Module 3

Accès à l'Internet

Modules de synthèse sur les litiges relatifs aux droits numériques et à la liberté d'expression en ligne

MEDIA DEFENCE

Publié par Media Defence : www.mediadefence.org
Ce module a été préparé avec l'aide d'ALT Advisory : https://altadvisory.africa/

Décembre 2020

Ce travail est soumis à la licence internationale « Creative Commons Attribution-NonCommercial 4.0 ». Cela signifie que vous êtes libre de partager et d'adapter ce travail à condition de mentionner le crédit approprié, de fournir un lien vers la licence et d'indiquer si des modifications ont été apportées. Tout partage ou adaptation de ce type doit être effectué à des fins non commerciales et doit être mis à disposition dans les mêmes conditions de « partage égal ». Les conditions de licence complètes sont disponibles à l'adresse https://creativecommons.org/licenses/by-ncsa/4.0/legalcode.

TABLE DES MATIÈRES

EXISTE-T-IL UN DROIT À L'INTERNET EN VERTU DU DROIT INTERNATIONAL ? 1
INTERFÉRENCES AVEC L'ACCÈS À L'INTERNET 5
QU'EST-CE QU'UNE FERMETURE D'INTERNET ? 6
QU'EST-CE QUE LE BLOCAGE ET LE FILTRAGE DES CONTENUS ? 7
QU'EST-CE QUE LA NEUTRALITÉ DU RÉSEAU ? 8
LIMITATION DU DROIT À LA LIBERTÉ D'EXPRESSION 9
LA SÉCURITÉ NATIONALE COMME MOTIF DE JUSTIFICATION 11
RESPONSABILITÉ DES INTERMÉDIAIRES 13
CONCLUSION 16

MODULE 3

ACCÈS À L'INTERNET

- **Un droit explicite à l'Internet n'a pas été reconnu dans le droit international. Toutefois, il est largement admis que l'accès à l'Internet permet d'exercer toute une série d'autres droits fondamentaux.**

- **Des pratiques telles que la fermeture de l'Internet, le blocage et le filtrage des contenus violent souvent les droits à la liberté d'expression et ne constituent pas une limitation justifiable.**

- **La sécurité nationale est souvent invoquée pour justifier une interférence avec l'accès à l'Internet, ainsi que d'autres interférences avec le droit à la liberté d'expression. Bien que la sécurité nationale figure parmi les objectifs légitimes de dérogation au droit à la liberté d'expression dans des circonstances appropriées, elle est souvent utilisée par les États pour réprimer la dissidence et dissimuler les abus de l'État.**

- **La « neutralité du Net » fait référence au principe selon lequel toutes les données de l'Internet doivent être traitées de la même manière sans interférence indue, et le concept promeut l'accès le plus large possible à l'information sur l'Internet.**

- **La responsabilité des intermédiaires est engagée lorsque les gouvernements ou les parties privées peuvent tenir les intermédiaires technologiques, tels que les fournisseurs d'accès internet (FAI) et les sites web, pour responsables des contenus illicites ou préjudiciables créés par les utilisateurs de ces services. Cette responsabilité a un effet dissuasif sur la liberté d'expression en ligne.**

EXISTE-T-IL UN DROIT À L'INTERNET EN VERTU DU DROIT INTERNATIONAL ?

Un droit explicite à l'Internet n'a pas encore été reconnu dans un traité international ou un instrument similaire. Cela a été la source de nombreux débats, et les arguments pour et contre le droit d'accès à l'Internet sont nombreux.

Arguments en faveur de l'accès à l'Internet en tant que droit de l'homme[1]	**Arguments contre l'accès à l'Internet en tant que droit de l'homme**
• **Nécessité**. Il existe un certain consensus non seulement sur l'utilité de l'Internet, mais aussi sur son rôle crucial en tant « qu'outil indispensable » pour les droits de l'homme et le développement au cours du siècle actuel. • **Existence implicite dans le droit international actuel des droits de l'homme**. Le plein exercice de la liberté d'expression, la participation à la vie culturelle et la jouissance des bienfaits scientifiques nécessitent l'accès à l'Internet. Les niveaux de vie actuels incluent la participation à la communauté au sens large de différentes manières, par exemple par la connexion à l'Internet. • **Inévitable**. Plusieurs pays, dont la Grèce, l'Estonie, la Finlande, l'Espagne, le Costa Rica et la France, ont affirmé ou reconnu un certain droit d'accès dans leur constitution, leur code juridique ou leurs décisions judiciaires. Ces documents sont plus facilement accessibles en ligne. • **Inséparabilité**. Les progrès technologiques modifient la manière dont les gens jouissent de leurs droits et les gouvernements doivent se pencher sur le lien entre ces droits et leurs méthodes actuelles de jouissance.	• **Aucun traité international ne crée directement un droit d'accès à l'Internet, bien que certains pays, principalement en Europe, aient une législation nationale qui le fait**. En termes simples, il ne s'agit pas d'un droit de l'homme si la communauté internationale ne l'a pas reconnu comme tel dans un instrument contraignant, et qu'il n'y a pas de discussion sur un nouveau traité pour le faire dans un quelconque forum. • **Analogie avec d'autres formes de médias**. Il n'y a pas de droit au téléphone, à la télévision, à la presse écrite (que ce soit pour la publier ou la recevoir) ou à tout autre média similaire qui a imposé aux États l'obligation de le fournir à leurs citoyens et d'en couvrir les coûts. • **Universalité**. L'accès à l'Internet n'est pas un droit économique qui peut être interprété à partir de l'article 11 du PIDESC et de l'article 25 de la DUDH, car ils sont représentatifs de niveaux de vie qui ne peuvent être considérés à la même échelle pour des pays ayant des stades de développement très différents. • **La nature comme un droit**. Même s'il y a une considération juridique de l'accès, il est établi non pas comme un droit individuel, mais comme une obligation pour les États.

[1] Juan Carlos Lara, « Internet access and economic, social and cultural rights », Association pour le progrès des communications (septembre 2015), pages 10 à 11 (accessible en anglais sur : https://www.apc.org/sites/default/files/APC_ESCR_Access_Juan%20Carlos%20Lara_September2015%20%281%29_0.pdf). Voir également le Rapport 2019 du groupe de haut niveau du secrétaire général des Nations unies sur la coopération numérique, qui note que « les droits de l'homme universels s'appliquent aussi bien en ligne que hors ligne ; la liberté d'expression et de réunion, par exemple, n'est pas moins importante dans le cyberespace que sur l'espace public », page 16 (accessible en anglais sur : https://www.un.org/en/pdfs/DigitalCooperation-report-for%20web.pdf). Dans l'affaire *« Delfi v Estonia »*, la Cour européenne des droits de l'homme a estimé qu'Internet constituait une plateforme sans précédent pour l'exercice du droit à la liberté d'expression (accessible sur : https://globalfreedomofexpression.columbia.edu/cases/delfi-as-v-estonia/).

