources.

Définition du journalisme et des nouveaux médias

Dans son Observation générale No 34, le Comité des droits de l'homme défini le journalisme comme suit :

> 44. Le journalisme est une fonction exercée par des personnes de tous horizons, notamment des reporters et analystes professionnels à plein temps ainsi que des blogueurs et autres particuliers qui publient eux-mêmes le produit de leur travail, sous forme imprimée, sur l'Internet ou d'autre manière, et les systèmes généraux d'enregistrement ou d'octroi de licence pour les journalistes par l'État sont incompatibles avec le paragraphe 3. Les régimes d'accréditation limitée peuvent être licites uniquement dans le cas où ils sont nécessaires pour donner aux journalistes un accès privilégié à certains lieux ou à certaines manifestations et événements. Ces régimes devraient être appliqués d'une manière qui ne soit pas discriminatoire et soit compatible avec l'article 19 et les autres dispositions du Pacte, en vertu de critères objectifs et compte tenu du fait que le journalisme est une fonction exercée par des personnes de tous horizons.

Le Comité des droits de l'homme a ainsi opté pour une approche fonctionnelle de la définition du journalisme. En d'autres termes, le journalisme est une activité qui consiste à rassembler et à diffuser des informations auprès du public via n'importe quel moyen de communication de masse.

Au niveau régional, le Conseil de l'Europe (COE) a adopté une approche similaire dans sa récente Recommandation CM/Rec (2011)7 sur une nouvelle conception des médias. Dans cette dernière, le Comité des ministres appelle les Etats membres à :[98]

– Adopter une conception des médias nouvelle et élargie, qui englobe tous ceux qui participent à la production et à la diffusion, à un public potentiellement vaste, de contenus (informations, analyses, commentaires, opinions, éducation, culture, art et divertissements sous forme écrite, sonore, visuelle, audiovisuelle ou toute autre forme) et d'applications destinées à faciliter la communication de masse interactive (réseaux sociaux par exemple) ou d'autres expériences interactives à grande échelle basées sur des contenus (jeux en ligne par exemple), tout en conservant (dans tous les cas susmentionnés) la surveillance ou le contrôle éditorial de ces contenus; [c'est nous qui soulignons]

– Evaluer la nécessité d'interventions réglementaires pour tous les acteurs fournissant des services ou des produits dans l'écosystème médiatique, pour garantir à toute personne le droit de chercher, de recevoir et de transmettre des informations conformément à l'Article 10 de la Convention européenne des droits de l'homme, et pour étendre à ces acteurs les garanties applicables contre les ingérences susceptibles de porter atteinte aux droits consacrés par l'article 10, notamment dans des situations risquant d'aboutir à une autolimitation ou à une autocensure injustifiées; [c'est nous qui soulignons]

Le Comité des ministres a proposé un certain nombre de critères à retenir pour déterminer quand une activité ou un acteur particulier doit être considéré comme un média: (i) l'intention d'agir en tant que média; (ii) la finalité et les objectifs sous-jacents des médias ; (iii) le contrôle éditorial; (iv) les normes professionnelles ; (v) le rayonnement et la diffusion; et (vi) les attentes du public.

De plus, le Comité a fourni une série d'indicateurs permettant de déterminer si un critère particulier est respecté. Par exemple, une organisation ou un individu engagé dans la diffusion de l'information répondra pleinement au critère relatif aux attentes du public si l'information est disponible, fiable, qu'elle fournit un contenu diversifié et respecte le principe de pluralisme, les normes professionnelles et déontologiques, et si elle est responsable et transparente. Dans le même temps, le Conseil des ministres a souligné que chacun des critères doit être appliqué de manière flexible.

Il est intéressant de noter que le Comité a soutenu que les blogueurs pouvaient être considérés comme des médias uniquement lorsqu'ils respectent certaines normes professionnelles dans une mesure suffisante. Il est utile de noter toutefois qu'au Royaume-Uni, le Code de Pratique s'applique aux citoyens journalistes uniquement lorsqu'ils soumettent des contenues à des journaux et des magazines qui ont souscrit au Code.99 La Commission de plaintes en matière de presse (PCC – Presse and Complaints Commission) a ainsi précisé que les « rédacteurs en chef et les éditeurs (qui endossent la responsabilité finale en vertu du système d'autorégulation) sont tenus de veiller à ce que le Code soit respecté non seulement par le personnel éditorial, mais également par les collaborateurs extérieurs à la rédaction, y compris ceux qui ne sont pas journalistes ». Cela suggère fortement que s'ils ne soumettent pas des contenus à des journaux, les blogueurs ne peuvent être assujettis aux mêmes droits et devoirs que les journalistes professionnels.

Réglementation des blogueurs et citoyens journalistes

Enregistrement

La définition du journalisme donnée par le Comité des droits de l'homme des Nations Unies (mentionnée ci-dessus) montre clairement que, à l'instar des journalistes professionnels, les blogueurs ne doivent pas être assujettis à une obligation d'enregistrement ou de licence. De même, ils doivent recevoir une accréditation uniquement quand celle-ci est nécessaire pour bénéficier d'un accès privilégié à certains lieux et/ou événements.

Contrôle éditorial limité

Dans sa Recommandation CM/Rec (2011)7 sur une nouvelle conception des médias ci-dessus mentionnée, le Comité des ministres du Conseil de l'Europe a reconnu que chaque niveau de contrôle éditorial exige un certain niveau de responsabilité éditoriale. En particulier, il a affirmé que :

> (…) il faudrait noter qu'à chaque niveau de contrôle éditorial correspond un certain niveau de responsabilité éditoriale. Une réponse différenciée et graduelle est nécessaire en fonction du degré de contrôle éditorial ou des modalités éditoriales (par exemple prémodération, par opposition à une postmodération).[100]

Cela suggère que tout cadre juridique touchant aux blogueurs et citoyens journalistes doit reconnaître qu'ils ont des obligations et des responsabilités plus réduites que les journalistes professionnels lorsqu'ils exercent leur liberté d'expression parce qu'ils ne disposent pas des mêmes ressources et moyens techniques que les journaux.

Responsabilité civile et pénale

La législation ne fait généralement aucune distinction entre les journalistes et le reste de la population en matière de responsabilité civile et pénale. Les blogueurs et les citoyens journalistes sont de ce fait assujettis à ces mêmes législations, comme par exemple les lois relatives à la diffamation. Cependant, la question se pose de savoir si les blogueurs et les citoyens doivent bénéficier des mêmes protections juridiques que les journalistes quand ils exercent l'activité de journaliste.

Protection juridique

A ce jour, il n'existe pas de normes juridiques internationales reconnues sur la protection juridique dont doivent bénéficier les citoyens journalistes et les blogueurs. Cependant, de même que les blogueurs ont le devoir, à l'instar de tous les citoyens, d'obéir à la loi, ils peuvent également utiliser des défenses accordées aux citoyens en vertu de la loi.

La question de savoir si les blogueurs et les citoyens journalistes peuvent bénéficier des principes juridiques qui régissent la protection des sources est plus problématique. Dans la Recommandation CM/Rec (2011)7 ci-dessus mentionnée, le Comité des ministres a stipulé que :

> [L]a protection des sources devrait s'étendre à l'identité des utilisateurs qui mettent à disposition des contenus d'intérêt public sur des espaces partagés en ligne conçus pour faciliter la communication de masse interactive (ou de groupe), y compris les plateformes de partage de contenu et les services de réseaux sociaux. Des dispositions peuvent être requises pour autoriser le recours à des pseudonymes (par exemple dans des réseaux sociaux) lorsqu'une divulgation de l'identité risque d'entraîner des mesures de rétorsion (par exemple en tant que conséquence de l'activisme dans le domaine politique ou des droits de l'homme).

