Tendances mondiales en matière de liberté d'expression et de développement des médias

Regards sur le numérique 2015

Éditions UNESCO

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

Tendances mondiales en matière de liberté d'expression et de développement des médias

Regards sur le numérique 2015

Éditions UNESCO

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

Publié en 2015 par
l'Organisation des Nations Unies pour l'éducation, la science et la culture
7, place de Fontenoy, 75352 Paris 07 SP, France

ISBN 978-92-3-200079-8

Titre original : *World Trends in Freedom of Expression and Media Development – Special Digital Focus 2015*
Publié en 2015 par l'Organisation des Nations Unies pour l'éducation, la science et la culture

Les désignations employées dans cette publication et la présentation des données qui y figurent n'impliquent de la part de l'UNESCO aucune prise de position quant au statut juridique des pays, territoires, villes ou zones, ou de leurs autorités, ni quant au tracé de leurs frontières ou limites. Les idées et les opinions exprimées dans cette publication sont celles des auteurs ; elles ne reflètent pas nécessairement les points de vue de l'UNESCO et n'engagent en aucune façon l'Organisation.

Cette publication se base sur trois autres études, en résumant leurs principaux arguments et soulignant les tendances concernées :

1. Gagliardone, I. et al. 2015. *Combattre les discours de haine sur Internet*. Collection de l'UNESCO sur la liberté de l'Internet. Paris: UNESCO. http://unesdoc.unesco.org/images/0023/002346/234620F.pdf
2. Posetti, J. (à venir). *Protéger les sources des journalistes à l'ère numérique*. Collection de l'UNESCO sur la liberté de l'Internet. Paris: UNESCO
3. MacKinnon, R. et al. 2014. *Promouvoir la liberté en ligne : le rôle des intermédiaires de l'Internet*. Collection de l'UNESCO sur la liberté de l'Internet. Paris: UNESCO / Internet Society. http://unesdoc.unesco.org/images/0023/002311/231162e.pdf

Cette publication a reçu le soutien de la Suède.

SWEDEN

L'Internet Society, les Fondations Open Society, le Centre pour les études de communication globale de l'école Annenberg de communication de l'Université de Pennsylvanie, l'Université d'Oxford, l'Association mondiale des journaux et des éditeurs de médias d'information (WAN-IFRA) ont également contribué à la réalisation de cet ouvrage.

Coordinatrice éditoriale : Rachel Pollack Ichou
Création graphique : UNESCO
Graphisme de la couverture : UNESCO
Illustrations : UNESCO
Mises en pages : UNESCO
Impression : UNESCO

Imprimé en France

Tendances mondiales en matière de liberté d'expression et de développement des médias : Regards sur le numérique 2015

Éditeur : Rachel Pollack Ichou, Chargée de projet, Section pour la liberté d'expression, Division de la liberté d'expression et du développement des médias, UNESCO

Combattre les discours de haine sur Internet

Auteurs :

Iginio Gagliardone, Chercheur associé, nouveaux médias et droits de l'homme, Centre d'études socio-juridiques, membre du Programme des politiques et droit des médias comparés (PCMLP), Université d'Oxford

Danit Gal, Etudiant, Master en sciences sociales de l'Internet, Université d'Oxford

Thiago Alves Pinto, Doctorant en droit, Université d'Oxford

Gabriela Martinez Sainz, Doctorante dans le domaine de l'éducation, Comité consultatif international de l'Université de Cambridge

Nicole Stremlau, Directrice du Programme de politiques et droit des médias comparés, Université d'Oxford

Protéger les sources des journalistes à l'ère numérique

Auteure et directrice de la recherche : Julie Posetti, Chercheuse associée, Association mondiale des journaux et des éditeurs de médias d'information (WAN-IFRA) ; Conférencière, Journalisme de radiodiffusion et de convergence, Université de Wollongong

Chercheurs universitaires :

Ying Chan, Directeur fondateur, Centre de journalisme et d'études des médias, Université de Hong Kong

Marcus O'Donnell, Maître de conférences en journalisme, Faculté de droit, des lettres et des arts, Université de Wollongong

Carlos Affonso Pereira de Souza, Vice-coordinateur, Centre pour la technologie et la société (CTS), Faculté de droit de la Fondation Getulio Vargas (FGV), Rio de Janeiro

Doreen Weisenhaus, Directeur du Projet de loi sur les médias, Professeur agrégé, Université de Hong Kong

Assistants de recherche diplômés, et collaborateurs de recherche de premier cycle :

Federica Cherubini, Responsable du programme, WAN-IFRA

Jake Evans, Editeur, *Australian Broadcasting Corporation* (ABC)

Emma Goodman, Chargée de recherche, Projet de politique des médias, *London School of Economics* (LES) ; Ancienne rédactrice, WAN-IFRA

Angelique Lu, Journaliste, BBC ; Ancienne stagiaire WAN-IFRA-Université de Wollongong

Alice Matthews, Journaliste, *Australian Broadcasting Corporation* (ABC) News ; Ancienne assistante de recherche, WAN-IFRA

Alexandra Sazonova-Prokouran, Etudiante, Université d'Oxford ; Ancienne stagiaire WAN-IFRA

Jessica Sparks, Etudiante en journalisme/droit, Université de Wollongong ; Ancienne stagiaire WAN-IFRA

Nick Toner, Co-fondateur/éditeur, VERSA News ; Etudiant, Université d'Oxford ; Ancien stagiaire WAN-IFRA

Farah Wael, Coordinatrice, Développement des médias et liberté de la presse, WAN-IFRA

Alexandra Waldhorn, Chargée de communication, Institut international de planification de l'éducation, UNESCO ; Ancienne conseillère pour la jeunesse, WAN-IFRA

Olivia Wilkinson, Etudiante, Université d'Oxford ; Ancienne stagiaire WAN-IFRA

Appui administratif : Ashleigh Tullis, journaliste, *Fairfax Media Wollondilly Advertiser* ; Ancienne stagiaire WAN-IFRA

Comité consultatif international :

Mark Pearson, Professeur en journalisme et médias sociaux, Université de Griffith

Julie Reid, Maître de conférences en études des médias, Département des Sciences de la communication, UNISA (Université d'Afrique du Sud)

Lillian Nalwoga, Présidente, Chapitre Ouganda de l'Internet Society ; Chargée de mission, Collaboration sur les politiques internationales en termes de TIC en Afrique orientale et australe (CIPESA)

Dan Gillmor, Directeur, *Knight Center* pour l'entrepreneuriat en médias numériques, Ecole Walter Cronkite de journalisme et communication de masse de l'Université d'Etat d'Arizona

Prisca Orsonneau, Avocat au Barreau de Paris, spécialisé en droit des médias et droits de l'homme ; Président du Comité juridique de Reporters sans frontières

Gayathry Venkiteswaran, Directrice exécutive, Alliance de la presse de l'Asie du Sud-Est

Mario Calabresi, Rédacteur en chef, *La Stampa*

Mishi Choudhary, Directrice juridique, *Software Freedom Law Centre*, et SFLC.in

Promouvoir la liberté en ligne : Le rôle des intermédiaires de l'Internet

Auteurs :

Rebecca MacKinnon, Directrice, *Ranking Digital Rights Project, New America Foundation*; Chercheur affilié, Centre d'études en communication globale, Ecole de communication d'Annenberg, Université de Pennsylvanie

Elonnai Hickok, Chercheur, Centre pour l'Internet et la société

Allon Bar, Coordonnateur de recherche, *Ranking Digital Rights Project*

Hae-in Lim, Chercheur, *Ranking Digital Rights Project*

Chercheurs :

Sara Alsherif, Chercheur, Programme sur la liberté d'information, *Support for Information Technology Center*

Celina Beatriz Mendes de Almeida Bottino, Institut pour la technologie et la société, Rio de Janeiro

Richard Danbury, Chercheur associé, Faculté de droit, Université de Cambridge

Elisabetta Ferrari, Centre pour les médias, les données et la société, Université d'Europe centrale, Budapest ; Doctorante, Ecole de communication d'Annenberg, Université de Pennsylvanie

Grace Githaiga, Associée, *Kenya ICT Action Network* (KICTANet)

Kirsten Gollatz, Responsable de projet, Institut Alexander von Humboldt pour l'Internet et la société

Elonnai Hickok, Chercheur, Centre pour l'Internet et la société

Hu Yong, Professeur agrégé, Production audiovisuelle, École de journalisme et de communication, Université de Pékin

Tatiana Indina, Candidate en sciences, chercheur associé, Centre pour l'étude des nouveaux médias et de la société

Victor Kapiyo, Responsable du programme – Protection des droits de l'homme, Section kényane de la Commission internationale des juristes (ICJ Kenya) ; *Kenya ICT Action Network* (KICTANet)

Peter Micek, Conseiller principal en politiques, Access

Agustín Rossi, Doctorant, Institut universitaire européen ; Chercheur non-résident, Global Public Policy Institute

Comité consultatif International :

Renata Avila, Responsable de la campagne mondiale, initiative *Web We Want*, Fondation World Wide Web ; Contributeur, Global Voices

Rasha Abdulla, Professeure agrégée et ancienne Présidente, Journalisme et Communication de masse, Université américaine du Caire

Sunil Abraham, Directeur exécutif, Centre pour l'Internet et la société

Peng Hwa Ang, Professeur, Université de technologie de Nanyang, Ecole de communication Wee Kim Wee

Eduardo Bertoni, Directeur du Centre d'études sur la liberté d'expression et l'accès à l'information (CELE), Ecole de droit de l'Université de Palerme

Seeta Peña Gangadharan, Membre du Programme, *New America's Open Technology Institute*

Leslie Harris, Directrice, *Harris Strategy Group LLC* ; ancienne Présidente Directeur générale, Centre pour la démocratie et la technologie

Dunstan Allison Hope, Directeur exécutif, Services consultatifs, BSR

Rikke Frank Jørgensen, Conseiller principal, Institut danois pour les droits de l'homme

Jeremy Malcolm, Analyste principal des politiques mondiales, *Electronic Frontier Foundation*

Pranesh Prakash, Directeur des politiques, Centre pour l'Internet et la société

Lucy Purdon, Responsable de programme, ICT, Institut pour les droits de l'homme et les affaires

David Sullivan, Directeur des politiques et des communications, *Global Network Initiative*

Ben Wagner, Directeur, Centre pour l'internet et les droits de l'homme, Université européenne Viadrina

Sécurité des journalistes

Auteur : Ming-Kuok Lim, Spécialiste adjoint du programme, Section pour la liberté d'expression, Division de la liberté d'expression et du développement de médias, UNESCO

Table des matières

Avant-propos d'Irina Bokova, Directrice générale de l'UNESCO

À l'heure où l'UNESCO célèbre son 70e anniversaire, notre mandat fondateur – « Promouvoir la libre circulation des idées, par le mot et l'image » – n'a jamais été plus important qu'aujourd'hui, pour faire progresser le droit à la liberté d'expression et pour favoriser la paix et le développement durable grâce à la liberté des médias, le pluralisme, l'indépendance et la sécurité des journalistes.

Tout au long du Sommet mondial sur la société de l'information (SMSI) et des événements qui ont suivi, l'UNESCO a partagé sa vision des sociétés du savoir inclusives, bâties sur les piliers que sont la liberté d'expression, l'accès universel à l'information et au savoir, le respect de la diversité culturelle et linguistique et l'accès à une éducation de qualité pour tous. Alors que les Nations Unies font le bilan des 10 dernières années du SMSI et encouragent activement les États membres à atteindre les Objectifs de développement durable (ODD), le travail de l'UNESCO dans ces domaines est d'autant plus vital, tout particulièrement en cette période de révolution technologique et de transformation profonde des sociétés.

L'environnement mondial de communication et d'information a été radicalement modifié par la diffusion des technologies numériques. Aujourd'hui, plus de 3 milliards d'hommes et de femmes à travers le monde utilisent Internet et plus de 6 milliards ont accès à des téléphones mobiles. Ces technologies ont élargi les perspectives de progrès vers des sociétés du savoir durables, mais elles ont aussi fait naître de nouvelles difficultés.

C'est dans ce contexte dynamique qu'en novembre 2013 l'UNESCO a été sollicitée par ses 195 États membres pour produire une étude approfondie sur les questions liées à Internet dans le cadre de son mandat, en mettant un accent particulier sur quatre

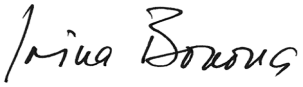
domaines : l'accès à l'information et au savoir, la liberté d'expression, le respect de la vie privée et l'éthique de l'information. L'étude ainsi publiée, *Des clés pour la promotion de sociétés du savoir inclusives*, explore ces thèmes mais aussi les options possibles pour la poursuite de cette action. Cette démarche s'appuie sur le mandat précédemment confié à l'UNESCO par les États membres lors de la Conférence générale de 2011, afin que l'UNESCO étudie les tendances mondiales en matière de liberté d'expression et de développement des médias. Elle s'inspire également du premier rapport *Tendances mondiales en matière de liberté d'expression et de développement des médias*, publié en 2014.

Le rapport *Des clés pour la promotion de sociétés du savoir inclusives* est unique car il élabore le concept d'« universalité d'Internet » qui désigne un Internet fondé sur les droits de l'homme, ouvert, accessible à tous et alimenté par la participation de multiples acteurs. Il montre également comment Internet peut favoriser la réalisation des Objectifs de développement durable, de l'élimination de la pauvreté à l'égalité des sexes en passant par la consommation et les schémas de production durables, la lutte contre le changement climatique et l'avènement de sociétés pacifiques et inclusives.

Le second rapport *Tendances mondiales en matière de liberté d'expression et de développement des médias* développe les principaux aspects de l'étude *Des clés pour la promotion de sociétés du savoir inclusives*. C'est donc une version mise à jour de la première édition des *Tendances mondiales*. Cette dernière couvrait l'ensemble des questions, tandis que la nouvelle édition approfondit son analyse en se concentrant sur les quatre thèmes spécifiques identifiés dans l'étude *Des clés pour la promotion de sociétés du savoir inclusives*. Le rôle de l'UNESCO est donc renforcé dans le domaine de l'amélioration des connaissances et de la compréhension, grâce à des recherches de grande qualité utiles à la construction de sociétés du savoir.

Les recherches présentées dans ce rapport n'auraient pas vu le jour sans le soutien sans faille du gouvernement suédois à qui j'exprime ma profonde reconnaissance. Je souhaiterais aussi remercier l'Internet Society, les Open Society Foundations, le Centre pour les études mondiales sur la communication de l'École de communication Annenberg à l'Université de Pennsylvanie, l'Université d'Oxford et l'Association mondiale des journaux et des éditeurs de médias d'information (WAN-IFRA).

Je suis convaincue que *Tendances mondiales en matière de liberté d'expression et de développement des médias – Regards sur le numérique 2015* deviendra une référence, tant pour les gouvernements, la société civile, le secteur privé, les universitaires et les étudiants, en cette période où la liberté d'expression n'a jamais été aussi importante.



Irina Bokova

I. INTRODUCTION

En 2011, durant leur 36e Conférence générale, les 195 États membres de l'UNESCO ont adopté une résolution demandant à l'Organisation de « suivre, en étroite collaboration avec d'autres organismes des Nations Unies et d'autres organisations concernées, actives dans ce domaine, la situation en matière de liberté de la presse et de sécurité des journalistes, et tout particulièrement les cas de violences à l'égard des journalistes commises dans l'impunité [...] et rendre compte des évolutions sur ces points à la Conférence générale. »

Pour exécuter son mandat, et avec le soutien du gouvernement suédois, l'UNESCO s'est lancée en 2012 dans un projet de recherche à grande échelle, assistée par un groupe consultatif rassemblant 27 experts internationaux. Sur la base de ces recherches, un résumé du rapport sur les tendances en matière de liberté de la presse et de sécurité des journalistes entre 2007 et la première moitié de 2013 a été soumis à la 37e Conférence générale en novembre 2013, sous la forme d'un document présentant les conclusions pertinentes. La version finale de *Tendances mondiales en matière de liberté d'expression et de développement des médias* a été lancée par la Directrice générale de l'UNESCO à Stockholm, en Suède, en mars 2014, avant d'être présentée dans les cinq régions de l'UNESCO.

Le premier rapport comblait un manque important dans les études contemporaines sur les médias et la communication. En effet, si d'autres études et rapports offraient des aperçus sur des dimensions ou des régions spécifiques, celui-ci a été le premier à consister en une analyse systématique des tendances concernant plusieurs aspects, notamment la liberté des médias, le pluralisme, l'indépendance et la sécurité, tout en accordant une attention particulière aux questions liées au genre.

Étant donné le succès du premier rapport *Tendances mondiales* et les besoins d'effectuer des recherches supplémentaires, l'UNESCO a lancé une deuxième édition de la série, qui cette fois approfondit son travail sur une sélection de tendances propres à l'ère numérique. *Tendances mondiales en matière de liberté d'expression et de développement des médias – Regards sur le numérique 2015* fournit une analyse substantielle des principaux domaines identifiés dans la première édition comme pouvant faire l'objet de recherches complémentaires, notamment les questions du discours de haine en ligne, de la protection des sources des journalistes et du rôle des intermédiaires de l'Internet dans la promotion de la liberté d'expression, et elle s'intéresse également, tout comme la première, à la sécurité des journalistes. Elle traite également des questions soulevées dans l'étude intitulée *Des clés pour la promotion de sociétés du savoir inclusives,* publiée en 2015 par l'UNESCO.

La présente publication est donc divisée en quatre chapitres thématiques :

1. **Combattre les discours de haine sur Internet** présente globalement les dynamiques qui caractérisent les discours de haine en ligne et certaines des mesures adoptées pour les contrer et les limiter. Il met également en avant les bonnes pratiques qui se développent au niveau local et au niveau international. On y trouve une analyse complète des cadres normatifs internationaux, régionaux et nationaux mis en place pour faire face à ce problème, et de leurs répercussions sur la liberté d'expression. Une importance particulière est donnée aux mécanismes sociaux et non réglementaires

pouvant être utiles pour contrer la production, la diffusion et l'impact des propos haineux en ligne.

2. **Protéger les sources des journalistes à l'ère numérique** s'inspire d'une recherche portant sur 121 États membres de l'UNESCO, laquelle actualise les données d'une précédente étude sur ces mêmes pays, menée par l'ONG Privacy International en 2007. Ce chapitre montre comment les cadres juridiques de protection des sources, qu'ils soient internationaux, régionaux ou nationaux, ont subi de fortes pressions depuis. Ils risquent de plus en plus de perdre leur efficacité, d'être restreintes ou de faire l'objet de compromis. Ce phénomène est une remise en cause directe des droits universels établis en faveur des droits de l'homme à la liberté d'expression et au respect de la vie privée et représente une menace sérieuse pour le journalisme d'investigation. Cette recherche contient une proposition à examiner : un outil d'évaluation en 11 points, utilisé pour mesurer l'efficacité des cadres juridiques de protection des sources à l'ère numérique.

3. **Promouvoir la liberté en ligne : le rôle des intermédiaires de l'Internet** informe sur les intermédiaires de l'Internet – qui servent d'intermédiaires pour les communications en ligne et rendent possibles plusieurs formes d'expression. Il montre que les intermédiaires peuvent à la fois promouvoir et restreindre la liberté d'expression, dans des juridictions et des circonstances variées, et avec des technologies et des modèles d'entreprises divers. Selon les Principes directeurs relatifs aux entreprises et aux droits de l'homme, si le devoir de protéger les droits de l'homme incombe en premier lieu aux gouvernements, cette responsabilité engage aussi les entreprises et ces deux types d'entités ont un rôle à jouer pour garantir réparation à ceux dont les droits ont été bafoués. Ce chapitre applique le cadre de référence « Protéger, respecter et réparer » aux politiques et pratiques d'entreprises représentant trois types d'intermédiaires (fournisseurs de service Internet, moteurs de recherche et plates-formes des réseaux sociaux) dans 10 pays. Les trois études de cas mettent en lumière les difficultés et les opportunités qui se présentent pour les différents intermédiaires, au regard de leur importance croissante.

4. **Sécurité des journalistes** examine les tendances récentes en matière de sécurité des journalistes, en présentant les statistiques de l'UNESCO pour 2013 et 2014 et les autres évolutions dans ce domaine jusqu'à août 2015. Il suit la structure du précédent rapport *Tendances mondiales* de l'UNESCO, en abordant la sécurité physique, l'impunité, l'incarcération des journalistes et les problématiques liées au genre. En outre, ce chapitre traite du renforcement sans précédent des cadres normatifs internationaux, ainsi que de l'élaboration de nouveaux mécanismes pratiques, de l'amélioration de la coopération entre les agences des Nations Unies, de l'élargissement de la collaboration avec la justice et les forces de l'ordre et des projets de recherche sur le sujet.

Les chapitres sur les discours de haine en ligne et le rôle des intermédiaires apparaissent dans la présente publication mais aussi dans l'étude approfondie de l'UNESCO sur les questions liées à Internet (voir « UNESCO : Promouvoir la liberté d'expression et le développement des médias à l'ère numériquer »), mais ils ont aussi fait l'objet de

publications indépendantes plus détaillées, au sein de la série d'études de l'UNESCO sur la liberté sur Internet.

Tout au long de cette nouvelle édition des *Tendances mondiales*, une attention particulière est accordée à l'égalité entre les sexes, l'une des Priorités de l'UNESCO. Comme dans la première édition, la question du genre fait ici référence aux expériences des femmes journalistes et aux effets des politiques et des pratiques pour les femmes.

Les tendances identifiées dans ce rapport permettent de mieux appréhender les opportunités et les difficultés qui bouleversent la liberté d'expression et le développement des médias, notamment celles causées par les technologies numériques. En partageant ainsi les connaissances et les bonnes pratiques, l'UNESCO fait progresser les droits de l'homme à l'ère numérique, en combattant les discours de haine sur Internet, en protégeant les sources des journalistes, en favorisant la liberté en ligne par la diffusion de bonnes pratiques à l'attention des intermédiaires de l'Internet et en renforçant la sécurité des journalistes, en ligne comme hors ligne.

II. UNESCO : PROMOUVOIR LA LIBERTÉ D'EXPRESSION ET LE DÉVELOPPEMENT DES MÉDIAS

L'UNESCO est l'agence des Nations Unies mandatée pour défendre la liberté d'expression, conformément à son Acte constitutif appelant à « la libre circulation des idées, par le mot et par l'image ». Cette mission est renforcée par la Déclaration universelle des droits de l'homme, qui affirme que « tout individu a droit à la liberté d'opinion et d'expression ». La liberté d'expression, et ses corollaires la liberté d'information et la liberté de la presse, s'applique à tous les médias, qu'il s'agisse des médias traditionnels comme la presse ou la radio ou des nouveaux médias numériques.

En 2013, les 195 membres de la Conférence générale de l'UNESCO ont adopté la Résolution 52, qui rappelle la Résolution A/HRC/RES/20/8 du Conseil des droits de l'homme « 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 également être protégés en ligne. Ces droits entrent dans les domaines de compétence de l'UNESCO et sont d'une importance cruciale pour le développement durable, la démocratie et le dialogue. À la demande des États membres, l'UNESCO s'intéresse aux tendances relatives à ces droits, et particulièrement au droit à la liberté d'expression. La Résolution 53, adoptée lors de la 36e session de la Conférence générale, demande à l'Organisation de « suivre, en étroite collaboration avec d'autres organismes des Nations Unies et d'autres organisations concernées, actives dans ce domaine, la situation en matière de liberté de la presse et de sécurité des journalistes, et tout particulièrement les cas de violences à l'égard des journalistes commises dans l'impunité, y compris en restant attentif aux suites judiciaires par l'intermédiaire du Conseil intergouvernemental du Programme international pour le développement de la communication (PIDC) et rendre compte des évolutions sur ces points à la Conférence générale ». Cette Résolution a étayé le premier rapport T*endances mondiales en matière de liberté d'expression et de développement des médias*,[1] qui a été lancé dans six villes du monde et inclut six sous-études régionales. La présente étude poursuit l'application de ce mandat en utilisant le cadre conceptuel du premier rapport *Tendances mondiales*, qui mettait l'accent sur les questions de la liberté, du pluralisme, de l'indépendance, de la sécurité et du genre. Elle répond également au mandat de la 37e Conférence générale de 2013, dont la Résolution 52 demande une étude approfondie et consultative des quatre dimensions de l'Internet relevant des attributions de l'UNESCO. Cette étude intitulée *Des clés pour la promotion de sociétés du savoir inclusives*, examine l'accès à l'information et au savoir, la liberté d'expression, le respect de la vie privée et les dimensions éthiques de la société de l'information.

Dans ce contexte, l'UNESCO reconnait que les technologies numériques ont pris un rôle de plus en plus central dans les sociétés, et que les questions relatives à la liberté d'expression en ligne, et ses interfaces avec le monde hors ligne, demandent une attention particulière de la part de l'Organisation. La sécurité des journalistes et la question de l'impunité font notamment l'objet d'un des chapitres suivants. La situation dans le monde réel a d'importantes conséquences sur le monde en ligne, et réciproquement. Le manque de sécurité dans une sphère a des répercussions sur la sécurité de l'autre sphère. L'UNESCO est donc de plus en plus sensible aux interfaces.

Au niveau des programmes, l'UNESCO travaille dans le monde entier à promouvoir la liberté d'expression sur toutes les plates-formes, qu'elles soient en ligne ou hors ligne, et

1 http://www.unesco.org/new/fr/world-media-trends

sur leur corrélation. Deux dimensions méritent d'être étudiées, correspondant à l'amont et à l'aval du processus de communication.

La première dimension de la libre expression est le droit de *transmettre* des informations et des opinions. Il s'agit là de la base du droit à la liberté de la presse, soit la liberté de publier une information à l'attention d'un large public. À l'ère du numérique, ce droit est particulièrement important pour tous ceux qui utilisent des médias traditionnels ou sociaux. Pour l'UNESCO, une réelle liberté de la presse se base sur la liberté des médias, le pluralisme, l'indépendance et la sécurité. Cela s'applique à tous les médias, y compris les médias créatifs et les médias sociaux, et non pas uniquement aux médias d'information. Dans cette perspective, la question de l'indépendance est d'autant plus cruciale pour ceux qui utilisent la liberté de la presse pour faire du journalisme. L'indépendance dépend de la liberté et du pluralisme, et dans le cas du journalisme, qu'il soit en ligne ou hors ligne, de l'existence de normes professionnelles sur la production et la circulation d'informations vérifiables et qui sont dans l'intérêt du public.

En bref, la liberté de la presse – comprise comme l'exercice du droit de communiquer des informations à grande échelle – découle de la liberté d'expression. La liberté des médias, le pluralisme, l'indépendance et la sécurité constituent l'environnement favorable nécessaire pour exercer la liberté de la presse. C'est dans ce contexte que le journalisme professionnel, descendant de la liberté d'expression, peut prospérer et contribuer à l'avènement de sociétés du savoir.

La seconde dimension de la liberté d'expression est le droit de *rechercher et de recevoir* l'information, ce qui forme la base du droit à l'information. Il s'agit là d'une des bases de la transparence, reconnue comme essentielle pour le développement et la démocratie. De grands progrès en matière de transparence sont rendus possibles par les technologies numériques, pour les institutions privées comme publiques, car elles permettent une responsabilisation sans précédent et le renforcement des pouvoirs des citoyens.

Ces deux dimensions de la liberté d'expression sont de plus en plus entremêlées avec le droit au respect de la vie privée, ce qui entraîne des synergies potentielles mais aussi des tensions. Un grand respect de la vie privée renforce la capacité des journalistes à s'appuyer sur des sources confidentielles pour informer le public, mais il peut également réduire la transparence et occulter des informations qui pourraient être d'intérêt public. Le manque de respect de la vie privée peut obliger des sources journalistiques à retenir des informations ou à s'autocensurer, de crainte d'être surveillées de manière arbitraire. Le manque de respect de la vie privée peut également entrainer une application excessive du principe de transparence, se traduisant par une intrusion injustifiée dans la vie privée des individus. La confiance dans les avantages des communications numériques peut être affectée par la manière dont une société traite le droit au respect de la vie privée dans les deux dimensions du droit à la liberté d'expression.

Bon nombre des travaux de l'UNESCO donnent un aperçu de la manière dont ces deux droits peuvent être respectés, en ligne comme hors-ligne, de leurs points d'interface et de la manière dont ils peuvent être équilibrés, si nécessaire, de manière harmonieuse et dans l'intérêt du public. L'Organisation veille à cela par la recherche, la surveillance, la sensibilisation, la défense, le renforcement des capacités et les conseils techniques.

Le Programme international pour le développement de la communication (PIDC) de l'UNESCO propose également des subventions aux projets visant à assurer des médias libres, pluralistes, indépendants et sécurisés, que ce soit en ligne ou hors ligne.

Au niveau de l'action normative pour la défense de la liberté d'expression et de la vie privée en ligne, l'UNESCO s'est activement impliquée et a contribué à des évènements à l'échelle mondiale comme régionale, notamment les principes de gouvernance de l'Internet de NETmundial et la feuille de route pour l'évolution future de la gouvernance de l'Internet, les recommandations du Conseil de l'Europe sur la liberté en ligne, la Déclaration africaine des droits et libertés de l'Internet, et le projet du septième programme-cadre de l'Union européenne « Managing Alternatives for Privacy, Property and Internet Governance ».

De plus, l'Organisation défend la liberté d'expression en ligne et le respect de la vie privée au niveau mondial, et s'engage avec les parties prenantes concernées dans des forums, des initiatives et des réunions à l'échelle mondiale, régionale et nationale. Parmi ces forums, citons entre autres le Forum sur la gouvernance de l'internet (IGF), le SMSI, l'Initiative NETmundial, l'Association internationale des études et recherches sur l'information (AIERI), le Forum mondial des médias, la coalition Freedom Online, et divers IGF régionaux.

Pour répondre à la Résolution 52, et comme mentionné ci-dessus, l'UNESCO a réalisé l'étude *Des clés pour la promotion de sociétés du savoir inclusives*, suite à la demande des États membres d'étudier les dimensions de l'accès au savoir et à la connaissance, de la liberté d'expression, de la vie privée et de l'éthique de la société de l'information. Cette activité sera présentée à la 38e session de la Conférence générale dans le cadre du Rapport de la Directrice générale sur la mise en œuvre des résultats du Sommet mondial sur la société de l'information (SMSI).[2]

Dans le cadre de son mandat, l'UNESCO a réalisé cette étude en mettant en place une procédure participative multipartite qui regroupait des gouvernements, le secteur privé, la société civile, des organisations internationales et la communauté technique. En juillet 2014, un questionnaire a été publié en ligne et diffusé par les réseaux sociaux et les principaux forums, ainsi que transmis directement aux États membres et à plus de 300 experts et organisations représentant la société civile, le monde universitaire, la communauté technique et les organisations intergouvernementales. Fin novembre 2014, l'UNESCO avait reçu 200 réponses exploitables. Le questionnaire a également été diffusé lors des forums mondiaux en rapport avec l'Internet, et un débat thématique sur la liberté d'expression et la vie privée en ligne a été organisé lors de la 29e réunion du Conseil du PIDC en novembre 2014. En parallèle aux consultations multipartites, l'UNESCO a commandé une série de publications sur certains sous-thèmes spécifiques afin de fournir une analyse approfondie et des recommandations en matière de liberté sur l'Internet à ses États membres et aux autres parties prenantes. Ces sous-études ont contribué à l'étude plus globale sur l'Internet, et certaines d'entre elles ont été publiées comme documents distincts dans la série de l'UNESCO concernant la liberté sur l'Internet.[3]

2 http://unesdoc.unesco.org/images/0023/002341/234144f.pdf

3 Voir UNESCO. *Études de l'UNESCO sur la liberté sur Internet*. http://www.unesco.org/new/en/communication-and-information/resources/publications-and-communication-materials/publications/publications-by-series/unesco-series-on-internet-freedom/

En plus des sous-études qui ont contribué à trois chapitres de la présente publication (à savoir *Combattre les discours de haine sur Internet, Protéger les sources des journalistes à l'ère numérique* et *Promouvoir les libertés en ligne : le rôle des intermédiaires de l'Internet*), l'UNESCO a également commandé un grand nombre de recherches dans le cadre de la série concernant la liberté sur l'Internet, dans le cadre de la Résolution 52 de la Conférence générale de 2013 :

1. **Construire une sécurité numérique pour le journalisme** : enquête sur une sélection de questions : Compte tenu de la compréhension limitée à l'échelle mondiale des menaces de sécurité liées aux développements du numérique, l'UNESCO a commandé cette recherche dans le cadre des efforts de l'Organisation pour mettre en œuvre le Plan d'Action des Nations Unies sur la sécurité des journalistes et la question de l'impunité. En examinant des cas disséminés partout dans le monde, la publication sert de ressource pour de nombreux acteurs. Elle étudie l'évolution des menaces et évalue des mesures anticipées, protectrices et préventives. Elle montre que la sécurité du journalisme englobe et dépasse la dimension technique. Des recommandations sont proposées à l'examen des États membres en ce qui concerne les gouvernements, les sources et contributeurs du journalisme, les organismes d'information, les formateurs, les entreprises et les organisations internationales.