• **Progression**. La notion de droits elle-même a la capacité de changer, à mesure que les contextes sociaux évoluent. L'importance croissante de l'Internet dans des contextes sociaux changeants rend nécessaire d'en assurer l'accès. • **Soutien du public**. Les enquêtes mondiales montrent une seule attitude prédominante à l'égard de l'accès à l'Internet : que celui-ci doit être reconnu comme un droit.[2]	• **Moyens de parvenir à une fin.** L'accès à l'Internet est constitué par une technologie, qui est un outil, et non un droit en soi. • L'**accès à l'Internet n'est pas absolument nécessaire pour participer à une communauté politique**. Une grande partie de la population mondiale n'a pas accès à l'Internet. Ce n'est que lorsque cette participation existe déjà et qu'elle est supprimée qu'elle attire l'attention. • **Inflation**. Prétendre qu'un intérêt est un droit fondamental ou de l'homme, sans tenir compte des conditions dans lesquelles il peut réellement être réalisé, gonfle le nombre de droits, diminuant la force des principaux droits de l'homme traditionnels. • **Flexibilité des droits de l'homme existants**. Il n'est pas nécessaire de « créer » de nouveaux droits en plus de ceux déjà reconnus, mais de garantir leur exercice et leur jouissance dans des contextes technologiques changeants. • **Effets secondaires**. Les politiques d'inclusion numérique comportent des préoccupations concernant le véritable bénéficiaire. D'une part, les politiques d'accès profiteront aux utilisateurs qui disposent de dispositifs permettant d'accéder à l'Internet, ce qui exacerbe les inégalités. D'autre part, l'absence de contrôle des gouvernements entraînerait la nécessité d'investir dans des entreprises de télécommunications privées, leur accordant ainsi un avantage économique avant les citoyens.

Il est de plus en plus reconnu que l'accès à l'Internet est indispensable à la jouissance d'un ensemble de droits fondamentaux. Le corollaire est que ceux qui n'ont pas accès à l'Internet sont privés de la pleine jouissance de ces droits, ce qui, dans de nombreux cas, peut exacerber des divisions socio-économiques déjà existantes. Par exemple, un manque

[2] The Internet Society, « Global Internet User Survey 2012 » (2012) (accessible en anglais sur : https://wayback.archive-it.org/9367/20170907075228/https://www.internetsociety.org/sites/default/files/rep-GIUS2012global-201211-en.pdf).

d'accès à l'Internet peut empêcher un individu d'obtenir des informations clés, de faciliter le commerce, de rechercher un emploi ou de consommer des biens et des services.

L'accès comporte deux dimensions distinctes, mais interdépendantes : (i) la possibilité de voir et de diffuser du contenu en ligne ; et (ii) la possibilité d'utiliser l'infrastructure physique pour permettre l'accès à ce contenu en ligne. En 2003, l'UNESCO a été l'un des premiers organismes internationaux à appeler les États à prendre des mesures pour réaliser un droit d'accès à l'Internet. À cet égard, elle a déclaré que :[3]

> « Les États membres et les organisations internationales doivent promouvoir l'accès à l'Internet en tant que service d'intérêt public par l'adoption de politiques appropriées afin de renforcer le processus d'autonomisation de la citoyenneté et de la société civile, et en encourageant la mise en œuvre appropriée de ces politiques et le soutien à celles-ci dans les pays en développement, en tenant dûment compte des besoins des communautés rurales.
> …
> Les États membres doivent reconnaître et promulguer le droit d'accès en ligne universel aux documents publics et détenus par les pouvoirs publics, y compris les informations pertinentes pour les citoyens dans une société démocratique moderne, en tenant dûment compte des préoccupations en matière de confidentialité, de respect de la vie privée et de sécurité nationale, ainsi que des droits de propriété intellectuelle dans la mesure où ils s'appliquent à l'utilisation de ces informations. Les organisations internationales doivent reconnaître et promulguer le droit pour chaque État d'avoir accès aux données essentielles relatives à sa situation sociale ou économique ».

En 2012, le Conseil des droits de l'homme des Nations unies (CDHNU) a adopté une importante résolution qui « appelle tous les États à faciliter l'accès à l'Internet et la coopération internationale visant à développer les médias et les moyens de communication de l'information dans tous les pays ».[4]

Les Objectifs de développement durable (ODD) des Nations unies reconnaissent que « la diffusion des technologies de l'information et des communications et l'interconnexion mondiale offrent un potentiel considérable pour accélérer le progrès humain, combler la fracture numérique et développer des sociétés de la connaissance ».[5] Les ODD appellent en outre les États à renforcer l'utilisation des technologies de l'information et de la communication (TIC) et d'autres technologies habilitantes pour promouvoir l'autonomisation des femmes,[6] et

---

[3] UNESCO, « Recommandation sur la promotion et l'usage du multilinguisme et l'accès universel au cyberespace », paragraphes 7 et 15 (accessible sur : http://portal.unesco.org/fr/ev.php-URL_ID=17717&URL_DO=DO_TOPIC&URL_SECTION=201.html).

[4] CDHNU, « Résolution portant sur la promotion, la protection et l'exercice des droits de l'homme sur Internet », A/HRC/20/L.13, 29 juin 2012, paragraphe 2 (accessible sur : https://digitallibrary.un.org/record/845728/files/A_HRC_32_L-20-FR.pdf). Ce point a été développé l'année suivante dans la « Résolution portant sur la promotion, la protection et l'exercice des droits de l'homme sur Internet » du CDHNU, A/HRC/Res/26/13, 14 juillet 2014 (accessible sur : https://hrlibrary.umn.edu/hrcouncil_res26-13.pdf).

[5] AGNU, « Transformer notre monde : le programme de développement durable à l'horizon 2030 », A/Res/70/1, 21 octobre 2015 au paragraphe 15 (accessible sur https://digitallibrary.un.org/record/809145?ln=fr).

[6] Au même en droit à l'objectif 5(b) en page 18.