Toutefois, la recommandation n'indique pas clairement si un blogueur ou un citoyen journaliste peut bénéficier de la protection des sources en lien avec l'information reçue des utilisateurs d'Internet ou autres. Néanmoins, le Comité des ministres a recommandé qu'une quelconque forme de soutien et de protection devait être accordée aux acteurs des médias, c'est-à-dire aux blogueurs, qui ne sont pas considérés comme des médias en vertu d'un certain nombre de critères fixés par le Comité mais qui « participent à l'écosystème médiatique ».[101]

Accès à l'information et TIC

Il existe une tendance mondiale à pousser les Etats, organisations intergouvernementales, la société civile et autres personnes à reconnaître le droit d'accès à l'information. Une somme de plus en plus grande de déclarations contraignantes en faveur du droit à l'information sont faites dans le cadre des mécanismes officiels des droits de l'homme. De nombreuses législations assurant la jouissance de ce droit ont été adoptées ces dernières années dans toutes les régions du monde et beaucoup d'organisations intergouvernementales ont mis en place des systèmes de divulgation de l'information qui sont révisés et mis à jour régulièrement.

Concernant les TIC, deux questions méritent une attention toute particulière : l'e-gouvernance et le libre accès aux données.

E-gouvernance and e-gouvernement

Les termes e-gouvernance and e-gouvernement sont souvent utilisés de manière interchangeable.

L'UNESCO définit ainsi l'e-gouvernance :

> L'e-gouvernance est l'utilisation par le secteur public des technologies de l'information et de la communication dans le but d'améliorer la fourniture d'information et de service, d'encourager la participation du citoyen au processus de décision et de rendre le gouvernement plus responsable, transparent et efficace.[102]

Le concept d'e-governement se réfère généralement à l'utilisation des technologies de l'information et de la communication par les gouvernements pour renforcer la gamme et la qualité de l'information et des services fournis aux citoyens, aux entreprises, institutions académiques, médias et institutions publiques, de manière efficace, moins bureaucratique et à meilleur marché. Une étude des Nations Unies sur l'état du e-gouvernement définit ce dernier comme l'utilisation de l'Internet et du web pour délivrer des informations et des services publics aux citoyens.[103]

L'objectif du e-gouvernement n'est pas simplement pour les services publics d'être présent sur le web ou d'informatiser ou numériser des dossiers publics mais également d'optimiser les services publics et de les rendre plus rapides, plus accessibles et transparents grâce aux technologies de l'information et de la communication. L'e-gouvernement transforme les modalités d'interaction entre le gouvernement et les citoyens, les entreprises et les autres gouvernements. A titre d'exemple, l'e-gouvernement peut englober les e-impôts, la e-santé et les e-transports.

Toute approche significative du e-gouvernement doit commencer par garantir un déploiement total de l'infrastructure de base d'Internet qui fournit des connexions rapides à tous les administrés, et un accès non discriminatoire à tous les e-services. Les Etats doivent aussi investir dans l'éducation à l'Internet et au monde numérique afin de renforcer la capacité des citoyens à utiliser les e-services.

Les Etats doivent également veiller à ce que l'information et les services proposés par l'e-gouvernement soient fiables et que l'information fournie par les utilisateurs soit fortement protégée à la fois technologiquement et juridiquement contre la surveillance et les abus. Les e-gouvernments doivent promulguer des lois solides sur la protection de la vie privée interdisant la création de liens et la combinaison de données personnelles soumises à des e-services différents et non liés, rendant possible la création de profils d'utilisateurs (« citoyen transparent »).

Les Etats doivent également fournir des e-services dans le respect de règles précises et dans la plus grande transparence s'agissant de quel organe public offre quels services à quelles conditions et sous quelles protections. Par exemple, les gouvernements se tournent de plus en plus vers les plateformes de réseaux sociaux pour atteindre les citoyens. Qu'ils quittent leur e-présence officielle (ou site) pour pénétrer les sphères publiques en ligne comme les plateformes de réseaux sociaux ou participer à des discussions en ligne avec leurs administrés, cela doit être fait de manière claire et non trompeuse et comprendre des coordonnées diverses (hors ligne) des fonctionnaires responsable de ce service.

Enfin, le gouvernements doivent installer des mécanismes indépendants de surveillance et de plainte pour tous les services e-gouvernement afin de garantir un fonctionnement adéquat de ces services ; des mécanismes de réparation pour les citoyens qui peuvent voir leurs droits bafoués par un e-service ; et les hotlines de lanceurs d'alerte à qui l'ont peut transmettre des informations sur des activités illicites ou des faits de corruption en toute sécurité et dans l'anonymat.

Données en libre accès (Open data)

Ce concept se réfère à la mise à disposition libre et gratuite de données publiques ou collectées soit par des organisations publiques, privées ou non gouvernementales, pour le compte du public dans l'intérêt de cette société. En tant que tel, le libre accès aux données (« open data ») doit être considéré comme une ressource commune. Les données en libre accès peuvent être statistiques, géographiques, cartographiques, des informations sur la circulation ou spatiales, des publications scientifiques et des recherches médicales rendues possibles grâce à des fonds publics, des données non personnelles rassemblées par une autorité judiciaire, un tribunal et une administration publique.

Condition préalable dans l'ère du numérique, l'open data est essentiel à une meilleure participation démocratique, à la transparence, l'ouverture et l'efficacité du gouvernement, mais aussi à la créativité, l'innovation et la croissance économique.

L'open data dépend d'une législation efficace sur la liberté d'information. En vertu du droit international, les gouvernements doivent démontrer que toute restriction de l'accès à l'information est prévue par la loi, est nécessaire dans une société démocratique et qu'elle poursuit un objectif légitime. Toute limitation de l'accès à l'information et toute restriction de l'accès à l'open data ne peut s'appliquer que si les gouvernements et les organes privés peuvent démontrer que la mise à disposition de ces données

engendrerait une violation spécifique des droits fondamentaux d'autrui ou de la société. La crainte d'un préjudice économique ne rentre pas en ligne de compte.