2. **Principes de la gouvernance de l'Internet : Analyse comparative** : Cette recherche analyse plus de 50 déclarations et cadres spécifiques à l'Internet et relevant des principes de l'Internet. Elle est née de la nécessité d'une étude spécifique des déclarations et cadres sous l'angle du mandat de l'UNESCO. La publication montre que, bien que chacun de ces documents ait une valeur propre, aucun d'entre eux ne répond pleinement aux priorités et au mandat de l'UNESCO. Elle présente également aux États membres le concept d'« Universalité de l'Internet », qui pourrait servir à définir clairement l'approche de l'Organisation dans les différents domaines que recouvrent les questions relatives à l'Internet et leurs recoupements avec les préoccupations de l'UNESCO. Ce concept est pertinent pour les travaux de l'Organisation dans de nombreux domaines – y compris pour la liberté d'expression et le respect de la vie privée, la progression de l'universalité dans l'éducation, l'inclusion sociale et l'égalité des sexes, le multilinguisme dans le cyberespace, l'accès à l'information et à la connaissance et la réflexion éthique sur la société de l'information.

3. **Enregistrement et liberté d'expression sur Internet** : L'UNESCO a commandé une étude sur le thème du droit à la liberté d'expression sur Internet, en particulier dans le domaine du journalisme. La restriction de l'accès aux moyens de communication est un problème qui affecte directement la liberté de la presse. Il découle de pratiques anciennes qui consistaient à filtrer et bloquer les informations, ce qui a un impact considérable sur le droit de rechercher et de recevoir des informations. Si on considère les normes internationales, la liberté d'expression est la norme et la restriction l'exception. Lorsque l'enregistrement sert à accorder une autorisation à publier, aux sens à la fois obligatoire et exclusif, il peut être considéré comme une forme de censure avant publication. Des tests stricts doivent donc être menés afin d'assurer que l'enregistrement peut se justifier par les droits internationaux, en termes de nécessité, de proportionnalité, de procédure régulière et d'objectif légitime. L'objet

de cette étude est de fournir des réponses actuelles et concrètes aux questions relatives à la permission de publier en ligne qui ont été récemment soulevées par les politiques, ainsi que par les régimes juridiques et réglementaires.

4. **Vie privée et éducation aux médias et à l'information** : L'UNESCO réalise une recherche à l'échelle mondiale sur la vie privée et l'éducation aux médias et à l'information. Elle explore la question des internautes ayant des compétences en matière d'éducation aux médias sur les différentes dimensions du respect de la vie privée, comme la conscience publique des droits au respect de la vie privée dans le cyberespace, et étudie notamment les régimes nationaux de protection des données, la capacité à évaluer comment la vie privée est respectée dans les contenus numériques et les communications accessibles aux utilisateurs, et la capacité à évaluer les limites légitimes de la vie privée en ligne. Elle cherche à collecter des données sur ces domaines, à la fois en rassemblant les données disponibles publiquement dans certains pays et dans certaines régions, et en analysant les pratiques en matière d'éducation aux médias et à l'information dans ces mêmes régions.

5. **Équilibre entre respect de la vie privée et transparence** : L'UNESCO a commandé une recherche mondiale sur l'équilibre entre le respect de la vie privée et la transparence, cette dernière étant évaluée dans sa relation avec la liberté d'expression. La recherche vise à démêler la complexité du sujet grâce à des informations normatives mais aussi empiriques, étendant l'analyse à des acteurs individuels, de la société civile, du secteur privé et des gouvernements. Elle traite aussi de la question de la confiance de l'utilisateur dans le fait que ses données personnelles ne seront pas diffusées de manière illégitime. Les risques que représentent la transparence pour le respect de la vie privée, et les risques réciproques, seront également présentés. Une analyse de cas p abordera les questions traitées et les leçons qui en découlent. Les bonnes pratiques en matière de réconciliation du respect de la vie privée et de la transparence sont identifiées en fonction de leur conformité avec les lois internationales.

6. **Vie privée et chiffrement** : Cette étude traite de la disponibilité de différents moyens de chiffrement et de leurs possibles applications, et présente rapidement les dernières avancées technologiques déployées sur Internet et dans les industries des communications. L'étude analyse le rapport entre le chiffrement et les droits de l'homme au niveau international, en intégrant également des cas locaux pertinents. Elle présente les développements juridiques en matière de restrictions gouvernementales sur le chiffrement dans certaines juridictions et analyse les différents choix de politiques dans ce domaine au niveau international, en proposant des idées pour améliorer l'« éducation au chiffrement ».

Par le biais de consultations multipartites et de sous-études, l'UNESCO a identifié quatre domaines de recherche comme étant des piliers indépendants de l'Internet. L'étude intitulée *Des clés pour la promotion de sociétés du savoir inclusives*, souligne l'intérêt général pour l'avenir de l'Internet en tant que ressource ouverte, fiable et mondiale, accessible à tous partout dans le monde. Elle analyse les questions de la technologie et des politiques comme moyens de soutenir un accès plus équitable et généralisé à l'information et au savoir, du renforcement de la liberté d'expression en tant qu'instrument

de la pratique démocratique et de la responsabilisation, et du renforcement de la confidentialité des informations personnelles.

L'étude a découvert que la liberté d'expression n'est pas un produit inéluctable des nouvelles technologies. La liberté d'expression doit être soutenue par des politiques et des pratiques, et nécessite que l'Internet soit considéré comme un moyen sûr d'exprimer son opinion. Par exemple, l'inquiétude que suscitent la surveillance et le filtrage en ligne donne l'impression que la liberté d'expression sur l'Internet est menacée. Des efforts majeurs sont nécessaires pour rétablir la confiance en ce qui concerne le respect de la vie privée, la sécurité et l'authenticité des informations et des savoir disponibles en ligne, et pour protéger la sécurité et la dignité des journalistes, des utilisateurs de réseaux sociaux et de toute personne publiant des informations ou des opinions en ligne.

Le rapport établit en outre que la liberté d'expression en ligne est liée au principe d'ouverture, particulièrement en ce qui concerne les droits internationaux qui demandent la transparence sur les restrictions du droit d'expression. Des opportunités ouvertes pour partager les idées et informations au sujet de l'Internet sont parties intégrantes des travaux de l'UNESCO pour promouvoir la liberté d'expression, le pluralisme des médias et le dialogue interculturel. Pour l'UNESCO, l'étude de la liberté d'expression en ligne doit aussi se pencher sur la manière dont les personnes utilisent leur accès à Internet et les TIC associées pour s'exprimer. L'éducation aux médias et à l'information pour tous les hommes et toutes les femmes est importante en la matière, notamment par l'engagement des jeunes et la lutte contre toute forme de haine, de racisme, de discrimination, et d'extrémisme violent dans le contexte numérique, du simple e-mail aux jeux vidéo en ligne.

Afin de discuter de la version préliminaire de l'étude, l'UNESCO a organisé en mars 2015 une conférence intitulée « InterCONNECTer les ensembles : options pour l'action future », regroupant quelques 400 participants des cinq continents au siège de l'UNESCO à Paris. L'événement a fourni une plate-forme pour explorer les découvertes de l'étude afin d'en préparer la finalisation. Il a également été l'occasion pour de nombreux conférenciers du monde entier de faire des présentations. La rencontre multipartite a adopté par une majorité écrasante un document final qui souligne l'importance de l'Internet pour le progrès humain et son rôle pour la promotion de sociétés du savoir inclusives. Celui-ci confirme les principes des droits de l'homme qui étayent l'approche de l'UNESCO sur les questions relatives à l'Internet ; et soutient les principes d'Universalité de l'Internet qui font la promotion d'une participation conforme aux principes **D.O.A.M.** (Droits de l'homme, Ouverture, Accessibilité, participation d'acteurs Multiples). Selon le rapport, ces quatre principes forment une logique d'accompagnement pour soutenir la poursuite du développement de l'Internet d'une manière qui améliorera l'accès à l'information et au savoir, la liberté d'expression, la vie privée et l'éthique.

Une Résolution adoptée lors de la 196e session du Conseil exécutif de l'UNESCO en avril 2015 recommande que le document final de la conférence InterCONNECTer les ensembles : options pour l'action future soit soumis à l'examen de la Conférence générale à sa 38e session et soit diffusé en tant que contribution non contraignante à l'élaboration du programme de développement pour l'après-2015, au processus d'examen global du Sommet mondial sur la société de l'information (SMSI) par l'Assemblée générale des

Nations Unies, ainsi qu'à la réunion de haut niveau décidée par l'Assemblée générale des Nations Unies dans sa Résolution 68/302. Ce document final a été utilisé dans le rapport *Des clés pour la promotion de sociétés du savoir inclusives* pour présenter les options d'actions futures.

En parallèle, l'UNESCO a aidé à façonner le programme de développement durable pour l'après-2015 en organisant des réunions sur les lignes d'action du SMSI et des événements avec l'IGF, pour souligner le rôle crucial de la gratuité, de l'indépendance et du pluralisme des médias ainsi que des principes de l'Universalité de l'Internet pour atteindre les Objectifs de développement durable. L'UNESCO a présenté le rapport *Des clés pour la promotion de sociétés du savoir inclusives* et organisé la 10e réunion de facilitation de la grande orientation C9 « Médias » lors du forum du SMSI de 2015. Trois ateliers et un forum ouvert ont été approuvés pour le 10e IGF qui aura lieu au Brésil en novembre 2015.

L'UNESCO s'est engagée de manière systématique dans l'ère numérique, en réalisant des recherches de pointe et en participant aux dialogues multipartites dans le but de renforcer les droits fondamentaux de liberté d'expression et de respect de la vie privée, aussi bien en ligne que hors ligne.

III. COMBATTRE LES DISCOURS DE HAINE SUR INTERNET[4]

4 Ce chapitre est tiré de Gagliardone, I. et al. 2015. *Combattre les discours de haine sur Internet*. Série de l'UNESCO sur la liberté d'Internet. Paris, UNESCO. http://unesdoc.unesco.org/images/0023/002332/233231e.pdf

1. INTRODUCTION

À mesure qu'augmente le nombre de participants aux échanges en ligne, une attention grandissante est portée sur la tendance des discours de haine sur Internet. Il est également évident qu'après des évènements dramatiques, on en appelle souvent à des mesures plus restrictives ou plus intrusives afin de limiter la capacité d'Internet à propager la haine et de la violence, même si les liens entre les paroles et les actes, entre les contenus en ligne et la violence hors Internet, ne sont pas clairement établis. Pour comprendre ce problème et les tendances qui en découlent, il faut analyser plusieurs points, à commencer par notre conception du phénomène. Ce chapitre propose une conception qui s'appuie sur les débats récents, puis évalue les évolutions des instruments normatifs internationaux. Il fait état de la tendance selon laquelle les fournisseurs Internet sont de plus en plus acteurs de la lutte contre les discours de haine et des normes qui leur sont applicables. Ensuite, il examine la signification plus large des tendances émergentes, en étudiant cinq réactions sociales aux discours de haine sur Internet : i) des efforts de recherche permettant de suivre l'émergence et la diffusion des discours de haine en ligne, en développant un système d'alerte précoce et des méthodes qui facilitent la distinction entre les différents types d'actes de parole ; ii) des actions coordonnées menées par des membres de la société civile qui cherchent à créer des coalitions nationales et internationales ; iii) des initiatives encourageant les réseaux sociaux et les fournisseurs d'accès à Internet à renforcer leur lutte contre les discours de haine en ligne ; iv) des campagnes et des initiatives d'éducation aux médias et à l'information afin de préparer les utilisateurs à interpréter les discours de haine et à y réagir ; et v) la modération des messages de haine par les médias d'information. Enfin, ce chapitre indique les enjeux majeurs des tendances à venir en ce qui concerne la perception des discours de haine et les compétences juridiques, avant de résumer les points principaux.

1.1 UNE CONCEPTION LARGE

Il existe un ensemble de liens très complexes entre les discours de haine d'une part et la liberté d'expression, les droits des individus, des groupes et des minorités d'autre part, sans oublier les concepts de dignité, de liberté et d'égalité et de sécurité des individus. La définition du terme « discours de haine » est fréquemment contestée. Comme expliqué ci-après dans la section 1.2, dans de nombreuses lois et textes réglementaires internationaux, il renvoie à une expression qui incite à causer du tort, dont la cible correspond à un certain groupe social ou démographique. Dans le cas de la haine raciale, la législation internationale inclut également les expressions qui peuvent favoriser un climat de préjugés et d'intolérance. Dans le langage courant, les définitions des discours de haine sont souvent plus larges encore, allant même parfois jusqu'à inclure des propos insultants à l'encontre des dirigeants au pouvoir ou bien désobligeants à l'égard de personnes particulièrement visibles. Ces référents variables illustrent une tendance actuelle : il n'y a pas de consensus autour d'une seule définition et le terme

« discours de haine » reste une formule consacrée qui peut s'appliquer à une très grande variété de discours.

Dans son acception la plus large, un « discours de haine » est source d'inquiétude non seulement car il est souvent perçu par principe comme une insulte, mais aussi parce qu'on suppose souvent qu'il est susceptible d'alimenter des actions qui peuvent donner lieu en pratique à une violation des droits. Même si le lien entre expression et action est loin d'être automatique, la sensibilité est accrue en particulier dans des moments critiques, notamment pendant les élections. Dans le même temps, le terme « discours de haine » peut se prêter à la manipulation : les opposants politiques peuvent s'accuser mutuellement de proférer des propos haineux ou bien les dirigeants peuvent utiliser ces accusations afin de juguler toute critique et toute dissidence.

Pour que cette analyse soit la plus large possible, dans ce chapitre, le terme « discours de haine » est utilisé de manière pragmatique, pour permettre l'étude de l'ensemble de définitions et de pratiques rassemblées dans cette vaste rubrique. Ainsi, bien que le concept de discours de haine soit difficile à cerner avec certitude, dans ce chapitre le terme renvoie aux discours qui remplissent des fonctions dégradantes ou déshumanisantes. En nous référant aux travaux de Jeremy Waldron, professeur à la New York University School of Law, nous affirmons dans ce chapitre que des propos considérés comme haineux envoient deux sortes de message. Le premier est envoyé au groupe ciblé et sa fonction est de déshumaniser et d'humilier les membres attribués à ce groupe. Le second consiste à faire savoir aux personnes qui partagent ces opinions qu'elles ne sont pas seules, de renforcer leur sentiment d'appartenance à un groupe. Les « discours de haine » reposent sur les tensions, qu'ils cherchent à reproduire et à amplifier. Ils unissent et divisent en même temps. Ils créent un « nous » et un « ils ». Dans ce chapitre, nous employons généralement le terme « discours de haine » au sens large de l'identification par opposition qui suppose une identité de groupe, sans limiter sa signification aux discours qui constituent précisément une incitation à causer du tort. Il est employé sans présumer que la fonction de ce type de discours est d'encourager les actes malfaisants.

Les propos haineux s'articulent autour d'un certain nombre d'axes tels que la race, l'origine ethnique, la langue, le sexe, la religion, l'orientation sexuelle ou la nationalité. Cependant, il est aussi évident que des idées fortement défendues ne doivent pas en soi être confondues avec des discours de haine. Les discours de haine concernent les antagonismes entre les individus et non pas les idées abstraites. Ils ne concernent pas l'hostilité vis-à-vis des idéologies politiques, des religions ou des croyances, même si c'est sur cette base que sont définis les groupes ciblés. On doit garder cette distinction à l'esprit pour limiter la « dérive sémantique » du terme « discours de haine ».

Le concept de discours de haine étant contesté car il est trop vaste et sujet à la manipulation, on a vu apparaître récemment des concepts plus restrictifs, qui s'appliquent uniquement aux propos haineux pouvant être décrits comme des « discours dangereux » ou des « discours attisant la peur ». Ces termes ont été proposés pour mettre l'accent sur la capacité de ces discours à causer de réels dommages ou à engendrer des actes violents. Si l'on retrouve des discours de haine – sous une forme ou une autre – dans de nombreux contextes, le concept de « discours dangereux » est apparu vers 2010. Défini par Susan Benesch, du Berkman Center for Internet and Society, il vise à isoler les

actes qui présentent une forte probabilité de « catalyser ou d'amplifier la violence, celle-ci provenant d'un groupe et étant dirigée contre un autre groupe ». Le concept de « discours attisant la peur » mis en lumière par Antoine Buyse, directeur de l'Institut des droits de l'homme aux Pays-Bas, a quant à lui été proposé pour qualifier un langage susceptible de créer progressivement une mentalité d'assiégé et de conduire, au bout du compte, à légitimer des actes violents. Fondée aussi sur l'étude des atrocités de masse, cette idée de « discours attisant la peur » nous permet de comprendre l'apparition progressive des conditions préalables au déclenchement de la violence et d'identifier, le cas échéant, les moments critiques où des contre-mesures pourraient être le plus efficaces. Enfin, il y a eu de plus en plus de tentatives pour faire avancer le débat sur les discours de haine au-delà de l'identification, la réglementation et l'élaboration de contre-mesures : on a cherché à comprendre qui étaient les personnes tenant des propos haineux et quelle était leur motivation. Ces recherches ont pour but de comprendre les caractéristiques et les causes propres à ce phénomène qui évolue rapidement, cela étant la condition préalable à l'élaboration de « solutions ». Les discours de haine, sur Internet comme en dehors, peuvent donc désormais être évalués en prenant en compte ces nuances afin de développer des réponses adaptées aux spécificités du problème considéré.

La prolifération des discours de haine en ligne ; telle qu'observée par Rita Izsák, Rapporteuse spéciale du Conseil des droits de l'homme des Nations Unies sur les questions relatives aux minorités, dans son rapport A/HRC/28/64, pose de nouveaux défis. S'il n'existe aucune statistique offrant une vue d'ensemble du phénomène, les plates-formes des réseaux sociaux tout comme les organisations créées dans le but de combattre les discours de haine ont reconnu que les messages haineux diffusés sur Internet sont de plus en plus courants et que la mise en place de ripostes appropriées fait l'objet d'une attention sans précédent. Selon HateBase, une application Web qui répertorie des cas de propos haineux sur Internet à travers le monde, la plupart de ces cas visent des individus et sont fondés sur l'origine ethnique et la nationalité, mais les incitations à la haine fondées sur la religion ou la classe sociale sont également en augmentation.

Appliquées aux discours de haine sur Internet, certaines mesures juridiques élaborées pour d'autres médias se révèlent inefficaces ou inadéquates. Il est nécessaire d'adopter des approches qui prennent en compte la nature spécifique des interactions propres aux technologies numériques de l'information et de la communication (TIC). Il y a un risque d'amalgame entre un tweet fulminant envoyé par un utilisateur qui n'a pas réfléchi aux conséquences de son acte et une menace réelle qui fait partie d'une campagne systématique d'incitation à la haine. De même, il faut faire la différence entre un message qui ne suscite aucune réaction — ou très peu — et un message qui se propage parmi les internautes tel un virus. Il faut en outre tenir compte des difficultés auxquelles sont confrontées les gouvernements et les tribunaux, notamment lorsqu'ils tentent de faire respecter une loi par une plate-forme de réseau social dont le siège se trouve dans un autre pays. Par conséquent, bien que les discours de haine ne soient pas intrinsèquement différents des autres discours semblables formulés hors Internet, ils posent des problèmes particuliers.

Ces problèmes sont liés à la permanence, à l'itinérance, à l'anonymat et au caractère transjuridictionnel des contenus numériques :

- D'abord, des propos haineux peuvent rester en ligne pendant très longtemps, sous différentes formes et sur de multiples plates-formes. Comme l'a remarqué Andre Oboler, PDG du Online Hate Prevention Institute : « Plus le contenu reste disponible sur le Web, plus les dommages causés aux victimes sont importants et plus le pouvoir des auteurs de ces messages est renforcé. » En fonction de l'architecture d'une plate-forme, on peut développer un sujet pendant plus ou moins longtemps. Les conversations sur Twitter autour des sujets les plus tendance peuvent faciliter la diffusion rapide des messages haineux, mais elles offrent aussi la possibilité aux personnes ayant une certaine influence de les ridiculiser et de mettre fin à des fils de discussion très suivis. Sur Facebook, en revanche, de nombreux fils de discussion peuvent se dérouler en parallèle et passer inaperçus en dehors d'une communauté restreinte, permettant ainsi que certains groupes soient calomniés pendant plus longtemps.

- Ensuite, les discours de haine en ligne peuvent aussi être itinérants. Lorsqu'un contenu est supprimé, il peut à nouveau être exprimé ailleurs, éventuellement sur la même plate-forme mais sous un pseudonyme différent, ou bien dans d'autres espaces en ligne. Quand un site Internet est fermé, on peut le rouvrir en utilisant un service d'hébergement dont la réglementation est moins stricte ou bien en hébergeant le site dans un pays où la législation est plus permissive à l'égard des discours de haine. Ce caractère itinérant signifie également que des idées qui, par le passé, n'auraient pas attiré l'attention du public peuvent bénéficier actuellement d'une grande visibilité parmi les internautes, grâce à la multitude des plates-formes.

- De plus, la longévité des contenus haineux sur Internet est unique, du fait de leur faible coût et de leur potentiel de réapparition immédiate.

- L'anonymat est la quatrième difficulté posée par les discours de haine en ligne. Danielle Keats Citron et Helen Norton, professeurs de droit, remarquent que : « Internet facilite l'expression anonyme et sous pseudonyme, qui peut tout aussi facilement accélérer les comportements destructifs qu'alimenter le débat public. » Certains gouvernements et certaines plates-formes de réseaux sociaux ont tenté de faire appliquer des mesures exigeant que les internautes utilisent leur vrai nom, mais elles ont été vivement contestées car elles se heurtent au droit du respect de la vie privée et au droit à la liberté d'expression. De surcroît, les actes de perturbation et les propos haineux en ligne proviennent, pour l'essentiel, de comptes sous pseudonymes qui ne sont pas nécessairement anonymes pour tout le monde. Les communications véritablement anonymes sur Internet sont rares car elles nécessitent que l'utilisateur emploie des méthodes très sophistiquées sur le plan technique pour dissimuler son identité. Malgré cela, l'anonymat perçu peut inciter certains acteurs à penser qu'ils ne pourront pas être identifiés comme les auteurs de leurs messages de haine.

- En dernier lieu, dans la mesure ou Internet n'est pas régi par une entité unique, les personnes concernées, ainsi que les organisations gouvernementales et non gouvernementales, devront peut-être aborder la question des intermédiaires d'Internet

au cas par cas, en laissant les propriétaires de chaque cyberespace décider de la manière dont ils traitent les actions des utilisateurs. Les intermédiaires de l'Internet risquent alors de devenir des tribunaux privés qui décident de la réglementation des contenus, question que nous traitons en profondeur plus loin dans ce rapport. La portée transnationale d'Internet constitue un obstacle supplémentaire : elle soulève en effet des problèmes de coopération transjuridictionnelle quant aux mécanismes juridiques visant à combattre les discours de haine. S'il existe bien des traités d'entraide judiciaire dans de nombreux pays, leur fonctionnement est extrêmement lent. La portée transnationale de nombreux intermédiaires privés d'Internet pourrait fournir un moyen plus efficace pour résoudre ces problèmes dans certains cas, même si ces organismes sont souvent affectés par des demandes transjuridictionnelles de données. Contrairement à la diffusion des discours de haine par le biais des médias traditionnels, la diffusion des propos haineux en ligne implique souvent une multitude d'acteurs, sciemment ou non. Lorsque les auteurs de messages haineux utilisent une plate-forme en ligne pour les diffuser, ils ne causent pas seulement du tort à leurs victimes, ils enfreignent aussi souvent les conditions d'utilisation de cette plate-forme et parfois même la législation nationale, selon l'endroit où ils se trouvent. Les victimes, de leur côté, se sentent parfois démunies face au harcèlement en ligne, ignorant vers qui se tourner pour demander de l'aide.

Sur la base de l'analyse présentée plus haut, ce chapitre aborde les tendances émergentes en matière de discours de haine sur Internet. S'il se concentre particulièrement sur les pays développés et en développement, il reconnaît par ailleurs que l'on rencontre actuellement les plus gros problèmes de discours de haine en ligne dans des pays où le degré de connectivité Internet est important. Cependant, cela peut laisser présager une évolution semblable dans d'autres pays, puisque les individus sont de plus en plus connectés à travers le monde. On pourrait envisager d'adapter une partie des solutions évaluées dans ce rapport en amont et de manière proactive, sans attendre l'apparition du problème.

1.2 RÉACTIONS JURIDIQUES ET SOCIALES

Les réactions aux discours de haine sur Internet les plus débattues sont principalement axées sur la définition et les moyens juridiques, mais cette approche comprend des risques et des limites.

Premièrement, il existe des liens inextricables entre pouvoir et législation, et l'on peut abuser de cette dernière pour limiter la liberté d'expression sous couvert de lutter contre les propos haineux. Il peut y avoir des dommages collatéraux à un discours qui, si certains le trouvent très offensant, n'enfreint pas les normes internationales portant sur la liberté d'expression. La question cruciale est ici de savoir à quelle catégorie appartiennent un « discours de haine » et sa réglementation, parmi les trois identifiées en 2012 par Frank La Rue, alors Rapporteur spécial des Nations Unies sur la promotion et la protection du droit à la liberté d'opinion et d'expression. Dans son rapport A/66/290, il distingue :

- Les discours qui constituent une infraction selon le droit international et peuvent faire l'objet de poursuites pénales ;
- Les discours qui ne sont pas passibles de sanctions pénales mais peuvent justifier une restriction et une action civile ; et
- Les discours qui ne donnent pas lieu à des sanctions pénales ou civiles, mais qui suscitent néanmoins des inquiétudes en matière de tolérance, de civilité et de respect d'autrui.

Il est évident que toutes les catégories mentionnées ci-dessus ne justifient pas une réaction juridique et qu'il faut, le cas échéant, faire la distinction entre les réactions relevant du droit pénal et celles relevant du droit civil. De même, il est clair que les réactions sociales peuvent avoir plusieurs rôles à jouer dans tous les cas, et notamment un rôle préventif. Tous ces éléments ont une influence décisive sur la manière dont différents discours de haine sont compris et traités.

Deuxièmement, la Rapporteuse spéciale des Nations Unies sur les questions relatives aux minorités remarque que les crimes motivés par la haine se produisent rarement sans des manifestations préalables de stigmatisation et de déshumanisation à l'égard de groupes ciblés et des incitations à commettre des actes inspirés par la haine. Dans le même temps, elle écrit : « Seuls les propos haineux les plus extrêmes, c'est-à-dire ceux qui constituent une incitation à la discrimination, à l'hostilité ou à la violence, sont généralement considérés comme illicites. » Cela montre bien que même si la législation a un rôle à tenir, les mesures juridiques ne sauraient être considérées comme des réponses suffisantes pour combattre toute la diversité des propos qui peuvent (mais ne le font pas toujours) favoriser un climat propice aux crimes haineux.

Troisièmement, en examinant la question des discours de haine uniquement sous l'angle juridique, on risque d'omettre que les sociétés évoluent par le biais de la contestation et des dissensions. Bien que les discours de haine soient blessants, ils peuvent aussi être vus comme la manifestation de tensions et d'inégalités profondément enracinées dans une société, lesquelles doivent être traitées au-delà des questions relevant purement de l'expression et au-delà des limites d'Internet.

Cette analyse souligne pourquoi il est important de suivre les tendances liées aux discours de haine à la fois sur le plan légal et sur le plan social. Par conséquent, ce chapitre présente maintenant un aperçu général de l'évolution des principaux instruments juridiques internationaux qui régissent les discours de haine, puis s'attache à étudier les réactions sociales.

2. MÉTHODOLOGIE

La stratégie de recherche adoptée pour la rédaction de ce chapitre s'appuie largement sur l'étude plus détaillée menée par l'UNESCO, *Combattre les discours de haine sur Internet*, qui quant à elle combinait plusieurs techniques de collecte et d'analyse de données, en commençant par une consultation approfondie de la documentation sur le sujet – y compris des textes juridiques qui examinent le traitement des discours de haine dans différents pays sur plusieurs continents et les études ethnographiques portant sur le comportement des utilisateurs de cyberespaces diffusant des propos haineux. Compte tenu de la nouveauté du phénomène étudié et de la rapidité de son évolution, l'analyse documentaire comprenait aussi des articles ne provenant pas de travaux universitaires mais publiés par des spécialistes sur leurs blogs, dans des revues spécialisées ou bien dans d'importants journaux et magazines en ligne.

Ce chapitre contient également des éléments obtenus lors d'entretiens semi-structurés réalisés auprès d'acteurs concernés, des représentants des plates-formes de réseaux sociaux – dont Facebook et Google – aux membres d'organisations de la société civile, en passant par des responsables politiques et des experts techniques. Nous avons également analysé des contenus produits par des organisations non gouvernementales (ONG) qui ont lancé des campagnes d'initiation aux médias et à la maîtrise de l'information visant à combattre les discours de haine en ligne et examiné les conditions générales d'utilisation des plates-formes des médias sociaux en ligne, tels que Facebook, Twitter et YouTube. L'objectif était de comprendre comment fonctionnent précisément la surveillance et la gestion des contenus en ligne. Nous avons également étudié la manière dont les campagnes d'initiation aux médias et à la maîtrise de l'information visaient divers publics et analysé leurs résultats ; enfin, nous avons considéré les stratégies adoptées par les groupes ou coalitions luttant contre la discrimination pour faire pression sur les médias sociaux. Malgré la variété des conceptions sur les discours de haine en ligne et des ripostes contre ce phénomène, nous avons posé des questions identiques dans chaque cas.

3. CADRES NORMATIFS

3.1 CADRES LÉGISLATIFS INTERNATIONAUX

Les discours de haine abordent les enjeux controversés de la dignité, de l'égalité, de la sécurité des individus et de la liberté d'expression. Ce terme n'est pas mentionné explicitement dans de nombreux documents et traités relatifs aux droits de l'homme, mais certains principes portant sur la dignité humaine, l'égalité et la liberté d'expression s'y réfèrent indirectement. Certains discours peuvent être perçus comme remettant directement en cause la dignité des personnes, mais aussi des groupes. Dans certains cas, un discours peut aussi considéré comme une incitation à la discrimination, ce qui enfreint le droit à l'égalité (bien que la relation entre les discours et les actes soit un tout autre sujet). Une autre question est celle du droit à la vie, à la liberté et à la sécurité des individus : il convient de déterminer si certains discours constituent une atteinte à ces droits, comme par exemple les appels à attaquer des personnes appartenant à un groupe particulier.

Tous ces droits sont garantis par la Déclaration universelle des droits de l'homme de 1948. Si l'on réunit tout cela, tout individu a droit à la liberté d'expression, à une protection contre toute violation de sa dignité et de son égalité, à la vie et à la sécurité. En d'autres termes, chacun a le droit d'être protégé contre les discours de haine dans la mesure où ces discours incluent des violations de ses autres droits. Cela suppose de parvenir à un équilibre entre les différents droits, qui préservent autant que possible l'essence de chacun d'eux. Il est donc crucial de définir des processus et des critères qui garantissent cet équilibre. Il est cependant important de garder à l'esprit que la proportionnalité, la nécessité et la légitimité, équilibrées dans le but de combattre les discours de haine, ne doivent pas aller trop loin pour protéger la liberté d'expression.

La Déclaration universelle des droits de l'homme a permis d'établir un cadre et un programme en matière de protection des droits de l'homme, mais elle est non contraignante. Un certain nombre de documents contraignants ont vu le jour par la suite afin d'offrir une protection plus solide à ces mêmes droits. Parmi ceux-là, le Pacte international relatif aux droits civils et politiques est le plus important et le plus complet sur la question des discours de haine et leur réglementation – même s'il n'emploie pas explicitement le terme « discours de haine ». D'autres instruments juridiques internationaux plus adaptés contiennent également des dispositions qui ont des répercussions sur la définition des discours de haine et sur l'identification des moyens de les combattre, notamment la Convention pour la prévention et la répression du crime de génocide (1951), la Convention internationale sur l'élimination de toutes les formes de discrimination raciale (1969) et la Convention sur l'élimination de toutes les formes de discrimination à l'égard des femmes (1981).