à s'efforcer de fournir un accès universel et abordable à l'Internet dans les pays les moins avancés d'ici 2020.[7]

La résolution des Nations unies sur l'Internet de 2016, adoptée par le Conseil des droits de l'homme des Nations unies, reconnaît que l'Internet peut accélérer les progrès vers le développement, y compris dans la réalisation des ODD, et affirme l'importance d'appliquer une approche fondée sur les droits pour fournir et étendre l'accès à l'Internet.[8] Elle affirme notamment l'importance d'appliquer une approche globale fondée sur les droits pour fournir et élargir l'accès à l'Internet,[9] et appelle les États à envisager de formuler et d'adopter des politiques publiques nationales liées à l'Internet, dont l'objectif central est l'accès universel et la jouissance des droits de l'homme.[10]

Que l'Internet soit considéré comme un droit autonome ou comme un outil permettant de faciliter la réalisation d'autres droits, les bases ont été fermement jetées pour la nécessité de réaliser l'accès universel à l'Internet. Les États sont simultanément tenus de prendre des mesures pour atteindre l'accès universel. Cependant, en réalité, l'accès universel à l'Internet est loin d'être réalisé. Cela est dû à une confluence de facteurs, notamment le manque de ressources financières pour pouvoir accéder à l'Internet, l'inadéquation des contenus pertinents au niveau local, les niveaux insuffisants de culture numérique et le manque de volonté politique pour en faire une priorité.

Dans l'affaire *« Kalda v Estonia »*, la Cour européenne des droits de l'homme (CEDH) a estimé que le droit à la liberté d'expression du requérant avait été violé par le refus d'une prison de lui donner accès à des sites Internet contenant des informations juridiques, car cela avait violé son droit à recevoir des informations.[11] La Cour européenne des droits de l'homme a noté que lorsqu'un État est disposé à permettre aux prisonniers d'accéder à l'Internet, comme dans l'affaire en question, celui-ci doit donner des raisons pour refuser l'accès à des sites spécifiques.[12]

INTERFÉRENCES AVEC L'ACCÈS À L'INTERNET

L'accès à l'Internet est parfois entravé par des fermetures d'accès, la perturbation des réseaux en ligne et des sites de médias sociaux, ainsi que par le blocage et le filtrage des contenus. De telles interférences peuvent poser de graves restrictions à l'exercice du droit à la liberté d'expression, ainsi qu'à la jouissance d'une série d'autres droits et services (notamment les

---

[7] Au même en droit à l'objectif 9(c) en page 21.

[8] CDHNU, « Résolution portant sur la promotion, la protection et l'exercice des droits de l'homme sur Internet », A/HRC/Res/32/13, 18 juillet 2016, paragraphe 2 (accessible sur : https://digitallibrary.un.org/record/845728/files/A_HRC_32_L-20-FR.pdf).

[9] Même endroit au paragraphe 5.

[10] Même endroit au paragraphe 12.

[11] Demande n° 17429, 19 janvier 2016 (accessible en anglais sur : https://hudoc.echr.coe.int/eng?i=001-160270).

[12] Même endroit au paragraphe 53. Dans la décision ultérieure de « *Jankovskis v Lithuania* », Demande nº 21575/08, 17 janvier 2017 (accessible sur : https://hudoc.echr.coe.int/eng?i=001-170354), également relative à un prisonnier qui s'était vu refuser l'accès à un site web contenant des informations liées à l'éducation, la CEDH a de nouveau confirmé le grief de violation du droit à la liberté d'expression formulé par le requérant.

services bancaires mobiles, le commerce en ligne et la possibilité d'accéder aux services gouvernementaux via l'Internet).

Le fait de perturber ou de bloquer l'accès aux services internet et aux sites web constitue une forme de restriction préalable. Les restrictions préalables sont des actions de l'État qui interdisent la parole ou d'autres formes d'expression avant qu'elles ne puissent avoir lieu.[13] En raison de l'effet paralysant que peut avoir la restriction préalable sur l'exercice du droit à la liberté d'expression, le Pacte international relatif aux droits civils et politiques (PIDCP) a été interprété comme prévoyant effectivement l'interdiction de la plupart des formes de restriction préalable de la liberté d'expression.[14] La Convention américaine des droits de l'homme contient une interdiction similaire.[15] Il est donc impératif, pour qu'une telle mesure soit admissible, qu'elle puisse se conformer au test de limitation en trois parties détaillé dans le module 1.

QU'EST-CE QU'UNE FERMETURE D'INTERNET ?

Une fermeture d'Internet peut être définie comme une perturbation intentionnelle de l'Internet ou des communications électroniques, les rendant inaccessibles ou effectivement inutilisables, pour une population spécifique ou dans un lieu donné, souvent pour exercer un contrôle sur le flux d'informations. En d'autres termes, cela se produit lorsque quelqu'un, que ce soit le gouvernement ou un acteur du secteur privé, perturbe intentionnellement l'Internet, un réseau de télécommunications ou un service internet, sans doute pour contrôler ou limiter ce que les gens disent ou font.[16] On parle aussi parfois de « coupe-circuit ».

Dans certains cas, cela peut entraîner une panne totale du réseau, ce qui entraîne l'arrêt complet de l'accès à l'Internet. Dans d'autres circonstances, cela peut également se produire lorsque l'accès aux communications mobiles, aux sites web ou aux médias sociaux et aux applications de messagerie est bloqué, ralenti ou rendu effectivement inutilisable.[17] Les fermetures peuvent toucher un pays entier, des villes ou des régions d'un pays, voire plusieurs pays, et ont été observées sur une période allant de quelques heures à plusieurs mois.[18]

---

[13] Conseil de l'Europe, « Prior Restraints and Freedom Of Expression: The Necessity of Embedding Procedural Safeguards in Domestic System » (mai 2018), (accessible en anglais sur : https://rm.coe.int/factsheet-prior-restraints-rev25may2018/16808ae88c).

[14] Cela a été déduit des *travaux préparatoires* du PIDCP que les restrictions préalables sont absolument interdites en vertu de l'article 19 du PIDCP. Voir Marc J. Bossuyt, « Guide to the "Travaux Preparatoires" of the International Covenant on Civil and Political Rights », Martinus Nijhoff (1987), page 398.

[15] Article 13 : « 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 nature, sans considération de frontières, sous une forme orale, écrite, imprimée ou artistique, ou par tout autre moyen de son choix. 2. L'exercice du droit prévu au paragraphe précédent n'est pas soumis à une censure préalable, mais fait l'objet d'une responsabilité ultérieure, qui est expressément établie par la loi dans la mesure nécessaire pour assurer : a. le respect des droits ou de la réputation d'autrui ; ou b. la protection de la sécurité nationale, de l'ordre public, de la santé ou de la moralité publiques ».

[16] *Idem*

[17] Rapport du Rapport spécial des Nations Unies (RSNU) sur la liberté d'expression à l'AGNU, A/HRC/35/22, 30 mars 2017 (Rapport du RSNU sur la liberté d'expression de 2017) au paragraphe 8 (accessible sur : https://digitallibrary.un.org/record/1298717/files/A_HRC_35_22-FR.pdf).