Les gouvernements et les entités privées ont mis du temps à ouvrir les bases de données qui ont été créées en rassemblant des données avec des fonds publics pour le public. De nombreux gouvernements ne divulguent pas ces données et le travail des autorités publiques est souvent effectué par des contractants privés qui conservent alors les données collectées pour le compte de l'Etat ou qui les rendent disponibles en contrepartie de frais importants. Très peu de gouvernements pratiquent des politiques de libre accès aux données.[104]

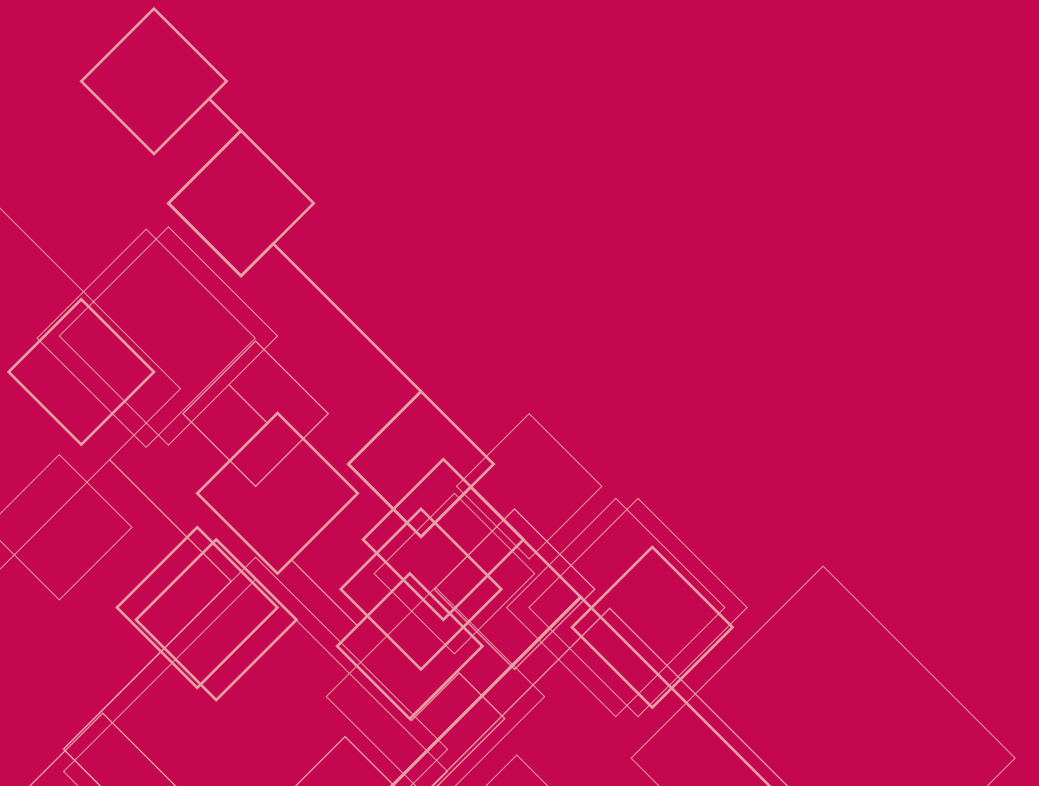
Au niveau international, la Déclaration de Berlin sur le libre accès à la connaissance en sciences exactes, sciences de la vie, sciences humaines et sociales[105] a été adoptée en 2003 par près de 500 universités, centres de recherche et scientifiques, et bibliothèques dans le monde entier. Son objectif est de fournir un accès libre et universel à l'héritage scientifique et culturel mondial. La déclaration définit deux conditions à une ouverture significative de l'accès :

> Leurs auteurs et les propriétaires des droits afférents concèdent à tous les utilisateurs un droit gratuit, irrévocable et mondial d'accéder à l'œuvre en question, ainsi qu'une licence les autorisant à la copier, l'utiliser, la distribuer, la transmettre et la montrer en public, et de réaliser et de diffuser des œuvres dérivées, sur quelque support numérique que ce soit et dans quelque but responsable que ce soit, sous réserve de mentionner comme il se doit son auteur (les règles usuelles de la collectivité continueront à disposer des modalités d'attribution légitime à l'auteur et d'utilisation responsable de l'œuvre publiée, comme à présent), tout comme le droit d'en faire des copies imprimées en petit nombre pour un usage personnel.
>
> Une version complète de cette œuvre, ainsi que de tous ses documents annexes, y compris une copie de la permission définie dans ce qui précède, est déposée (et, de fait, publiée) sous un format électronique approprié auprès d'au moins une archive en ligne, utilisant les normes techniques appropriées (comme les définitions des Archives Ouvertes [Open Archives]), archive gérée et entretenue par une institution académique, une société savante, une administration publique, ou un organisme établi ayant pour but d'assurer le libre accès, la distribution non restrictive, l'interopérabilté et l'archivage à long terme.[106]

Le libre accès aux données exige de s'engager à rendre les informations et les données accessibles à tous et sans discrimination et à fournir des contrats de licence pour l'open data. Compte tenu du volume des données ouvertes potentielles, les informations classifiées en open data doivent être également traitées de manière à pouvoir naviguer aisément dans les bases de données et les filtres à l'aide de mots clés afin de pouvoir trouver l'information recherchée dans un court délai.

Il est également important que chaque politique relative au libre accès aux données, eu égard au respect des droits de l'homme, veille à ce qu'il y ait une distinction nette entre les données non personnelles qui doivent être ouvertes et en libre accès et les données personnelles qui bénéficient d'une protection en vertu des normes internationales relatives aux droits de l'homme.

Cadre réglementaire de l'Internet



Gouvernance de l'Internet

L'Internet a évolué hors d'un cadre juridique et réglementaire en l'absence d'orientation ou de supervision d'organisations internationales comme l'International Telecommunications Union (ITU). A son début, c'était une entreprise mondiale qui, en tant que telle, n'était pas soumise à la compétence juridictionnelle d'un Etat et d'un gouvernement particulier. L'Internet s'est développé par le biais de ce que l'on appelle aujourd'hui des procédures « pluripartites » comprenant des acteurs étatiques et non étatiques qui étaient fondées sur l'autorégulation de ses utilisateurs et des codes interopérables reconnus par ses fournisseurs de services et d'infrastructure.

Bien que la notion de « gouvernance d'Internet » ne soit pas clairement définie et recouvre toute une gamme de questions en rapport avec la gouvernance, elle porte essentiellement sur la question de savoir quels groupes, s'il y en a, doivent avoir le contrôle des différents aspects techniques, économiques, juridiques et réglementaires qui concernent le cadre décentralisé dans lequel l'Internet est intégré.

Bien que l'Internet ne soit pas un système hiérarchique, ses caractéristiques respectent des règles hiérachiques très strictes. C'est le cas du système de noms de domaine (Domain Name System ou DNS), composé de 13 serveurs racines, qui est géré par l'ICANN (Internet Corporation for Assigned Names and Numbers) ou Société pour l'attribution des noms de domaine et des numéros sur Internet, une entreprise enregistrée aux Etats-Unis. Le DNS définit comment des adresses Internet et des domaines génériques de premier niveau (comme .com ou .org) et des noms de domaine de code pays de premier niveau (comme .uk et .za) se traduisent par des adresses de Protocole Internet (adresses IP). L'ICANN rend des comptes au Département américain du commerce auquel il est lié par un « Memorandum of Understanding »[107] ; son siège social se trouve en Californie.[108] La modification des spécifications des serveurs racines n'est possible qu'avec l'approbation du Département du commerce. La structure administrative particulière de l'ICANN a été critiquée par beaucoup d'Etats qui ont soutenu que les changements de leur domaine code pays de premier niveau ne pourraient être possibles qu'avec le consentement de l'administration américaine. Ces pays préféreraient internationaliser cet aspect technique de la gouvernance d'Internet et le placer sous égide intergouvernementale et le droit international.[109]

La question du comment et qui doit diriger l'Internet était à l'ordre du jour du premier Sommet mondiale sur la société de l'information (SMSI), qui s'est tenu sous l'égide des Nations Unies à Genève en décembre 2003, et auquel ont participé 175 gouvernements.[110] Au cours de ce sommet, la notion de « gouvernance d'Internet » a été créée afin de donner un nom à cette problématique complexe.