Le Pacte international relatif aux droits civils et politiques est l'instrument juridique auquel on se réfère le plus souvent dans les discussions portant sur les discours de haine et leur

réglementation. L'article 19 garantit le droit à la liberté d'expression et inclut également des dispositions générales auxquelles doit se conformer toute restriction de ce droit afin d'être légitime. Toutefois, l'article 20 restreint expressément la liberté d'expression dans les cas d' « appel à la haine nationale, raciale ou religieuse qui constitue une incitation à la discrimination, à l'hostilité ou à la violence ». Conscient des tensions causées par l'article 20, le Comité des droits de l'homme a souligné que l'article 20 était parfaitement compatible avec l'article 19.

Pour aller plus loin, dans le Pacte international relatif aux droits civils et politiques, le droit à la liberté d'expression n'est pas un droit absolu. Il peut être légitimement restreint par les États dans certaines circonstances limitées qui sont « fixées par la loi et qui sont nécessaires au respect des droits ou de la réputation d'autrui » ou « à la sauvegarde de la sécurité nationale, de l'ordre public, de la santé ou de la moralité publiques ». Dans son Observation générale n°34, le Comité des droits de l'homme explique que les restrictions imposées par les États peuvent inclure des propos en ligne selon l'article 19 (3) du Pacte international relatif aux droits civils et politiques. Il ajoute qu'elles « devraient viser un contenu spécifique, les interdictions générales de fonctionnement frappant certains sites et systèmes ne sont pas compatibles avec le paragraphe 3. »

Entre l'article 19 (3) et l'article 20, on remarque une différence entre les restrictions optionnelles ou obligatoires à l'exercice à la liberté d'expression. L'article 19 (3) énonce que l'exercice de la liberté d'expression « peut en conséquence être soumis à certaines restrictions », dans la mesure où elles sont fixées par la loi et nécessaires à certains buts légitimes. L'article 20 stipule, lui, que tout appel à la haine qui constitue une incitation à la discrimination, à l'hostilité ou à la violence « est interdit par la loi ». Malgré les indications sur la gravité des délits d'expression qui devraient être interdits selon l'article 20, le sujet demeure complexe. Il existe notamment une zone grise qui empêche d'établir des distinctions claires entre (i) des propos haineux, (ii) des propos incitant à la haine et (iii) des propos haineux qui constituent tout particulièrement une incitation aux préjudices que sont la discrimination, l'hostilité ou la violence. Ainsi, tandis que les États ont l'obligation d'interdire des propos considérés comme « un appel à la haine qui constitue une incitation à la discrimination, à l'hostilité ou à la violence », conformément à l'article 20 (2), l'interprétation à donner à ce paragraphe n'est pas clairement définie. En conséquence, les restrictions de la liberté d'expression, fondées sur les dispositions du Pacte international relatif aux droits civils et politiques, pourraient donner lieu à des abus. Les Principes de Camden, une série de normes élaborées par l'ONG ARTICLE 19 en concertation avec des spécialistes des droits de l'homme, définissent des critères précis visant à éviter une mauvaise application de l'article 20 (2). L'article 20 doit faire l'objet d'une interprétation étroite afin d'éviter qu'il soit utilisé abusivement.

La Convention internationale sur l'élimination de toutes les formes de discrimination raciale de 1965 a également des incidences sur la conceptualisation des différentes formes de discours de haine, même si ce terme n'y apparaît pas non plus explicitement. Cette Convention et le Pacte international relatif aux droits civils et politiques diffèrent sur trois points. Premièrement, les discours de haine tels que les définit la Convention sont uniquement ceux qui font référence à la race ou l'origine ethnique. Deuxièmement, la Convention impose aux États parties une obligation plus stricte que l'article 20 du

Pacte international relatif aux droits civils et politiques, qui couvre la pénalisation d'idées racistes qui ne sont pas nécessairement une incitation à la discrimination, à l'hostilité ou à la violence. Troisièmement, le concept d'« appel à la haine » contenu dans le Pacte international relatif aux droits civils et politiques est plus précis que les propos discriminatoires décrits dans la Convention internationale sur l'élimination de toutes les formes de discrimination raciale, dans la mesure où ce concept nécessite la prise en compte de l'intention de l'auteur et non l'expression prise isolément. La simple diffusion d'idées fondées sur la supériorité ou la haine raciale, ou même toute incitation à la discrimination ou à la violence raciale, sont passibles de sanctions conformément à la Convention. Tandis que dans le Pacte international relatif aux droits civils et politiques, selon l'article 20 (2), il est nécessaire de prouver l'intention d'inciter à la haine pour que l'infraction soit sanctionnée.

Le Comité pour l'élimination de la discrimination raciale a activement abordé les discours de haine en 2002, dans sa Recommandation générale n° 29, A/57/18, qui recommande aux États parties de prendre des mesures contre la diffusion, « par l'intermédiaire des médias de masse et par Internet », d'idées prônant la supériorité ou l'infériorité liée à la caste ou tentant de justifier la violence, la haine ou la discrimination à l'encontre de communautés fondées sur l'ascendance. Il appelle à prendre des mesures strictes contre toute incitation à la discrimination ou à la violence contre les communautés, y compris par Internet, et pour sensibiliser les professionnels des médias à la nature et aux conséquences de la discrimination fondée sur l'ascendance. Ces points, qui reflètent les références faites à la diffusion de l'expression par la Convention internationale sur l'élimination de toutes les formes de discrimination raciale, revêtent une importance particulière pour Internet, car exprimer des idées dans certains contextes en ligne peut immédiatement revenir à les propager. Ceci concerne également les espaces auparavant privés qui ont commencé à jouer un rôle public, comme par exemple les plates-formes des réseaux sociaux.

Tout comme la Convention internationale sur l'élimination de toutes les formes de discrimination raciale, la Convention pour la prévention et la répression du crime de génocide vise à protéger des groupes définis par la race, la nationalité ou l'origine ethnique, bien qu'elle étende aussi ses dispositions aux groupes religieux. Cependant, en matière de discours de haine, la Convention sur le génocide s'applique uniquement aux actes qui incitent publiquement au génocide, reconnus comme « des actes commis dans l'intention de détruire, ou tout ou en partie, un groupe national, ethnique, racial ou religieux ».

Les discours de haine fondés spécifiquement sur le sexe (contrairement aux actes discriminatoires) ne sont pas traités en profondeur par la législation internationale. La Convention sur l'élimination de toutes les formes de discrimination à l'égard des femmes, entrée en vigueur en 1981, impose aux États l'obligation de condamner la discrimination à l'égard des femmes sous toutes ses formes, et de « prévenir les actes de violence sexiste, d'enquêter sur ces actes et de les sanctionner ». Le Comité des droits de l'homme a également exprimé « sa vive inquiétude face aux actes de violence et de discrimination commis dans toutes les régions du monde contre des individus en raison de leur orientation sexuelle ou de leur identité sexuelle. »

Dans quelle mesure les propos de haine sont-ils liés à de tels actes ? Cette question fait débat. Cependant, dans sa Recommandation générale n°28, le Comité des droits de l'homme invite les États parties à « fournir des renseignements sur les mesures légales prises pour limiter la publication et la diffusion » de matériels pornographiques qui présentent les femmes comme des objets de traitement dégradant.

Pour résumer, le Pacte international relatif aux droits civils et politiques permet les restrictions nécessaires au respect des droits ou de la réputation d'autrui ou à la protection de la sécurité nationale, de l'ordre public, de la santé et de la moralité publiques ; et dans certains contextes cette disposition est susceptible de s'appliquer aux expressions qui pourraient être considérées comme des « discours de haine ». Le Pacte international relatif aux droits civils et politiques prévoit également des restrictions dans les cas d' « appel à la haine nationale, raciale ou religieuse qui constitue une incitation à la discrimination, à l'hostilité ou à la violence ». Il est évident que ces deux dimensions établissent des normes sur les conditions limitant certains discours qui pourraient être catégorisés comme « discours de haine », dans la mesure où ces restrictions sont fixées par la loi et nécessaires. La Convention internationale sur l'élimination de toutes les formes de discrimination raciale établit quant à elle une base normative pour restreindre la diffusion d'idées fondées sur la supériorité raciale (ce qui est aussi une forme de protection du respect du droit à l'égalité).

Pour faire face à la complexité de la situation et aux risques d'un usage abusif des normes internationales pour limiter le discours légitime, les Nations Unies ont récemment cherché à créer des espaces visant à promouvoir une compréhension commune de ce que sont les discours de haine et de la façon dont on doit les combattre, ainsi que l'importance du respect des droits de l'homme en ligne. Dans le même temps, les organes directeurs de l'Assemblée générale des Nations Unies, du Conseil des droits de l'homme des Nations Unies et de l'UNESCO ont définitivement reconnu que les droits de l'homme s'appliquent aussi bien en ligne qu'hors ligne. Ces évolutions conjuguées mettent en place le contexte nécessaire pour lutter contre les discours de haine sur Internet.

L'organisation d'une série de réunions consultatives par le Haut-Commissariat des Nations Unies aux droits de l'homme (HCDH) a été une étape importante de ce processus. Ces réunions ont conduit en 2012 à la rédaction du Plan d'action de Rabat sur l'interdiction de « toute expression de haine nationale, raciale ou religieuse qui constitue une incitation à la discrimination, l'hostilité ou la violence ». Le Plan d'action de Rabat reconnaît que, malgré les obligations pour les États signataires du Pacte international relatif aux droits civils et politiques, de nombreux cadres juridiques ne contiennent pas l'interdiction légale de ce type d'incitation. En outre, certaines lois qui l'interdisent emploient une terminologie qui est en contradiction avec l'article 20 du Pacte international relatif aux droits civils et politiques. Ce Plan propose également un critère préliminaire en six parties visant à identifier les messages haineux en prenant en compte le contexte, le locuteur, l'intention, le contenu, l'étendue du discours et la probabilité selon laquelle le discours peut réellement inciter à causer du tort à autrui. En ce sens, il n'est pas supposé que tous les propos haineux sont susceptibles de se traduire en préjudices réels ou d'en entraîner. En revanche, la méthode proposée permet de repérer les discours qui doivent faire l'objet d'une attention particulière.

Toutefois, dans le cas des discours de haine en ligne, l'accent mis par le Plan d'action de Rabat sur les acteurs au niveau national, et en particulier sur les États, risque de minimiser l'importance des plates-formes privées des réseaux sociaux, qui opèrent à un niveau transnational. Ces acteurs peuvent jouer un rôle crucial dans l'interprétation des discours de haine ainsi que dans l'autorisation ou la limitation de leurs expressions. En outre, le Plan de Rabat n'accorde que peu d'attention au problème de l'incitation à la haine pour des motifs liés au sexe, à l'orientation sexuelle ou à la langue.

La législation internationale permet non seulement aux États de prendre des mesures pour limiter le discours de haine, mais elle inclut aussi certaines dispositions autorisant toute personne à déposer une plainte relative à des discours haineux : le Comité des droits de l'homme reçoit les plaintes individuelles concernant le Pacte international relatif aux droits civils et politiques ; le Comité pour l'élimination de la discrimination raciale reçoit les plaintes concernant la Convention internationale sur l'élimination de toutes les formes de discrimination raciale ; et dans le cas de la Convention sur l'élimination de toutes les formes de discrimination à l'égard des femmes, c'est le Comité pour l'élimination de la discrimination à l'égard des femmes qui est chargé d'examiner les plaintes. Cependant, les personnes ne peuvent déposer plainte que contre un État qui a expressément autorisé ces mécanismes.

Les différents avis sur l'équilibre à maintenir entre la liberté d'expression et les restrictions en matière de propos haineux trouvent leur concrétisation dans les instruments régionaux normatifs relatifs aux droits de l'homme. Ces documents complètent les traités internationaux en reflétant les particularités régionales qui ne sont pas mentionnées dans les traités universels. Ces instruments régionaux peuvent s'avérer particulièrement efficaces pour faire respecter la protection des droits de l'homme, comme par exemple la Cour européenne des droits de l'homme, qui statue sur davantage d'affaires de discours haineux que le Comité des droits de l'homme des Nations Unies. Toutefois, les instruments régionaux relatifs aux droits de l'homme ne doivent pas être en contradiction avec les normes internationales, ni imposer des restrictions plus sévères aux droits fondamentaux. La plupart de ces instruments régionaux ne contiennent pas d'articles consacrés en particulier à l'interdiction des discours de haine, mais, de manière plus générale, ils autorisent les États à limiter la liberté d'expression – les dispositions s'appliquant à certains cas spécifiques. Dans les paragraphes qui suivent, nous examinons dans quelle mesure le droit à la liberté d'expression et ses restrictions sont définis au niveau régional et de quelle façon les documents régionaux complètent les autres textes en vigueur qui permettent la définition et la limitation des discours de haine.

La **Convention américaine relative aux droits de l'homme** décrit les restrictions à la liberté d'expression dans des termes proches de ceux du Pacte international relatif aux droits civils et politiques à l'article 19 (3). La Convention a en outre ajouté une clause de limitation spécifique interdisant la censure préalable ; cependant, afin de mieux protéger les enfants, elle autorise la censure préalable dans le cadre de la « protection morale des enfants et des adolescents ». L'Organisation des États américains a également adopté une autre déclaration sur les principes de la liberté d'expression, qui inclut une clause spécifique prévoyant que « l'assujettissement de l'expression à des conditions prédéterminées, telles la véracité, l'opportunité et l'impartialité, est incompatible avec le droit à la liberté

d'expression reconnu dans les instruments internationaux ». La Cour interaméricaine a déclaré que les mesures préventives étaient incompatibles avec la liberté d'expression et que les États devraient plutôt opter pour « l'imposition ultérieure de sanctions à l'encontre des coupables de ces abus ». La Cour soumet à un test les États qui souhaitent mettre en œuvre des restrictions à la liberté d'expression car ces dernières doivent correspondre aux motifs préalablement établis propres à engager la responsabilité ; être définies par la loi, poursuivre des objectifs légitimes et être « nécessaires pour atteindre les objectifs susmentionnés ». Enfin, le système interaméricain dispose d'un Rapporteur spécial pour la liberté d'expression, dont l'étude approfondie sur les discours de haine a conclu que le système interaméricain des droits de l'homme différait de l'approche des Nations Unies et de celle de l'Europe sur un point essentiel : le système interaméricain ne traite que des discours de haine qui conduisent réellement à la violence, et ce sont uniquement ces types de discours qui peuvent faire l'objet de restrictions.

La **Charte africaine des droits de l'homme et des peuples** adopte une approche différente dans l'article 9 (2), en autorisant des restrictions de certains droits dans la mesure où elles entrent « dans le cadre des lois et règlements ». Ce concept a fait l'objet de critiques et il existe une vaste quantité de documents juridiques sur les clauses dites « de récupération » et leur interprétation. Les remarques portent principalement sur le fait que les pays peuvent manipuler leur propre législation et affaiblir ainsi l'essence même du droit à la liberté d'expression. Il importe toutefois d'ajouter que la Déclaration de principes sur la liberté d'expression en Afrique énonce un niveau d'exigence plus élevé pour les restrictions à la liberté d'expression. Elle affirme que le droit à la liberté d'expression « ne doit pas faire l'objet de restrictions pour des raisons d'ordre public ou de sécurité nationale sauf s'il existe un risque réel de menace contre un intérêt légitime et qu'il y a un lien étroit de causalité entre la menace et l'expression ».

En 1990, l'Organisation de la conférence islamique (renommée depuis Organisation de la coopération islamique – OCI) a adopté la **Déclaration du Caire sur les droits de l'homme en Islam** qui, dans son préambule, énonce que les droits de l'homme doivent être « conformes à la Charria ». Certains estiment que cette clause a des répercussions sur le seuil des restrictions et qu'elle est la raison pour laquelle les États membres de l'OCI ont appelé à la pénalisation de tout discours qui, au-delà des cas de violence imminente, inclut « des actes ou des discours qui dénotent une intolérance ou une haine manifeste ».

La **Charte arabe des droits de l'homme**, adoptée par le Conseil de la Ligue des États arabes en 2004, inclut à l'article 32 des dispositions qui s'appliquent également à la communication sur Internet, garantissant « le droit à 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 ». Le paragraphe 2 stipule : « Ces droits et libertés sont exercés dans le cadre des principes fondamentaux de la société ». Cette position diffère de celle du Comité des droits de l'homme, dans son Observation générale n°22, qui stipule que « les restrictions apportées à la liberté de manifester une religion ou une conviction pour protéger la morale doivent être fondées sur des principes qui ne procèdent pas d'une tradition unique ».

La **Déclaration de l'ASEAN sur les droits de l'homme** inclut le droit à la liberté d'expression à l'article 23. L'article 7 de la Déclaration prévoit des restrictions générales,

affirmant que « le respect des droits de l'homme doit être considéré à la fois sur le plan régional et national, en tenant compte des différents contextes politiques, économiques, législatifs, sociaux, culturels, historiques et religieux ». À cet égard, le Haut-Commissariat aux droits de l'homme a rappelé les dispositions de la Déclaration de Vienne qui affirme que, en dépit des différences, « les États ont le devoir, quels que soient leurs systèmes politiques, économiques et culturels, de promouvoir et de protéger tous les droits de l'homme et les libertés fondamentales ».

Certains textes régionaux sont potentiellement plus restrictifs en matière de liberté d'expression que les normes internationales. Dans d'autres textes régionaux, en revanche, les critères permettant d'évaluer la légitimité des restrictions de la liberté d'expression sont encore plus étroits que dans les normes internationales. La Charte des droits fondamentaux de l'Union européenne, dont l'article 11 proclame le droit à la liberté d'expression, affirme à l'article 54 que la Charte ne doit pas être interprétée comme impliquant « des limitations plus amples celles qui sont prévues par la présente Charte ». La Convention européenne des droits de l'homme implique des critères stricts de nécessité et de proportionnalité pour les restrictions de la liberté d'expression. La Cour européenne des droits de l'homme fait la distinction entre les discours de haine et le droit de tout individu à exprimer librement ses opinions, même si d'autres personnes s'en offusquent.

Le Conseil de l'Europe a publié en 2000 une Recommandation de politique générale portant sur la lutte contre la diffusion de matériels racistes, xénophobes et antisémites par Internet. La Convention du Conseil de l'Europe sur la cybercriminalité, datant de 2001, pose les règles de l'entraide concernant les pouvoirs d'investigation et offre aux pays signataires un mécanisme permettant de traiter les données informatiques qui incluraient les discours de haine transnationaux en ligne. En 2003, le Conseil de l'Europe a ajouté à la Convention sur la cybercriminalité un Protocole additionnel relatif aux discours racistes et xénophobes en ligne, qui impose aux États membres l'obligation d'ériger en infraction pénale les insultes racistes et xénophobes en ligne, fondées sur « la race, la couleur, l'ascendance, l'origine nationale ou ethnique, ou la religion ». Neuf pays en dehors de l'Europe ont désormais signé ou ratifié cette Convention.

Remarque importante pour tout ce qui précède, il est à noter que des documents internationaux récents, tels que l'Observation générale n°34 du Comité des droits de l'homme et le Plan d'action de Rabat, ont mis l'accent sur la réciprocité entre la liberté d'expression et la protection contre les discours de haine. Il est très complexe d'assurer un équilibre entre la liberté d'expression et les restrictions apportées aux discours de haine et cela explique la diversité des conceptions juridiques des propos haineux à travers le monde et les difficultés que pose l'interprétation de la loi dans chaque cas donné. Néanmoins, toute restriction juridique doit toujours être considérée comme adjacente au droit, plus vaste, à la liberté d'expression. Comme l'indique l'Observation générale n°34 « le rapport entre le droit et la restriction, entre la règle et l'exception, ne doit pas être inversé ».

3.2 CADRES POUR LES ACTEURS PRIVÉS

Les instruments juridiques internationaux et régionaux examinés ci-dessus offrent aux *États* un cadre permettant de combattre les discours de haine, conformément à leur devoir de promouvoir et de protéger les droits fondamentaux, qui inclut aussi celui de maintenir un équilibre entre le droit à la liberté d'expression et les droits à la dignité, à l'égalité et à la sécurité des individus. Néanmoins, lorsqu'il s'agit de réprimer les discours de haine *sur Internet*, les États ne sont pas toujours les acteurs les plus efficaces. Les intermédiaires de l'Internet, tels que les plates-formes des réseaux sociaux, les fournisseurs de service Internet ou les moteurs de recherche, stipulent dans leurs conditions générales d'utilisation qu'ils sont susceptibles d'intervenir en permettant, restreignant ou canalisant la création de contenus spécifiques et l'accès à ces contenus. Une grande quantité d'interactions en ligne ont lieu sur les plates-formes des réseaux sociaux qui transcendent les juridictions nationales et qui ont élaboré leurs propres définitions des discours de haine et leurs propres mesures pour les combattre. Lorsqu'un utilisateur enfreint les conditions générales d'utilisation, le contenu de ce qu'il ou elle a posté peut être supprimé de la plate-forme ou bien la visibilité de ses messages peut être restreinte, de façon qu'ils ne soient pas accessibles dans un pays donné.

Les principes dont s'inspirent les conditions générales d'utilisation, ainsi que les mécanismes que chaque entreprise élabore afin d'en garantir la mise en œuvre, ont d'importantes conséquences sur la capacité des internautes à s'exprimer en ligne et sur leur protection contre les discours de haine. La plupart des intermédiaires engagent des négociations avec les gouvernements nationaux, dont l'étendue varie en fonction du type d'intermédiaire, du lieu où se situe le siège de l'entreprise et du régime juridique applicable. Les fournisseurs d'accès à Internet sont les plus directement concernés par la législation nationale parce qu'ils doivent être domiciliés dans un pays donné pour fonctionner. Les moteurs de recherche ont de plus en plus tendance à s'adapter au régime de responsabilité s'appliquant aux intermédiaires en vigueur dans les juridictions de leur siège social et également à celui en vigueur dans les pays auxquels ils fournissent leurs services, en supprimant des liens vers des contenus de manière proactive ou bien à la demande des autorités. Les plates-formes des réseaux sociaux, quant à elles, adoptent des approches variées.

Malgré la diversité du secteur, il est depuis peu évident que tous les intermédiaires de l'Internet gérés par des entreprises privées ont le devoir de respecter les droits de l'homme. Cela est définit dans les Principes directeurs relatifs aux entreprises et aux droits de l'homme, élaborés par le HCDH des Nations Unies en 2011. Ce document met l'accent sur la responsabilité des entreprises dans la défense des droits de l'homme. À cette fin, les intermédiaires de l'Internet, de même que toute autre entreprise, devraient « évaluer les incidences effectives et potentielles sur les droits de l'homme, regrouper les constatations et leur donner une suite, suivre les mesures prises et faire savoir comment sont solutionnées ces incidences. » Les Principes directeurs des Nations Unies indiquent également que, dans les cas où il y a violation des droits de l'homme, les entreprises devraient « prévoir des mesures de réparation ou collaborer à leur mise en œuvre suivant des procédures légitimes ». Dans le cas des intermédiaires d'Internet en rapport avec leur conception des discours de haine, cela signifie qu'ils doivent s'assurer que des mesures

sont mises en place pour identifier les discours de haine et y apporter des réponses adéquates.

Ces principes sont cependant encore trop rarement référencés dans les documents d'orientation politique intermédiaire et trop rarement appliqués dans la pratique quotidienne des entreprises. L'un des obstacles à leur mise en œuvre est le fait qu'une société du secteur privé a le droit de fixer des conditions générales d'utilisation qui peuvent être plus restrictives en matière de liberté d'expression que les restrictions qu'un État est censé autoriser conformément aux normes internationales, telles que le Pacte international relatif aux droits civils et politiques. Cela s'apparente à certains égards à la situation de la presse, où chaque média a le droit d'établir sa propre politique éditoriale, même si les médias sociaux reposent aussi clairement sur le discours des utilisateurs, contrairement aux médias d'information, où le discours provient des personnes employées par la plate-forme elle-même. Autre obstacle : comment les entreprises, dans la mesure où elles se conforment aux normes internationales relatives aux droits de l'homme, décident-elles de maintenir un équilibre entre la liberté d'expression et le respect de la vie privée, de l'égalité ou de la dignité, et qu'elles sont les mesures de réparations existantes ? Enfin, les entreprises ont du mal à prendre des décisions quand les lois nationales ne sont pas conformes aux normes internationales relatives aux droits de l'homme, notamment en matière de restrictions légitimes à la liberté d'expression. La situation est dynamique et continue d'évoluer.

Dans le même temps, on constate une évolution dans la manière dont les intermédiaires de l'Internet ont élaboré des définitions très variées des discours de haine et mis au point des directives tout aussi diverses visant à les réglementer. Certaines entreprises n'utilisent pas le terme « discours de haine », mais disposent d'une liste descriptive de termes connexes. Les conditions générales d'utilisation de Yahoo ! interdisent la diffusion de « tout contenu qui serait illégal, nuisible, menaçant, abusif, harcelant, retors, diffamatoire, vulgaire, obscène, calomnieux, constituant une violation de la vie privée d'un tiers, haineux ou répréhensible sur le plan racial, ethnique ou autre ». De même, Twitter n'interdit pas explicitement les discours de haine, mais avertit ses utilisateurs qu'ils « peuvent être exposés à des Contenus qui pourraient être offensants, blessants, inexacts ou inappropriés, ou, dans certains cas, à des messages mal référencés ou trompeurs ». L'entreprise indique également qu'elle ne pourra être tenue responsable des contenus. Les conditions générales d'utilisation sont complétées par les Règles de Twitter, à l'attention des utilisateurs, et Twitter a réagi aux demandes de suppression des contenus s'apparentant à des discours de haine émanant des gouvernements et des organisations de la société civile.

D'autres entreprises font explicitement référence aux discours de haine. YouTube, par exemple, dans ses conditions d'utilisation, cherche à trouver un équilibre entre le respect de la liberté d'expression et les restrictions de certains types de contenus. Tout en affirmant « encourager la liberté d'expression », YouTube déclare : « Nous n'approuvons pas les contenus incitant à la haine : les contenus qui attaquent ou dénigrent un groupe en raison de son origine ethnique, sa religion, son handicap, son sexe, son âge, son statut d'ancien combattant ou son orientation/identité sexuelle ». Cette définition est donc plus large que celle du Pacte international relatif aux droits civils et politiques, qui interdit

uniquement des discours de haine qui constituent un appel à la haine et une incitation à la discrimination, à l'hostilité ou à la violence. Voilà un cas de figure où une entreprise privée est plus restrictive que la législation internationale et même que certaines lois régionales ou nationales sur les discours de haine.

Facebook, dans ses conditions d'utilisation, interdit tout contenu nuisible, menaçant ou qui risquerait d'inciter à la haine ou à la violence. Dans les Standards de la communauté, il est précisé que : « Facebook supprime tout discours de haine, notamment tout contenu qui s'en prend directement à des personnes en raison de leur race, leur origine ethnique, leur appartenance nationale, leur religion, leur orientation sexuelle, leur sexe, leur identité sexuelle, leur handicap ou leur maladie ». Microsoft a établi des règles spécifiques concernant les discours de haine pour plusieurs de ses applications. Dans le cas des téléphones portables, l'entreprise interdit les applications qui « incluent tout contenu prônant la discrimination, la haine ou la violence, fondées sur des considérations relatives à la race, l'origine ethnique, la nationalité, la langue, le sexe, l'âge, le handicap, la religion, l'orientation sexuelle, le statut d'ancien combattant ou l'appartenance à un quelconque groupe social ». L'entreprise a également fixé un règlement pour les jeux en ligne, qui interdit tout contenu suggérant « des discours haineux, des sujets religieux faisant l'objet de controverses et des événements historiques ou d'actualité délicats ». C'est là un autre exemple d'entreprise privée qui se montre plus restrictive que les législations régionales ou internationales sur les discours de haine. En effet, « les sujets religieux faisant l'objet de controverses et les événements historiques ou d'actualité délicats » ne sont pas nécessairement interdits dans le droit international, ni ne sont considérés automatiquement comme discriminatoires. Néanmoins, afin de promouvoir ce qu'elle considère comme une communauté virtuelle plus sécurisée, l'entreprise Microsoft a choisi d'imposer une réglementation restrictive sur certains des produits qu'elle offre. En revanche, ces conditions d'utilisation peuvent s'avérer plus permissives que les restrictions légales imposées par certaines juridictions locales.

Généralement, seule une petite minorité d'utilisateurs lit les conditions générales d'utilisation et il existe différents niveaux de « qualité » parmi les divers types de règlements. L'analyse des tendances montre que la question n'est pas seulement de savoir comment les intermédiaires de l'Internet définissent les discours de haine, mais aussi comment ils appliquent leurs définitions. On se heurte ici au problème de la responsabilité de ces intermédiaires. Beaucoup d'entre eux soutiennent qu'ils ne génèrent ni ne contrôlent les contenus en ligne, et que par conséquent leur responsabilité devrait être limitée. Cette interprétation leur permet de s'exempter du pré-filtrage ou de la modération des contenus et n'engage leur responsabilité qu'après publication, si des contenus qui enfreignent la loi et/ou leurs conditions d'utilisation leur sont signalés. Il existe dans le monde entier différents régimes de responsabilité qui ont des impacts différents, mais à terme, il n'y aura probablement qu'une juridiction qui pourra ordonner légalement qu'une entreprise limite certains propos sur Internet, même si elle sera difficile à définir en fonction du lieu où se situe le siège de l'entreprise, du lieu de stockage des données et du lieu où elles sont accessibles.

La notion de responsabilité limitée différencie les intermédiaires de l'Internet des médias d'information. Cependant, ce qui fait débat, c'est la mesure dans laquelle les médias

d'information devraient bénéficier d'une responsabilité limitée pour des commentaires générés par les utilisateurs sur leurs sites. Leurs pratiques et leurs conditions générales d'utilisation relatives à la modération des contenus, de même que leurs systèmes d'autorégulation tels que les conseils de presse pourraient en tout cas se révéler importants pour les intermédiaires de l'Internet. Quant aux fournisseurs de services Internet, leur responsabilité devant une juridiction donnée est relativement claire. Tout comme les autres intermédiaires d'Internet, ils peuvent définir leurs propres paramètres lorsqu'ils offrent un service, mais comme ils sont tenus au principe de la territorialité, ils ont tendance à respecter la législation du pays dans lequel ils offrent leur service. Ils sont donc plus réactifs que d'autres intermédiaires aux demandes extérieures de retrait de contenus.

La question est plus complexe dans le cas des plates-formes des réseaux sociaux, dont la portée est internationale. Étant donné le volume énorme de données qu'elles traitent, les plates-formes des réseaux sociaux se fondent principalement sur les notifications d'utilisateurs qui signalent des contenus qu'ils considèrent comme déplacés, choquants ou dangereux. Les plates-formes décident alors, la plupart du temps conformément à leurs conditions d'utilisation, si les contenus signalés doivent être supprimés ou non ou bien si elles doivent prendre d'autres mesures afin de restreindre l'accès à ces contenus ou d'empêcher leurs auteurs d'utiliser les services de la plate-forme. En l'absence d'un pouvoir juridictionnel couvrant plusieurs pays et ayant autorité sur l'entreprise et compte tenu des compétences et de la portée limitées d'une seule juridiction (excepté celle du lieu où est domiciliée la plate-forme), beaucoup d'intermédiaires ont tendance à fonctionner conformément à leurs propres conditions générales d'utilisation à l'échelle mondiale.

Hormis d'anciennes directives divulguées par les employés d'entreprises vers lesquelles les plates-formes de réseaux sociaux externalisaient en partie la réglementation des contenus, on connaît peu de choses sur la façon dont les conditions d'utilisation se traduisent dans la pratique : qu'est-ce qui est conservé, filtré ou supprimé ? Certains ont suggéré que Facebook élaborait un ensemble de normes objectives visant à agir sur des propos qui, selon l'entreprise, risquent de susciter des actes violents. Mais des responsables de l'entreprise ont indiqué que Facebook s'efforçait d'éviter une approche théorique et préférait, autant que possible, tenir compte du contexte.