[18] *Idem*

Il convient de noter que pour procéder à des fermetures, les gouvernements ont généralement besoin de l'action d'acteurs privés qui exploitent les réseaux ou facilitent le trafic sur les réseaux.[19] Comme l'a fait remarquer le Rapporteur spécial des Nations unies (RSNU) sur la liberté d'expression, les attaques à grande échelle sur les infrastructures de réseau commises par des parties privées, telles que les attaques par déni de service distribué (connues sous le nom de « DDoS »), peuvent également avoir des effets de fermeture.

Un tribunal de la CEDEAO juge illégale la fermeture d'Internet

Dans une affaire historique confirmant que les fermetures d'Internet constituent une forme de restriction préalable, en juin 2020, la Cour de justice de la Communauté économique des États de l'Afrique de l'Ouest (CEDEAO) a jugé que les fermetures d'Internet mises en œuvre par le gouvernement togolais en 2017 étaient illégales.[20]

QU'EST-CE QUE LE BLOCAGE ET LE FILTRAGE DES CONTENUS ?

Bien qu'il s'agisse d'une mesure moins radicale qu'une fermeture complète de l'Internet, le blocage et le filtrage des contenus en ligne peuvent également entraver la pleine jouissance du droit à la liberté d'expression.

Le blocage/filtrage a été défini comme suit :

> « [L]a différence entre "filtrage" et "blocage" est une question d'échelle et de perspective.
>
> - Le filtrage est généralement associé à l'utilisation d'une technologie qui bloque les pages en fonction de certaines caractéristiques, telles que les schémas de trafic, les protocoles ou les mots clés, ou sur la base de leur lien perçu avec un contenu jugé inapproprié ou illégal ;
> - Le blocage, en revanche, consiste généralement à empêcher l'accès à des sites web, domaines, adresses IP, protocoles ou services spécifiques figurant sur une liste noire ».[21]

Par exemple, en mars 2020, des sites de médias sociaux ont été bloqués en Guinée lors d'un référendum ;[22] et en octobre de la même année, une fermeture générale d'Internet a suivi pendant les élections générales.[23] Même après le rétablissement de la connexion générale, les utilisateurs ont signalé que certains sites, en particulier Facebook, sont restés bloqués

---

[19] *Idem*

[20] Cour de justice de la CEDEAO, procès n° ECW/CCJ/APP/61/18 (2020) (accessible en anglais sur : http://prod.courtecowas.org/wp-content/uploads/2020/09/JUD_ECW_CCJ_JUD_09_20.pdf).

[21] ARTICLE 19, « Freedom of expression unfiltered: How blocking and filtering affect free speech », octobre 2016, page 7 (accessible en anglais sur : https://www.article19.org/data/files/medialibrary/38588/Blocking_and_filtering_final.pdf).

[22] Access Now, « A broken promise to #KeepItOn : Guinea cuts internet access and blocks social media on referendum day » (2020) (accessible sur : https://www.accessnow.org/a-broken-promise-to-keepiton-guinea-cuts-internet-access-and-blocks-social-media-on-referendum-day/).

[23] Access Now, « How internet shutdowns are threatening 2020 elections, and what you can do about it » (2020) (accessible sur : https://www.accessnow.org/internet-shutdowns-2020-elections/).

pendant quelques semaines de plus. La Guinée est malheureusement loin d'être le seul pays africain à mettre en œuvre de telles techniques ces dernières années.[24]

QU'EST-CE QUE LA NEUTRALITÉ DU RÉSEAU ?

La neutralité du réseau (ou « neutralité du Net ») fait référence au principe selon lequel toutes les données de l'Internet doivent être traitées de la même manière sans interférence indue et promeut l'accès le plus large possible à l'information sur l'Internet.[25] En d'autres termes, les FAI doivent traiter toutes les données qui transitent sur leurs réseaux de manière équitable, sans discrimination indue en faveur d'une application, d'un site web ou d'un service particulier.[26] La discrimination à cet égard peut consister à affecter l'information de manière à interrompre, ralentir ou altérer de toute autre manière le transfert de toute donnée, sauf à des fins légitimes de gestion du réseau, telles que le désengorgement ou le blocage de spams.[27]

Le rapport de 2017 du RSNU pour la liberté d'expression décrit deux manières principales dont la neutralité du réseau peut être affectée :[28]

- **Les systèmes de priorisation payante** - lorsque des fournisseurs accordent un traitement préférentiel à certains types de trafic internet par rapport à d'autres pour un paiement ou un autre avantage commercial.
- **Taux nul** - qui est la pratique consistant à ne pas facturer l'utilisation des données internet associées à une application ou à un service particulier ; les autres services ou applications, quant à eux, sont soumis à un coût mesuré.

Dans divers pays d'Afrique, l'accès aux contenus à taux nul a fait l'objet d'un débat important, notamment en ce qui concerne les sites de réseaux sociaux qui offrent un certain accès gratuit aux utilisateurs. D'une part, le taux nul donne accès à des personnes qui, autrement, n'auraient peut-être pas pu accéder à l'Internet, et peut servir de passerelle aux utilisateurs pour comprendre les possibilités que l'Internet peut offrir. D'autre part, le taux nul peut conduire à une concurrence déloyale et peut fausser la perception des utilisateurs en ne permettant que l'accès à des sites particuliers.[29]

---

[24] BBC, « Africa internet: Where and how are governments blocking it? » (2020) (accessible en anglais sur : https://www.bbc.com/news/world-africa-47734843).

[25] Rapport 2017 du RSNU sur la liberté d'expression ci-dessus, point nº 17 au paragraphe 23.

[26] Electronic Frontier Foundation, « Net neutrality » (accessible en anglais sur : https://www.eff.org/issues/net-neutrality).

[27] American Civil Liberties Union, « What is net neutrality? » (accessible en anglais sur : https://www.aclu.org/issues/free-speech/internet-speech/what-net-neutrality).

[28] Rapport de 2017 de l'UNSR sur la liberté d'expression ci-dessus, point nº 17 aux paragraphes 24 à 28.

[29] Pour une discussion sur le taux zéro en Afrique, voir Research ICT Africa, « Much ado about nothing? Zero-rating in the African context », 12 septembre 2016 (accessible en anglais sur : https://www.researchictafrica.net/publications/Other_publications/2016_RIA_Zero-Rating_Policy_Paper_-_Much_ado_about_nothing.pdf).