Le sommet de Genève n'a pas porté les fruits escomptés en termes de gouvernance d'Internet ; cependant, il a produit la Déclaration de principes de Genève[111] qui souligne que :

> La communication est un processus social fondamental, un besoin essentiel de l'être humain et la base de toute organisation sociale. Elle est le pivot de la société de l'information. Toute personne, où que ce soit dans le monde, devrait avoir la possibilité de participer à la société de l'information et nul ne devrait être privé des avantages qu'elle offre.[112]

Ses principes appellent également tous les acteurs à :

> (…) prendre les mesures appropriées, notamment préventives, déterminées par la loi, pour empêcher les utilisations abusives des TIC, par exemple les actes délictueux dictés par le racisme, la discrimination raciale et la xénophobie, ainsi que l'intolérance, la haine et la violence qui en résultent, de même que toutes les formes de maltraitance des enfants, en particulier la pédophilie et la pornographie infantile, ainsi que la traite et l'exploitation d'êtres humains.[113]

Le premier SMSI a été suivi par un Groupe de travail sur la gouvernance de l'Internet (GTGI ou WGIG en anglais) chargé de développer une définition claire de la notion de « gouvernance de l'Internet », de discuter de la possibilité de mettre en place une surveillance internationale des ressources critiques d'Internet et de spécifier les questions et les différents problèmes afférents, ainsi que de proposer des recommandations aux décideurs politiques. Le Groupe de travail sur la gouvernance de l'Internet a confirmé que les questions de gouvernance de l'Internet englobent des aspects juridiques importants, notamment les droits à la vie privée, les droits d'auteurs, la cybercriminalité, et la protection des donnés et qu'il faut discuter de mécanismes permettant de répondre à des questions comme l'autorégulation et les compétences juridictionnelles.

Dans la période préparatoire du second Groupe de travail qui s'est réuni à Tunis en novembre 2005 en présence de près de 170 gouvernements, plusieurs Etats ont prôné l'internationalisation de l'ICANN ainsi que, plus généralement, d'une gouvernance de l'Internet au sein d'un cadre des Nations Unies.[114] L'Union européenne a proposé la création d'un mécanisme d'arbitrage et de résolution de conflit basé sur la législation internationale en cas de conflit sur toutes les questions liées aux noms, nombres et adresses.[115]

Le Groupe de Travail de Tunis n'a pas donné de résultats et n'a pas conclu d'accord sur la manière de gouverner l'Internet dans le futur mais, à l'instar du premier SMSI de 2003, ses documents finaux, l'Engagement de Tunis et l'Agenda de Tunis pour la société de l'information, ont reconnu que la liberté d'expression et la libre circulation des informations, des idées et des connaissances sont essentielles pour la Société de l'information et favorisent le développement.[116] L'Agenda de Tunis a également fourni une « définition de la gouvernance de l'Internet » :

> [L]'élaboration et l'application par les Etats, le secteur privé et la société civile, chacun selon son rôle, de principes, normes, règles, procédures de prise de décision et programmes communs propres à modeler l'évolution et l'utilisation de l'Internet.[117]

Pour empêcher que le sommet n'aboutisse à un échec, il a été convenu d'ajouter un troisième forum au SMSI et au GTGI, le Forum sur la gouvernance de l'Internet (Internet Governance Forum - IGF). Selon l'Agenda de Tunis, le Forum sur la gouvernance de l'Internet doit être multilatéral, multipartite, démocratique et transparent. Entre autres points, il a pour mandat de:

- Traiter les questions de politique publique relatives aux principaux éléments de la gouvernance de l'Internet afin de contribuer à la viabilité, à la robustesse, à la sécurité, à la stabilité et au developpement de l'Internet.
- Maintenir la liaison avec les organisations intergouvernementales et d'autres institutions appropriées sur les questions relevant de leur mandat.
- Promouvoir la prise en compte des principes du SMSI dans les mécanismes de gouvernance de l'Internet et de l'évaluer régulièrement.
- Aider à trouver les solutions aux problèmes découlant de l'utilisation et de la mauvaise utilisation de l'Internet, qui préoccupent particulièrement l'usager ordinaire.[118]

L'IGF s'est réuni pour la première fois en 2006 à Athènes et il se tient dorénavant tous les ans. Il n'a aucun pouvoir de décision et ne peut que proposer des recommandations non contraignantes.

Alors que les SMSI et les IGF annuels continuent de discuter sur la question de savoir si l'Internet ou certains de ses aspects bénéficieraient ou souffriraient d'une gouvernance institutionnalisée et juridiquement réglementée qui maintiendrait cette plateforme ouverte et libre, le DNS continue d'être sous le contrôle de l'ICANN qui dépend toujours du Département du commerce américain.

Initiatives régionales

En 2011, le Conseil de l'Europe a adopté les Dix principes de la gouvernance de l'Internet.[119] Ces principes reconnaissent, entre autres, l'universalité, l'ouverture et l'intégrité de l'Internet, l'approche pluripartite de la gouvernance de l'Internet, et la gestion décentralisée et l'interopérabilité de l'Internet. Ces principes stipulent que :

> Les dispositions pour la gouvernance de l'Internet doivent assurer la protection de tous les droits et libertés fondamentaux et affirmer leur universalité, leur indivisibilité, leur interdépendance et leur corrélation, conformément au droit international des droits de l'homme. Elles doivent également veiller au respect plein et entier de la démocratie et de l'Etat de droit et elles devraient promouvoir le développement durable. Tous les acteurs publics et privés devraient reconnaître et respecter les droits de l'homme et les libertés fondamentales dans leur fonctionnement et leurs activités ainsi que dans la conception de nouveaux services, technologies et applications. Ils devraient être au fait des évolutions qui conduisent à l'amélioration des droits et libertés fondamentaux, mais également de celles qui constituent des menaces pour ces mêmes droits et libertés fondamentaux, et participer pleinement aux efforts visant à reconnaître de nouveaux droits.

Il faut également noter que, avec les acteurs publics, les acteurs privés sont appelés à respecter les droits humains et les libertés fondamentales lorsqu'ils développent, offrent et exploitent leurs services et applications.

Compétence juridictionnelle

Le caractère mondial de l'Internet ne respecte plus les frontières strictes et le contrôle des Etats individuels. Certains gouvernements craignent que l'Internet sape leur souveraineté judiciaire dans la mesure où l'extraterritorialité est un problème majeur dès qu'un contenu culturellement, moralement ou politiquement sensible est en jeu.

L'évolution des normes et de la jurisprudence internationales a été lente. Toutefois, les initiatives et normes suivantes doivent être mentionnées :

– Dans les Recommandations d'Amsterdam de 3003, le Représentant de l'OSCE pour la liberté des médias a demandé que « les contenus illégaux doivent faire l'objet de poursuites dans le pays d'origine ».[120] Le mot « origine » reste vague, dans la mesure où le Représentant n'a pas spécifié si le contenu devait y être produit ou téléchargé, s'il était destiné au public d'un pays particulier, ou écrit dans la (ou les) langues, ou par un citoyen, ou un résident, de ce pays.

– La Déclaration conjointe 2005 des mandataires spéciaux pour la liberté d'expression précisait la question de l'« origine » en affirmant que « dans les affaires liées au contenu d'Internet, la territorialité ne devrait entrer en ligne de compte que dans l'Etat de résidence de l'auteur du contenu ou dans les Etats auxquels le contenu est spécifiquement destiné. La juridiction ne doit pas être établie simplement parce que le contenu a été téléchargé dans un Etat donné. »[121] Dans leur Déclaration conjointe de 2010, les rapporteurs spéciaux exprimaient leur préoccupation à propos des « règles juridictionnelles qui permettent d'engager des poursuites, en particulier dans les affaires de diffamation, n'importe où, conduisant à une approche du plus petit dénominateur commun »[122], mais ils n'ont pas proposé des directives juridictionnelles supplémentaires.