Il apparaît qu'au fil du temps, certaines entreprises deviennent plus attentives aux réclamations des utilisateurs. Ainsi, en 2012, Facebook a mis en place un système permettant aux utilisateurs qui signalent un contenu jugé inapproprié de suivre leurs réclamations jusqu'à ce que le problème soit réglé. L'entreprise a également fourni aux utilisateurs des outils permettant de « socialiser » la signalisation : les utilisateurs peuvent en effet avertir d'abord l'auteur d'un contenu particulier en privé avant de demander formellement à Facebook de supprimer ce contenu. Ces nouvelles possibilités sont des mesures intéressantes qui viennent s'ajouter aux autres méthodes visant à combattre les propos considérés comme haineux, même si nous manquons encore de preuves attestant de leur efficacité et du degré de satisfaction des utilisateurs à leur égard. Parallèlement, on assiste à de grands débats autour de la légitimité d'acteurs commerciaux à déterminer quels propos sont autorisés, en dépit de leur statut privé et des caractéristiques des activités en ligne. Ce point est détaillé dans la suite de ce rapport.

Pour résumer, nous avons analysé dans ce qui précède l'ensemble des législations internationales et régionales et abordé les tendances émergentes qui font des entreprises transnationales intermédiaires de l'Internet des lieux et des acteurs majeurs de la question des discours de haine sur Internet et de la réglementation sur ce thème. Différentes définitions des discours de haine sont apparues au sein de cette mosaïque disparate que forment les instruments internationaux, eux-mêmes appliqués de diverses manières par les gouvernements et les entreprises privées. Alors que les acteurs impliqués devraient tous chercher à appliquer les normes fixées par les traités universels, la réalité concrète est complexifiée par la relative autonomie des intermédiaires d'Internet et leur rôle essentiel dans les communications en ligne. De plus, les réglementations nationales risquent d'être longues à définir, difficiles à mettre en œuvre et influencées par les décisions politiques. C'est dans ce contexte que la société réagit de plusieurs manières aux discours perçus comme haineux sur Internet.

4. ANALYSE DES RÉACTIONS SOCIALES

Cette analyse cherche à donner un aperçu nuancé des réactions sociales suscitées par des préoccupations sur les discours de haine et la violence. Les sections qui suivent traitent du suivi des contenus, de la mobilisation, de la pression exercée sur les intermédiaires, du renforcement des connaissances des utilisateurs par des campagnes d'initiation aux médias et à la maîtrise de l'information, et de la modération des contenus dans les médias d'information.

4.1 SUIVRE ET ANALYSER LES DISCOURS DE HAINE

Un climat propice aux discours de haine est particulièrement susceptible d'engendrer de la violence dans des situations où les enjeux politiques sont importants, par exemple en période électorale. On s'intéressera, dans cette partie, aux questions d'ordre général que soulèvent les mesures concrètes mises au point pour éviter la prolifération des propos haineux sur Internet en pareilles circonstances. Une initiative se prête bien à des observations d'ordre général : le projet de recherche UMATI, lancé en septembre 2012, avant les élections de mars 2013 au Kenya. Il a suivi le discours en ligne dans le pays en vue d'évaluer la fréquence et la virulence des propos diffamatoires. Ces expériences ont donné aux parties prenantes l'occasion d'analyser quels étaient les problèmes soulevés et les personnes ciblées et de réfléchir collectivement au potentiel de certains propos de conduire à la violence.

En 2007, le Kenya a tenu les élections les plus contestées et les plus violentes depuis son retour au multipartisme en 1991, avec plus de 1 000 morts et 600 000 personnes déplacées. Ce furent les premières élections où les nouvelles technologies de la communication et de l'information ont fait partie intégrante de la course électorale. Les médias sociaux, les courriels et les SMS ont été utilisés à des niveaux sans précédent pour rassembler les sympathisants et diffuser l'information, mais aussi pour faire courir des rumeurs : différents groupes politiques ont laissé entendre que leurs opposants planifiaient des attaques, des assassinats et des expulsions d'individus et de communautés. De faux documents ont été fabriqués et diffusés en ligne pour semer le doute sur les candidats à la présidentielle. Face à la violence, le Kenya a mis en place une Commission nationale pour la cohésion et l'intégration qui a collaboré avec les médias et les forces de l'ordre pour lutter contre les tensions ethniques.

Dans ce contexte, un groupe de chercheurs et d'entrepreneurs s'est réuni en amont de la campagne électorale de 2013 et a lancé le projet UMATI (qui signifie « foule » en Kiswahili) qui vise à suivre les occurrences de propos diffamatoires sur Internet. L'objectif global d'UMATI était de détecter les signes de tensions grandissantes parmi les citoyens kényans afin de montrer des différentes phases du processus électoral et de tirer le signal d'alarme avant l'explosion de la violence. Les élections ont eu lieu en mars 2013 et le

projet a duré neuf mois, entre septembre 2012 et mai 2013. Il a suivi les contenus publiés par les Kényans sur les blogs, forums et journaux en ligne ainsi que sur Facebook et Twitter, en anglais mais aussi dans les principales langues parlées au Kenya. S'appuyant sur la définition du « discours dangereux » élaborée par Susan Benesch, qui le considère comme la sous-catégorie de discours de haine présentant le plus fort potentiel de catalyse de la violence, l'équipe d'UMATI a défini des critères pratiques pour faire le tri parmi les différents propos et évaluer leur potentiel à entraîner la violence. Les chercheurs ont évalué ces questions en fonction de l'influence du locuteur sur la communauté en ligne, du contenu des déclarations et du contexte social et historique dans lequel s'inscrivait le discours. Les propos ont donc pu être classés en trois catégories : propos blessants, discours modérément dangereux et discours dangereux. Le suivi quotidien, le replacement des différents actes de langage dans un contexte global et la prise en compte d'autres variables – notamment les cibles des propos diffamatoires et le lien ou non des actes de langage avec des événements spécifiques – ont permis de suivre l'évolution du discours de haine dans le temps et de comprendre de manière plus nuancée les risques réels et perçus.

Les conclusions du projet UMATI qui étudiait la relation entre le discours et l'occurrence ou l'absence d'actes de violence pendant les élections au Kenya en 2013 montrent plus largement combien il est complexe d'établir un lien entre des propos tenus sur Internet et des actes commis. Contrairement aux élections précédentes, celles de 2013 se sont globalement déroulées dans le calme. Non pas que le discours de haine ait été moins corrosif ou généralisé. Malgré l'absence de point de référence qui permettrait d'effectuer des comparaisons précises, en 2013, le projet UMATI a tout de même repéré des cas graves, retentissants et persistants de propos diffamatoires et d'appels à la violence. Ces propos, néanmoins, ne se sont pas directement traduits par de la violence sur le terrain. Comme l'équipe l'a suggéré, d'autres facteurs ont probablement joué un rôle plus important que les expressions de haine pour expliquer les actes violents ou, en l'occurrence, pacifiques. Les nombreux appels à la paix, émanant de différents secteurs de la société, notamment des médias, groupes religieux et hommes politiques des différents bords de l'échiquier politique, ont créé un climat où les actes de violence étaient durement condamnés.

Le projet UMATI a aussi été l'occasion de comparer la façon dont le public percevait les discours de haine, avec la perception des universitaires et des cercles politiques. En menant une enquête parmi la population kényane, le projet a montré que la majorité des participants considéraient les insultes personnelles, la propagande et les commentaires négatifs sur les politiciens comme un discours de haine. De même, leur notion de discours de haine était plus large que la définition donnée dans la Constitution kényane de 2010, dont l'article 33 interdit « la propagande en faveur de la guerre, l'incitation à la violence, le discours de haine ou l'apologie de la haine qui constitue une incitation au racisme, un dénigrement des autres ou une incitation à leur faire du mal ». Comme Nanjira Sambuli, chef du projet UMATI, l'a expliqué, connaître la notion de discours de haine telle qu'elle est perçue par les Kényans permet non seulement de débattre de la signification de ce discours, mais aussi de l'intégrer à une discussion plus vaste sur la liberté d'expression.

Enfin, le projet a montré comment les différentes plateformes de réseaux sociaux pouvaient constituer divers moyens de diffusion des discours de haine et de lutte contre ceux-ci. Seulement 3 % des propos diffamatoires recensés par le projet UMATI avaient été publiés sur Twitter, contre 90 % sur Facebook. Le rapport final d'UMATI donne des éléments d'explication, en signalant ce qui différencie l'architecture de ces deux sites. Sur Facebook, des groupes et des pages peuvent continuer d'exister tout en étant inactifs, et les utilisateurs peuvent adopter des comportements différents dans des espaces différents. Un utilisateur peut avoir un profil personnel « propre » tout en postant des messages de haine sur des pages ou dans des groupes spécifiques. Sur Twitter, au contraire, toutes les publications d'un utilisateur sont conservées sous un seul répertoire d'information et peuvent être vues par toutes les personnes qui suivent cet utilisateur.

Pour remettre en cause les discours de haine, le projet a montré comment les différentes plateformes permettaient des réponses différentes et plus ou moins efficaces. Souvent, les tweets considérés comme inacceptables étaient dénigrés et leurs auteurs publiquement tournés en ridicule. Dans certains cas, le « contrevenant » était même forcé à revenir sur ses propos à cause de la réaction du public, et/ou de fermer tout bonnement son compte Twitter. Comme le rapport iHub l'a conclu, « l'architecture particulière des fils de conversation sur Twitter facilite [ce type de réaction], étant donné que toutes les publications sont enregistrées sur un seul fil et sont visibles par tous ». L'étude a montré que ce type de réaction était plus rare sur Facebook, l'architecture de la plateforme cloisonnant davantage les conversations et les rendant moins accessibles à un vaste public.

Une telle démarche de suivi et d'analyse des discours de haine extrêmes en ligne pourrait bien devenir une tendance reprise dans d'autres circonstances ailleurs.

4.2 MOBILISER LA SOCIÉTÉ CIVILE

L'expérience du Myanmar offre un exemple de solutions positives que la société civile peut mettre en place pour sensibiliser le public et contrer les voix de la haine. Après l'adoption d'une nouvelle constitution en 2008 et l'organisation d'élections en 2010, le pays s'est lancé sur une nouvelle voie, vers une plus grande ouverture et une meilleure inclusion sociale. Le gouvernement a mené des réformes dans des secteurs clés, notamment les médias, où des espaces de débat se sont développés. En 2013, seulement 1,2 % de la population avait accès à Internet et 12 % à la téléphonie mobile (contre moins de 1 % en 2009). Les deux entreprises qui ont remporté les contrats de développement de l'infrastructure des TIC au Myanmar se sont engagées à atteindre une couverture de plus de 90 % en cinq ans pour le réseau mobile. Dans ce contexte, certaines personnes ont utilisé les médias sociaux pour diffuser des appels à la violence. En 2014, la Rapporteuse spéciale des Nations Unies sur les questions relatives aux minorités a exprimé son inquiétude face à la propagation de la désinformation, du discours de haine et de l'incitation à la violence, à la discrimination et à l'hostilité dans les médias et sur Internet. La tension croissante en ligne est allée de pair avec des cas de violence réelle qui ont fait des centaines de morts et des milliers de déplacés, même s'il serait simpliste

de chercher un lien direct de cause à effet entre le discours en ligne et le passage à l'acte dans la réalité.

Avec l'émergence rapide de nouveaux espaces en ligne, bien qu'ils ne concernent qu'une petite partie de la population, des tensions fortement enracinées ont ressurgi sous une forme nouvelle. Dans la mesure où Facebook est rapidement devenue la plate-forme favorite des citoyens faisant leurs premiers pas en ligne, faire face à l'intolérance et au discours de haine sur Internet est un problème qui prend de l'ampleur. Dans cet environnement, certains individus et groupes ont prôné un usage plus agressif de ce média, surtout ceux qui se sentaient protégés par le sentiment d'agir pour le bien et pour la défense de leur vision de l'intérêt national. Des figures politiques ont aussi utilisé les médias en ligne pour des causes particulières. Sur les médias sociaux, des termes péjoratifs ont été utilisés pour faire référence aux minorités. Face à cette situation complexe, divers acteurs ont commencé à se mobiliser, cherchant à proposer des solutions susceptibles d'éviter la montée de la violence. Facebook a cherché à jouer un rôle plus actif dans la surveillance des utilisations de sa plateforme au Myanmar, en formant des partenariats avec des organisations locales et en faisant traduire en langue birmane les lignes directrices élaborées pour signaler les problèmes. Le ministre de l'Information du Myanmar s'est engagé à prendre des mesures supplémentaires pour lutter contre le discours de haine en ligne et a fait part du souhait de son pays de tisser des liens plus étroits avec les États-Unis en vue de trouver des moyens efficaces de limiter le discours de haine en ligne. Ce sont les solutions créatives trouvées par la société civile locale que nous analysons ci-dessous.

La société civile locale s'est élevée avec vigueur pour condamner ouvertement la propagation des discours de haine, tout en appelant à trouver d'autres recours que la censure. Parmi les solutions les plus innovantes, on citera le *Panzagar*, qui en birman signifie littéralement « discours fleuri » : il s'agit d'une campagne pour s'opposer ouvertement au discours de haine. Le but de l'initiative était d'offrir un joyeux exemple de la façon dont les personnes peuvent interagir, aussi bien en ligne qu'en dehors. Les fleurs sont très symboliques au Myanmar et la campagne a encouragé les utilisateurs de Facebook à actualiser leur profil en présentant une photo d'eux une fleur à la bouche. La campagne a reçu beaucoup d'attention, tant au niveau national qu'international mais, comme l'ont reconnu certains militants, le message véhiculé doit s'implanter parmi ceux qui vivent dans les zones rurales et parmi les moins éduqués. Des coalitions efficaces doivent être formées et les chefs religieux largement respectés doivent être ralliés à la cause. Par ailleurs, il ne suffit pas d'encourager à « le dire avec des fleurs », il faut aussi dénoncer la violence. Les militants sont conscients de la nécessité de clarifier les limites de ce qui peut ou ne peut pas être dit, ainsi que le rôle de l'État dans la résolution de ce problème.

Si des initiatives telles que *Panzagar* ont permis de rassembler différents groupes autour d'une même cause, les groupes de la société civile ne sont pas forcément unanimes quant aux solutions à adopter face au phénomène des discours de haine. Certains sont contre l'adoption de lois qui puniraient plus sévèrement les discours de haine, tandis que d'autres y sont favorables. Afin de poursuivre cette dynamique de transition, les militants estiment qu'il est important que la solution apportée au problème des discours

de haine vienne de la société civile. Les militants locaux se sont concentrés sur des solutions locales, plutôt que d'essayer de mobiliser la société civile dans son ensemble sur ces questions – contrairement à d'autres campagnes en ligne qui ont réussi à attirer l'attention de la communauté internationale sur des problèmes relativement négligés. Des initiatives telles que celle mise en avant par la *Save Darfur Coalition* dans le cadre de la guerre civile au Soudan, ou par l'organisation *Invisible Children* avec la campagne Kony2012 qui dénonçait les atrocités commises par l'Armée de résistance du Seigneur, sont des exemples connus. Comme les observateurs de ces campagnes l'ont souligné, des solutions internationales comme celles-ci peuvent avoir des répercussions négatives sur la capacité à trouver des solutions au niveau local.

Le cas du Myanmar est un exemple de la façon dont les organisations de la société civile peuvent se mobiliser de manière proactive pour créer des coalitions locales capables de répondre aux menaces qui apparaissent. Comme les militants l'ont reconnu, l'équilibre entre les solutions locales, la sensibilisation du public international, la production de résultats intéressants sur le plan local et la nécessité de protéger un fragile processus de transition est difficile à maintenir. Néanmoins, leurs efforts montrent que la mobilisation contre la haine en ligne peut être une arme face aux conflits trouvant des répercussions sur le Web.

Cette expérience, ainsi que les différents éléments mentionnés ci-dessus dans la section 4.2, sont peut-être révélateurs d'une possible tendance émergente largement appliquée dans d'autres pays.

4.3 FAIRE PRESSION SUR LES ENTREPRISES PRIVÉES

Diverses organisations qui ont lutté contre le discours de haine sous d'autres formes, ou qui ont défendu les droits de groupes spécifiques par le passé, se voient jouer un rôle de plus en plus important sur Internet. Ce phénomène est particulièrement frappant dans les pays développés, où la pénétration d'Internet est élevée et où les entreprises privées sont les intermédiaires clés. Le présent chapitre s'intéresse aux campagnes et initiatives menées aux États-Unis, en Australie et au Royaume-Uni, où des problèmes de haine en ligne en lien avec la religion, la race et le sexe sont apparus. Les organisations telles que l'Anti-Defamation League (ADL) et le Women, Action and the Media (WAM!) (États-Unis) ; le Online Hate Prevention Institute (Australie) ; le Sentinel Project (Canada) ; et le TellMAMA – Measuring Anti-Muslim Attacks (Royaume-Uni) se sont de plus en plus investis dans la lutte contre le discours de haine en ligne, en ciblant les intermédiaires Internet pour leur demander d'agir plus fortement contre ce phénomène et en sensibilisant les utilisateurs.

Dans certains cas, les organisations s'emploient principalement à faire directement pression sur les entreprises privées en s'appuyant sur des situations spécifiques et en lançant des négociations. Dans ce cadre, les organisations en question peuvent faire valoir leur point de vue par l'intermédiaire de campagnes en ligne, de plaintes et de blocus organisés, de lettres ouvertes, de pétitions en ligne et d'appels vigoureux à la mobilisation de leurs sympathisants, aussi bien en ligne qu'en dehors. Cependant, ce

sont surtout les organisations qui se font les chefs de file d'une cause spécifique. Un second type d'initiatives mis en avant parmi certaines de ces organisations consiste à recueillir les plaintes d'utilisateurs concernant certains types de contenus. Cette activité semble particulièrement intéressante si on la met en relation avec la procédure adoptée par les intermédiaires Internet pour résoudre les cas de discours de haine. Si certaines entreprises ont commencé à publier des rapports de transparence répertoriant les demandes faites par les gouvernements concernant la publication ou la suppression de données, informations et contenus, elles ne publient pas de telles informations pour les demandes faites par des utilisateurs à titre individuel. Lorsque des particuliers signalent un contenu comme étant inapproprié, ils peuvent être tenus informés de l'état d'avancement du traitement de leur plainte, mais cette procédure reste généralement cachée des autres utilisateurs et des organisations. Cela limite donc la possibilité de mieux comprendre ce que les personnes jugent comme étant des propos blessants, irrespectueux, insultants ou haineux. Diverses initiatives font appel à l'externalisation ouverte (crowdsourcing) pour les demandes de sanctions face à certains types de messages, dont HateBase, qui émane du Sentinel Project et de Mobiocracy ; la plate-forme de signalement des incidents islamophobes mise en place par TellMAMA ; et Fight Against Hate, du Online Hate Prevention Institute. Ces initiatives servent d'outils innovants pour garder la trace des propos diffamatoires sur les réseaux sociaux et de la façon dont ils sont réglementés par les différentes entreprises.

HateBase s'emploie à cartographier les discours de haine déployés dans les messages accessibles publiquement sur les plates-formes des réseaux sociaux, afin d'obtenir une carte géographique des contenus haineux diffusés en ligne. Cela permet à la fois d'avoir une vision globale et un aperçu plus précis des termes spécifiques qui sont utilisés, ainsi que des tendances et des cibles les plus courantes de ces propos diffamatoires. Cette base de données comporte en outre une fonction complémentaire permettant de signaler individuellement des cas de discours de haine en ligne, qui est utilisée pour améliorer la précision et l'ampleur de l'analyse, les utilisateurs vérifiant les exemples signalés et confirmant leur caractère haineux au sein d'une communauté donnée. De même, Fight Against Hate permet de signaler les discours de haine proférés sur différents réseaux sociaux sur une plate-forme unique, ce qui aide aussi les utilisateurs à garder trace du nombre de personnes ayant signalé des contenus haineux, du lieu où ces contenus ont été publiés, du temps qu'il a fallu aux entreprises privées pour réagir et de la modération effective (ou non) de ces contenus. Enfin, TellMAMA, organisation basée au Royaume-Uni, offre une fonction similaire permettant de signaler des cas observés sur différents sites sur une seule plate-forme, bien qu'elle se concentre exclusivement sur les contenus anti-musulmans. Cette plate-forme de signalement facilite aussi la constitution d'un dossier sur les incidents à caractère racial ou religieux pour analyse ultérieure. Les cas signalés sont traités par l'organisation, qui contacte ensuite les victimes et les aide à suivre la procédure appropriée pour porter certains incidents à la connaissance des autorités compétentes chargées de faire appliquer la loi. Les informations enregistrées sont également utilisées pour repérer les tendances relatives aux discours de haine, tenus en ligne et en dehors, à l'égard des musulmans au Royaume-Uni.

Concernant l'importance qu'il y a à générer des données empiriques, le PDG du Online Hate Prevention Institute, Andre Oboler, a indiqué que de telles plates-formes offraient la

possibilité de rendre les demandes visibles aux autres utilisateurs enregistrés, ce qui leur permet de garder trace de la date où un contenu a été signalé pour la première fois, du nombre de personnes qui l'ont signalé et du temps nécessaire en moyenne pour qu'il soit retiré. Par ces moyens, ainsi que d'autres, ces organisations peuvent s'inscrire au sein d'ensembles plus vastes d'acteurs participant à un débat sur la nécessité de trouver un équilibre entre liberté d'expression et respect de la dignité humaine et de l'égalité. L'exemple ci-dessous l'illustre bien ; une page Facebook exprimant de la haine à l'égard des aborigènes d'Australie a fini par être retirée par Facebook même si elle n'enfreignait pas ses conditions d'utilisation, car elle a été jugée insultante par tout un éventail d'acteurs, notamment la société civile et des groupes de pression, des régulateurs et des particuliers.

Ce cas montre comment une vaste controverse au niveau des simples citoyens, au sujet de propos diffamatoires publiés en ligne, peut atteindre les organisations et autorités gouvernementales compétentes et les conduire à participer à leur tour activement au débat en ligne et à faire pression sur les entreprises privées pour résoudre la question. En 2012, une page Facebook ridiculisant les aborigènes d'Australie, intitulée « Aboriginal Memes », a causé un tollé local en ligne qui s'est manifesté par un flot organisé pour signaler le contenu abusif, une vaste couverture médiatique, une campagne sur les réseaux sociaux et une pétition en ligne assortie d'une lettre ouverte exigeant que Facebook supprime le contenu visé. Le terme de meme (mème Internet) fait référence dans ce cas à une forme d'expression visuelle faisant passer des messages courts au moyen d'une série d'images, assorties d'inscriptions intégrées dans le corps de ces images.

Le vaste soutien manifesté sur Internet en faveur de la lutte contre la page Facebook « Aboriginal Meme » a pu être observé à travers différentes plates-formes de réseaux sociaux et d'information, suscitant aussi un intérêt accru parmi les chaînes d'information étrangères. En réponse à l'agitation des médias, Facebook a publié une déclaration officielle, reconnaissant que certains contenus peuvent être « controversés, blessants ou même illégaux ». En réponse à cette déclaration, le Commissaire australien aux droits de l'homme a affirmé qu'il désapprouvait la page controversée, ainsi que l'application par Facebook du premier amendement de la constitution américaine sur une question qui concernait un contrevenant d'origine australienne et des victimes d'origine australienne.

La pétition en ligne a été élaborée pour réagir de plus belle face au refus de Facebook de supprimer le contenu, refus manifesté par l'envoi automatique d'un message standard à plusieurs personnes ayant signalé le contenu abusif. La lettre ouverte accompagnant la pétition expliquait que le contenu était considéré comme insultant en raison d'attaques répétées à l'encontre d'un groupe spécifique, pour motifs racistes et exigeait que Facebook prenne des mesures en retirant les pages concernées et d'autres pages similaires visant les Australiens autochtones. Facebook a temporairement retiré ces pages pour examiner leur contenu. Après discussions avec le Commissaire à la lutte contre la discrimination raciale et le Online Hate Prevention Institute, Facebook est parvenu à la conclusion que le contenu ne contrevenait pas à ses conditions d'utilisation et a autorisé les pages à continuer d'exister, sous réserve que le mot « controversé » soit ajouté à leur titre, de façon à indiquer clairement qu'elles comportaient des contenus controversés.

Une deuxième phase a été déclenchée après qu'un utilisateur de Facebook a commencé à cibler des militants anti-haine en les attaquant personnellement avec des propos diffamatoires dans le cadre de l'affaire de la page Aboriginal Memes. Facebook a réagi en retrouvant et en bannissant les nombreux comptes factices qu'il avait créés, tout en l'autorisant à garder un compte en fonctionnement. Enfin, dans un troisième temps, Facebook a interdit l'accès à la page controversée en Australie après que le Commissaire à la lutte contre la discrimination raciale et l'Autorité australienne des communications et des médias ont publiquement exprimé leurs inquiétudes. La page Facebook bannie reste cependant fonctionnelle et accessible hors d'Australie, et continue de propager les contenus haineux publiés sur d'autres pages accessibles en Australie. Pour essayer d'empêcher certains utilisateurs précis de diffuser davantage les images controversées, ces derniers se sont vu interdire l'utilisation de Facebook pendant 24h.

Dans le cas présenté maintenant, les organisations impliquées se sont saisies d'une controverse en ligne de longue date et ont agi au-delà de leur rôle d'intermédiaires chargés de relayer les plaintes, en faisant elles-mêmes activement et fortement pression sur les entreprises, exigeant une modération plus rigoureuse des contenus, ainsi que des mesures d'autoréglementation supplémentaires et pérennes. En 2013, le groupe Women, Action and the Media (WAM!) et le Everyday Sexism Project, au Royaume-Uni, ont lancé une campagne commune montrant les pages de publicités d'entreprises de renom qui diffusaient des images sexistes. En réponse à cette campagne, Nissan et la compagnie d'assurance Nationwide ont retiré leurs publicités de Facebook. Voyant leur succès, les organisateurs, soutenus par des sympathisants et militants en ligne, ont commencé à adresser des plaintes écrites et des photos de diverses publicités sur des pages propageant des discours de haine à d'autres grandes entreprises comme Dove et American Express sur leurs plateformes des médias sociaux, les exhortant à suivre l'exemple. À l'issue de cette campagne, 15 grandes entreprises ont décidé de retirer leurs publicités de Facebook.

La campagne comportait également une lettre ouverte rédigée par les deux groupes susmentionnés, faisant la liste des pages encourageant le viol et la violence à l'égard des femmes, exigeant que celles-ci soient supprimées et que Facebook révise sa politique de réglementation des contenus. Outre la lettre ouverte, une pétition en ligne sur change.org a recueilli plus de 225 000 signatures et contribué à sensibiliser les internautes. Les participants à la campagne ont décidé d'aller plus loin en organisant une manifestation de grande ampleur devant le lieu de réunion des actionnaires de Facebook, en publiant le nom de toutes les entreprises de renom qui utilisaient la plate-forme à des fins publicitaires, en appelant les personnes à leur envoyer des lettres de plainte et en exhortant ces sociétés à retirer leurs publicités de Facebook. En outre, les militants ont aussi fait appel des journalistes économiques sur leurs pages sur les médias sociaux, leur demandant d'analyser les pertes budgétaires que Facebook pourrait subir compte tenu du nombre croissant d'entreprises qui se retiraient. La campagne en ligne, qui utilisait le hashtag #FBrape, a poussé Facebook à contacter les organisations concernées pour leur demander de mettre en place une coopération. La campagne #FBrape n'a reçu une certaine attention des médias qu'une fois qu'elle a réussi à faire pression sur l'entreprise pour qu'elle se lance dans une lutte active contre les contenus haineux ciblant les femmes.

Il s'agissait d'un coup d'éclat visant des entreprises précises et leurs campagnes de publicité et non pas seulement Facebook directement.

Cependant, dans un premier temps, Facebook n'a pas réellement coopéré, l'entreprise maintenant que les pages recensées dans la lettre ouverte n'enfreignaient pas ses conditions d'utilisation. Néanmoins, peu après le début de la campagne, quand les entreprises ont commencé à se retirer, le contenu diffamatoire a rapidement été retiré. Facebook a alors publié une déclaration officielle sur son site, indiquant son intention d'éclaircir ses conditions d'utilisation et ses politiques de régulation des contenus, et de promouvoir la coopération avec les organisations œuvrant pour la défense de la liberté d'expression tout en évitant que des discours de haine en ligne ne visent des groupes et individus spécifiques. Reconnaissant qu'elle ne parvenait pas à repérer et à retirer efficacement les propos haineux, l'entreprise a fait part de sa volonté de réviser et d'actualiser ses directives en matière de modération des discours de haine, d'offrir à ses modérateurs de contenus une formation de meilleure qualité, et de renforcer sa collaboration avec les organisations concernées afin de faciliter une action commune et rapide en vue de mieux faire barrage aux contenus haineux et aussi d'agir pour que les diffuseurs de ces contenus répondent de leurs actes.

Dans un autre cas en lien avec celui-ci, Twitter a aussi pris position contre le harcèlement des femmes en collaboration avec le WAM!, en lançant un projet pilote conjoint sous la forme d'une plate-forme dont le but était de faire modérer le contenu signalé dans les 24h. L'objectif de ce signalement par les victimes de propos abusifs à l'égard des femmes est double : permettre au WAM! de récolter des données sur les contenus insultants, et particulièrement sur le harcèlement sexiste en ligne, afin d'étudier le phénomène en profondeur ; et aider Twitter à améliorer ses mécanismes de réglementation vis-à-vis de la discrimination et des abus sexistes. Cet outil demande aux femmes de nommer les utilisateurs individuels qui les harcèlent ou les tweets précis qu'elles trouvent insultants, de définir le type de harcèlement dont il s'agit et de répondre à des questions d'ordre général sur le nombre de fois où elles ont été harcelées, sur quelles plates-formes et si le harcèlement en question émanait d'un ou plusieurs utilisateurs. Une fois le signalement effectué, les demandes sont étudiées par le WAM! puis transmises à Twitter pour une enquête plus approfondie et pour modération. Le programme pilote a fonctionné pendant trois semaines, au cours desquelles 700 plaintes auraient été déposées et plus de 100 personnes auraient trouvé de l'aide pour obtenir une réaction plus rapide de la part de Twitter. WAM! prévoit de produire un rapport sur les données recueillies, en vue de parvenir à une meilleure compréhension des discours de haine à l'égard des femmes en ligne.

Il semblerait que la lutte contre les discours perçus comme haineux en ligne commence à préoccuper un certain nombre d'acteurs, des gouvernements aux entreprises privées en passant par les fournisseurs de services Internet, ainsi qu'un nombre croissant d'organisations actives et de victimes. De nombreux particuliers et communautés en ligne luttent également quotidiennement aux côtés des organisations plus formelles contre les contenus diffamatoires sur Internet. Toutefois, cette lutte nécessite une action à grande échelle afin de faire en sorte que les discours de haine en ligne puissent être repérés et supprimés de manière efficace, dans leur contexte et à long terme. Cela suppose de

donner aux utilisateurs les outils pour qu'ils puissent repérer et combattre eux-mêmes les discours de haine de manière autonome sans faire obstacle à l'exercice légitime de la liberté d'expression, créant ainsi des espaces d'expression plus ouverts.

Les intermédiaires de l'Internet, et les plates-formes des réseaux sociaux en particulier, ont fait des progrès dans leurs interventions en cas de discours de haine présumé : ils interagissent consciencieusement avec les utilisateurs qui signalent des contenus et rendent leurs procédures de réglementation plus transparentes. Des responsables de Facebook ont indiqué que l'entreprise s'appuyait sur le travail de plusieurs équipes pour examiner les différents types de contenus dans les différentes langues, afin de traiter les cas signalés le plus rapidement et le plus efficacement possible. En outre, Facebook a lancé un tableau de bord permettant de signaler des contenus, grâce auquel les utilisateurs peuvent suivre la procédure de traitement de leurs demandes. La communication individuelle avec chaque utilisateur est ainsi améliorée. Adoptant des mécanismes similaires pour traiter les discours de haine, Twitter a mis en place un bouton permettant de signaler des contenus en 2013, en réponse à une pétition en ligne lancée par un particulier.

En résumé, on constate que de plus en plus, les intermédiaires de l'Internet travaillent en étroite coopération avec différentes organisations afin d'apporter des solutions rapides et efficaces au discours de haine sur leurs plates-formes. Dans le même temps ils soulignent aussi qu'ils accordent autant d'attention aux plaintes déposées par des particuliers et qu'ils les traitent aussi rigoureusement que les pétitions et autres formes d'actions collectives. Dans une certaine mesure, ces entreprises commencent aussi à publier des rapports afin d'informer les utilisateurs de tout changement dans leurs politiques et paramètres de confidentialité, bien que peu d'entre elles ne fournissent des informations sur le rapport quantitatif entre les contenus signalés par des particuliers et les demandes officielles de transparence faites par des autorités gouvernementales. Les actions des groupes militants, parfois associés à des représentants de l'État jouent un rôle important, tout particulièrement dans les cas où – pour diverses raisons – il est difficile et/ou problématique pour les gouvernements eux-mêmes de traiter le problème.