LIMITATION DU DROIT À LA LIBERTÉ D'EXPRESSION

En 2016, le RSNU sur la liberté d'expression a noté que « le blocage des plateformes internet et la fermeture des infrastructures de télécommunications sont des menaces persistantes, car même si elles sont fondées sur la sécurité nationale ou l'ordre public, elles tendent à bloquer les communications de millions de personnes ».[30] Cela constitue une limitation évidente du droit à la liberté d'expression, et peut limiter encore davantage toute une série d'autres droits.

La déclaration commune de 2011 sur la liberté d'expression et l'Internet souligne le caractère flagrant de ces limitations :[31]

> « (a) Le blocage obligatoire de sites web entiers, d'adresses [de protocole internet (IP)], de ports, de protocoles de réseau ou de types d'utilisation (tels que les réseaux sociaux) est une mesure extrême (analogue à l'interdiction d'un journal ou d'un diffuseur) qui ne peut être justifiée que conformément aux normes internationales, par exemple lorsque cela est nécessaire pour protéger les enfants contre les abus sexuels.
>
> (b) Les systèmes de filtrage de contenu imposés par un gouvernement ou un fournisseur de services commerciaux et qui ne sont pas contrôlés par l'utilisateur final constituent une forme de censure préalable et ne peuvent être justifiés comme une restriction de la liberté d'expression.
>
> (c) Les produits conçus pour faciliter le filtrage par l'utilisateur final devraient être accompagnés d'informations claires à l'intention des utilisateurs finaux sur leur mode de fonctionnement et les pièges potentiels en termes de filtrage trop inclusif ».

Les fermetures d'Internet et de télécommunications qui impliquent des mesures visant à empêcher ou à perturber intentionnellement l'accès à l'information en ligne ou sa diffusion constituent une violation de la législation sur les droits de l'homme.[32] Dans la résolution de 2016 des Nations unies sur l'Internet, le Conseil des droits de l'homme des Nations unies a déclaré qu'il « condamne sans équivoque les mesures visant à prévenir ou à interrompre intentionnellement l'accès à l'information en ligne ou sa diffusion, en violation du droit international des droits de l'homme, et appelle tous les États à s'abstenir de prendre de telles mesures et à y mettre fin ».[33]

Comme indiqué dans l'Observation générale n° 34 :[34]

> « Toute restriction au fonctionnement des sites web, des blogs ou de tout autre système de diffusion de l'information basé sur l'Internet, électronique ou autre, y compris les

---

[30] Rapport du RSNU sur la liberté d'expression à l'AGNU, A/71/373, 6 septembre 2016 (Rapport 2016 du RSNU sur la liberté d'expression) au paragraphe 22 (accessible sur : https://digitallibrary.un.org/record/844396/files/A_71_373-FR.pdf).

[31] Mécanismes internationaux pour la promotion de la liberté d'expression, « Déclaration commune sur la liberté d'expression et l'Internet », 1er juin 2011 (Déclaration commune 2011) (accessible sur : https://www.achpr.org/public/Document/file/French/declaration_crime_liberte_dexpression.pdf).

[32] Rapport 2017 du RSNU sur la liberté d'expression ci-dessus, point nº 17 au paragraphe 8.

[33] Résolution de 2016 de l'ONU sur l'Internet ci-dessus, point nº 8 au paragraphe 10.

[34] Observation générale nº 34 au paragraphe 43.

> systèmes de soutien à cette communication, tels que les fournisseurs d'accès Internet ou les moteurs de recherche, n'est autorisée que dans la mesure où elle est compatible avec [l'article 19(3) du PIDCP]. Les restrictions autorisées doivent généralement être spécifiques au contenu ; les interdictions génériques d'exploitation de certains sites et systèmes ne sont pas compatibles avec [l'article 19(3) du PIDCP]. Il est également incompatible avec [l'article 19(3) du PIDCP] d'interdire à un site ou à un système de diffusion de l'information de publier du matériel au seul motif qu'il pourrait être critique envers le gouvernement ou le système politique et social adopté par le gouvernement ».

Le RSNU sur la liberté d'expression a noté que les fermetures d'Internet sont souvent ordonnées secrètement et sans fondement juridique, et violent l'exigence selon laquelle les restrictions doivent être prévues par la loi.[35] De même, les fermetures ordonnées en vertu de lois et règlements formulés de manière vague, ou de lois et règlements adoptés et appliqués en secret, ne satisfont pas non plus à l'exigence de légalité.[36] Dans certains pays, cela a conduit le gouvernement à promulguer de nouvelles lois pour permettre expressément des fermetures.[37]

Le RSNU sur la liberté d'expression a en outre noté que les fermetures de réseaux ne répondent invariablement pas au critère de nécessité,[38] et sont généralement disproportionnées.[39] Les États cherchent souvent à justifier cette situation par des raisons de sécurité nationale, qui sont examinées plus loin. Par exemple, le Tchad a bloqué les médias sociaux pendant une période de 472 jours en 2018,[40] ostensiblement pour des raisons de sécurité. Une procédure a été engagée contre deux fournisseurs d'accès Internet,[41] mais l'accès a été rétabli peu après.

---

[35] Rapport 2017 du RSNU sur la liberté d'expression au paragraphe 9.

[36] Même endroit au paragraphe 10.

[37] En Inde, par exemple, après qu'Internet a été fermé plus de 40 fois au cours de l'année 2017, le ministère des télécommunications a publié en août 2017 de nouvelles règles, les « Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules », permettant au gouvernement de fermer les services téléphoniques et Internet en cas d'urgence publique ou pour des raisons de sécurité publique. Le gouvernement s'était auparavant appuyé sur l'article 144 du code pénal qui visait à empêcher « l'obstruction, la gêne ou le préjudice » pour imposer des restrictions sur Internet. Cette évolution juridique a suscité des réactions mitigées. D'une part, les nouvelles règles signifieraient potentiellement que, si le gouvernement devait persister à fermer l'Internet, cela pourrait se faire de manière plus organisée. D'autre part, des inquiétudes ont été exprimées quant à l'absence de définition des termes « urgence publique » ou « sécurité publique », et au potentiel que ces nouvelles règles pourraient avoir pour la censure en ligne. Voir : par exemple, http://www.hindustantimes.com/india-news/govt-issues-first-ever-rules-to-carry-out-internet-shutdowns-in-india/story-Drn0MnxJAp58RoZoFI7u4L.html.)

[38] Rapport 2017 du RSNU sur la liberté d'expression ci-dessus, point nº 17 au paragraphe 14.

[39] Même endroit au paragraphe 15.

[40] Quartz Africa, « Chad has now spent a full year without access to social media » (2019) (accessible en anglais sur : https://qz.com/africa/1582696/chad-has-blocked-whatsapp-facebook-twitter-for-a-year/).