– La Déclaration conjointe 2011 des Rapporteurs spéciaux soulignait que « la compétence juridictionnelle dans les cas liés aux contenus d'Internet doit être restreinte aux Etats ayant un lien réel et essentiel avec les cas concernés, en règle générale parce que l'auteur y réside, que le contenu incriminé y est téléchargé et/ou est dirigé contre cet Etat. Les parties privées doivent pouvoir saisir une juridiction donnée si elles prouvent qu'elles ont subi un préjudice substanciel dans cette même juridiction ».[123] Cependant, il convient de mentionner que ladite « règle du upload » (par laquelle la responsabilité d'un contenu est attachée à la juridiction ou le téléchargement a été effectué) et la « règle du download» (qui assujettit le contenu à toutes les juridictions où l'information a été téléchargée) sont – en soi et hors du contexte plus large – mal conçues et permissives dans la mesure où elles encouragent un « forum shopping » et risquent de faire jouer une juridiction contre une autre. La règle du download obligerait également les usagers, auteurs, éditeurs et compagnies hébergeantes à être soumises toujours à la législation de toutes les juridictions où le contenu pourrait être lu et être accessible.

End notes

[1] Voir, par exemple, OSCE, La liberté d'expression et l'Internet, 2010; disponible à http://www.osce.org/fom/80723. Le rapport 2011 du Rapporteur spécial des Nations Unies pour la liberté d'expression, A/66/290, 10 août 2011; sur le site http://www.ohchr.org/Documents/Issues/Opinion/A.66.290.pdf.

[2] Déclaration universelle des droits de l'homme, Résolution de l'Assemblée Générale des Nations Unies 217A (III), 10 décembre 1948.

[3] Voir Filartiga c. Pena-Irala, 630 F. 2d 876 (1980) (US Circuit Court of Appeals, 2nd circuit).

[4] Pacte international relatif aux droits civils et politiques, Résolution de l'Assemblée générale des Nations Unies 2200A (XXI) du 16 décembre 1966, entré en vigueur le 23 mars 1976.

[5] Observation générale N° 34, CCPR/C/GC/34.

[6] Ibid., par. 12.

[7] Ibid., par. 17.

[8] Ibid., par. 39.

[9] Résolution A/HRC/20/L.13, adoptée le 29 juin 2012.

[10] Rapport 2011 du Rapporteur spécial, op.cit, par. 16.

[11] Déclaration conjointe des quatre mandataires spéciaux sur la protection de la liberté d'expression sur l'Internet, juin 2011, disponible sur http://www.osce.org/fom/78309. Par ailleurs, deux autres déclarations conjointes des mandataires spéciaux ont porté sur la liberté d'expression sur l'Internet : la Déclaration conjointe de 2005 sur la régulation de l'Internet et les mesures antiterroristes et la Déclaration conjointe de 2010 sur les dix principaux défis de la liberté d'expression. Toutes les déclarations conjointes des Rapporteurs spéciaux sont disponibles sur http://www.osce.org/fom/66176.

[12] Ibid., Déclaration 2011 sur la liberté d'expression et l'Internet.

[13] Ibid.

[14] Voir Comité des droits de l'homme, Velichkin c. Biélorussie, Communication No. 1022/2001, U.N. Doc. CCPR/C/85/D/1022/2001 (2005).

[15] Voir Comité des droits de l'homme, Leonardus J.M. de Groot c. Pays-Bas, No. 578/1994, U.N. Doc. CCPR/C/54/D/578/1994 (1995).

[16] Comité des droits de l'homme, Observations finales sur la République arabe syrienne, CCPR/CO/84/SYR.

[17] Ibid.

[18] Rapport 2011 du Rapporteur spécial des Nations Unies pour la liberté d'expression, op.cit.

[19] Adoptée le 27 juin 1981, OAU Doc. CAB/LEG/67/3 rev. 5, 21 I.L.M. 58 (1982), entrée en vigueur le 21 octobre 1986.

[20] Adoptée lors de la 32e Session de la Commission africaine des droits de l'homme et des peuples, 17-23 octobre 2002.

[21] Déclaration américaine des droits et devoirs de l'homme, OEA/Ser.L./V.II.23, doc. 21, rev. 6 (1948).

[22] Adoptée lors de la Conférence spécialisée interaméricaine sur les droits de l'homme, 22 novembre 1969, Traité OEA Serie No.36; 114 UNTS 123; 9 ILM 99 (1969), entrée en vigueur le 18 juillet 1978.

[23] Adoptée par la Commission interaméricaine des droits de l'homme lors de sa 108e Session ordinaire, 19 octobre 2000, disponible sur http://www.iachr.org/declaration.htm.

[24] Disponible à http://www.asean.org/news/asean-statement-co.mmuniques/item/asean-human-rights-declaration.

[25] Adoptée le 22 mai 2004, entrée en vigueur le 15 mars 2008.

[26] Adoptée le 4 novembre 1950, entrée en vigueur le 3 septembre 1953.

[27] Charte des droits fondamentaux de l'Union européenne, 2000/C 364/01, adoptée le 7 décembre 2000, entrée en vigueur le 1er décembre 2009; à consulter sur http://www.europarl.europa.eu/charter/pdf/text_en.pdf. L'Article 11 stipule que: « Toute personne a droit à la liberté d'expression. Ce droit comprend la liberté d'opinion et la liberté de recevoir ou de communiquer des informations ou des idées sans qu'il puisse y avoir ingérence d'autorités publiques et sans considération de frontières. La liberté des médias et leur pluralisme sont respectés. »

[28] Recommandation CM/Rec(2011)7.

[29] Recommandation CM/Rec(2011)8.

[30] Par exemple, entre 2005 et 2010, la Cour européenne a statué uniquement sur dix affaires relatives à la liberté d'expression et aux TIC (Internet, email, et données électroniques); et en 2011-juillet 2013, elle a jugé huit affaires. Voir aperçu sur : http://www.echr.coe.int/Documents/FS_New_technologies_ENG.pdf.

[31] En novembre 2011, la Cour de justice de l'Union européenne a rendu deux décisions importantes. Dans l'affaire Scarlet Extended SA c. SABAM, C-70/10, elle a défendu la protection de la liberté d'expression dans la bataille contre le « piratage » en ligne en jugeant que les mesures contraignant les FAI à installer des systèmes de filtrage et de blocage pour empêcher le partage illégal de fichiers sur des réseaux pair-à-pair étaient contraires aux droits fondamentaux, notamment au droit au respect de la vie privée et au droit à l'information; à consulter sur http://curia.europa.eu/juris/liste.jsf?language=en&num=C-70/10. Dans l'affaire SABAM c. Netlog, C-360/10, février 2012, la Cour de justice de l'Union européenne a confirmé que les systèmes généraux de contrôle et de filtrage installés empêcher les infractions à la propriété intellectuelle étaient disproportionnés. Elle a jugé que, à l'instar des FAI, les réseaux sociaux ne pouvaient être contraints de contrôler et filtrer les communications de leurs utilisateurs afin d'empêcher des infractions au droit d'auteur ; à consulter sur http://curia.europa.eu/juris/document/document.jsf?docid=119512&doclang=EN.