4.4 COMBATTRE LES DISCOURS DE HAINE SUR INTERNET PAR L'INITIATION AUX MÉDIAS ET À LA MAÎTRISE DE L'INFORMATION

Alors que les chapitres précédents ont surtout abordé les réponses apportées en réaction à la prolifération des discours de haine sur Internet, celui-ci offre un aperçu des tentatives visant à fournir des solutions plus structurelles, à travers l'éducation. Il livre une analyse d'une série d'initiatives les citoyens, en particulier les jeunes, pour qu'ils prennent conscience des enjeux et des réactions possibles face aux discours perçus haineux sur Internet.

L'éducation à la citoyenneté a pour but de préparer les individus à être des citoyens informés et responsables, à travers l'étude des droits, libertés et responsabilités ;

elle a été employée de diverses manières, dans des pays en paix comme dans des sociétés sortant d'un conflit violent. Un de ses principaux objectifs est la sensibilisation aux droits politiques, sociaux et culturels des individus et des groupes, y compris à la liberté d'expression, et aux responsabilités et conséquences sociales qui en découlent. Le lien entre l'éducation à la citoyenneté et le discours de haine est double : il s'agit d'une part d'acquérir les connaissances et les compétences nécessaires pour repérer les discours de haine, et d'autre part de donner aux individus les moyens de contrecarrer les propos haineux. L'un des défis actuels de l'éducation à la citoyenneté est d'adapter ses objectifs et stratégies au monde numérique, en proposant les connaissances et les compétences, non seulement en matière d'argumentation, mais aussi de technologie, dont le citoyen peut avoir besoin pour lutter contre les discours de haine sur Internet. Le nouveau concept de citoyenneté numérique est proposé par certains des organismes : il intègre les objectifs fondamentaux de l'éducation aux médias et à l'information en vue de développer les compétences techniques et l'esprit critique des usagers et des producteurs des médias, en lien avec les questions éthiques et civiques d'ordre plus général.

On citera à cet égard l'éducation à la citoyenneté mondiale (ECM), l'un des axes stratégiques de travail du programme Éducation (2014-2017) de l'UNESCO et l'une des trois priorités de l'Initiative mondiale pour l'éducation avant tout (GEFI) du Secrétaire général de l'ONU. L'éducation à la citoyenneté mondiale vise à doter les apprenants de tous âges de valeurs, connaissances et compétences fondées sur les droits de l'homme, la justice sociale, la diversité, l'égalité des sexes et la sauvegarde de l'environnement et favorisant le respect de ces éléments. L'ECM donne des compétences aux apprenants ainsi que des occasions d'exercer leurs droits et de s'acquitter de leur devoir pour promouvoir un monde et un avenir meilleurs pour tous.

Dans cette perspective plus large, l'UNESCO et bien d'autres organisations, regroupées au sein de l'Alliance mondiale des partenaires de l'éducation aux médias et à l'information, veulent favoriser l'autonomie des utilisateurs. L'éducation aux médias et à l'information est un concept global qui regroupe diverses compétences de base (à la fois en ligne et hors ligne). Il comporte le développement des compétences et aptitudes techniques nécessaires à l'utilisation des technologies numériques, ainsi que les connaissances et capacités nécessaires à la recherche, l'analyse, l'évaluation et l'interprétation de textes spécifiques issus des médias, la création de messages médiatiques et la prise de conscience de l'influence des médias aux plans social et politique. Il est désormais essentiel d'acquérir des compétences multiples et complémentaires pour exercer pleinement ses droits et ses devoirs en matière de communication.

L'apparition des nouvelles technologies et des médias sociaux a joué un rôle important dans cette évolution. Les particuliers ne sont plus de simples consommateurs de messages médiatiques : ils sont aujourd'hui des producteurs, des créateurs et des détenteurs d'informations, ce qui se traduit par de nouveaux modèles de participation qui interagissent avec les modèles traditionnels. Les stratégies d'enseignement évoluent en conséquence ; il ne s'agit plus simplement de favoriser l'esprit critique dans la lecture des messages médiatiques mais aussi d'apprendre à créer de manière autonome du contenu

médiatique. La notion d'éducation aux médias et à l'information continue d'évoluer visiblement, prenant désormais en compte la dynamique d'Internet. Elle commence à intégrer les questions d'identité, d'éthique et de droits dans le cyberespace (voir la Déclaration de Paris sur l'éducation aux médias et à l'information à l'ère numérique).

Certaines de ces connaissance et compétences peuvent être particulièrement importantes lorsqu'il s'agit de repérer les discours de haine sur Internet et d'y répondre. Le présent chapitre analyse une série d'initiatives visant à fournir des informations et des outils pratiques aux utilisateurs d'Internet pour qu'ils deviennent des citoyens numériques actifs. Les projets et organisations concernés sont :

- « No place for hate », projet de l'Anti-Defamation League (ADL), États-Unis ;
- « In other words », projet de la Province de Mantoue et de la Commission européenne ;
- « Faire face à la haine sur Internet », projet d'HabiloMédias, Canada ;
- « Mouvement contre le discours de haine », projet du Département de la jeunesse du Conseil de l'Europe ;
- « Online hate prevention », projet du Online Hate Prevention Institute, Australie

Bien que les initiatives et organisations présentées possèdent des caractéristiques spécifiques et poursuivent des objectifs qui leur sont propres, toutes insistent sur l'importance de l'éducation aux médias et à l'information et des stratégies éducatives comme moyens efficaces de contrecarrer les discours de haine. Elles soulignent qu'une approche axée sur l'éducation représente une solution plus structurelle et plus viable face aux discours de haine, si l'on considère, par comparaison, combien il est complexe de décider de supprimer ou de censurer un contenu en ligne, ou combien il peut être long et coûteux d'intenter des actions en justice si l'on veut obtenir des résultats tangibles. Beaucoup sont d'avis que l'ensemble de compétences relevant de l'éducation aux médias et à l'information peut autonomiser les individus et les doter des connaissances et aptitudes dont ils ont besoin pour répondre aux discours perçus comme haineux de manière plus immédiate. Cela peut être particulièrement important, compte tenu de l'accent que les plates-formes des réseaux sociaux mettent sur le signalement à titre individuel des cas de propos insultants, d'incitations à la haine ou de harcèlement.

Les personnes impliquées dans ces initiatives, cependant, reconnaissent l'importance de pouvoir se référer à un cadre normative et juridique dans leur action. La plupart des initiatives prévoient une éducation aux instruments et procédures juridiques mises en œuvre pour poursuivre les auteurs de discours de haine sur Internet et beaucoup incitent à voir les aspects juridiques et éducatifs comme complémentaires.

L'un des dénominateurs communs des initiatives analysées est l'accent mis sur le développement des facultés de pensée critique et sur un usage des médias sociaux intégrant une réflexion éthique, comme acquis de base de l'éducation aux médias et à l'information pour la lutte contre les discours de haine sur Internet. On part du principe que ces acquis dans le domaine des médias et de l'information peuvent renforcer les capacités individuelles de repérer et de contester les discours de haine en ligne ; de comprendre certains de ses présupposés, partis pris et préjugés ; et encourager l'élaboration d'arguments pour les contrer. Les initiatives présentées ici remplissent aussi

un autre rôle important : elles montrent que le repérage des discours de haine sur Internet n'est pas nécessairement aussi simple qu'il y paraît.

Les initiatives analysées sont destinées à des publics divers concernés et touchés par le discours de haine en ligne. Les organisations participantes étudiées ici concentrent leurs efforts sur les groupes vulnérables et sur ceux susceptibles d'être visés par la haine ou d'être recrutés par des groupes prônant la haine. Les enfants et les jeunes sont l'un des principaux publics visés par ces initiatives. Les parents, les enseignants et la communauté scolaire sont aussi généralement considérés comme un public important, de par leur rôle dans l'exposition des enfants aux contenus haineux et dans la protection des enfants face à ces contenus. Les autres groupes visés sont les groupes susceptibles de façonner le paysage juridique et politique de la lutte contre les discours de haine sur Internet, notamment les décideurs politiques et les ONG, ainsi que ceux qui peuvent avoir une grande influence sur la communauté en ligne en l'exposant à des propos haineux, en particulier les journalistes, blogueurs et militants. Un récapitulatif des différents publics visés par les initiatives analysées est présenté dans le Tableau 1.

Tableau 1 : Publics visés par chaque initiative éducative

	Enfants	Jeunes	Enseig-nants	Parents	Respons-ables politiques	Blogueurs	ONG	Grand public
Anti-Defamation League (ADL)	X	X	X	X	X			
In Other Words					X	X	X	X
Mouvement contre le discours de haine		X				X		X
HabiloMédias	X	X	X	X				
Online Hate Prevention		X				X	X	X

Les objectifs de chaque projet sont étroitement liés aux intérêts et aux besoins du public visé par chaque initiative. Par exemple, HabiloMédias a développé un jeu vidéo en ligne destiné aux enfants de 12 à 14 ans, qui a été conçu pour accroître la capacité des élèves à reconnaître les partis pris, les préjugés et la propagande haineuse. Dans ce jeu vidéo, lorsqu'ils repèrent différents degrés de préjugés et de discrimination, sous forme de blagues, nouvelles ou vidéos, les enfants doivent déterminer en quoi ces messages sont susceptibles d'inciter à la haine, puis développer des stratégies pour faire face au problème, en choisissant soit d'ignorer ces messages, soit d'y réagir frontalement.

L'ADL a focalisé une grande partie de ses efforts de sensibilisation et d'éducation sur les enseignants et les parents, en leur fournissant des informations essentielles sur la façon d'aborder les questions de haine et de violence avec les enfants et d'encourager les jeunes à réagir de la manière la plus appropriée. Le Mouvement contre le discours de

haine a organisé des sessions de formation à l'intention des blogueurs et des militants d'associations pour la jeunesse afin qu'ils puissent partager leurs expériences avec les discours de haine sur Internet et les meilleures pratiques pour lutter contre ces discours. Ces sessions de formation visent à promouvoir une compréhension fondamentale des discours de haine au niveau et à sensibiliser le public sur l'influence que les blogueurs et les militants peuvent avoir pour venir à bout des contenus haineux. En revanche, le projet « In Other Words » a cherché à influencer les décideurs politiques et la société civile pour qu'ils surveillent différents types de médias. Il préconise l'utilisation d'informations exactes dans les représentations des minorités et groupes vulnérables dans les médias, encourageant la société à exercer une surveillance pour éviter la diffusion de stéréotypes, préjugés et autres types de discours discriminatoires.

Malgré les particularités du contenu de chacune de ces initiatives et des publics qu'elles visent, elles poursuivent toutes trois un grand objectif éducatif commun : informer sur les discours de haine, les analyser et y répondre. Ces trois objectifs peuvent être considérés dans un ensemble qui comporte des objectifs progressifs associés à des objectifs spécifiques, chacun mettant l'accent sur différents aspects du problème et proposant des solutions spécifiques pour répondre aux discours de haine en ligne. On en trouvera un résumé dans le Tableau 2.

Tableau 2 : Objectifs et buts éducatifs

Information	Analyse	Action
– Sensibiliser au discours de la haine et à ses conséquences – Faire passer et diffuser les informations – Communiquer sur le cadre juridique pertinent	– Repérer et évaluer le discours de haine – Analyser les causes courantes et les présupposés et préjugés sous-jacents – Reconnaître les partis-pris – Signaler et mettre au jour le discours de haine	– Réagir face au discours de haine – Écrire contre le discours de haine – Changer la narration du discours de haine – Assurer un suivi des médias

Le premier objectif éducatif porte sur la diffusion de l'information sur les discours de haine, notamment par la sensibilisation au phénomène, à ces différentes formes et à ces conséquences possibles. Les initiatives donnent aussi des informations sur les cadres juridiques nationaux, régionaux et internationaux applicables. Elles peuvent prendre diverses formes : les vidéos « No Hate Ninja Project - A Story About Cats, Unicorns and Hate Speech » du Mouvement contre le discours de haine, par exemple ; le tutoriel interactif en ligne « Faire face à la haine sur Internet » d'HabiloMédias ; ou la boîte à outils mise au point dans le cadre du projet « In Other Words ».

Le deuxième objectif éducatif est plus complexe, il porte sur la compréhension et l'analyse du discours de haine sur Internet. Cette analyse comporte des évaluations des différents types de discours de haine sur Internet, qui expriment notamment du racisme, du sexisme et de l'homophobie, et des multiples formes qu'il peut prendre. Un aspect important de l'analyse est l'examen critique du discours de haine, qui permet d'en déterminer les causes courantes et de comprendre quels sont les présupposés et

préjugés qui le sous-tendent. Ce processus analytique permet aux individus de signaler et de mettre au jour le contenu haineux publié sur Internet. Des exemples de projets répondant à cet objectif éducatif sont le forum de discussion « No Hate » et la plate-forme « Reporting hate speech ». Le forum de discussion, géré par le Mouvement contre la haine sur Internet, permet aux jeunes de débattre de ce qui constitue un contenu haineux et de montrer quelques exemples qu'ils ont déjà rencontrés de ce type de discours en ligne. La plate-forme conçue par le Online Hate Prevention Institute permet à des particuliers de signaler et de surveiller le discours de haine sur Internet en mettant au jour ce qu'ils perçoivent comme un contenu offensant, en effectuant un suivi de certains sites Web, forums et groupes, et en examinant les supports incitant à la haine mis au jour par d'autres personnes.

Enfin, le troisième objectif éducatif déterminé dans ces initiatives porte sur la promotion de mesures de lutte contre les propos haineux. Les ressources relevant de cet objectif éducatif visent à promouvoir des actions et réponses concrètes face aux discours de haine sur Internet. Les actions proposées varient en fonction de l'orientation particulière du projet et de l'organisation, selon qu'elle est plus de nature plus ou moins combative ou dans la confrontation ; néanmoins, l'aspect le plus important reste de donner aux particuliers les moyens de répondre aux propos haineux et de lutter activement contre. On citera par exemple les sessions de formation pour blogueurs, journalistes et militants organisées par le Mouvement contre le discours de haine ; les supports pédagogiques et plans d'enseignement mis au point par HabiloMédias ; et les politiques de surveillance des médias proposées par le projet « In Other Words ».

Si certaines organisations et initiatives se concentrent sur le contenu du discours de haine sur Internet, d'autres mettent l'accent sur l'aspect personnel de ce discours, en attirant l'attention sur les victimes ou sur l'incidence générale sur la communauté. Quel que soit leur point de mire, la plupart des projets considèrent le développement de compétences numériques comme un élément essentiel pour prévenir, mettre au jour et combattre les discours de haine sur Internet. Les outils et stratégies analysés montrent toutes sortes d'approches pour développer de telles compétences, des simples modes d'emploi les plus élémentaires aux formations les plus complexes et spécialisées. La vaste gamme de formats étudiée dans le cadre des différentes initiatives permettent d'atteindre et d'attirer des publics très divers.

Cependant, on manque encore d'évaluations objectives et il est difficile de savoir dans quelle mesure ces initiatives réussissent à lutter contre le discours de haine ou à toucher les groupes qui sont les plus susceptibles de se livrer à ce genre de discours sur Internet. Par exemple, même si les initiatives et ressources d'HabiloMédias ont reçu de multiples récompenses et distinctions, rien n'indique clairement qui utilise le plus ces ressources et il est difficile d'évaluer les résultats des programmes. Dans le cas du projet « In Other Words », les résultats escomptés prévoyaient l'élaboration de matériel à diffuser, mais on ne dispose d'aucune information pour savoir comment ce matériel a été utilisé depuis sa publication ou quels publics ont été atteints. Par ailleurs, dans le cas du « Mouvement contre le discours de haine », qui a mis au point différents supports et ressources (vidéos, manuels de formation, outils pédagogiques, et plate-forme en ligne servant à signaler les contenus haineux), aucune instruction claire et publique n'explique comment évaluer

l'incidence ou en rendre compte. Si la plupart de ces initiatives sont louables et ont le potentiel d'offrir de puissants outils de lutte contre les discours de haine au niveau structurel, il faudra disposer de plus d'informations pour comprendre comment les individus intègrent les compétences nouvellement acquises dans leur vie quotidienne et quelle incidence cette intégration a effectivement sur leur activité en ligne. Ce besoin devra être pris en compte à mesure que les réactions aux discours de haine en ligne continueront d'évoluer.

4.5 MODÉRATION DES CONTENUS DANS LES MÉDIAS D'INFORMATION

Mis à part les abus observés dans les journaux à scandale, les reportages sur les discours de haine ne représentent généralement pas une incitation à la discrimination, l'hostilité ou la violence. Ils visent plutôt à informer, dans l'intérêt du public, sur des réalités qui doivent être connues. Cependant, les médias d'information doivent de plus en plus souvent repérer les discours postés par les utilisateurs sur leurs plates-formes en ligne et y réagir. Plusieurs systèmes et pratiques ont été analysés dans deux études : un examen des dérogations juridiques et institutionnelles en Europe du Sud-Est, par l'Institut albanais des médias et le rapport *Modération des commentaires en ligne : meilleures pratiques émergentes*, par l'Association mondiale des journaux et des éditeurs de médias d'information, qui passe en revue les pratiques de 104 médias d'information dans 63 pays. Gérer les flux constants de messages des utilisateurs sans restreindre l'expression légitime est un vrai défi pour les médias d'information. Il met en avant le besoin d'adopter des politiques encadrant la définition que chaque institution donne aux discours de haine, pour déterminer les réponses adaptées qui peuvent être apportées. Cela suppose que chaque organe médiatique mette en place un système de surveillance, ne serait-ce qu'un mécanisme permettant aux lecteurs de signaler les incidents qui sont ensuite examinés par les éditeurs de la plate-forme. Les médias gagneraient à échanger sur les pratiques de surveillance et à débattre des discours de haine en ligne avec les intermédiaires de l'Internet, malgré le statut différents des deux entités. Le Ethical Journalism Network (Réseau du journalisme éthique) a publié un plan en cinq points permettant aux rédactions d'identifier les discours de haine, tant dans la couverture médiatique que dans les commentaires des utilisateurs et d'y répondre en conséquence. On pourrait voir se généraliser (en ligne comme en dehors) une tendance qui consisterait à instrumentaliser le journalisme pour combattre les discours de haine. Néanmoins, il est de notoriété publique que l'un des remèdes aux discours néfastes se trouve dans le respect des normes professionnelles du journalisme et dans la communication au public d'informations crédibles sur l'existence, le statut et l'impact de ces discours dans une société donnée.

5. CONCLUSION ET RECOMMANDATIONS

L'apparition et la diffusion du discours de haine sur Internet sont un phénomène qui ne cesse d'évoluer. On assiste actuellement à l'émergence d'un ensemble de mesures prises pour faire face à un phénomène complexe et encore mal compris, et au développement par les sociétés de réponses sur mesure et coordonnées impliquant tout un éventail d'acteurs. Dans ce contexte, les solutions concrètes doivent être fondées sur une meilleure compréhension de la manière dont les différentes formes d'expression se font jour, interagissent et éventuellement se dissipent sur Internet. L'apparition de chaque solution présentée dans ce chapitre est liée à des circonstances uniques, mais leur analyse et leur diffusion offrent une palette complète de méthodes adaptables à différents contextes par les diverses parties prenantes, pour rendre ces tendances efficaces. Plusieurs points généraux peuvent être signalés concernant les tendances en matière de discours de haine et des réponses à y apporter :

5.1 DÉFINITION ET COMPRÉHENSION

- Il est probable que les institutions internationales se gardent de fournir des définitions trop strictes des discours de haine. Ce principe de précaution semble être partagé par des acteurs importants du secteur privé qui façonnent la communication en ligne. Les plates-formes des réseaux sociaux ont jusqu'à présent évité de proposer des règles et des procédures trop strictes pour déterminer quel type de contenu devait être supprimé. Certaines d'entre elles ont essayé de « mutualiser » le processus de modération, permettant aux utilisateurs de résoudre certaines controverses en échangeant entre eux grâce à la plate-forme. Des nuances sont ainsi possibles et cela évite une approche trop mécanique.

- Des définitions plus étroites ont été proposées et elles pourraient être adoptées plus largement par une variété d'acteurs, afin de donner précisément la priorité au cas les plus graves de discours de haine en ligne, dans un monde où circulent d'immenses quantités d'informations. Les termes de « discours dangereux » et de « discours attisant la peur » ont notamment été définis. Ces concepts offrent des outils pour repérer et décrire des formes particulières de discours de haine, mais aussi éventuellement pour signaler les cas critiques ou les zones de danger où il peut être nécessaire d'apporter des solutions collectives pour éviter la propagation de la violence. C'est également important pour évaluer les liens entre les expressions de haine sur Internet et le véritable dommage causé (hostilité, discrimination, violence, etc.). Les éléments qui caractérisent la communication en ligne, notamment l'anonymat réel ou perçu des utilisateurs et la façon dont un message donné peut atteindre instantanément de larges publics, rendent les choses particulièrement complexes. Nous ne disposons pas encore de recherches systématiques sur les relations entre discours de haine en

ligne et actes violents hors ligne, mais ce besoin pourrait donner lieu à des études dans les années à venir.

- De plus, l'adoption exclusive d'une approche plus restreinte pourrait avoir un revers. L'accent mis sur le potentiel d'un acte de langage de conduire à la violence risque de conduire à une vision étroite se cantonnant à des considérations d'ordre public. Mettre l'accent uniquement sur la violence peut favoriser des solutions qui privilégient l'État (en tant qu'acteur exerçant le contrôle légitime du recours à la violence), au détriment éventuel d'autres acteurs susceptibles de proposer des solutions différentes ou complémentaires. Cependant, d'autres interprétations du discours de haine se concentrent plutôt sur le respect de la dignité humaine au sens large, donnant aux victimes des actes de langage le pouvoir d'exiger le respect et d'être défendues, et les plaçant elles, plutôt que l'État ou un autre acteur, au centre des solutions concrètes. Cette approche n'est pas dénuée de problèmes et de contradictions, car une trop forte mise en avant de la dignité peut conduire à une surenchère de relativisme ou de soutien à des idées particularistes qui ne sont pas en accord avec les droits de l'homme. Cela suggère néanmoins que lorsqu'on s'attaque au discours de haine sur Internet, différentes perspectives devraient être prises en considération et comparées les unes aux autres, pour leur capacité à expliquer ce phénomène et ses liens complexes avec la violence réelle, mais aussi à offrir des solutions qui reflètent une approche plus globale.

- Paradoxalement, la complexité associée à la définition de la notion de discours de haine est aussi l'occasion de développer des interprétations locales communes des différentes normes internationales sur ce sujet. Celui-ci opère comme une sorte de « signifiant vide ». C'est un terme qui peut sembler aller de soi, mais pour lequel les gens donnent généralement des descriptions très diverses lorsqu'on leur pose la question. Cela peut poser problème, par exemple si l'on émet des accusations de messages haineux aux fins de discréditer un propos légitime ou de justifier la censure. Voilà des cas où la critique ou la ridiculisation d'individus, d'opinions ou de croyances peuvent être étiquetés comme discours de haine – même si cela va bien au-delà des paramètres définis par le Pacte international relatif aux droits civils et politiques. Les caractéristiques du terme en tant que signifiant vide, cependant, peuvent aussi offrir des possibilités à différents acteurs de se réunir et de débattre de questions qu'il serait difficile d'aborder autrement. Il est probable que cette tendance à discuter des problématiques soulevées par les discours de haine se généralise, à mesure que le phénomène s'amplifie.

5.2 JURIDICTION

- Les efforts visant à repérer les discours de haine en ligne et à y répondre ont, pour une large part, été portés par les gouvernements. Cependant, on constate actuellement que les intermédiaires de l'Internet, c'est-à-dire les services qui jouent un rôle de médiateur dans la communication en ligne, pèsent de plus en plus lourd dans l'équation, aussi bien en autorisant qu'en limitant certains propos. Beaucoup d'entre eux, en particulier

les moteurs de recherche et les plates-formes des réseaux sociaux, s'étendent sur plusieurs pays et réglementent les interactions des utilisateurs en fonction de leurs propres définitions du discours de haine, qui sont plus ou moins clairement en accord avec la législation internationale sur les droits de l'homme. Ils comptent largement sur l'intervention des utilisateurs pour leur signaler les contenus considérés comme répréhensibles et lorsqu'un cas est porté à leur attention, la réponse par défaut est de se prononcer sur la base de leurs propres conditions d'utilisation. Cependant, les modalités de fonctionnement des intermédiaires d'Internet et la relation de ces dernières avec les règles et règlementations nationales et internationales, les groupes de pressions et les utilisateurs individuels sont en constante évolution.

- Les entreprises privées elles-mêmes, ainsi que de nombreux acteurs de la société civile, semblent particulièrement mal à l'aise lorsque des organismes privés sont mandatés pour agir comme des tribunaux et décider de ce qui doit ou non être proposé en ligne. Un débat est en cours pour déterminer dans quelle mesure ces tribunaux fictifs se distinguent de l'autoréglementation volontaire, par laquelle les entreprises mettent leurs propres voies de recours à disposition des plaignants individuels, même si ces derniers conservent le droit de résoudre un différend particulier en passant par les tribunaux nationaux en cas d'échec. La territorialisation des espaces en ligne sur le plan juridique, cependant, pourrait conduire à une fragmentation progressive d'Internet, avec des États ou groupes d'États qui imposeraient leurs propres règles et détruiraient le potentiel du Web d'échanges par-delà les frontières et de rapprochement entre les populations. On assisterait à un scénario où Internet serait vécu différemment d'un endroit à l'autre, et où la norme de libre circulation des informations serait assujettie à l'exceptionnalisme national ou régional. L'accent ne serait plus mis sur les normes communes, mais sur les différences entre les pays.

- La plupart des intermédiaires d'Internet préfèrent adopter de plus en plus une approche fondée sur l'usage. Facebook, par exemple, a activé une fonction de « social reporting » offrant aux utilisateurs la possibilité d'envoyer un message à une personne publiant des informations qu'ils n'apprécient pas mais qui ne violent pas les conditions d'utilisation de Facebook. Une autre option, qui est cependant loin de se généraliser même si elle est proposée par Facebook, permet à un utilisateur de demander à un autre de retirer un contenu spécifique en passant par l'intermédiaire. Les plates-formes de réseaux sociaux ont parfois modifié ou amélioré les mécanismes de surveillance et de modération de contenus. Cette façon de faire a impliqué divers degré de collaboration avec les gouvernements, mais dans ces cas le caractère informel a pu être mis en avant pour limiter la responsabilité et l'obligation de transparence tant des États que des entreprises privées. Si dans certains cas ce mode de fonctionnement informel est bien adapté au caractère fluide des discours de haine sur Internet, son application au cas par cas et de manière sporadique est un inconvénient. Parfois, la différence peut tenir à la capacité d'un groupe de pression de toucher la corde sensible et non à l'importance ou à la recevabilité d'un cas spécifique de discours perçu comme haineux, ni à sa violation (ou non) des restrictions en matière de liberté d'expression.

- Cette tendance du recours aux intermédiaires pour agir sur les discours de haine va se poursuivre, mais elle sera de plus en plus influencée par les groupes de la société civile (aussi bien nationaux que transnationaux) et par des gouvernements particuliers.

5.3 COMPRÉHENSION

- Le caractère inadmissible des messages de haine donne apparemment de fortes raisons de limiter ceux-ci et de faire taire leurs auteurs en les bannissant d'une plate-forme, voire d'Internet. Ces raisons, bien qu'elles puissent être disproportionnées et qu'elles ne répondent donc pas au critère de nécessité qui définit la légitimité d'une restriction, ont tendance à prendre de l'ampleur après des événements dramatiques. Dans ces moments-là, les autorités peuvent appeler à prendre des mesures fortes pour mettre un frein à la capacité d'Internet de propager la haine et la violence, même si les liens entre violence en ligne et violence réelle sont peut-être ténus. Dans ce contexte, les efforts déployés pour repérer et comprendre le phénomène des discours de haine avec pour objectif non pas simplement de le contrer et de l'éliminer, mais aussi de saisir de quoi il est l'expression, sont particulièrement difficiles. Ils restent néanmoins très importants, même si la tendance est aux réactions hâtives ou disproportionnées. On a montré la nécessité de recherches portant sur l'identité des personnes occupant les espaces extrémistes sur Internet, sur les raisons qui les poussent à dire ce qu'ils disent et sur la façon dont ils interprètent leurs propos, car elles pourraient révéler des conclusions souvent contre-intuitives. De telles études sont encore rares, mais une meilleure compréhension des mécanismes susceptibles de conduire à certains types de langage peut inspirer des solutions innovantes qui ne se fondent pas uniquement sur la répression. Par exemple, y a-t-il des liens entre les inégalités économiques et les discours de haine ? Comment certaines personnes peuvent-elles exploiter avec succès les discours de haine à des fins partisanes et pourquoi nombre de leurs victimes sont-elles la plupart du temps issues de milieux vulnérables ou défavorisés ? Y a-t-il un rapport entre l'accès à l'éducation et les discours de haine ? Les réponses à des questions comme celles-ci peuvent mettre en avant l'utilité de politiques proactives et concrètes pour une plus grande inclusion sociale, à préférer aux mesures réactives ciblant exclusivement le discours de haine, qui n'est qu'un symptôme de maux plus profonds. Cette approche est ostensiblement peu développée.

- On reconnaît maintenant partiellement que les discours de haine sur Internet recouvrent un ensemble très large de phénomènes qui varient en partie selon la plate-forme sur laquelle ils sont exprimés. Il y en effet des différences significatives entre les architectures de ces plates-formes et cela a des répercussions importantes sur la manière dans les discours de haine se propagent et peuvent être contrés. Une compréhension plus précise de la façon dont chaque plateforme peut autoriser ou limiter la production et la diffusion de différents types de messages peut ainsi représenter un facteur très important dans l'élaboration de solutions appropriées.

- Les grandes plates-formes de réseaux sociaux ont principalement adopté une démarche réactive pour gérer les messages de haine signalés par leurs utilisateurs et

déterminer si oui ou non ces messages contrevenaient à leurs conditions d'utilisation. Ces plates-formes pourraient, cependant, jouer un rôle plus proactif. Elles ont accès à des quantités colossales de données qui peuvent être mises en relation, analysées et associées à des événements du monde réel qui permettraient une compréhension plus nuancée des mécanismes qui caractérisent les discours de haine en ligne. De très nombreuses données sont déjà collectées et analysées à des fins commerciales. Des efforts similaires pourraient être faits dans le cadre de la responsabilité sociale des entreprises qui possèdent ces plates-formes, ce qui contribuerait à accumuler des connaissances nouvelles susceptibles d'être partagées avec un large éventail de parties prenantes. La pression exercée par des parties prenantes extérieures pourrait favoriser plus de transparence et un meilleur partage des données.

- Plusieurs initiatives préconisant une meilleure éducation aux médias et à l'information dans divers domaines ont commencé à voir le jour comme solution plus structurelle au problème des discours de haine sur Internet. Compte tenu de l'exposition croissante des jeunes aux médias sociaux, les informations sur la façon de repérer les discours de haine et d'y réagir pourraient prendre une importance croissante. Si certains établissements scolaires ont manifesté leur intérêt pour l'intégration progressive d'une éducation aux médias et à l'information dans leurs programmes, ces initiatives restent éparses et n'atteignent souvent pas les plus vulnérables, celles qui ont le plus besoin d'être mis en garde contre les risques des discours de haine sur Internet comme en dehors et d'apprendre comment les contrer. Il est particulièrement important que ces modules anti-discours de haine soient intégrés dans les pays où le risque de violence généralisée est le plus élevé. Il est aussi nécessaire d'intégrer à ces programmes des modules engageant une réflexion sur l'identité, de façon que les jeunes soient capables de détecter les tentatives de manipulation de leurs émotions en faveur de la haine et qu'ils aient les moyens de faire valoir leur droit individuel d'avoir eux-mêmes le contrôle de ce qu'il sont et de ce qu'ils veulent devenir. Des initiatives anticipées et préventives comme celles-ci devraient aussi être accompagnées de mesures destinées à évaluer leur incidence sur le comportement réel des élèves, en ligne et en dehors, ainsi que sur leur capacité à repérer les messages de haine et à y réagir. Il est essentiel pour la lutte contre les discours de haine que l'éducation aux médias et à l'information soit largement utilisée dans les années à venir, notamment par les autorités pédagogiques nationales.