[41] Africa News, « Chadian lawyers challenge ongoing social media shutdown » (2018) (accessible en anglais sur : https://www.africanews.com/2018/08/21/chadian-lawyers-challenge-ongoing-social-media-shutdown//).

Litige sur la fermeture de l'Internet au Cameroun

Media Defence aide actuellement à plaider une affaire devant le Conseil constitutionnel du Cameroun. En janvier 2020, l'Internet a été fermé suite aux protestations contre l'arrestation de dirigeants de la société civile qui résistaient aux efforts du gouvernement pour imposer les systèmes juridiques et éducatifs francophones dans ces régions à prédominance anglophone. L'Internet est resté fermé pendant 93 jours et a été remis en service quelques heures après que Veritas Law ait déposé un recours constitutionnel. Le recours constitutionnel a été lancé pour obliger le gouvernement à rétablir l'Internet et pour que le Conseil constitutionnel puisse empêcher le gouvernement de fermer l'Internet à l'avenir. Plus d'informations ici.

En ce qui concerne le blocage et le filtrage des contenus, il peut en effet y avoir des circonstances dans lesquelles de telles mesures sont justifiables. Par exemple, en ce qui concerne les sites web distribuant de la pornographie enfantine. Ces mesures sont toujours nécessaires pour satisfaire au test en trois parties d'une limitation justifiable. Cela devra être évalué au cas par cas.

De même, des limitations de la neutralité du réseau peuvent également être autorisées dans certaines circonstances, par exemple à des fins légitimes de gestion du réseau. Toutefois, en règle générale, il ne devrait pas y avoir de discrimination dans le traitement des données et du trafic Internet, quels que soient le dispositif, le contenu, l'auteur, l'origine et/ou la destination du contenu, du service ou de l'application.[42] En outre, les intermédiaires Internet doivent être transparents quant aux pratiques de gestion du trafic ou de l'information qu'ils emploient, et les informations pertinentes sur ces pratiques doivent être mises à disposition sous une forme accessible à toutes les parties prenantes.[43]

LA SÉCURITÉ NATIONALE COMME MOTIF DE JUSTIFICATION

La sécurité nationale est souvent invoquée pour justifier une interférence avec l'accès à l'Internet, ainsi que d'autres interférences avec le droit à la liberté d'expression.[44] Si cet objectif peut, dans des circonstances appropriées, être légitime, il peut également être utilisé pour réprimer la dissidence et dissimuler les abus de l'État.

La nature secrète de nombreuses lois, politiques et pratiques de sécurité nationale, ainsi que le refus des États de divulguer des informations sur la menace à la sécurité nationale, tendent à exacerber cette préoccupation. En outre, les tribunaux et autres institutions ont souvent fait

[42] Déclaration commune 2011 ci-dessus, point nº 31 au paragraphe 5(a).

[43] Même endroit au paragraphe 5(b).

[44] Pour une discussion plus complète sur la sécurité nationale au sens large, voir Richard Carver, « Training Manual on International and Comparative Media and Freedom of Expression Law », pages 77 à 88 (accessible en anglais ici : https://www.mediadefence.org/resources/mldi-manual-on-freedom-of-expression-law/).

preuve de déférence envers l'État pour déterminer ce qui constitue la sécurité nationale. Comme nous l'avons déjà indiqué :[45]

> « L'utilisation d'un concept amorphe de sécurité nationale pour justifier des limitations invasives à la jouissance des droits de l'homme est très préoccupante. Le concept est défini au sens large et est donc vulnérable à la manipulation par l'État comme moyen de justifier des actions qui visent des groupes vulnérables tels que les défenseurs des droits de l'homme, les journalistes ou les militants. Elle sert également à justifier le secret souvent inutile qui entoure les enquêtes ou les activités des services répressifs, ce qui porte atteinte aux principes de transparence et de responsabilité ».

Le principe XIII(2) de la Déclaration de principes sur la liberté d'expression en Afrique prévoit que la liberté d'expression ne doit pas être restreinte pour des raisons d'ordre public ou de sécurité nationale « sauf s'il existe un risque réel de préjudice à un intérêt légitime et s'il existe un lien de causalité étroit entre le risque de préjudice et l'expression ».

Comme indiqué dans les Principes de Johannesburg sur la sécurité nationale, la liberté d'expression et l'accès à l'information (les Principes de Johannesburg) :[46]

> « (a) Une restriction que l'on cherche à justifier pour des raisons de sécurité nationale n'est légitime que si son but véritable et son effet démontrable sont de protéger l'existence ou l'intégrité territoriale d'un pays contre l'emploi ou la menace de la force, ou sa capacité à répondre à l'emploi ou à la menace de la force, qu'elle provienne d'une source extérieure, comme une menace militaire, ou d'une source intérieure, comme une incitation au renversement violent du gouvernement.
>
> (b) En particulier, une restriction que l'on cherche à justifier pour des raisons de sécurité nationale n'est pas légitime si son but véritable ou son effet démontrable est de protéger des intérêts sans rapport avec la sécurité nationale, y compris, par exemple, de protéger un gouvernement contre l'embarras ou la révélation d'actes répréhensibles, ou de dissimuler des informations sur le fonctionnement de ses institutions publiques, ou d'ancrer une idéologie particulière, ou de réprimer des troubles industriels ».

Le principe 7 va plus loin en indiquant que l'exercice pacifique du droit à la liberté d'expression ne doit pas être considéré comme une menace pour la sécurité nationale ni faire l'objet de restrictions ou de sanctions.

Un autre principe important contenu dans les Principes de Johannesburg est le principe 23, qui prévoit que « l'expression ne peut être soumise à la censure préalable dans l'intérêt de la

---

[45] Rapport du RSNU sur la liberté d'expression à l'AGNU, A/HRC/23/40, 17 avril 2013 au paragraphe 60 (accessible sur : https://digitallibrary.un.org/record/756267/files/A_HRC_23_40-FR.pdf).

[46] Principe 2 des Principes de Johannesburg sur la sécurité nationale, la liberté d'expression et l'accès à l'information, novembre 1996 (accessible sur http://hrlibrary.umn.edu/instree/Fjohannesburg.html#:~:text=I%20PRINCIPES%20GENERAUX&text=Toute%20personne%20a%20droit%20%C3%A0,autre%20moyen%20de%20son%20choix.). Les principes de Johannesburg ont été élaborés par un groupe d'experts en droit international, en sécurité nationale et en droits de l'homme, réuni en vertu de l'ARTICLE 19. Ils ont été approuvés par le RSNU sur la liberté d'expression de l'époque.

protection de la sécurité nationale, sauf en cas de danger public exceptionnel menaçant la vie du pays ». D'une manière générale, la restriction préalable de l'expression est inadmissible. Les mesures décrites ci-dessus peuvent souvent donner lieu à une restriction préalable du contenu, et ont donc un effet paralysant sur la jouissance du droit à la liberté d'expression.