[32] Voir, par exemple, le témoignage du Représentant spécial de l'OSCE pour la liberté des médias à la Commission Helsinki U.S. en juillet 2011; à consulter sur http://www.osce.org/fom/81006.

[33] Déclaration de Principes, Construire la société de l'information : un défi mondial pour le nouveau millénaire, WSIS-03/GENEVA/DOC/4-E, 12 décembre 2003, disponible sur http://www.itu.int/wsis/docs/geneva/official/dop.html.

[34] Observation générale N° 34, par. 15.

[35] Rapport 2011 du Rapporteur spécial des Nations Unies, op.cit., par. 79.

[36] Ibid., par. 3.

[37] Ibid. par. 85.

[38] Déclaration conjointe 2011, op. cit., par. 6 e).

[39] Bureau du Représentant de l'OSCE pour la liberté des médias, La liberté d'expression sur l'Internet : étude des dispositions juridiques et des pratiques liées à la liberté d'expression, la libre circulation de l'information et le pluralisme des média sur l'Internet dans les Etats membres de l'OSCE, p. 14.

[40] L'Article 5A par. 2 de la Constitution grecque stipule que tous les individus ont le droit de participer à la Société de l'information. L'accès facilité à l'information diffusée électroniquement ainsi que la production, l'échange et la diffusion de l'information constituent une obligation de l'Etat, toujours dans le respect des garanties des articles 9, 9A et 19.

[41] En Estonie, la loi 2000 sur les Télécommunications, Article 5 par. 1, stipule que tous les clients souhaitant avoir accès au réseau téléphonique public disposeront de cet accès de manière uniforme et raisonnable ; cela comprend les services Internet universellement accessibles à tous les abonnés, sans considération de leur situation géographique, à un prix unique. De plus, le Public Information Act (2000), Article 33, garantit à chacun la possibilité d'avoir un accès libre à l'information publique sur l'Internet dans les bibliothèques publiques.

[42] Dans sa Décision n° 2009-580 DC du 10 juin 2009, le Conseil constitutionnel français qui statuait sur la constitutionnalité de la loi Hadopi-I a affirmé que l'accès aux services en ligne était un droit humain fondamental.

[43] L'amendement No. 331/2009 de la loi finlandaise No. 393/2003 relative au marché des communications oblige les sociétés de télécommunications à fournir à chaque citoyen une connexion Internet d'au moins 1 megabit/seconde, avec un objectif de 100 megabit/seconde d'ici à 2015.

[44] La loi N° 2/11 de mars 2011, Economie durable, Article 52, a ajouté l'accès au haut débit à ses services universels, et stipulé que la connexion haut débit d'1 megabit/seconde devait être fournie par le biais de toute technologie. Elle a également stipulé que les conditions d'accès au haut débit devaient être établies par décret royal dans un délai de quatre mois à partir de l'entrée en vigueur de la Loi.

[45] Dans sa décision No. 09-013141-0007-CO du 30 juillet 2010, la Cour suprême du Costa Rica a affirmé que l'accès aux technologies de l'information et de la communication devient un outil fondamental pour faciliter l'exercice des droits fondamentaux et de la participation démocratique… Cela comprend le droit fondamental d'accès à ces technologies, en particulier le droit d'accès à l'Internet ou au World Wide Web.

[46] Voir, par exemple, Organe des régulateurs européens des communications électroniques (ORECE), A view of traffic management and other practices resulting in restrictions to the open Internet in Europe, 29 mai 2012.

[47] Ibid.

[48] Déclaration conjointe 2011, op.cit., Article 5.

[49] Adoptées lors de la 3134e Session du Conseil Transports, Télécommunication et Energie, Bruxelles, 13 décembre 2011; à consulter sur http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/trans/126890.pdf.

[50] Résolution du Parlement européen sur l'Internet ouvert et la neutralité d'Internet en Europe, adoptée le 17 novembre 2011, P7_TA(2011)0511.

[51] Résolution du Parlement européen sur l'achèvement du marché unique numérique, adoptée le 11 décembre 2012, 2012/2030(INI).

[52] Résolution du Parlement européen sur une stratégie pour la liberté numérique dans la politique étrangère de l'Union, adoptée le 11 décembre 2012, 2012/2094(INI).

[53] Le Chili est le premier pays à avoir adopté des mesures sur la neutralité du net dans les amendements à sa loi sur les télécommunications entrés en vigueur en mai 2011. Les FAI ne sont pas autorisés à ralentir, bloquer, limiter ou défavoriser des contenus, des applications ou des services ; voir http://www.neutralidadsi.org/2010/07/13/camara-de-diputados-aprueba-el-proyecto-de-ley-de-neutralidad-en-la-red/.

[54] Les amendements à la Loi du 8 mai 2012 sur les Télecommunications interdisent aux fournisseurs de télécommunications de bloquer ou limiter des services tels que Skype ou WhatsApp, des SMS sur Internet [Short Message Service) et de faire en sorte que le prix de leurs services Internet dépende des services utilisés par l'abonné. Alors que le trafic peut être régulé afin d'empêcher une saturation ou de protéger le réseau (à condition que les FAI « traitent le trafic de même type sur un pied d'égalité »), il ne peut être bloqué sauf quand cela est nécessaire pour protéger l'intégrité et la sécurité du réseau ou des terminaux des utilisateurs.

[55] L'Article 203 de la Loi sur les communications économiques du 20 décembre 2012, qui englobe aussi la neutralité du Net, confirme le caractère ouvert et neutre de l'Internet et contraint les FAI et les opérateurs d'Internet à « préserver l'ouverture et la neutralité de l'Internet afin qu'ils ne puissent pas gêner, suspendre ou ralentir le trafic sur Internet au niveau des services ou des applications individuels, ou à prendre des mesures pour affaiblir ces services ou applications ». Les exceptions portent sur la prévention de la saturation du réseau, la préservation de l'intégrité et de la sécurité du réseau, des mesures restreignant les communications non sollicitées, comme prévu par la loi et les décisions d'un tribunal. La loi stipule que les exceptions doivent être « proportionnées, non discriminatoires, limitées dans le temps et appliquées dans la mesure nécessaire pour réaliser leurs objectifs ».

[56] Le 21 décembre 2010, la Commission fédérale des communications américaine (FCC - US Federal Communications Commission) a publié la réglementation 'Formal Complaint Procedures, Preserving the Open Internet and Broadband Industry Practices' (FCC 10-201), qui a pour but de protéger la neutralité du net. La réglementation respecte trois principes fondamentaux : les FAI doivent pratiquer une gestion transparente du réseau ; ils ne sont pas autorisés à bloquer des sites et des services licites ; et les fournisseurs de service haut débit ne peuvent pas défavoriser déraisonnablement le trafic licite sur le réseau.