5.4 RÉSUMÉ

- Il est probable qu'on ne parvienne pas avant un certain temps à un consensus autour d'une définition détaillée et universellement reconnue du discours de haine. On voit apparaître clairement une variété d'engagements dans ce domaine.

- Le problème des discours de haine en ligne nécessite des solutions collectives. Comme l'a montré cette étude, certains aspects spécifiques aux discours de haine en ligne risquent de rendre les réponses impliquant une seule entité ou un nombre réduit

d'acteurs très inefficaces. Le problème des discours de haine en ligne ne pourra pas être résolu par un seul acteur, ni par une solution unique.

- Internet dépasse les frontières et les phénomènes aussi complexes que les discours de haine en ligne ne peuvent pas être traités facilement en s'appuyant exclusivement sur le pouvoir des États. Par exemple, il serait difficile pour la plupart d'entre eux d'identifier et de poursuivre toutes les personnes publiant des messages haineux.

- Comme cela a été proposé par la Rapporteuse spéciale des Nations Unies sur les questions relatives aux minorités, les États pourraient collaborer avec des organisations et participer à des projets pour combattre les discours de haine, y compris sur Internet, notamment en apportant un soutien financier.

- Les intermédiaires de l'Internet, quant à eux, ont tout intérêt à préserver une indépendance relative et une image « propre ». Ils ont cherché à y parvenir en faisant preuve de réactivité face aux pressions exercées par les groupes de la société civile, les particuliers et les gouvernements. Cependant, ces négociations se font jusqu'à présent au cas par cas et elles n'ont pas donné lieu au développement de principes globaux et collectifs conformes à la législation internationale sur les droits de l'homme.

- Certaines des personnes interrogées dans le cadre de cette étude ont suggéré que bon nombre d'utilisateurs semblent être désormais insensibles face aux discours de haine en ligne. Davantage d'initiatives structurelles sont nécessaires pour expliquer non seulement comment certains propos peuvent être signalés, mais aussi pourquoi il est important de créer des espaces communs d'échanges autour de la question des discours de haine. Cette attitude silencieuse ou passive pourrait être améliorée pour encourager à s'éloigner des extrêmes haineux, grâce à des militants s'attaquant aux discours de haine en ligne avec des contre-discours.

IV. PROTÉGER LES SOURCES DES JOURNALISTES À L'ÈRE NUMÉRIQUE[5]

5 Ce chapitre est tiré de Posetti, J. (à venir). *Protéger les sources des journalistes à l'ère numérique*. Paris, UNESCO.

1. INTRODUCTION

À l'échelle internationale, les lois sur la protection des sources risquent de plus en plus de perdre leur efficacité, d'être restreintes ou de faire l'objet de compromis à l'ère numérique. Ce phénomène est une remise en cause directe des droits universels établis en faveur des droits de l'homme à la liberté d'expression et au respect de la vie privée et de leur importance pour la liberté de la presse et le journalisme indépendant. Pour évaluer cette tendance, il faut commencer par mettre au jour les principes et les raisons qui sous-tendent la protection des sources journalistiques.

Les journalistes comptent sur une protection des leurs sources, garantie par la loi et par l'éthique, pour rassembler et révéler des informations dans l'intérêt du public. Dans de tels cas, les sources peuvent exiger la confidentialité pour se protéger d'attaques physiques ou de sanctions économiques ou professionnelles suite à leurs révélations. L'utilisation de sources confidentielles n'est pas contraire à la pratique du journalisme professionnel qui suppose de faire appel à de multiples sources, de vérifier et de corroborer les informations. Cette démarche est d'autant plus importante pour la crédibilité quand des sources de ce type sont utilisées. Cependant, sans elles, de nombreuses enquêtes journalistiques n'auraient sans doute pas été dévoilées. Même les reportages qui consistent à recueillir l'opinion des passants et les présentations de fonds reposent sur la certitude que les journalistes respectent la confidentialité quand cela leur est demandé.

Tous ces éléments expliquent la forte tradition de protection juridique des sources à l'échelle internationale, en reconnaissance de la fonction essentielle des sources confidentielles pour le journalisme de « défense » ou de « responsabilisation ». Ils expliquent aussi pourquoi partout dans le monde les journalistes sont soumis à l'obligation éthique de ne pas révéler l'identité de leurs sources confidentielles. Bien que le professionnalisme journalistique exclut d'encourager ou de cautionner les infractions à la loi, qui peuvent prendre la forme de fuites non autorisées, quand il en résulte des informations d'intérêt public, la pertinence de leur publication doit être évaluée. Ainsi, le respect de la confidentialité est un moyen de ne pas compromettre la circulation d'informations susceptibles de contribuer à la lutte contre la corruption ou les violations des droits de l'homme.

Cependant, dans de nombreux cas, cette confidentialité n'est pas reconnue par la législation et les journalistes peuvent être légalement contraints de révéler leurs sources, sous peine de sanctions, de poursuites ou d'emprisonnement. La protection juridique peut comporter des exceptions, notamment en cas de menaces majeures contre la vie, lorsqu'un journaliste est accusé d'un crime ou qu'il a été témoin d'un crime grave. La limite légale et son interprétation varient d'un pays à l'autre, mais selon le principe généralement adopté la confidentialité est la norme et la divulgation des sources est l'exception.

La protection de la confidentialité des sources est valorisée par la société, car elle est souvent considérée comme un moyen de compenser efficacement les quelques cas dans lesquels des journalistes ont abusé du concept de confidentialité, par exemple en

inventant des sources ou en ne vérifiant pas leurs informations avant la publication. De tels abus finissent toujours par être mis au jour et ils sont fortement condamnés par les organisations professionnelles des journalistes. Ces dernières soulignent que le recours à des sources anonymes doit être réservé à des cas de stricte nécessité, pour éviter à ces sources d'être exposées, dans le cadre d'un travail journalistique d'intérêt public. Par conséquent, les normes relatives à la liberté d'expression valident dans le monde entier le principe de confidentialité. Il protège directement les journalistes, en reconnaissant leur obligation professionnelle de ne pas dévoiler l'identité des sources anonymes et aussi indirectement les sources elles-mêmes, par l'engagement des journalistes. Cependant, ce principe ne fonctionne en pratique que lorsque l'identité de la source ne peut pas être facilement découverte par d'autres moyens et lorsqu'il existe des limitations juridiques à l'utilisation de cette information, dans les cas où l'anonymat n'est plus garanti.

La protection de la confidentialité des sources est justifiée dans les instruments internationaux et régionaux (voir les chapitres 4 et 5 ci-après), en grande partie par la nécessité de garantir la libre circulation des informations et notamment celles fournies par les lanceurs d'alertes. Sans cela, il est probable que les détenteurs d'informations sensibles soient « effrayés » et hésitent à les communiquer. Autre répercussion, si les médias d'information ou les journalistes savent ou soupçonnent qu'ils subiront des pressions pour révéler leurs sources, ils risquent de ne plus autant rechercher ou utiliser les informations reçues sous couvert de confidentialité, ce qui limite la diffusion d'informations d'intérêt public.

L'essor des moyens de communication et de surveillance numérique, parallèlement à une sensibilité accrue aux questions de sécurité dans de nombreux pays, remet en question les protections juridiques traditionnelles des sources journalistiques. À l'époque des technologies analogiques, l'engagement pris par les journalistes de refuser d'identifier leurs sources constituait sans doute une protection importante pour un informateur anonyme. En revanche, à l'ère du journalisme numérique, de la surveillance de masse, de la conservation obligatoire des données et de la divulgation d'information par des intermédiaires, cette protection traditionnelle peut s'effondrer.

Les avancées technologiques, ainsi que les changements de méthode dans la police et les services de renseignement, redéfinissent la notion de respect de la vie privée et la protection des sources journalistiques. Grâce à ces avancées technologiques, les forces de l'ordre et les agences en charge de la sécurité nationale sont passées d'une démarche de détection des crimes déjà commis à une démarche de prévention des menaces. À l'ère numérique, ce n'est pas le crime qu'un journaliste ou une source commettent – ou qu'ils sont soupçonnés d'avoir commis – qui peut justifier qu'ils soient surveillés, mais bien la simple utilisation d'une technologie mobile, d'une boîte e-mail, de réseau sociaux et d'Internet. Les communications des journalistes se retrouvent donc de plus en plus souvent prises dans les filets des forces de l'ordre et les agences de sécurité nationale. Il faut ajouter à cela les cas où les communications de certains journalistes ou de certaines sources font expressément l'objet d'une surveillance ciblée. Un rapport publié en 2014 par le Haut-Commissariat aux droits de l'homme remarque : « l'absence d'une législation nationale et/ou d'une mise en œuvre adéquates, la faiblesse des garanties procédurales et l'inefficacité des contrôles ». Ces manquements revêtent une importance particulière

pour la confidentialité professionnelle des journalistes, y compris en ce qui concerne leurs communications numériques avec leurs sources.

Parallèlement à ces évolutions, on a vu se développer ces dix dernières années de plus en plus de lois restrictives relatives à la lutte contre le terrorisme et à la sécurité nationale, susceptibles de restreindre les mesures de protection légales existantes et notamment les lois concernant la protection des sources. Dans ce cadre, de plus en plus d'informations sont donc « classifiées » et les exceptions qui permettraient qu'elles soient révélées dans l'intérêt du public sont réduites et toute divulgation (y compris, dans certains cas par des journalistes) d'informations classées secrètes est érigée en infraction pénale, sans que soient prévues des exceptions dans l'intérêt du public. Cette tendance sécuritaire, de même que la surveillance de l'activité numérique, peut avoir un effet négatif sur les journalistes et leurs sources et limiter ou refréner le journalisme dans l'intérêt du public, tout particulièrement le journalisme d'investigation qui s'appuie sur des sources confidentielles. Dans cette situation complexe, le droit à la confidentialité évolue à l'ère numérique.

Dans ce contexte où la sécurité est source de préoccupations, on s'interroge sur les acteurs du journalisme susceptibles d'invoquer une protection de leurs sources à l'ère numérique. Ce débat suppose de définir par inclusion les termes « journalisme » et « journaliste », pour répondre à des questions telles que : « Qui peut prétendre être couvert par la loi sur la protection des sources ? » Une autre problématique concerne l'application de ces lois de protection à tous les actes de journalisme, y compris aux démarches et communications numériques avec les sources, et non pas à la publication de contenus fondés sur ces communications.

2. MÉTHODOLOGIE

Ce chapitre rassemble des données quantitatives et des analyses qualitatives du monde entier sur la question de la protection des sources des journalistes à l'ère numérique. Ces recherches ont été menées par la WAN-IFRA, l'Association mondiale des journaux et des éditeurs de médias d'information qui accueille le Forum mondial des éditeurs (WEF), et une version plus complète a été publiée en même temps que le présent rapport.

2.1 STRUCTURATION DE LA RECHERCHE

Les chercheurs ont « transformé en données exploitables » un rapport rédigé en 2007 par David Banisar à la demande de l'ONG Privacy International et intitulé *Réduire les sources au silence : enquête internationale sur la protection des sources journalistiques et les menaces à leur encontre*. Pour cela, ils ont extrait manuellement et par recherche de mots-clés les informations de ce document pour a) identifier chaque pays mentionné dans le rapport, et b) déterminer pour quels pays des recherches complémentaires étaient nécessaires pour renforcer les données existantes, afin que l'étude de 2007 puisse servir de point de référence. Cela a entraîné la création d'une base de données listant chaque pays mentionné dans le rapport de 2007, ainsi que les différents types de protection légale en vigueur dans le monde.

Cette démarche a permis d'identifier 124 territoires dans le rapport de Privacy Intenational, mais la présente étude étant limitée aux États membres de l'UNESCO, nous examinons seulement 121 pays. C'est sur cette sélection de pays (voir Annexe 3) que portent les recherches présentées ici.

2.2 VEILLE DOCUMENTAIRE

Une fois les données initiales définies, chaque pays a été assigné à un chercheur ou un assistant-chercheur, en fonction des compétences linguistiques de l'équipe, pour un exercice de cartographie qualitative appelé veille documentaire. Cet exercice consistait à :

a) préparer une analyse de la documentation existante (en particulier des ouvrages universitaires, des revues et des principaux rapports)

b) consulter les bases de données en ligne des sources juridiques, des organes législatifs et des ONG concernées dans chaque pays.

c) consulter les sites Internet d'information

d) contacter les organisations membres de la WAN-IFRA et ses affiliés pour obtenir leur contribution

e) contacter des sources dans les différents pays

La collecte des données a commencé le 1er août 2014 et a pris fin le 20 juillet 2015.

2.3 ANALYSE DES DONNÉES DE CHAQUE PAYS

Une fois l'étude portant sur chaque pays terminée, nous avons distingué les pays dans lesquels des évolutions ont eu lieu entre 2008 et la première moitié de 2015. En fin de compte, la protection juridique des sources des journalistes a changé dans 84 des 121 pays étudiés (69 %).

2.4 ENQUÊTES

Une série de questions a été mise en ligne pour faire participer les communautés de journalistes, d'universitaires, de juristes, de spécialistes de la liberté d'expression et d'internautes partout dans le monde. Plus précisément, on leur a demandé d'identifier les modifications des systèmes juridiques et réglementaires concernant la protection des sources depuis 2007, de nommer les principaux experts/acteurs à contacter pour de futurs entretiens qualitatifs et de proposer des cas d'étude. Cette enquête a été lancée en octobre 2014 et s'est terminée en janvier 2015.

Les résultats pertinents d'une précédente enquête en ligne, lancée pendant le Forum mondial des éditeurs à Turin (Italie) en juin 2014, ont été synthétisés avec ceux de l'enquête menée dans le cadre de la présente étude commandée par l'UNESCO. Cette première enquête cherchait des preuves de l'impact des révélations d'Edward Snowden au sujet de la surveillance dans les salles de presse à travers le monde, en termes de modification de la formation et de la pratique en matière de protection des sources et des questions de sécurité numérique en général. En outre, les données pertinentes issues de l'étude globale de l'UNESCO sur les questions liées à Internet ont été prises en compte pour répondre à la question : « Dans quelle mesure les lois protègent-elles le journalisme sur interface numérique et les sources des journalistes ? »

En tout, 134 personnes venues de 35 pays – chaque région UNESCO étant représentée – ont répondu à ces différentes enquêtes. On a recherché dans les résultats de ces dernières des preuves de changement dans les cadres juridiques relatifs à la protection des sources et des informations sur les aspects propres au numérique. Ces éléments sont venus compléter les comptes rendus régionaux présentés ci-dessous, pour permettre l'identification d'experts/d'acteurs et l'élaboration d'études thématiques.

2.5 ENTRETIENS QUALITATIFS

Des dizaines d'acteurs clés spécialistes du journalisme, de la législation et de la liberté d'expression ont été identifiés grâce à la veille et aux enquêtes. Finalement, 49 personnes venues de 22 pays ont été retenues, en fonction de leur expertise et afin de garantir un équilibre entre les genres et entre les régions.

2.6 TABLES RONDES

Deux tables rondes sur la recherche se sont déroulées pendant la phase finale de l'étude. La première a eu lieu à Washington, DC, pendant le Forum mondial des éditeurs en juin 2015. La *Foreign Press Association* et le *Frontline Club* de Londres ont organisé conjointement la seconde en juillet 2015. Les contributions des participants à ces deux tables rondes ont été mises à profit pour actualiser et renforcer l'analyse de l'étude.

2.7 ÉTUDE THÉMATIQUE

De nombreuses études de cas potentielles ont été identifiées durant les phases de veille et d'enquête. Trois études thématiques ont été choisies pour une analyse approfondie, afin de garantir la bonne représentation des principales problématiques, ainsi que de la diversité régionale et linguistique. La troisième, un ***modèle d'outil d'évaluation pour les cadres juridiques relatifs à la protection des sources***, est présentée ici. Elle porte sur le développement d'un outil d'évaluation en 11 points, utilisé pour mesurer l'efficacité des cadres juridiques de protection des sources à l'ère numérique en s'appuyant sur des entretiens qualitatifs détaillés avec des experts internationaux.

3. PRINCIPALES CONCLUSIONS ET RECOMMANDATIONS

1. Dans 84 des 121 États membres de l'UNESCO étudiés dans ce rapport (69 %), on a constaté des évolutions quant à la protection des sources journalistiques entre 2007 et la première moitié de 2015, la plupart ayant un impact négatif.
2. La question de la protection des sources est désormais indissociable de celles de la surveillance de masse, de la surveillance ciblée et de la conservation des données, ainsi que des répercussions des lois relatives à la lutte contre le terrorisme/la sécurité nationale, et du rôle des entreprises tierces d'Internet, les « intermédiaires ».
3. Les mesures de protection juridique et réglementaire des sources des journalistes risquent de plus en plus de perdre leur efficacité, d'être restreintes ou de faire l'objet de compromis.
4. Sans un renforcement considérable des protections juridiques et la restriction de la surveillance et de la conservation des données, le journalisme d'investigation, qui s'appuie sur des sources confidentielles, sera très difficile à exercer à l'ère numérique, et dans de nombreux autres cas les journalistes seront confrontés à la réticence des sources potentielles.
5. La transparence et la responsabilité en matière de surveillance à la fois massive et ciblée, mais aussi de conservation des informations, ont une importance cruciale pour que les sources confidentielles puissent continuer à contacter les journalistes.
6. Les États doivent introduire ou mettre à jour des lois sur la protection des sources qui leur sont propres.
7. Il convient de définir les « actes de journalisme », à distinguer du rôle de « journalistes », afin de déterminer qui est susceptible de bénéficier des lois de protection des sources.
8. Pour maximiser leurs bénéfices, les lois sur la protection des sources devraient être renforcées parallèlement aux protections juridiques offertes aux lanceurs d'alertes qui, de fait représentent une grande partie des sources des journalistes.
9. Les lois sur la protection des sources doivent couvrir l'ensemble des processus journalistiques et des communications avec les sources confidentielles – y compris les appels, les communications sur les médias sociaux et les e-mails – ainsi que les contenus publiés à partir des informations de ces sources.
10. De plus en plus, les journalistes adaptent leurs pratiques afin de protéger partiellement leurs sources, mais les menaces qui pèsent sur l'anonymat et de chiffrement des données rendent ces adaptations inefficaces.
11. Ces menaces sur la protection des sources à l'ère numérique représentent un coût financier très significatif (lié aux outils de sécurité numérique, à la formation et au conseil juridique). Elle a également un impact majeur sur la production et la portée du journalisme d'investigation basé sur des sources confidentielles.
12. Il est nécessaire d'éduquer les journalistes et les acteurs de la société civile à la sécurité numérique.
13. Les journalistes et autres professionnels qui ont besoin de sources confidentielles pour informer dans l'intérêt du public devraient peut-être former leurs sources pour qu'elles adoptent des méthodes de contact et de partage d'informations sécurisées.

4. IDENTIFICATION DES THÈMES PRINCIPAUX

Les données rassemblées pour cette recherche ont confirmé l'existence de quatre tendances principales affectant la protection juridique des sources des journalistes à l'ère numérique, qui se chevauchent et se recoupent.

Pour les principaux thèmes propres à l'ère numérique qui se sont dégagés des recherches présentées dans ce chapitre, on observe partout dans le monde ces tendances : 1) les lois concernant la sécurité nationale et la lutte contre le terrorisme qui élargissent le champ des « informations classifiées » et limitent les exceptions accordées aux actes de journalisme, risquent de prendre le dessus sur les lois concernant la protection des sources ; 2) l'utilisation généralisée de la surveillance massive et ciblée des journalistes et de leurs sources affaiblit les cadres juridiques de protection des sources en interceptant les communications des journalistes avant la publication des reportages ; 3) les mesures exigeant des intermédiaires qu'ils conservent de plus en plus longtemps des informations concernant les citoyens représentent un risque supplémentaire pour les communications des journalistes avec des sources confidentielles ; 4) les débats visant à savoir si les acteurs des médias numériques doivent être couverts ou non par les lois sur la protection des sources là où elles existent s'intensifient à travers le monde. Toutes les évolutions régionales concernant le cadre juridique de protection des sources présentées ci-après, qu'il s'agisse de changements législatifs, de jurisprudence, d'incidents ou de révélations, s'articulent autour de ces quatre grands thèmes.

5. CADRES RÉGLEMENTAIRES ET NORMATIFS INTERNATIONAUX

Dans les instruments internationaux cités ci-dessous, la protection des sources est considérée comme un élément nécessaire à la libre circulation des informations, qui est elle-même un aspect essentiel de plusieurs accords internationaux sur les droits de l'homme. Dans ces documents, il est supposé que des « circonstances exceptionnelles » sont requises pour justifier que des journalistes lèvent l'anonymat sur des sources confidentielles. Par conséquent, le besoin de connaître l'identité de la source doit être jugé essentiel et la divulgation de cette information n'est justifiée que dans le cas où elle présente un « intérêt vital ».

5.1 ORGANES DES NATIONS UNIES

5.1.1 Résolutions

2012 : Résolution du Conseil des droits de l'homme (A/HRC/RES/21/12) sur la sécurité des journalistes, adoptée en septembre 2012

2012 : Résolution adoptée par le Conseil des droits de l'homme des Nations Unies (Doc ONU A/HRC/RES/20/8) ° sur la promotion, la protection et l'exercice des droits de l'homme sur Internet qui reconnaît la nécessité du respect équitable des droits des citoyens, quel que soit l'environnement.

La première Résolution souligne « qu'il est indispensable de mieux protéger tous les professionnels des médias et les sources journalistiques ». La seconde affirme que « les droits dont les personnes jouissent hors ligne doivent également être protégés en ligne ». Ce sont des prises de position importantes en faveur de l'extension des mesures existantes de protection des sources pour les méthodes journalistiques analogiques à la sphère numérique.

2013 : Résolution adoptée par l'Assemblée générale des Nations Unies (A/RES/68/163) sur la sécurité des journalistes et la question de l'impunité (2013)

Cette Résolution reconnaît que « […] le journalisme est en perpétuelle évolution car il se nourrit de l'ensemble des contributions des organismes de médias, des particuliers et de diverses organisations qui cherchent, reçoivent et transmettent des informations et des idées de toute nature, sur Internet ou ailleurs, exerçant par là leur liberté d'opinion et d'expression, conformément à l'article 19 du Pacte international relatif aux droits civils et politiques et concourant ainsi à façonner le débat public. » Elle reconnaît également

que les évolutions de la définition donnée au « journalisme » doivent être évoquées lors des débats concernant la portée des mesures de protection des sources et elle insiste sur la valeur du journalisme pour l'intérêt du public. Elle rappelle son approbation du Plan d'action des Nations Unies sur la sécurité des journalistes et la question de l'impunité, qui affirme que des efforts mis en œuvre pour mettre fin aux crimes visant les journalistes devraient s'appliquer non seulement aux journalistes reconnus officiellement mais également aux défenseurs des droits de l'homme, aux professionnels des médias communautaires et aux journalistes citoyens.

En novembre 2013, la 37e session de la conférence générale de l'UNESCO a adopté une Résolution concernant les « Questions relatives à Internet, y compris l'accès à l'information et au savoir, la liberté d'expression, le respect de la vie privée et la dimension éthique de la société de l'information ».

Cette Résolution reconnaît formellement l'importance du journalisme d'investigation pour la société, et le rôle que joue le respect de la vie privée pour garantir sa fonction : « […] le respect de la vie privée est essentiel pour protéger les sources journalistiques, qui permettent à une société de bénéficier du journalisme d'investigation et de renforcer la bonne gouvernance ainsi que l'état de droit, et ce même respect de la vie privée ne doit pas être sujet à des ingérences arbitraires ou illicites ».

Les réponses à une enquête accompagnant l'étude de l'UNESCO sur des questions liées à Internet ont mis en avant l'importance des positions des Nations Unies sur la question de la protection des sources journalistiques. L'étude finalisée, qui a puisé dans les recherches préliminaires découlant de celle-ci, a proposé (parmi tout un ensemble d'options) aux 195 États membres de l'UNESCO de « reconnaître le besoin d'une protection accrue de la confidentialité des sources des journalistes à l'ère numérique. » Cette étude sur les questions liées à Internet et à l'ordre du jour de la Conférence générale 2015 de l'UNESCO.

En décembre 2013, l'Assemblée générale des Nations Unies a adopté une Résolution sur le droit à la vie privée à l'ère du numérique. (A/C.3/68/167)

Cette dernière a été co-écrite par 57 États membres et elle invite tous les États à « […] respecter et à protéger le droit à la vie privée, notamment dans le contexte de la communication numérique. […] à prendre des mesures pour faire cesser les violations de ces droits et à créer des conditions qui permettent de les prévenir, notamment en veillant à ce que la législation nationale applicable soit conforme aux obligations que leur impose le droit international des droits de l'homme. » La Résolution précise que l'assemblée est « profondément préoccupée par l'incidence néfaste que la surveillance ou l'interception des communications, y compris en dehors du territoire national, ainsi que la collecte des données personnelles, notamment à grande échelle, peuvent avoir sur l'exercice et la jouissance des droits de l'homme. »

Elle invite également les États à « revoir leurs procédures, leurs pratiques et leur législation relatives à la surveillance et à l'interception des communications, et à la collecte de données personnelles, notamment à grande échelle, afin de défendre le droit à la vie privée en

veillant à respecter pleinement toutes leurs obligations au regard du droit international » et à « à créer des mécanismes nationaux de contrôle indépendants efficaces qui puissent assurer la transparence de la surveillance et de l'interception des communications et de la collecte de données personnelles qu'ils effectuent, le cas échéant, et veiller à ce qu'ils en répondent, ou à les maintenir en place s'ils existent déjà », en insistant sur la nécessité pour les États de respecter pleinement toutes leurs obligations au regard du droit international des droits de l'homme.

L'Assemblée générale a également prié la Haut-Commissaire des Nations Unies aux droits de l'homme de lui présenter, un rapport sur « la protection et la promotion du droit à la vie privée dans le contexte de la surveillance et de l'interception des communications numériques et de la collecte des données personnelles sur le territoire national et à l'extérieur, y compris à grande échelle ». L'Assemblée générale, tout comme la Résolution adoptée par le conseil des droits de l'homme en 2012 (Doc ONU A/HRC/20/L.13), affirme également que « les droits dont les personnes jouissent hors ligne doivent également être protégés en ligne ». Par son invitation à protéger le droit à la vie privée, notamment dans le contexte de la communication numérique, cette Résolution de l'Assemblée générale des Nations Unies est pertinente pour la question de la protection des sources. En effet, le droit au respect de la vie privée en ligne s'applique également aux journalistes et notamment à leurs interactions avec des sources confidentielles. Les lanceurs d'alertes – qui représentent une bonne partie des sources confidentielles journalistes – sont plus à même de communiquer directement en ligne avec des journalistes qui peuvent faire valoir le respect de leur droit à la vie privée pour protéger leurs communications professionnelles.

2014 : Résolution adoptée par le Conseil des droits de l'homme des Nations Unies (A/HRC/RES/27/5) sur la sécurité des journalistes

Cette Résolution reconnaît « le risque particulier que courent les journalistes d'être la cible d'une surveillance illégale ou arbitraire et/ou de l'interception de leurs communications, en violation de leurs droits au respect de la vie privée et à la liberté d'expression. » Cette constatation fait directement écho aux questions de la protection des sources et de la sécurité des journalistes et de leurs sources.

Décembre 2014 : Résolution de l'Assemblée générale des Nations Unies sur la sécurité des journalistes et la question de l'impunité (A/RES/69/185)

Cette Résolution de l'assemblée générale des Nations Unies fait deux observations, l'une sur le rôle du journalisme qui concourt à façonner le débat public, et l'autre sur « le risque particulier que courent les journalistes d'être la cible d'une surveillance illégale ou arbitraire ou de voir leurs communications interceptées, en violation de leurs droits au respect de la vie privée et à la liberté d'expression. »

5.1.2 Rapports, recommandations, déclarations et observations

Juillet 2011 : Bureau du Pacte international relatif aux droits civils et politiques, Comité des droits de l'homme des Nations Unies, Observation générale n°34

Cette observation reconnaît la liberté d'opinion et d'expression comme « le fondement de toute société libre et démocratique » qui constitue « la base de l'exercice sans réserve d'un grand nombre d'autres droits de l'homme. » Il y est dit que l'existence « d'une presse et d'autres moyens d'information libres, sans censure et sans entraves » est essentielle pour garantir la liberté d'opinion et d'expression. L'Observation recommande la protection de toutes les formes d'expression et de leurs moyens de diffusion, y compris les modes d'expression électroniques et Internet.

2012 : Déclaration de Carthage – Participants à la Conférence de la Journée mondiale de la liberté de la presse organisée par l'UNESCO :

Cette déclaration a souligné les défis que représentent les communications en ligne pour la préservation de la liberté d'expression et des droits à la vie privée, essentiels à la pratique du journalisme d'investigation.

Juin 2013 : Rapport du Rapporteur spécial (Frank La Rue) sur la promotion et la protection du droit à la liberté d'opinion et d'expression, pour le Conseil des droits de l'homme

Dans ce rapport, M. La Rue conclut que : « les États ne peuvent garantir que les individus sont en mesure de rechercher et de recevoir des informations ou de s'exprimer librement sans respecter, protéger et promouvoir leur droit à la vie privée. » Cette déclaration a mis en avant les liens entre la liberté d'expression, l'accès à l'information et le respect de la vie privée qui sous-tend la protection des sources.

En juillet 2013, Navi Pillay, qui était alors Haut-Commissaire des Nations Unies aux droits de l'homme, a mis en lumière le rôle du droit au respect de la vie privée pour la protection des individus qui dévoilent des informations relatives aux droits de l'homme.

En s'appuyant sur le cas d'Edward Snowden, Mme Pillay affirme que les systèmes juridiques nationaux doivent aménager des solutions permettant aux individus qui dénoncent les violations des droits de l'homme d'exprimer leurs inquiétudes sans craindre des représailles. Cela s'applique également aux sources confidentielles car, bien que le respect de la confidentialité par les journalistes ne couvre pas nécessairement l'acte de divulgation en lui-même, la peur des représailles influe sur la confiance qu'accorde une source à un journaliste lorsque ce dernier s'engage à respecter la confidentialité. Ainsi, plus la peur des représailles est grande, plus l'effet dissuasif est grand.

Mme Pillay a déclaré que les droits au respect de la vie privée, à l'accès à l'information et à la liberté d'expression étaient étroitement liés. Elle a aussi explicitement mis en avant le besoin pour les individus « de pouvoir être sûrs que leurs communications privées ne sont pas indûment examinées par l'État. » Faute de quoi, les sources pourraient être dissuadées, ce qui, par conséquent, entraînerait un « gel » des informations. C'est là une autre perspective pertinente pour la question de la confidentialité des sources des journalistes.

Rapport de 2013 (A/HRC/23/40) du Rapporteur spécial des Nations Unies sur la promotion et la protection du droit à la liberté d'opinion et d'expression, Franck La Rue :

Ce rapport remarque que : « Les journalistes doivent pouvoir compter sur la confidentialité, la sécurité et l'anonymat de leurs communications. Un environnement dans lequel la surveillance est généralisée, sans être limitée par le respect de procédures ou par un contrôle judiciaire, ne peut pas garantir le respect de la protection des sources. » Cette déclaration de M. La Rue met en avant l'impact que la surveillance peut avoir sur le journalisme, en particulier celui qui dépend de sources confidentielles.

En février 2014, les Nations Unies ont accueilli un séminaire rassemblant des experts sur le thème du droit au respect de la vie privée à l'ère numérique (Genève).