De même, la lutte contre le terrorisme en tant que justification supposée de la fermeture de réseaux ou d'autres interférences avec l'accès à l'Internet doit également être traitée avec prudence. Comme le souligne l'Observation générale n° 34, les médias jouent un rôle important dans l'information du public sur les actes de terrorisme, et ils doivent être en mesure de s'acquitter sans entrave de leurs fonctions et devoirs légitimes.[47] Si les gouvernements peuvent soutenir que les fermetures d'Internet sont nécessaires pour interdire la diffusion de nouvelles sur les attaques terroristes afin de prévenir la panique ou les imitations, il a été constaté au contraire que le maintien de la connectivité peut atténuer les préoccupations de sécurité publique et aider à faire état de l'ordre public.[48]

Au minimum, si l'on veut limiter l'accès à l'Internet, il faut que les lois, les politiques et les pratiques sur lesquelles on s'appuie soient transparentes, que les termes « sécurité nationale » et « terrorisme » soient clairement définis et qu'un contrôle indépendant et impartial soit exercé.

RESPONSABILITÉ DES INTERMÉDIAIRES

La responsabilité des intermédiaires est engagée lorsque les gouvernements ou les parties privées peuvent tenir les intermédiaires technologiques, tels que les FAI et les sites web, pour responsables des contenus illicites ou préjudiciables créés par les utilisateurs de ces services.[49] Cela peut se produire dans diverses circonstances, notamment en cas de violation des droits d'auteur, de piratage numérique, de litiges relatifs à des marques de commerce, de gestion de réseau, de pollupostage et d'hameçonnage, de « cybercriminalité », de diffamation, de discours de haine, de pornographie enfantine, de « contenu illégal », de contenu offensant, mais légal, de censure, de lois et règlements en matière de radiodiffusion et de télécommunications, et de protection de la vie privée.[50]

Un rapport publié par l'UNESCO identifie les défis suivants auxquels sont confrontés les intermédiaires :[51]

- Limiter la responsabilité des intermédiaires pour les contenus publiés ou transmis par des tiers est essentiel à l'essor des services internet qui facilitent l'expression.

---

[47] Observation générale nº 34 au paragraphe 46.

[48] Rapport 2017 du RSNU sur la liberté d'expression ci-dessus, point nº 17 au paragraphe 14.

[49] Alex Comninos, « The liability of internet intermediaries in Nigeria, Kenya, South Africa and Uganda: An uncertain terrain » (2012), page 6 (accessible en anglais sur : https://www.apc.org/sites/default/files/READY%20-%20Intermediary%20Liability%20in%20Africa_FINAL_0.pdf).

[50] *Idem*

[51] Rebecca MacKinnon et autres, « Fostering freedom online: The role of internet intermediaries » (2003), pages 179 à 180 (accessible en anglais sur : https://unesdoc.unesco.org/ark:/48223/pf0000231162_eng).

- Les lois, politiques et réglementations qui obligent les intermédiaires à restreindre, bloquer et filtrer les contenus dans de nombreuses juridictions ne sont pas suffisamment compatibles avec les normes internationales des droits de l'homme en matière de liberté d'expression.
- Les lois, politiques et pratiques relatives à la surveillance gouvernementale et à la collecte de données auprès des intermédiaires, lorsqu'elles ne sont pas suffisamment compatibles avec les normes relatives aux droits de l'homme, empêchent les intermédiaires de protéger adéquatement la vie privée des utilisateurs.
- Alors que les procédures régulières exigent généralement que l'application de la loi et la prise de décision soient transparentes et accessibles au public, les gouvernements sont souvent opaques quant aux demandes adressées aux entreprises pour la restriction du contenu, la remise des données des utilisateurs et d'autres exigences de surveillance.

Il est généralement admis que le fait d'exonérer les intermédiaires de toute responsabilité pour les contenus générés par d'autres protège le droit à la liberté d'expression en ligne. Cette exonération peut être obtenue soit par un système d'immunité absolue de responsabilité, soit par un régime qui ne fixe la responsabilité des intermédiaires qu'après leur refus d'obéir à l'ordre d'un tribunal ou d'un autre organe compétent de retirer le contenu contesté.

En ce qui concerne ce dernier point, la déclaration commune de 2011 prévoit que les intermédiaires ne devraient être responsables du contenu de tiers que lorsqu'ils interviennent spécifiquement dans ce contenu ou refusent d'obéir à un ordre de retrait adopté conformément aux garanties d'une procédure régulière par un organe de contrôle indépendant, impartial et faisant autorité (tel qu'un tribunal).[52]

La Cour européenne des droits de l'homme a examiné la responsabilité des intermédiaires dans plusieurs cas :

- En 2013, dans l'affaire *« Delfi AS v Estonia »*, la CEDH a examiné la responsabilité d'un portail d'information sur Internet pour des commentaires offensants qui ont été publiés par des lecteurs en dessous d'un de ses articles d'information en ligne.[53] Le portail s'est plaint que le fait d'être tenu responsable des commentaires de ses lecteurs violait son droit à la liberté d'expression. La CEDH a rejeté l'affaire, estimant que la détermination de la responsabilité par les tribunaux nationaux constituait une restriction justifiée et proportionnée de la liberté d'expression parce que les commentaires étaient très offensants ; le portail ne les a pas empêchés de devenir publics, a profité de leur existence et a permis à leurs auteurs de rester anonymes. Elle a également noté que l'amende imposée par les tribunaux estoniens n'était pas excessive.
- En 2016, dans l'affaire *« Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v Hungary »*, la CEDH a examiné la responsabilité d'un organisme d'autorégulation des fournisseurs de contenu internet et d'un portail d'information sur Internet pour des

[52] Déclaration commune 2011 ci-dessus, point n° 31 aux paragraphes 2(a) à (b).

[53] Demande n° 64569/09, 10 octobre 2013 (accessible sur : hhttsp://hudoc.echr.coe.int/eng?i=001-155105).

commentaires en ligne vulgaires et offensants publiés sur leurs sites.[54] La CEDH a réaffirmé que, même s'ils ne sont pas des éditeurs de commentaires au sens traditionnel du terme, les portails d'information sur Internet doivent néanmoins assumer des devoirs et des responsabilités. La CEDH a estimé que, bien qu'offensant et vulgaire, le commentaire n'avait pas constitué un discours illégal, et a confirmé l'allégation de violation du droit à la liberté d'expression.