[57] Première loi introduite en France en 2009, la Loi favorisant la diffusion et la protection de la création sur Internet (HADOPI-I). Toutefois, le Conseil constitutionnel français a déclaré, dans sa Décision 2009-580 DC du 10 juin 2009, que cette loi était contraire à la Déclaration des droits de l'homme et du citoyen, et a décidé que seule une cour de justice ou un juge pouvait imposer une coupure d'accès à Internet. La deuxième loi HADOPI-II imposait la tenue d'un examen judiciaire avant de suspendre l'accès à Internet; toutefois, la déconnexion pour une période d'un an a été conservée. Enfin, le 9 juillet 2013, le gouvernement a publié un décret supprimant la peine complémentaire de la suspension d'accès à Internet, voir http://www.culturecommunication.gouv.fr/Espace-Presse/Communiques/Publication-du-decret-supprimant-la-peine-complementaire-de-la-suspension-d-acces-a-Internet. Toutefois, des juges pourront continuer à imposer des amendes allant jusqu'à 1 500 EUR pour des infractions répétées. Une législation similaire a été votée au Royaume-Uni avec le Digital Economy Act de 2010, paragraphes 3-16. En raison des contestations juridiques des FAI britanniques, selon lesquels la loi ne respectait pas les dispositions européennes relatives à la protection de la vie privée et leur imposait une charge financière excessive, l'entrée en vigueur de certaines dispositions de la loi a été reportée. Cependant, alors que deux dispositions permettant aux tribunaux de bloquer l'accès à certains sites ont été supprimées après de vives critiques, la loi permet à Ofcom d'appliquer une réponse graduée en cas d'infraction au droit d'auteur, y compris d'appliquer une mesure technique qui (a) limite le débit ou autre capacité du service fourni à un abonné, (b) empêche un abonné d'utiliser le service pour accéder à un contenu particulier, ou limite une telle utilisation, (c) suspend le service fourni à un abonné ou (d) limite d'une autre façon le service proposé à un abonné.

[58] Rapport 2011 du Rapporteur spécial, op.cit., par. 78 et 79.

[59] Déclaration conjointe 2011, op.cit., Article 6c).

[60] Voir SABAM c. Netlog, op.cit.; et Scarlet Extended SA c. SABAM, op.cit.

[61] Par exemple, en Turquie, le blocage de la majorité des contenus ne repose pas sur une décision judiciaire mais sur des décisions prises par une autorité administrative.

[62] Voir, par exemple, Bureau du Représentant de l'OSCE pour la liberté des médias, La liberté d'expression sur l'Internet – Etude des dispositions juridiques et des pratiques liées à la liberté d'expression, la libre circulation de l'information et le pluralisme des médias sur Internet dans les Etats membres de l'OSCE, 2012, p. 204ff.

[63] Déclaration conjointe 2011, op. cit. Article 3.

64 Voir Ahmet Yıldırım c. Turquie, Requête no. 3111/10, décision du 18 décembre 2012. L'affaire concernait la décision d'un tribunal de bloquer l'accès au module de création de sites Google Sites, qui entre autres, hébergeait le site du requérant et celui d'un utilisateur accusé d'outrage à la mémoire d'Atatürk. La Cour a estimé que la mesure n'était pas prévue par la loi du fait qu'elle n'était pas raisonnablement prévisible et conforme à l'Etat de droit. De plus, la décision de bloquer tous les sites Google a découlé d'une demande par un organe administratif d'étendre la portée initialement limitée de l'ordre de blocage (limitée au site spécifique) au domaine tout entier. La Cour a par ailleurs estimé que le tribunal turc avait manqué d'appliquer le test de la nécessité quand il a pris sa décision sur le blocage.

65 Rapport 2011 du Rapporteur spécial des Nations Unies, op.cit.

66 Recommandation CM/Rec(2012)3 du Comité des ministres aux Etats membres sur la protection des droits de l'homme dans le contexte des moteurs de recherche, adoptée par le Comité des ministres le 4 avril 2012.

67 Recommandation CM/Rec(2012)4 du Comité des ministres aux Etats membres sur la protection des droits de l'homme dans le cadre des services de réseaux sociaux, adoptée par le Comité des ministre le 4 avril 2012.

68 Par exemple, wired.com a signalé que de mi-2010 à mi-2013, les autorités américaines chargées de l'application de la loi, usant de dispositions sur la confiscation civile, ont saisi plus de 1700 noms de domaine de sites et de blogs ayant prétendument violé la disposition relative aux droits à la propriété intellectuelle (en vertu du Programme 'Operation in Our Sites'). Beaucoup de ces domaines fonctionnaient légalement de l'extérieur des Etats-Unis ; voir http://www.wired.com/threatlevel/2013/06/domains-seized.

69 ACLU, ICE Domain Name Seizures Threaten Due Process and 1st Amendment Rights, 20 juin 2012; à consulter sur http://www.aclu.org/blog/free-speech-national-security-technology-and-liberty/ice-domain-name-seizures-threaten-due.

70 Les Etats ont adopté des approches différentes en matière de responsabilité des prestataires intermédiaires d'Internet, à commencer par des protections étendues contre la responsabilité des fournisseurs de services jusqu'à une responsabilité conditionnelle (procédure de notification et de retrait), et responsabilité globale ou stricte pour les intermédiaires. Pour plus d'information, voir ARTICLE 19, Intermédiaires d'Internet: le dilemme de la responsabilité, août 2013.

71 Par exemple, la Freedom House note que sur les 47 pays qu'elle a récemment examinés, vingt ont connu des évolutions négatives depuis 2011. Même dans les pays qui ont connu des améliorations notables, la tendance générale est à l'augmentation des restrictions à la liberté sur Internet. Voir Freedom House, La liberté sur le Net 2012, p. 1, à consulter sur http://www.freedomhouse.org/sites/default/files/resources/FOTN%202012%20Overview%20Essay.pdf.

72 C'est par exemple le cas de la Russie; voir http://www.nytimes.com/2013/04/01/technology/russia-begins-selectively-blocking-Internet-content.html?_r=0.

73 Voir Joe McNamee, Internet intermediaries: the new cyber police?, 2011, à consulter sur http://www.giswatch.org/en/freedom-association/Internet-intermediaries-new-cyberpolice.

74 Conseil des droits de l'homme, Document A/HRC/17/27 du 16 mai 2011, à consulter sur http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf.

75 Rapport 2011 du Rapporteur spécial des Nations Unies, op.cit.

76 Mécanismes internationaux pour la promotion de la liberté d'expression, Déclaration conjointe sur l'Internet et la lutte contre le terrorisme, 21 décembre 2005.

77 Déclaration conjointe 2011, op.cit., Article 2.

78 Conseil de l'Europe, Comité des ministres, Déclaration sur la liberté de communication sur l'Internet, adoptée le 28 mai 2003.

79 Directive 2000/31/EC du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur (Directive sur le commerce électronique).

80 Ibid. et Déclaration sur la liberté de communication sur l'Internet, op.cit.

81 Déclaration sur la liberté de communication et Internet, Ibid.

82 Voir Mark Sableman, Link Law Revisited: Internet Linking Law at Five Years, 2001; à consulter sur http://www.btlj.org/data/articles/vol16/sableman/sableman.pdf. Voir également Etude sur la responsabilité des prestataires intermédiaires d'Internet, Markt/2006/09/E (Service Contract ETD/2006/IM/E2/69), 12 novembre 2007, à consulter sur http://ec.europa.eu/internal_market/e-commerce/docs/study/liability/final_report_en.pdf.

83 Mouvement Raëlien Suisse v. Suisse, Requête no. 16354/06, 13 juillet 2012.

84 Ibid.

85 Crookes c. Newton, 2009 BCCA 392, 15 septembre 2009; à consulter sur http://www.courts.gov.bc.ca/jdb-txt/CA/09/03/2009BCCA0392err1.htm.

[86] Rapport 2011 du Rapporteur spécial des Nations Unies, op.cit. par. 16.

[87] Ibid., par. 18.