Durant cet événement, le Rapporteur, M. La Rue, a appelé de ses vœux un mandat spécial des Nations Unies pour la protection du droit au respect de la vie privée, en ajoutant : « Le respect de la vie privée et la liberté d'expression sont non seulement liés, il facilite également la participation citoyenne, le droit à une presse libre, l'exercice de la liberté d'opinion, le rassemblement des individus, l'exercice de la liberté d'association et la capacité à critiquer les politiques publiques. »

Juillet 2014 – Résumé de la réunion-débat du Conseil des droits de l'homme sur la question de la sécurité des journalistes : Rapport du HCDH

Le résumé indique que : « La question de savoir si le cadre juridique en place était suffisant pour garantir la sécurité et la protection des journalistes et des professionnels des médias a été évoquée à plusieurs reprises au cours du débat. Il ne s'agissait pas seulement de la protection physique contre les menaces et la violence, mais aussi de la protection contre les ingérences, notamment judiciaires et administratives. » En outre, il y est remarqué que l'avènement de nouvelles formes de journalisme (notamment sur les réseaux sociaux et la blogosphère) avait « accru la vulnérabilité des médias et donné lieu à des ingérences illégales dans la vie privée et les activités des journalistes. Pareilles ingérences devaient être condamnées et l'indépendance des médias, traditionnels ou numériques, devait être favorisée. »

Selon ce résumé, M. La Rue a déclaré que la confidentialité et l'anonymat des journalistes étaient également des éléments fondamentaux de la liberté de la presse. Les intervenants ont également noté que « les blogueurs, les journalistes en ligne et les journalistes

citoyens jouaient un rôle important dans la protection des droits de l'homme [et] ont aussi indiqué que la protection des journalistes devait couvrir tous les nouveaux journalistes, professionnels ou non. » C'est une affirmation pertinente pour répondre à la question de l'application d'une protection juridique aux sources des journalistes. Enfin, la réunion a conclu que les lois relatives à la sécurité nationale et à la lutte contre le terrorisme ne devraient pas être utilisées pour faire taire les journalistes.

Tous ces éléments éclairent les discussions sur le droit des journalistes à recevoir et à transmettre des informations obtenues par des sources confidentielles dans l'intérêt du public, sans ingérence.

Rapport 2014 de l'UNESCO sur les Tendances mondiales en matière de liberté d'expression et de développement des médias.

La menace que représente la surveillance pour le journalisme est soulignée dans ce rapport mondial, qui met en lumière le rôle de lois relatives à la sécurité nationale, à la lutte contre le terrorisme et à la lutte contre l'extrémisme, parfois utilisées comme instruments pour « restreindre le débat légitime et empêcher l'expression d'opinions divergentes dans les médias tout ou justifiant une intensification de la surveillance, évolution que l'on peut considérer comme contraire au droit à la vie privée et préjudiciable à la liberté d'expression. » Le rapport indique plus loin que : « Dans beaucoup de pays, les organismes chargés de la sécurité nationale ont désormais accès aux documents des journalistes, à leur boîte mail et à leurs conversations téléphoniques, ainsi qu'à une immense collection de données qui pourraient leur permettre de surveiller les journalistes, leurs sources et les lanceurs d'alertes. »

Juillet 2014 : « Le droit à la vie privée à l'ère du numérique : Rapport du Haut-Commissariat des Nations Unies aux droits de l'homme

L'Assemblée générale des Nations Unies a commandé ce rapport sur la protection et la promotion du droit à la vie privée dans le contexte de la surveillance et de l'interception des communications numériques et de la collecte des données personnelles sur le territoire national et à l'extérieur, y compris à grande échelle. Ce dernier a conclu qu'à l'ère du numérique, les technologies des communications ont aussi renforcé les moyens dont disposent « les pouvoirs publics, les entreprises et les particuliers pour surveiller, intercepter et collecter les données. »

Le rapport fait également état d'un risque que les données massives permettent de ré-identifier les données apparemment « anonymes ». La question de la collecte des métadonnées (c'est-à-dire des données qui indiquent des comportements réguliers, par exemple le nombre et la durée des appels entre deux individus plutôt que leur contenu) est aussi très pertinente pour la protection des sources. L'effet dissuasif sur les sources potentielles, compte tenu du risque de profilage et de mise en danger que posent la conservation des données et l'analyse des données massives, en est davantage accru.

Le rapport affirme par ailleurs qu'il « incombe à la puissance publique de démontrer que l'immixtion est à la fois nécessaire et proportionnée au risque spécifique à traiter. Les

programmes de surveillance de masse ou à grande échelle peuvent donc être jugés arbitraires, même s'ils servent un objectif légitime et ont été adoptés sur la base d'un régime juridique accessible. » Il conclut que les institutions publiques s'en remettent de plus en plus aux acteurs du secteur privé pour conserver les données (souvent dans le cadre de la législation sur la conservation obligatoire des données, qui est une caractéristique récurrente des programmes de surveillance) « au cas où ». Il ajoute que de telles mesures ne sont ni « nécessaires » ni « proportionnées ».

Citant une décision de la Cour européenne des droits de l'homme, le rapport affirme qu'il est de la responsabilité de l'État de veiller à ce que toute immixtion dans la vie privée, la famille, le domicile ou la correspondance soit autorisée par des textes législatifs « suffisamment précis ». Il constate que les États partagent leurs renseignements et outrepassent les limites s'appliquant à la surveillance de leurs propres citoyens. Cela a des répercussions évidentes sur le travail des journalistes, en particulier pour les correspondants étrangers et les journalistes menant des enquêtes internationales.

Le rôle des intermédiaires est également mentionné dans ce rapport. Il s'agit d'un nouvel aspect important, pertinent pour la question de la protection des sources des journalistes. En effet, ces intermédiaires qui peuvent avoir accès aux communications numériques « privées » des journalistes avec des sources confidentielles (tels que les moteurs de recherche, les fournisseurs Internet, les opérateurs de télécommunications et les réseaux sociaux) sont soumis à des pressions croissantes pour remettre ces données aux pouvoirs publics ou des entreprises, que ce soit dans le cadre de procédures judiciaires ou de démarches extrajudiciaires. Ce phénomène est de plus en plus officialisé : dès lors que la fourniture de services de télécommunications passe du secteur public au secteur privé, on observe, selon le rapport, une « délégation de la force publique et des responsabilités quasi judiciaires aux intermédiaires Internet […] La promulgation de prescriptions légales faisant obligation aux entreprises d'adapter leurs réseaux en vue d'éventuelles écoutes téléphoniques est un sujet de réelle préoccupation, du fait en particulier qu'elle créée un cadre favorable aux mesures de surveillance à grande échelle. » Le rapport note que « sur tous les continents, les autorités publiques utilisent à la fois des mécanismes juridiques formels et des méthodes secrètes pour accéder à des contenus et à des métadonnées. »

Novembre 2014 : Décision du Conseil du Programme international pour le développement de la communication (PIDC) de l'UNESCO

En 2014, le Conseil du PIDC, qui rassemble 39 États membres, a favorablement accueilli le Rapport biennal de la Directrice générale sur la sécurité des journalistes et la question de l'impunité, dans lequel le terme « journalistes » désigne l'ensemble des« journalistes, des professionnels des médias et des producteurs de médias sociaux qui sont à l'origine d'un important travail de journalisme dans l'intérêt du public. » Le Conseil a en outre réaffirmé l'importance de la condamnation « des assassinats de journalistes, de professionnels des médias et de producteurs de médias sociaux à l'origine d'un travail de journalisme et qui sont assassinés ou pris pour cible dans l'exercice de leur profession. »

Mai 2015 : Rapport du Haut-Commissariat pour les droits de l'homme sur le chiffrement, l'anonymat et le cadre normatif relatifs aux droits de l'homme, par le Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, David Kaye

Dans ce rapport, le nouveau Rapporteur spécial a mis l'accent sur les rôles essentiels joués par le chiffrement et l'anonymat. D'après M. Kaye, ces deux moyens de défense – utilisés séparément ou conjointement – instaurent un espace de confidentialité qui sert à mettre les opinions à l'abri de la curiosité extérieure. Il remarque que le chiffrement et l'anonymat revêtent une importance particulière dans les environnements hostiles.

Il souligne également leur importance pour les journalistes, les chercheurs, les juristes et les membres de la société civile qui souhaitent protéger leurs sources et les communications qu'ils entretiennent avec ces dernières. Il indique que les personnes qui tentent de rechercher, de recevoir et de répandre des informations et des idées peuvent être contraintes d'avoir recours à l'anonymat et au chiffrement, en particulier dans les environnements où la censure est une pratique courante. Une autre question pertinente abordée par M. Kaye est celle de la tendance qu'ont certains États à lutter contre les outils permettant l'anonymat, tels que le réseau Tor, les serveurs proxy ou les VPN, en y interdisant l'accès. Il est évident que pareilles mesures peuvent remettre en cause les tentatives de protection des sources confidentielles des journalistes dans le contexte des communications numériques.

M. Kaye reconnaît par ailleurs que de nombreux États jugent licite de préserver l'anonymat des sources journalistiques. Cependant, il signale que : « Les États enfreignent souvent l'anonymat des sources dans la pratique, même lorsqu'il est prévu par la loi. », et met en avant les pressions exercées sur les journalistes, qui vont à l'encontre dispositions juridiques, directement ou progressivement. Autres points relevés par le Rapporteur spécial, la pratique de plus en plus courante qui consiste à rendre obligatoire l'enregistrement des cartes SIM et son impact sur les communications confidentielles, notamment entre les journalistes et leurs sources. Il déclare que plus de 50 pays d'Afrique imposent (ou sont en passe d'imposer) l'enregistrement des cartes SIM, ce qui suppose de fournir des données identifiables, et que « de telles politiques nuisent directement à l'anonymat [...] et peuvent donner aux gouvernements la capacité de surveiller les personnes et les journalistes bien au-delà de tout intérêt légitime qu'il pourrait faire valoir. » M. Kaye conclut que les États devraient favoriser et promouvoir le renforcement de l'anonymat et du chiffrement et il recommande spécifiquement de renforcer les dispositions juridiques et réglementaires permettant aux défenseurs des droits de l'homme et aux journalistes de sécuriser leurs communications.

6. INSTRUMENTS LÉGISLATIFS RÉGIONAUX ET CADRES NORMATIFS RELATIFS AUX DROITS DE L'HOMME

6.1 INSTITUTIONS EUROPÉENNES

Au niveau régional, les organisations et les pouvoirs législatifs européens font des efforts significatifs pour identifier et limiter les risques qui pèsent sur la protection des sources dans l'environnement numérique.

6.1.1 Résolutions, déclarations, observations, commentaires, recommandations, rapports et lignes directrices du Conseil de l'Europe

Septembre 2007 : Lignes directrices adoptées par le Comité des Ministres du Conseil de l'Europe sur la protection de la liberté d'expression et d'information en temps de crise.

Ces lignes directrices recommandent que les États membres du Conseil de l'Europe adoptent la Recommandation N °R (2000) 7 sur le droit des journalistes de ne pas révéler leurs sources d'information, dans le droit et dans la pratique.

Les principes suivants sont énoncés dans l'Annexe à la Recommandation n° R (2000) 7 :

- ***Principe 1 (Droit de non-divulgation des journalistes)***

Le droit et la pratique internes des États membres devraient prévoir une protection explicite et claire du droit des journalistes de ne pas divulguer les informations identifiant une source [...]

- ***Principe 2 (Droit de non-divulgation d'autres personnes)***

Les autres personnes qui, à travers leurs relations professionnelles avec les journalistes, prennent connaissance d'informations identifiant une source à travers la collecte, le traitement éditorial ou la publication de cette information, devraient bénéficier de la même protection en application des présents principes.

- ***Principe 3 (Limites au droit de non-divulgation)***

a) *Le droit des journalistes de ne pas divulguer les informations identifiant une source ne doit faire l'objet d'autres restrictions que celles mentionnées à l'article 10, paragraphe 2 de la Convention. [...]*

b) La divulgation des informations identifiant une source ne devrait être jugée nécessaire que s'il peut être établi de manière convaincante :

i. que des mesures raisonnables alternatives à la divulgation n'existent pas ou ont été épuisées par les personnes ou les autorités publiques qui cherchent à obtenir la divulgation, et

ii. que l'intérêt légitime à la divulgation l'emporte clairement sur l'intérêt public à la non-divulgation, en conservant à l'esprit que :

- *un impératif prépondérant quant à la nécessité de la divulgation est prouvé ;*
- *les circonstances présentent un caractère suffisamment vital et grave ;*
- *la nécessité de la divulgation est considérée comme répondant à un besoin social impérieux, et*
- *les États membres jouissent d'une certaine marge d'appréciation pour juger de cette nécessité, mais cette marge est sujette au contrôle de la Cour européenne des Droits de l'Homme.*

c) Les exigences précitées devraient s'appliquer à tous les stades de toute procédure où le droit à la non-divulgation peut être invoqué.

- ***Principe 4 (Preuves alternatives aux sources des journalistes)***

Dans une procédure légale à l'encontre d'un journaliste aux motifs d'une atteinte alléguée à l'honneur ou à la réputation d'une personne, les autorités compétentes devraient, pour établir la véracité de ces allégations, examiner toute preuve à leur disposition en application du droit procédural national et ne devraient pas pouvoir requérir à cette fin la divulgation par un journaliste des informations identifiant une source.

- ***Principe 5 (Conditions concernant la divulgation)***

a) La proposition ou demande visant à introduire une action des autorités compétentes en vue d'obtenir la divulgation de l'information identifiant une source ne devrait pouvoir être effectuée que par les personnes ou autorités publiques ayant un intérêt légitime direct à la divulgation.

b) Les journalistes devraient être informés par les autorités compétentes de leur droit de ne pas divulguer les informations identifiant une source, ainsi que des limites de ce droit, avant que la divulgation ne soit demandée.

c) Le prononcé de sanctions à l'encontre des journalistes pour ne pas avoir divulgué les informations identifiant une source devrait seulement être décidé par les autorités judiciaires au terme d'un procès permettant l'audition des journalistes concernés conformément à l'article 6 de la Convention.

d) Les journalistes devraient avoir le droit que le prononcé d'une sanction pour ne pas avoir divulgué leurs informations identifiant une source soit soumis au contrôle d'une autre autorité judiciaire.

e) Lorsque les journalistes répondent à une demande ou à une injonction de divulguer une information identifiant une source, les autorités compétentes devraient envisager de prendre des mesures pour limiter l'étendue de la divulgation, par exemple en excluant le public de la divulgation, dans le respect de l'article 6 de la Convention lorsque cela est pertinent, ainsi qu'en respectant elles-mêmes la confidentialité de cette divulgation.

- ***Principe 6 (Interceptions des communications, surveillance et perquisitions judiciaires et saisies)***

a) Les mesures suivantes ne devraient pas être appliquées si elles visent à contourner le droit des journalistes, en application des présents principes, de ne pas divulguer des informations identifiant leurs sources :

i. les décisions ou mesures d'interception concernant les communications ou la correspondance des journalistes ou de leurs employeurs,

ii. les décisions ou mesures de surveillance concernant les journalistes, leurs contacts ou leurs employeurs, ou

iii les décisions ou mesures de perquisition ou de saisie concernant le domicile ou le lieu de travail, les effets personnels ou la correspondance des journalistes ou de leurs employeurs, ou des données personnelles ayant un lien avec leurs activités professionnelles.

b) Lorsque des informations identifiant une source ont été obtenues de manière régulière par la police ou les autorités judiciaires à travers l'une quelconque des actions précitées, même si cela pourrait ne pas avoir été le but de ces actions, des mesures devraient être prises pour empêcher l'utilisation ultérieure de ces informations comme preuve devant les tribunaux, sauf dans le cas où la divulgation serait justifiée en application du Principe 3.

- ***Principe 7 (Protection contre l'auto-accusation)***

Les principes posés par le présent texte ne doivent en aucune façon limiter les lois nationales sur la protection contre l'auto-accusation dans les procédures pénales et les journalistes devraient, dans la mesure où ces lois s'appliquent, jouir de cette protection s'agissant de la divulgation des informations identifiant une source.

En ce qui concerne la définition du terme de « journaliste », la Recommandation affirme que les lois devraient protéger « toute personne physique ou morale pratiquant à titre régulier ou professionnel la collecte et la diffusion d'informations au public par l'intermédiaire de tout moyen de communication de masse ». Les lignes directrices adoptées par le Conseil de l'Europe en 2007, qui font référence à la Recommandation n° R (2000) 7, recommandent en outre que « les représentants de la loi ne [demandent pas] aux professionnels des médias de leur transmettre les informations ou remettre les documents qu'ils ont rassemblés dans le cadre de la couverture de situations de crise. »

2010 : Rapport sur la protection des sources des journalistes, par l'Assemblée parlementaire du Conseil de l'Europe

Ce rapport affirme que « la protection des sources d'information des journalistes constitue une condition essentielle au libre exercice du journalisme et au respect du droit du public d'être informé des questions d'intérêt général. » Notant que les violations de la protection des sources sont fréquentes, il met en avant la nécessité de limiter les exceptions à la protection juridique des sources. Il fait état de l'émergence de nouvelles menaces pour la protection des sources des journalistes à l'ère numérique. Par ailleurs, il appelle « les États membres qui ne disposent pas d'une législation stipulant le droit des journalistes de ne pas divulguer leurs sources d'information à adopter une loi dans ce sens », conforme à la jurisprudence de la Cour européenne des droits de l'homme et aux Recommandations du Comité des Ministres.

2011 : Commissaire aux Droits de l'Homme du Conseil de l'Europe document thématique sur la protection des journalistes contre la violence à leur encontre

Ce rapport du Commissaire aux Droits de l'Homme du Conseil de l'Europe établit un lien direct entre la protection des sources des journalistes et la sécurité de ces derniers. Il cite également un arrêt rendu par la Cour européenne des droits de l'homme en 1996 [Goodwin c. Royaume-Uni (27 mars 1996)] qui affirme que « la protection des sources journalistiques est l'une des pierres angulaires de la liberté de la presse. » La Cour a conclu qu'en l'absence d'un « impératif prépondérant d'intérêt public », une ordonnance de divulgation « ne saurait se concilier avec l'Article 10 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales (CEDH), qui garantit la liberté d'expression. » C'est cette affaire qui a conduit le Comité des Ministres du Conseil de l'Europe à adopter la Recommandation N °R (2000) 7 sur le droit des journalistes de ne pas révéler leurs sources d'information. Le Conseil de l'Europe réaffirme le besoin de protection, afin que les protections fondamentales accordées aux sources des journalistes ne soient pas affaiblies par des efforts visant à renforcer la sécurité, rappelant une déclaration (2005) conformément à laquelle les États membres ne doivent pas remettre en cause la protection des sources au nom de la lutte contre le terrorisme, et remarquant que « la lutte contre le terrorisme ne justifie pas que les autorités publiques contournent ce droit en outrepassant les limites fixées » [Article 10 de la CEDH et Recommandation R (2000) 7].

2011 : L'Assemblée parlementaire du Conseil de l'Europe a adopté la Recommandation 1950 sur la protection des sources des journalistes.

Cette Recommandation réaffirme le rôle central de la protection des sources pour que le journalisme puisse exercer sa fonction démocratique. Elle reconnaît également le « nombre élevé de cas » de violation de la protection des sources en Europe, ainsi que l'importance de cette protection pour le journalisme d'investigation. La Recommandation demande que les exceptions à la protection des sources soient strictement définies et correspondent aux termes de l'Article 10 de la CEDH, afin d'éviter que les autorités n'exigent trop fréquemment la divulgation des sources. Elle signale par ailleurs

l'importance des sources confidentielles dans la police et le système judiciaire et le droit des journalistes à ne pas les révéler. Le problème que pose la conservation des données pour la protection des sources est aussi évoqué dans la Recommandation. En outre, la Recommandation fait référence à l'importance de l'application des principes relatifs au partage d'informations confidentielles aux intermédiaires : c'est un aspect pertinent compte tenu de la pression croissante exercée sur ces intermédiaires pour qu'ils remettent des données aux autorités ou aux parties d'un procès, ce qui est contraire aux lois sur la protection des sources.

Elle propose que le Comité des Ministres appelle les États membres à :

- légiférer sur la protection des sources.
- réexaminer leurs législations nationales sur la surveillance, la lutte contre le terrorisme, la conservation des données et l'accès aux archives des télécommunications.
- coopérer avec les organisations de journalistes et les organisations défendant la liberté des médias pour établir des lignes directrices à l'intention des procureurs et de la police, ainsi que des outils de formation pour les juges, sur le droit des journalistes de ne pas révéler leurs sources d'information.
- rédiger pour les pouvoirs publics et les fournisseurs de services privés des lignes directrices sur la protection de la confidentialité des sources journalistiques en cas d'interception ou de divulgation de données informatiques et de données relatives au trafic des réseaux informatiques.

La Recommandation a également fait état de la nécessité d'étendre la protection des sources aux plates-formes médias non traditionnelles, pour répondre à l'évolution des pratiques professionnelles, des modes de publication et de diffusion et du rôle des médias sociaux, mais aussi des sources et des publics participatifs. Cependant, la Recommandation ne considère pas les blogueurs et les acteurs des médias sociaux comme des journalistes et estime par conséquent qu'ils ne devraient pas pouvoir invoquer les lois de protection des sources. Néanmoins, la confusion entre les termes « journalisme » et « journalistes » pourrait, de fait, exclure un nombre significatif de blogueurs qui sont réellement des acteurs du journalisme – tels que les blogueurs universitaires ou spécialisés dans le droit, ou encore les militants des organisations de défense des droits de l'homme qui utilisent les médias sociaux, ainsi que les professeurs de journalisme et leurs étudiants.

Les synergies existantes entre les protections accordées aux lanceurs d'alertes et les cadres juridiques protégeant les journalistes de l'obligation de révéler leurs sources sont aussi mentionnées dans la Recommandation.

2014 Déclaration adoptée du Comité des Ministres relative à la protection du journalisme et à la sécurité des journalistes et des autres acteurs des médias :

Cette Déclaration affirme que l'application arbitraire ou disproportionnée des lois en matière de diffamation, de sécurité nationale ou de terrorisme « a un effet paralysant sur

l'exercice du droit de communiquer des informations et des idées et [qu'elle] conduit à l'autocensure. » En outre, « un accès rapide et libre aux informations, par principe, et une protection renforcée des sources des journalistes sont essentiels au bon exercice du journalisme, en particulier du journalisme d'investigation. » Le Comité soutient également que « si elle est menée sans les garanties nécessaires, la surveillance des journalistes et des autres acteurs des médias peut menacer l'exercice légitime du droit à la liberté d'expression, voire la sécurité des personnes concernées. Ils peuvent également amoindrir la protection des sources journalistiques. » Le Comité s'engage également à envisager de nouvelles mesures pour assurer l'harmonisation des législations et pratiques en matière de diffamation, de lutte contre le terrorisme et de protection des sources journalistiques avec la CEDH.

Janvier 2015 : Commission des questions juridiques et des droits de l'homme du Conseil de l'Europe, Rapport sur les opérations de surveillance massive/Résolution et Recommandation

Ce rapport, préparé par le Rapporteur Pieter Omtzigt, sur l'impact de la surveillance massive sur les droits de l'homme, traite des implications de ce phénomène pour la protection des sources des journalistes dans un contexte de liberté d'expression et d'accès aux informations. Il signale l'effet dissuasif de cette pratique sur les communications des journalistes avec des sources confidentielles et les limitations que cela entraîne pour la révélation d'informations dans l'intérêt du public.

Janvier 2015 : Résolution et Recommandation du Conseil de l'Europe sur les opérations de surveillance de masse

Le 26 janvier 2015, la Commission des questions juridiques et des droits de l'homme du Conseil de l'Europe a adopté unanimement une Résolution et une Recommandation basées sur le Rapport précité. Dans la Résolution, l'Assemblée parlementaire se déclare « profondément préoccupée par les pratiques de surveillance massive » révélées par Edward Snowden, qui « mettent en danger les droits de l'homme fondamentaux, notamment le droit au respect de la vie privée [et] le droit à la liberté d'information et d'expression ». Elle s'inquiète également de « la collecte massive de données à caractère personnel par les entreprises privées et du risque que des acteurs étatiques ou non étatiques puissent accéder à ces données et les utiliser à des fins illégales », ainsi que de « l'usage extensif de lois et de règlements secrets, de tribunaux secrets et d'interprétations secrètes de ces lois, qui ne font pas l'objet de contrôles suffisants ». La Commission a invité le Comité des Ministres à envisager « d'adresser une recommandation aux États membres en vue de garantir la protection de la vie privée à l'ère du numérique et la sécurité d'Internet, à la lumière des menaces que représentent les techniques de surveillance massive qui ont fait l'objet de récentes révélations ».

6.1.2 Résolutions, déclarations, rapports et lignes directrices du Conseil de l'Union européenne

Mai 2014 : Conseil de l'Union européenne – Lignes directrices de l'UE en matière de droits de l'homme, relatives à la liberté d'expression en ligne et hors ligne

Ces lignes directrices indiquent que : « Les États devraient protéger par la loi le droit des journalistes de ne pas divulguer leurs sources, de façon que les journalistes puissent continuer à informer sur des sujets d'intérêt public sans que leurs sources n'aient à craindre de représailles. » Elles signalent aussi que l'UE « soutiendra l'adoption de législations qui offrent une protection adéquate aux lanceurs d'alertes et les réformes visant à garantir juridiquement le droit des journalistes de ne pas dévoiler leurs sources. »

6.2 LES AMÉRIQUES

En 1994, la Conférence continentale sur la liberté d'expression, rassemblée à Mexico, a adopté la Déclaration de Chapultepec. Le principe 3 de cette Déclaration affirme : « Aucun journaliste ne peut être contraint à révéler ses sources. » En s'appuyant sur la Déclaration de Chapultepec, la Commission interaméricaine des droits de l'homme (CIDH) a approuvé en 2000 une Déclaration de principes sur la liberté d'expression, document qui oriente l'interprétation de l'Article 13 de la Convention interaméricaine des droits de l'homme. L'Article 8 de la Déclaration stipule que « Tout acteur de la communication sociale a le droit de préserver la confidentialité de ses sources d'information, de ses notes et de ses archives personnelles et professionnelles. » L'utilisation du terme « acteur de la communication sociale » renvoie au débat sur la question « Qui est journaliste ? » dans le cadre des lois sur la protection des sources.

En 2013, le rapport de la CIDH intitulé *Violence à l'encontre des journalistes et des professionnels des médias : Normes interaméricaines et pratiques nationales en matière de prévention, de protection et de poursuite des auteurs*, par le Bureau de la Rapporteuse spéciale sur la liberté d'expression, définit les journalistes comme « les personnes qui observent les évènements et en rendent compte, qui décrivent et analysent des évènements ; les déclarations, les politiques et toutes les propositions susceptibles d'avoir un effet sur la société, dans le but de systématiser ces données et de rassembler des faits et des analyses pour informer certains secteurs de la société ou la société dans son ensemble. » Il précise que cette définition inclut « tous les professionnels des médias et le personnel auxiliaire, ainsi que les professionnels des médias communautaires et les "journalistes citoyens" ».

6.3 AFRIQUE

L'Article 9 de la Charte africaine des droits de l'homme donne à toute personne le droit de recevoir des informations, mais aussi celui d'exprimer et de diffuser ses opinions. La Déclaration de principes sur la liberté d'expression en Afrique, publiée en 2002 par la Commission africaine des droits de l'homme et des peuples, fournit aux États membres de l'Union africaine des directives détaillées sur la protection des sources. Elle stipule que « les journalistes ne doivent pas être obligés de révéler leurs sources d'information ou autres documents détenus dans le cadre de l'exercice de la fonction de journaliste, sauf si c'est en conformité avec les principes suivants » :

- *L'identité de la source est nécessaire dans une enquête ou des poursuites relatives à un crime grave, ou pour assurer la défense d'une personne accusée d'infraction pénale ;*
- *L'information ou une information similaire menant au même résultat ne peut pas être obtenue ailleurs ;*
- *L'intérêt public de la divulgation prime sur la menace à la liberté d'expression ; et*
- *La divulgation a été ordonnée par un tribunal, après une audition complète.*

6.4 INSTITUTIONS INTERRÉGIONALES

6.4.1 Organisation pour la sécurité et la coopération en Europe

La Représentante de l'OSCE pour la liberté des médias publie régulièrement des déclarations et des commentaires concernant les violations des cadres juridiques de protection des sources ou les menaces qui pèsent sur ces derniers. Les Recommandations sur la sécurité des journalistes, rédigées en juin 2011 à Vilnius, incluent une recommandation encourageant les législateurs à « améliorer la sécurité des conditions de travail des journalistes, en adoptant une législation qui favorise la liberté des médias, notamment par la garantie du libre accès aux informations, la protection des sources confidentielles et la dépénalisation des activités des journalistes. »

6.4.2 L'Organisation de coopération et de développement économiques

Rapport de mars 2014 « Le guide CleanGovBiz Toolkit pour l'intégrité »

Le rapport pose les questions suivantes : « L'anonymat des sources journalistiques est-il garanti ? Si oui, comment ? » Il reconnaît l'importance de l'anonymat des sources, « car il peut être dangereux pour des membres de la société civile de fournir à des

journalistes des informations, en particulier si elles dénoncent des manquements graves ou concernent des faits de corruption. » Le rapport affirme que forcer un journaliste à divulguer ses sources dans les affaires de corruption serait irréfléchi. En citant par ailleurs la Recommandation N °R (2000) 7du Comité des Ministres du Conseil de l'Europe, il souligne que lever l'anonymat des sources confidentielles des sources des journalistes ferait peser un risque plus grand sur la capacité des individus de partager des informations et donc sur la capacité du public à en recevoir. En outre, il précise que cette protection « ne devrait pas seulement s'appliquer aux informateurs des journalistes, mais aussi à leur lieu de travail et à leurs recherches. » Et il fait valoir que : « Les exceptions devraient seulement être accordées par un juge et uniquement pour les témoins clés de crimes graves ». Ainsi, il insiste sur l'importance de définir strictement les restrictions, afin que les journalistes puissent clairement informer leurs sources des risques qu'elles encourent.

7. BILAN PAR RÉGION UNESCO

Comme indiqué plus haut, des évolutions des environnements juridiques et réglementaires relatifs aux protections accordées aux journalistes, ont été constatées dans 84 des121 pays étudiés dans ce rapport (69 %), au cours de la période 2007-2015. Faute de place, l'analyse détaillée n'est pas présentée ici, mais les résultats, reproduits dans la version plus complète de l'étude, illustrent un impact majoritairement négatif ou potentiellement négatif sur la protection des sources. Ces évolutions ont été repérées et analysées dans chacune des cinq régions UNESCO, un accent particulier étant mis sur les thèmes principaux identifiés :

1. La priorité donnée aux lois concernant la sécurité nationale/la lutte contre le terrorisme
2. Le rôle de la surveillance (qu'elle soit massive ou ciblée) sur l'affaiblissement des protections
3. Les rôles des intermédiaires et de la conservation des données
4. La modification des critères donnant droit une protection – Qui est journaliste ? Qu'est-ce que le journalisme ?
5. Autres dimensions propres au numérique (par exemple l'anonymat)
6. Autres dimensions sans lien avec le numérique

Pourcentage de pays présentant des évolutions des environnements juridiques et réglementaires relatifs aux protections accordées aux journalistes, 2007-2015

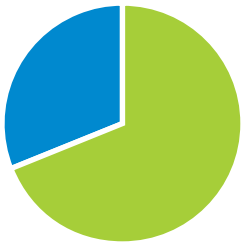
66%
Europe et Amérique du Nord
25/38 pays

85%
Amérique Latine et Caraïbes
17/20 pays

75%
Asie et Pacifique
18/24 pays

56%
Afrique
18/32 pays

86%
Région arabe
6/7 pays



69% **Mondial** 84/121 pays

7.1 AFRIQUE

Des évolutions pertinentes en matière de protection des sources ont été observées entre 2007 et 2015 dans 18 des 32 pays examinés dans la région Afrique. Néanmoins, en 2015 les lois sur la protection des sources restent limitées. Dans leur grande majorité, les réformes juridiques relatives à la confidentialité des sources et à sa protection menées en Afrique ces 8 dernières années ne concernaient pas la sphère numérique. Dans plusieurs États, les cadres juridiques de protection des sources ont été menacés par des demandes visant à introduire de larges exceptions au droit des journalistes de ne pas divulguer leurs sources, pour des raisons de « sécurité nationale », et à ériger en infraction pénale le non-respect de ces exceptions. Dans le même temps, des allégations de surveillance de masse se sont fait entendre dans certains pays. Le numérique et les risques associés sont peu évoqués dans ces évolutions. C'est probablement parce que la pénétration d'Internet est encore faible dans la région. Par conséquent, bon nombre des différentes questions liées à la collecte d'informations numériques ou à la publication d'informations en ligne n'ont pas encore fait l'objet d'un débat national dans de nombreux pays d'Afrique. À l'heure actuelle, plusieurs gouvernements ne voient pas la nécessité de réguler les médias numériques – qu'il s'agisse de protéger ou de restreindre le journalisme – notamment parce que seul un nombre relativement faible de personnes y ont accès. Cette approche pourrait changer à l'avenir, car de plus en plus d'utilisateurs peuvent régulièrement consulter des informations en ligne.