- En 2017, dans l'affaire *« Tamiz v United Kingdom »*, Royaume-Uni, la CEDH a eu à se pencher sur la portée de la responsabilité des intermédiaires.[55] Le requérant, un ancien homme politique du Royaume-Uni, avait prétendu devant les tribunaux nationaux qu'un certain nombre de commentaires de tiers publiés par des utilisateurs anonymes sur le site Blogger.com de Google étaient diffamatoires. Devant la CEDH, le requérant a fait valoir que son droit au respect de sa vie privée avait été violé parce que les tribunaux nationaux avaient refusé de lui accorder un recours contre l'intermédiaire. Sa demande a finalement été rejetée par la CEDH au motif que l'atteinte à sa réputation aurait été insignifiante. La CEDH a souligné le rôle important que jouent les fournisseurs d'accès Internet pour faciliter l'accès à l'information et le débat sur un large éventail de droits politiques, sociaux et culturels, et a semblé approuver l'argument selon lequel les fournisseurs d'accès Internet ne doivent pas être dans l'obligation de surveiller le contenu ou d'enquêter de manière proactive sur les activités diffamatoires potentielles sur leurs sites.

D'autres tribunaux ont pris des positions plus définitives en matière de responsabilité des intermédiaires. Par exemple, la Cour suprême de l'Inde a interprété le droit interne comme ne prévoyant la responsabilité de l'intermédiaire que lorsqu'un intermédiaire a eu effectivement connaissance effective d'une décision de justice, ou lorsqu'un intermédiaire a été notifié par le gouvernement qu'un des actes illégaux prescrits par la loi va être commis et

---

[54] Demande n° 22947/13, 2 février 2016 (accessible sur : https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-155105%22]}).

[55] *Tamiz v United Kingdom*, Demande nº 3877/14, 19 septembre 2017 (accessible sur : https://hudoc.echr.coe.int/eng?i=001-178106). Media Defence, en collaboration avec une coalition d'organisations, a soumis à la CEDH des propositions de principes pour les intermédiaires, basées sur les meilleures pratiques de la législation nationale, les avis du Comité des ministres du Conseil de l'Europe (COE) et des titulaires de mandats spéciaux.

Dans l'affaire susmentionnée portée devant la CEDH, Media Defence et une coalition d'autres organisations. Les propositions de principes sont les suivantes :

- Les intermédiaires ne doivent pas être les arbitres de la légalité des contenus affichés, stockés ou transférés par les utilisateurs de leurs services.
- En supposant qu'ils n'aient pas contribué au contenu ou manipulé celui-ci, les intermédiaires ne doivent pas être responsables du contenu affiché, stocké ou transféré en utilisant leurs services, à moins et jusqu'à ce qu'ils ne se soient pas conformés à une ordonnance d'un tribunal ou d'un autre organe compétent pour retirer ou bloquer un contenu spécifique.
- Nonobstant ce qui précède, les intermédiaires ne doivent en aucun cas être responsables des contenus, à moins que ceux-ci n'aient été portés à leur connaissance de telle manière que l'intermédiaire puisse être considéré comme ayant une connaissance effective de l'illégalité de ces contenus.
- L'obligation de surveiller le contenu en permanence est incompatible avec le droit à la liberté d'expression énoncé à l'article 10 de la Convention européenne des droits de l'homme.

Les soumissions sont accessibles ici https://www.mediadefence.org/sites/default/files/blog/files/20160407%20Tamiz%20v%20UK%20Intervention%20Filing.pdf.

que l'intermédiaire a ensuite omis de supprimer ou de désactiver l'accès à ces informations.[56] En outre, la Cour suprême d'Argentine a estimé que les moteurs de recherche n'ont pas l'obligation de contrôler la légalité des contenus de tiers auxquels ils renvoient, notant que ce n'est que dans des cas exceptionnels de « préjudice grave et manifeste » que les intermédiaires pourraient être tenus de désactiver l'accès.[57]

Compte tenu du rôle essentiel joué par les intermédiaires dans la promotion et la protection du droit à la liberté d'expression en ligne, il est impératif qu'ils soient protégés contre toute ingérence injustifiée (de la part d'acteurs publics et privés) qui pourrait avoir un effet délétère sur ce droit. Par exemple, étant donné que la capacité et la liberté d'un individu à exercer son droit à la liberté d'expression en ligne dépendent de la nature passive des intermédiaires en ligne, tout régime juridique qui amène un intermédiaire à appliquer une restriction ou une autocensure excessive à l'égard du contenu communiqué par l'intermédiaire de ses services aura en fin de compte un effet négatif sur le droit à la liberté d'expression en ligne. Le RSNU a noté que les intermédiaires peuvent servir de rempart important contre l'excès d'emprise des gouvernements et du secteur privé, car ils sont généralement les mieux placés pour repousser une fermeture, par exemple.[58] Toutefois, cela ne peut être véritablement réalisé que dans des circonstances où les intermédiaires peuvent le faire sans crainte de sanctions ou de pénalités.

CONCLUSION

Bien que le droit d'accès à l'Internet ne soit pas encore expressément reconnu par le droit international, il est largement considéré comme un instrument de la liberté d'expression et, comme pour tous les droits de l'homme, il ne peut être limité de manière justifiée que si un test en trois parties est rempli. En outre, les restrictions imposées à l'Internet peuvent porter indûment atteinte à la liberté d'expression et aux droits qui y sont associés. Dans un monde numérique qui se développe rapidement, l'Internet devient de plus en plus un espace contesté et il est utilisé aussi bien par ceux qui cherchent à défendre les droits fondamentaux que par ceux qui cherchent à les limiter. La bonne compréhension de concepts tels que la fermeture de l'Internet, le blocage et le filtrage des contenus, la neutralité du réseau et la responsabilité des intermédiaires est de plus en plus nécessaire pour protéger et promouvoir pleinement le droit à la liberté d'expression en ligne.

---

[56] *« Shreya Singhal v Union of India »*, Demande nº 167/2012 aux paragraphes 112-118 (accessible en anglais sur : https://www.livelaw.in/summary-of-the-judgment-in-shreya-singhal-vs-union-of-india-read-the-judgment/).

[57] *María Belén Rodriguez v Google*, Fallo R.522.XLIX (accessible sur : http://www.stf.jus.br/repositorio/cms/portalStfInternacional/newsletterPortalInternacionalJurisprudencia/anexo/Fallo_R.522.XLIX__Corte_Suprema_da_Argentina__28_oct._2014.pdf). La décision a été décrite dans le rapport de 2016 du RSNU sur la liberté d'expression au paragraphe 52.

[58] Rapport 2017 du RSNU sur la liberté d'expression au paragraphe 50.