[88] Ibid.

[89] Ibid., par. 38.

[90] Ibid., par. 28.

[91] Par exemple, la Convention du Conseil de l'Europe sur la cybercriminalité, adoptée le 23 novembre 2001 à Budapest, ne contient pas de définition de la cybercriminalité mais dresse une liste des infractions passibles de sanctions par les Etats membres. Voir, http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=ENG. Le Manuel sur la prévention et le contrôle des crimes liés à l'informatique englobe les fraudes, les falsifications et les accès non autorisés dans sa définition des crimes liés à l'informatique ; voir http://www.uncjin.org/Documents/EighthCongress.html. L'Assemblée parlementaire de l'OTAN considère que les cyberattaques équivalent à la cybercriminalité, au cyberterrorisme, ou à la cyberguerre, selon le type d'acteur et les motivations concernés. Voir Assemblée parlementaire de l'OTAN, Rapport annuel 2009 de la réunion du comité, 173 DSCFC 09 E BIS – NATO et Cyberdéfense; à consulter sur http://www.nato-pa.int/default.asp?SHORTCUT=1782.

[92] Le terme « boot net » est utilisé pour démarrer (ou « relancer ») à partir du réseau une procédure ou une série d'opérations qui chargent et démarrent le système d'exploitation.

[93] Rapport 2011 du Rapporteur spécial des Nations Unies, op.cit. par. 34.

[94] Résolution portant sur la « création d'une culture mondiale de la cybersécurité », A/RES/57/239, Jan. 31, 2003; sur http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_57_239.pdf.

[95] Convention sur la cybercriminalité de la Convention de l'Europe, op.cit., Préambule.

[96] Ibid. Article 27(4) (a),

[97] C.f., par exemple, Iran: Computer Crime Laws, 11 janvier 2012, à consulter sur www.article19.org/resources.php/resource/2922/en/iran:-computer-crimes-law; Iraq: Draft Informatics Crimes Law, 26 octobre 2011, à consulter sur www.article19.org/resources.php/resource/2792/en/iraq:-draft-informatics-crimes-law; ou Brazil: Draft Computer Crime Bill, 7 septembre 2012; à consulter sur http://www.article19.org/resources.php/resource/3432/en/brazil:-draft-computer-crime-bill.

[98] Recommandation CM/Rec(2011)7 sur une nouvelle conception des médias, à consulter sur https://wcd.coe.int/ViewDoc.jsp?id=1835645&Site=COE.

[99] Voir le site de la Commission de plaintes en matières de presse, sur http://www.pcc.org.uk/faqs.html#faq2_13.

[100] Voir Recommandation CM/Rec (2011)7, op.cit.

[101] Ibid.

[102] Voir UNESCO, Les activités en communication et information, http://portal.unesco.org/ci/en/ev.php-URL_ID=3038&URL_DO=DO_TOPIC&URL_SECTION=201.html.

[103] Division de l'économie et de l'administration publiques des Nations Unies & la Société américaine de l'administration publique (American Society for Public Administration), Benchmarking E-government: A global perspective – Assessing the progress of member states, mai 2002, p. 1; à consulter sur http://unpan1.un.org/intradoc/groups/public/documents/UN/UNPAN021547.pdf. L'étude distingue cinq stades de l'e-gouvernement : le stade émergent où une simple présence officielle du gouvernement est établie en ligne ; le stade renforcé où l'information fournie devient plus dynamique ; le stade interactif où les utilisateurs peuvent télécharger des formulaires officiels et entrer en interaction sur le web ; l'étape transactionnelle permettant aux utilisateurs de payer des services et autres transactions en ligne ; et enfin l'étape « fluide » qui correspond à une intégration totale des e-services des deux côtés des frontières administratives et à tous les niveaux de l'administration.

[104] Par exemple, l'Autriche, la Suisse et certains Etats fédéraux allemands ont commencé à ouvrir un accès libre aux données; voir http://gov.opendata.at/site/. http://opendata.ch/, ou http://opendata.service-bw.de/Seiten/default.aspx.

[105] A consulter sur : www.zim.mpg.de/openaccess-berlin/berlin_declaration.pdf.

[106] Ibid.

[107] Memorandum of Understanding du 25 novembre 1998; disponible sur http://www.icann.org/en/about/agreements/mou-jpa/icann-mou-25nov98-en.htm.

[108] L'ICANN a entre-temps conclu de nouveaux memorandum avec des commissions nationales et régionales de télécommunications et des organisations internationales comme l'UNESCO, l'Association russe des réseaux et services, la Commission interaméricaine des télécommunications de l'OEA, l'Union africaine des télécommunications, l'Organisation des télécommunications du Commonwealth, et la Pacific Islands Telecommunications Association. Ils sont tous consultables à l'adresse http://www.icann.org/en/about/agreements/partnership-mous. En règle générale, ces memorandum ont pour objectif de favoriser la coopération, l'échange d'information et la construction de partenariats entre les unions des télécommunications et l'ICANN sur des questions liées à la gouvernance d'Internet. Le but est de favoriser le développement des technologies de l'information et de la communication, qui sont liées à la sécurité et la stabilité de l'Internet. Avec l'UNESCO, l'ICANN a conclu un memorandum pour soutenir l'introduction de noms de domaine de premier niveau internationalisés qui permettent aux utilisateurs de créer et utiliser des domaines dans des caractères propres à leur langue.

[109] David P. Fidler, « Internet Governance and International Law: The Controversy Concerning Revision of the International Telecommunication Regulations », American Society of International Law – Insights, Volume 17, Vol. 6, 7 février 2013.

[110] A consulter sur http://www.itu.int/wsis/implementation/igf/index.html.

[111] Déclaration de Principes, Construire la société de l'information : un défi mondial pour le nouveau millénaire, WSIS-03/GENEVA/DOC/4-E, 12 décembre 2003; à consulter sur http://www.itu.int/wsis/docs/geneva/official/dop.html.

[112] Ibid.

[113] Ibid.

[114] Tous les documents et positions gouvernementales en rapport avec le SMSI de Tunis en 2005 peuvent être consultés sur http://www.itu.int/wsis/documents/listing-all.asp?lang=en&c_event=pc2|3&c_type=all.|.

[115] Voir Proposition sur la gouvernance de l'Internet de l'Union européenne (UK), WSIS-II/PC-3/DT/21, PrepCom-3, Genève, 19-30 septembre 2005.

[116] Engagement de Tunis, WSIS-05/TUNIS/DOC/7-E, 18 novembre 2005.

[117] Voir WSIS-05/TUNIS/DOC/6(Rev. 1)-E, 18 novembre 2005, par. 34; sur http://www.itu.int/wsis/docs2/tunis/off/6rev1.html.

[118] Ibid, par. 72.

[119] Déclaration du Comité des ministres sur les principes de la gouvernance de l'Internet, adoptée par le Comité des ministres le 21 septembre 2011 lors de la 1121e réunion des Délégués des ministres, à consulter sur https://wcd.coe.int/ViewDoc.jsp?id=1835773.

[120] OSCE, Recommandations d'Amsterdam, 14 juin 2003, à consulter sur http://www.osce.org/fom/41903.

[121] Déclaration conjointe 2005, op.cit.

[122] Voir Déclaration conjointe du dixième anniversaire : les dix défis clés pour la liberté d'expression au cours de la prochaine décennie, sur http://www.osce.org/fom/41439.

[123] Déclaration conjointe 2011, op.cit.