7.2 RÉGION ARABE

Des évolutions ont lieu dans six des sept pays étudiés dans la région entre 2007 et la première moitié de 2015 (86 %). Les plus significatives d'entre elles concernaient la surveillance massive et les sphères non numériques. Une seule évolution digne d'intérêt a été constatée dans le domaine des intermédiaires. Cela peut être dû à la pénétration encore limitée d'Internet ou aux stricts contrôles exercés sur ce moyen de communication dans certaines zones de la région. Bien que les activités sur Internet dans les États arabes demeurent relativement limitées comparées à d'autres régions du monde, le nombre croissant d'utilisateurs a conduit trois pays à introduire des lois régulant l'utilisation d'Internet depuis 2007, avec des conséquences possibles sur la protection des sources. Deux des pays étudiés ont changé les critères définissant qui peut invoquer la loi sur la protection des sources. La protection des sources dans les sphères non numériques a été modifiée dans quatre des six pays dans lesquels les évolutions ont été constatées.

Il convient de remarquer que la méthodologie appliquée pour cette étude a exclu certains États arabes qui ont subi des transformations dramatiques depuis 2007. Il est donc recommandé que des études complémentaires approfondies soient menées dans tous les États arabes de l'UNESCO, afin de vérifier quels effets a eu l'évolution spectaculaire des environnements de communication sur la protection des sources dans la région.

7.3 ASIE ET PACIFIQUE

Depuis 2007, la situation concernant la protection des journalistes a évolué dans 18 des 24 pays analysés dans la région Asie et Pacifique (75 %). La protection des sources a été affaiblie par l'impact négatif qu'ont eu sur les libertés civiles des mesures prises pour renforcer la sécurité nationale, la surveillance massive et la conservation des données, l'implication des intermédiaires et les définitions ambiguës proposées pour les termes « journaliste » et « blogueur », ainsi que par un certain nombre de problématiques liées ou non à la sphère numérique. Les évolutions les plus remarquables ont eu lieu dans les huit pays confrontés à des problèmes de sécurité nationale. Sept d'entre eux ont mis en place des mesures liées à la surveillance massive et à la conservation des données pendant la période étudiée et cinq ont revu leur définition des termes « journaliste » et « blogueur », pour déterminer qui a accès à la protection des sources.

7.4 EUROPE ET AMÉRIQUE DU NORD

Dans 25 des 38 pays examinés dans la région Europe et Amérique du Nord entre 2007 et 2015 (66 %), les lois relatives à la protection des sources ont évolué de manière significative. Ces évolutions reflétaient les principaux thèmes associés aux nouveaux effets du numérique sur les cadres juridiques de protection des sources : a) impact des questions de sécurité nationale/de lutte contre le terrorisme ; b) surveillance ; c) conservation/transmission des données et rôle des intermédiaires ; d) questions sur l'accès au droit à la protection des sources ; e) risque accru de divulgation des sources lorsque des communications journalistiques conservées au format numérique sont saisies durant des enquêtes.

7.5 AMÉRIQUE LATINE ET CARAÏBES

Des modifications significatives à la couverture des lois sur la protection des sources ont été observées entre 2007 et 2015 dans 17 des 20 pays examinés dans la région Amérique latine et Caraïbes (85 %) – tous les pays concernés se trouvent en Amérique latine. Le thème de la surveillance est clairement apparu dans 10 des pays étudiés, dont cinq ont mis en place de nouvelles lois permettant la conservation et/ou l'interception de données. Quatre pays ont proposé des amendements aux lois sur le secret d'État ou la classification des informations, au titre desquelles désormais les personnes révélant de telles informations sont dans certains cas passibles de peines d'emprisonnement. Si dans plusieurs de ces pays des lois sont en vigueur pour protéger les sources des journalistes, il est de plus en plus évident que ces mêmes sources peuvent être identifiées par d'autres moyens : interception, menaces, perquisitions, accès aux données stockées et biométrie, entre autres. Dans bon nombre de pays examinés en Amérique latine, ces facteurs, auxquels s'ajoutent la classification et la restriction des informations au nom de la sécurité nationale, ont rendu la plupart des protections offertes aux sources des journalistes symboliques plutôt que réellement efficaces, face aux effets de la corruption et du crime organisé.

Néanmoins, trois pays d'Amérique latine ont introduit de nouvelles lois sur la protection des sources.

8. ÉTUDE THÉMATIQUE : VERS UN CADRE INTERNATIONAL D'ÉVALUATION DE LA PROTECTION DES SOURCES

Ce chapitre aborde la mise au point d'un cadre en 11 points visant à évaluer l'efficacité des systèmes juridiques de protection des sources à l'ère numérique. Ce dernier a été élaboré à partir du contenu des entretiens qualitatifs détaillés menés auprès de 31 experts internationaux venus des cinq régions de l'UNESCO : juristes, universitaires et spécialistes des droits de l'homme, du journalisme professionnel ou des TIC. Les entretiens se sont faits en tête-à-tête, par Skype, par téléphone ou par e-mail, entre novembre 2014 et février 2015. Après une étude initiale des problématiques et en concertation avec l'UNESCO, les chercheurs ont présenté un projet de norme en huit points, soumis à l'examen des experts. Il a ensuite été développé et élargi pour devenir un outil d'évaluation en 11 points, grâce à la contribution des experts.

Ce nouvel outil est conçu pour être appliqué à toutes les situations internationales, afin d'évaluer l'efficacité des cadres juridiques de protection des sources dans un État particulier en tenant compte des lois et des principes internationaux relatifs aux droits de l'homme.

Principes à prendre en compte pour évaluer les cadres juridiques de protection des sources au niveau international

Un cadre solide et global de protection des sources devrait idéalement prendre en compte la nécessité de :

1. reconnaître la valeur, pour l'intérêt public, de la protection des sources, qui s'appuie légalement sur les droits à la liberté d'expression (y compris la liberté de presse) et au respect de la vie privée. Ces protections devraient être inscrites dans la constitution et/ou dans la législation nationale ;

2. reconnaître que la protection des sources devrait couvrir tous les actes de journalisme, quels que soient la plate-forme, le service ou le support sur lesquels ils sont stockés et publiés. Cela devrait également inclure les données numériques et les métadonnées ;

3. reconnaître que la protection des sources ne devrait pas dépendre de l'enregistrement ou de l'octroi d'une licence aux professionnels du journalisme ;

4. reconnaître l'impact potentiellement négatif sur le journalisme d'intérêt public et la société dans son ensemble, de l'enregistrement massif, de la surveillance, du stockage et de la collecte d'informations fournies par des sources.

5. affirmer que l'État et les acteurs privés (y compris des intermédiaires) qui interceptent les communications numériques de journalistes doivent les traiter en respectant la confidentialité (reconnaissant par ailleurs qu'il est souhaitable que la conservation et

l'utilisation de telles données soient également conformes au droit au respect de la vie privée) ;

6. protéger les actes de journalisme des opérations de surveillance ciblée, de la conservation de données et de la divulgation de documents permettant de remonter aux sources confidentielles ;

7. définir les exceptions à tous les points précédents de manière très stricte, afin que le principe de protection des sources reste la norme effective ;

8. faire en sorte que ces exceptions soient accordées si les critères de nécessité et de proportionnalité sont respectés – en d'autres termes, lorsque la divulgation est la seule solution possible, l'intérêt public à la divulgation l'emporte clairement sur la légitimité de la protection et les conditions de la divulgation préservent autant que possible de confidentialité ;

9. mettre au point une procédure judiciaire transparente et indépendante, permettant de faire appel des exceptions autorisées et de veiller à ce que les agents des forces de l'ordre et les acteurs du système judiciaire soient informés des principes qui sous-tendent cette procédure ;

10. ériger en infraction pénale les violations arbitraires, non autorisées et délibérées de la confidentialité des sources par des acteurs tiers ;

11. reconnaître que les lois sur la protection des sources peuvent être renforcées par une législation complémentaire concernant les lanceurs d'alerte.

Des recherches supplémentaires pourraient permettre de créer un recueil de lois types et de décisions exemplaires concernant les exceptions et le critère de nécessité. Un résumé de ce recueil pourrait être ajouté à ce modèle d'évaluation des cadres.

9. PROBLÉMATIQUES LIÉES AU GENRE

Les femmes journalistes courent des risques supplémentaires dans l'exercice de leur métier, aussi bien sur Internet qu'en dehors. Dans le monde réel, on compte parmi ces risques le harcèlement sexuel, les agressions et le viol. Dans la sphère numérique, les actes de harcèlement et les menaces violentes sont monnaies courantes. De même, les femmes courent davantage de risques quand elles lancent des alertes ou informent des journalistes. Cela se manifeste de diverses manières, en lien avec la protection des sources à l'ère numérique. Les difficultés rencontrées, détaillées plus bas, peuvent être résumées ainsi :

1. Lorsqu'elles traitent avec des sources confidentielles, les femmes journalistes courent plus de risques que leurs confrères masculins.
2. Les femmes courent plus de risques physiques lorsqu'elles rencontrent des journalistes et qu'elles leur révèlent des informations confidentielles.
3. Les risques physiques encourus par les femmes journalistes et des femmes sources dans le cadre de communications confidentielles peuvent les pousser à privilégier les modes de communication numériques, ce qui pose des problèmes particuliers.
4. Les mesures visant à sécuriser les communications numériques, telles que le chiffrement, sont probablement encore plus utiles aux femmes qu'aux hommes.

Facteurs spécifiques à prendre en compte

1. *Les femmes, qu'elles soient journalistes ou sources confidentielles, doivent pouvoir utiliser des moyens de communication numériques.*

Les femmes journalistes couvrant les conflits ou les activités du crime organisé sont particulièrement exposées à des risques d'attaques physiques, notamment des agressions sexuelles et des actes de harcèlement. Dans certains contextes, leur mobilité peut être restreinte parce qu'elles sont la cible de menaces manifestes, ou bien parce que des interdits culturels limitent leurs libertés en public, en les empêchant par exemple de rencontrer en tête-à-tête un informateur. Par conséquent, les femmes journalistes doivent souvent pouvoir compter sur des dispositifs numériques sécurisés pour communiquer avec leurs sources.

Les femmes qui informent des journalistes peuvent courir les mêmes risques – en particulier si leur contact est un homme et/ou si elles doivent respecter des interdits culturels, ou bien si elles travaillent dans des zones de conflit. En outre, les femmes victimes de violences au sein de leur famille n'ont parfois pas la possibilité de quitter leur domicile et doivent donc utiliser des moyens de communication numériques. Ces facteurs sont des difficultés supplémentaires que doivent surmonter les femmes, aussi bien les journalistes que les sources, pour préserver la confidentialité à l'ère numérique.

2. *La sécurité numérique est primordiale pour les femmes, qu'elles soient journalistes ou sources.*

Les femmes journalistes doivent pouvoir utiliser des moyens de communication numériques sécurisés afin que les risques inhérents à leur métier ne soient pas augmentés lorsqu'elles travaillent dans des zones de conflit ou sur des sujets sensibles, telles que la corruption ou le crime. Dans pareils contextes, la possibilité que leurs communications avec leurs sources soient secrètement interceptées et analysées augmentent le risque physique qu'elles courent, de même que leurs sources. Le chiffrement des échanges et d'autres mesures défensives sont donc essentiels pour garantir que leurs déplacements ne soient pas surveillés et que l'identité de leurs sources reste confidentielle.

Les risques posés par la révélation de l'identité des sources confidentielles sont d'autant plus importants quand il s'agit de femmes. Par conséquent elles doivent pouvoir accéder à des méthodes sécurisées de communication numérique, pour limiter autant que possible les risques de détection et de divulgation. Il faut aussi que leurs moyens d'entrer en contact avec les journalistes soient suffisamment sécurisés, afin de garantir que les reportages concernant les femmes soient diffusés, ce qui permet la participation des femmes au journalisme dans l'intérêt du public. Cela peut également limiter les difficultés du journalisme d'investigation dont les sources confidentielles sont des femmes. Des protections juridiques fortes garantissant la confidentialité et appliquées en tenant compte des spécificités liées au genre sont également nécessaires, en particulier en ce qui concerne les obligations de divulgation ordonnées par la justice.

3. *Harcèlement et menaces en ligne*

Les femmes journalistes et les sources qui communiquent via Internet, et notamment au moyen d'applications mobiles, sont plus à même de subir des actes de harcèlement ou des menaces violentes qui font explicitement référence à leur sexe. Ces risques doivent être compris et réduits pour éviter qu'un effet dissuasif n'empêche davantage les femmes de participer aux activités journalistiques, en tant que professionnelles ou en tant que sources.

10. CONCLUSION

Des changements significatifs ont été observés dans le domaine de la protection juridique des sources des journalistes entre 2007 à la première moitié de 2015. On a constaté quelques avancées vers une reconnaissance préliminaire des difficultés par les acteurs internationaux, mais ces dernières sont moins connues au niveau national. Les évolutions enregistrées au cours des 8 dernières années dans 69 % des États (84 pays sur 121) sont généralement contraires à la mise en place d'une protection forte des sources à l'ère numérique. Les cadres juridiques relatifs à la protection des sources sont particulièrement mis sous pression à l'ère numérique car les protections qu'ils accordent subissent inutilement des dommages collatéraux. En effet, face à la grande importance donnée aux questions de sécurité, les sociétés pourraient perdre les avantages que représentent ces dispositions particulières.

Le droit au respect de la vie privée qui influe sur la protection des sources et plus généralement sur la liberté d'expression, et dont dépend partiellement le respect de la confidentialité pour les journalistes et les lanceurs d'alerte, est directement remis en question. Dans une grande partie des pays étudiés, les cadres existants sont affaiblis par des lois relatives à la sécurité nationale, à la lutte contre le terrorisme et à la conservation des données, qui priment sur les lois de protection des sources ; ou bien ils risquent de l'être par des opérations de surveillance ciblée ou massive. D'autres menaces voient également le jour, en raison de la pression exercée sur les intermédiaires pour qu'ils transmettent des informations susceptibles de lever l'anonymat des sources, en réponse à des demandes approuvées par les tribunaux ou par l'État. Les mesures techniques permettant de garantir la confidentialité sont elles aussi de plus en plus remises en cause, par exemple par des demandes visant à limiter l'anonymat ou à interdire le chiffrement.

Autre question majeure, celle du droit à la protection : à une époque où les citoyens et les autres acteurs de la communication sociale peuvent publier directement pour atteindre leur propre public et où tous ceux qui partagent une information dans l'intérêt du public sont reconnus par les Nations Unies comme des acteurs légitimes du journalisme, à qui devraient s'appliquer les lois sur la protection des sources ? D'un côté, on peut considérer souhaitable d'élargir la définition légale du terme « journaliste » pour apporter une protection adéquate aux journalistes citoyens (qu'ils travaillent en ligne ou en dehors) et la jurisprudence prend peu à peu en compte cette redéfinition. Toutefois, d'un autre côté, cela peut donner lieu à des débats sur l'octroi de licences et l'enregistrement de ceux qui exercent de journalisme et souhaitent être reconnus comme tels pour que leurs sources bénéficient d'une protection. C'est pourquoi, à l'heure actuelle, la réponse à la question de l'accès aux lois sur la protection des sources s'appuie sur la définition et l'identification des « actes de journalisme », plutôt que sur des descriptifs professionnels.

Les journalistes et les organismes d'information sont en train d'adapter leurs pratiques, en renforçant leur sécurité numérique et en revenant à des méthodes « pré-numériques » pour communiquer avec leurs sources confidentielles. Mais tant que chaque État et organe régional n'aura pas réexaminé et renforcé son cadre juridique de protection des sources, l'adaptation des méthodes de reportages et le retour aux fondamentaux de l'époque analogique (qui par ailleurs n'est pas toujours possible, notamment pour les femmes

journalistes comme nous l'avons évoqué plus haut) ne suffiront pas à garantir la protection des sources à l'ère numérique. À une époque où les méthodes d'espionnage s'appuient sur des technologies de pointe, il est également nécessaire que les États revoient leurs pratiques en termes de surveillance et de contrôle, conformément aux Résolutions de l'Assemblée générale des Nations Unies sur le respect de la vie privée. En outre, les États doivent restreindre les lois sur la conservation et la transmission des données, optimiser les mesures de responsabilité et de transparence (qui, en ce qui concerne les données des journalistes, s'appliquent aussi bien aux États qu'aux entreprises) et prévoir dans la législation sur la sécurité nationale des exceptions réservées aux actes de journalisme.

V. PROMOUVOIR LA LIBERTÉ EN LIGNE : LE RÔLE DES INTERMÉDIAIRES D'INTERNET[6]

6 Ce chapitre a été rédigé à partir de MacKinnon , R. et al . 2014. *Promouvoir la liberté en ligne : le rôle des intermédiaires de l'Internet*. Série de l'UNESCO sur la liberté d'Internet. Paris, UNESCO/ Internet Society. http://unesdoc.unesco.org/images/0023/002311/231162e.pdf

1. INTRODUCTION

À mesure qu'Internet a évolué, le rôle joué par les entreprises du secteur privé est apparu de plus en plus clairement. Parmi elles, le moteur de recherche Google, le réseau social Twitter et le fournisseur de services Internet et de télécommunications Vodafone sont des exemples d'*intermédiaires d'Internet*, ainsi appelés car ils servent d'intermédiaires pour les communications en ligne et rendent possibles plusieurs formes d'expression. Ils peuvent aussi entraver, arbitrer et défendre ces expressions, ou encore faire office de « gardiens » de certaines d'entre elles. Pourtant, leurs pouvoirs ne peuvent être pleinement compris que lorsqu'ils sont mis en relation avec ceux de l'État. Les rapports entre les intermédiaires de l'Internet, les États et les normes relatives aux droits de l'homme sont complexes : en effet, les intermédiaires opèrent souvent dans plusieurs juridictions et les États s'attendent à ce qu'ils respectent les législations nationales, elles-mêmes plus ou moins conformes aux normes internationales sur les droits de l'homme. Pour certains, ces entreprises fournissent des technologies « libératrices », grâce auxquelles les opprimés peuvent se défaire de leurs chaînes. D'autres sont plus critiques : ils leur reprochent de ne pas faire assez pour protéger le droit à la vie privée des utilisateurs et de permettre au secteur privé et aux gouvernements de surveiller plus facilement les utilisateurs, sans avoir de comptes à rendre. Les intermédiaires sont de plus en plus conscients du rôle majeur et positif qu'ils ont à jouer pour promouvoir les droits de l'homme. Cependant, s'ils veulent protéger la liberté d'expression et le droit à la vie privée et ne pas violer ces droits, ils doivent davantage respecter les normes internationales en termes de transparence, de nécessité, de proportionnalité, de finalité légitime et de légalité.

Ce chapitre examine les évolutions récentes des politiques et des pratiques de ces intermédiaires en matière de protection de la liberté d'expression et de la vie privée des utilisateurs, en s'appuyant sur l'étude *Promouvoir les libertés en ligne : le rôle des intermédiaires de l'Internet*, menée en 2014 par l'UNESCO. Cette publication a alimenté l'étude complète de l'UNESCO sur les questions liées à Internet, demandée par les États membres dans la Résolution 61 de la 37e Conférence générale en 2013 et publiée en 2015 sous le titre *Des clés pour la promotion de sociétés du savoir inclusives : Accès à l'information et au savoir, liberté d'expression, respect de la vie privée et éthique sur un Internet mondial.*

1.1 ENTREPRISES ET DROITS DE L'HOMME

Traditionnellement, la législation internationale sur les droits de l'homme porte surtout sur la conduite des États et trouve son origine dans les déclarations et les accords conclus entre États. Au cours des dernières décennies, cependant, les responsabilités des entreprises en termes de droits de l'homme ont été progressivement reconnues et il est admis que ces dernières devraient rendre des comptes dans ce domaine. Dans la mesure où la plupart des intermédiaires d'Internet sont gérés par des entreprises privées, ce chapitre reprend les principes relatifs aux entreprises et aux droits de l'homme établis

par les Nations Unies dans le cadre de référence « Protéger, respecter et réparer ». Il affirme que si le devoir de protéger les droits de l'homme incombe en premier lieu aux gouvernements, cette responsabilité engage aussi les entreprises et ces deux types d'entités doivent garantir un accès à des moyens efficaces de réparation.

Cette perspective s'est développée et a donné naissance à de nouvelles tendances au cours des cinq dernières années. En 2011, le Conseil des droits de l'homme des Nations Unies a soutenu l'adoption des Principes directeurs relatifs aux entreprises et aux droits de l'homme, résultats de six années de recherche et de consultation des entreprises, des gouvernements et des membres de la société civile, menées par le Représentant spécial du Secrétaire général des Nations Unies pour les entreprises et les droits de l'homme. Ces Principes directeurs affirment tout d'abord qu'il est du devoir des États de protéger lorsque des entreprises portent atteinte aux droits de l'homme sur leur territoire et/ou sous leur juridiction et d'« énoncer clairement qu'ils attendent de toutes les entreprises domiciliées sur leur territoire et/ou sous leur juridiction qu'elles respectent les droits de l'homme dans toutes leurs activités. » Ces Principes sont universels et s'appliquent à toute entreprise, non pas seulement aux intermédiaires d'Internet. Dans son rapport de juin 2014 à l'Assemblée générale, Mme Navi Pillay, Haut-Commissaire des Nations unies aux droits de l'homme, a écrit : « Une entreprise a la responsabilité de faire respecter les droits de l'homme dans le cadre de toutes ses activités mondiales, où que se trouve ses utilisateurs, et ce, indépendamment du fait que l'État s'acquitte ou non de ses propres obligations en matière de droits de l'homme. »

Ce chapitre identifie les différentes tendances dans ce que les intermédiaires de l'Internet font ou peuvent encore faire pour optimiser la liberté d'expression dans divers juridictions et contextes, avec des technologies et des modèles d'entreprises variés. Toutefois, pour les repérer et les comprendre, il faut d'abord examiner de plus près la nature de ces intermédiaires et leur rapport à la liberté d'expression.

1.2 INTERMÉDIAIRES

Pour Thomas F. Cotter, spécialiste du droit, un intermédiaire est « toute entité qui permet la communication d'informations d'une partie à une autre. » Dans un rapport de 2010, l'OCDE explique que les intermédiaires de l'Internet « rassemblent ou facilitent les transactions entre des tiers sur Internet. Ils mettent à disposition, hébergent, transmettent et répertorient des contenus, produits et services créés par des tiers sur Internet ; ou bien fournissent à des tiers des services sur Internet. » La plupart des définitions du terme « intermédiaire », y compris celle retenue dans ce chapitre, excluent explicitement les producteurs de contenu. Plus précisément, l'OCDE exclut de la fonction d'intermédiaire « les activités par lesquelles les fournisseurs de services mettent à disposition, hébergent, transmettent et répertorient des contenus et des services qu'ils ont eux-mêmes créés. » À ce titre, les éditeurs et autres médias qui créent et diffusent des contenus originaux ne sont pas considérés comme des intermédiaires. Parmi ces entités, on compte les sites d'information qui publient des articles écrits et édités par leur personnel ou par des

collaborateurs invités ; ou bien des services d'abonnement vidéo qui recrutent ou invitent des producteurs pour qu'ils créent des vidéos qui sont ensuite diffusées aux abonnés.

Cependant, de nombreuses entités proposent des services hybrides et sont donc dans une certaine mesure des intermédiaires. Pour déterminer ce qu'on peut attendre des médias sociaux, par exemple, il est important d'évaluer dans quelle mesure ce sont des intermédiaires et dans quelle mesure ils exercent un rôle de média. En 2011, le Conseil de l'Europe a adopté une définition élargie du terme « médias ». Pour définir si un nouvel acteur est ou non un média, six critères sont examinés, parmi lesquels l'intention d'agir comme un média, le contrôle éditorial et l'application de normes professionnelles. Certaines parties prenantes ont toutefois exprimé des inquiétudes, en signalant que les efforts mis en œuvre par certains États pour définir des intermédiaires en tant que « médias » ont restreint davantage la liberté d'expression. S'il y a bien des similitudes potentielles entre les médias et les intermédiaires dans certains cas, il y a aussi des différences significatives dans leur évolution. Les médias sont généralement juridiquement responsables de leur contenu car ils exercent un contrôle éditorial. En revanche, les intermédiaires ont une responsabilité juridique limitée, dans la mesure où le contenu qu'ils hébergent provient d'acteurs sur lesquels ils n'ont pas de contrôle (voir 2.2 ci-après).

Tous les intermédiaires de l'Internet exploités à des fins commerciales étudiés dans ce chapitre demandent à leurs utilisateurs d'accepter des « conditions de service » avant la première utilisation du service. Il arrive que ces conditions restreignent la liberté d'expression des utilisateurs, bien qu'elle soit protégée par la loi dans certaines juridictions. Si l'application de ces conditions peut parfois être considérée comme une fonction éditoriale, son fondement juridique aux États-Unis et en Europe, lieux de naissance des premiers intermédiaires d'Internet, ne se trouve pas dans la législation sur les médias, mais dans la législation sur les contrats et les transactions commerciales.

1.2.1 Types d'intermédiaires

Ce chapitre est consacré aux services et plates-formes dont l'activité consiste surtout à héberger, mettre à disposition et répertorier des contenus créés par d'autres, ou à en faciliter la transmission et l'échange. À mesure que le rôle des intermédiaires pour l'économie mondiale du savoir a pris de l'ampleur, plusieurs organisations ont cherché à décrire ou à catégoriser les types d'intermédiaires selon leur rôle et leur fonction. Parmi elles, l'OCDE, le Rapporteur spécial des Nations Unies sur la liberté d'opinion et d'expression et les organisations de la société civile. Le tableau ci-dessous permet de comparer les principaux types d'intermédiaires que ces organisations ont caractérisés ou choisis d'examiner.

Tableau 1 : Catégorie et principaux exemples d'intermédiaires d'Internet

<table>
<tr><th>OCDE</th><th>Rapporteur spécial Frank La Rue</th><th>ARTICLE 19</th><th>Centre pour la démocratie et la technologie</th><th>Partenaires mondiaux</th></tr>
<tr><td rowspan="2">Fournisseurs d'accès et de service Internet</td><td rowspan="2">Fournisseurs de service Internet (FSI)</td><td rowspan="2">Fournisseurs de service Internet (FSI)</td><td rowspan="2">Fournisseurs d'accès/FSI
Opérateurs réseau et opérateurs de téléphonie mobile</td><td>Niveau physique : rend possible les communications</td></tr>
<tr><td>Connectivité & code : le langage ou les protocoles de la communication</td></tr>
<tr><td>Service de traitement des données et hébergeurs Web</td><td></td><td>Hébergeurs Web</td><td>Bureaux d'enregistrements et registres de noms de domaines
Sociétés d'hébergement Web</td><td rowspan="5">Applications : Outils permettant de naviguer sur le Web</td></tr>
<tr><td>Moteurs de recherche et portails sur Internet</td><td>Moteurs de recherche</td><td>Moteurs de recherche</td><td>Moteurs de recherche et portails sur Internet</td></tr>
<tr><td>Intermédiaires du commerce électronique</td><td rowspan="2"></td><td rowspan="2"></td><td rowspan="2">Plates-formes dédiées au commerce électronique et marchés en ligne</td></tr>
<tr><td>Systèmes de paiement en ligne</td></tr>
<tr><td>Plates-formes des réseaux participatifs</td><td>Plates-formes des blogs
Communautés en ligne
Plates-formes des réseaux sociaux</td><td>Plates-formes des réseaux sociaux</td><td>Prestataires de services en ligne
En général, tout site hébergeant du contenu créé par les utilisateurs ou permettant les communications entre utilisateurs</td></tr>
</table>

Cette démarche met en évidence que chaque intermédiaire exerce des fonctions différentes et adopte des architectures techniques différentes. Par exemple, les fournisseurs de service Internet (FSI) connectent les appareils d'un utilisateur à Internet, tandis que les hébergeurs Web, les bureaux d'enregistrement et les registres de noms de domaines permettent aux sites Internet d'être publiés et accessibles en ligne. Les moteurs de recherche rendent accessible une partie du Web en permettant aux internautes de faire des recherches sur leurs bases de données. Ils sont souvent un relais essentiel entre les sites Internet et les utilisateurs. Les réseaux sociaux permettent aux internautes d'échanger des textes, des photos et des vidéos, mais aussi de publier du contenu à l'intention de leur réseau de contacts ou du grand public.

Elle indique également qu'à ces intermédiaires correspondent des modèles d'entreprises divers. Afin de fournir un accès Internet et/ou un service de télécommunications, les

entreprises doivent exploiter des équipements et des services dans les juridictions où leurs clients résident physiquement. Ce type de service nécessite des investissements importants, en termes de ressources, d'équipements et de personnel dans ces juridictions, ainsi que l'obtention d'un agrément de l'État et le respect de la législation locale en vigueur. Ainsi, les États exercent une forte influence sur les FSI.

Les mêmes acteurs ne fournissent pas nécessairement tous un service de télécommunications et un accès Internet. La plupart des services de fourniture d'accès Internet s'appuient surtout sur l'infrastructure de transmission technique des télécommunications, ce qui peut être utilisé comme moyen discret d'interdire ou de limiter l'accès à certains FSI ou à des utilisateurs de leurs clients. Les FSI, quant à eux, peuvent également limiter l'accès à un autre niveau, sans passer par les opérateurs de l'infrastructure des télécommunications. Les FSI sont dépendants de l'infrastructure des télécommunications, et par conséquent les intermédiaires réseaux sont particulièrement concernés par la réglementation des États.

A contrario, d'autres intermédiaires, tels que les hébergeurs Web, les bureaux d'enregistrement et les registres de noms de domaine, les moteurs de recherche et les réseaux sociaux, n'ont pas obligatoirement besoin d'implanter du personnel, des équipements ou d'autres ressources physiques dans la zone géographique où se trouvent les utilisateurs auxquels ils fournissent leurs services. Grâce à l'architecture ouverte et interopérable d'Internet, un utilisateur dans un pays donné peut faire une recherche sur Google, créer un site auprès d'un hébergeur Web ou communiquer avec des amis sur Facebook sans qu'aucune de ces entreprises n'aient de personnel, de locaux ou d'équipements dans le pays en question. Par conséquent, les intermédiaires de l'Internet – de même que leurs utilisateurs – peuvent ne pas être soumis au contrôle des États dans lesquels ils n'ont pas de siège ni de présence physique.

Cette indépendance relative est précisément la raison pour laquelle les spécialistes considèrent que les nouveaux médias, en particulier les médias sociaux, favorisent la liberté d'expression dans les contextes où l'expression hors ligne est fortement régulée par l'État. Dans la pratique, cependant, de plus en plus d'États limitent les activités de ces intermédiaires en exerçant un contrôle sur le niveau inférieur, les fournisseurs de télécommunications et les FSI, ce qui permet d'entraver l'accès à Internet. Les États sont en mesure de menacer d'interdire l'accès d'un service particulier à tous les utilisateurs se trouvant sous leur juridiction si les intermédiaires établis ailleurs ne respectent pas leur législation et ils le font de plus en plus souvent. En visant les intermédiaires à différents niveaux, les États peuvent exercer un contrôle sur les expressions en ligne des utilisateurs ou sur l'accès à l'information, même en dehors de leur juridiction nationale. Ils peuvent également déléguer ces contrôles aux intermédiaires, sans avoir à surveiller eux-mêmes les individus.

1.2.2 Modes de restrictions

Selon leur type et les services qu'ils offrent, les intermédiaires peuvent contrôler comment leurs utilisateurs communiquent et avec qui. Ils ont accès aux informations créées par les utilisateurs, ainsi qu'à un ensemble de données directement liées aux utilisateurs. C'est

pourquoi les intermédiaires jouent un rôle essentiel dans la promotion et la protection des droits à la liberté d'expression et au respect de la vie privée. Ce sont aussi des agents grâce auxquelles les autorités peuvent surveiller, réglementer et contrôler les activités des individus en ligne et leur accès à l'information. La liberté d'expression peut être restreinte par l'intermédiaire des FSI, des moteurs de recherche et des médias sociaux, surtout aux deux niveaux suivants :

1. **Au niveau du réseau**, les fournisseurs de services de télécommunications et les FSI peuvent limiter la liberté d'expression au moyen des trois méthodes suivantes :

    a) ***Filtrage*** : l'accès à des sites Internet entiers, à des pages spécifiques ou à des mots-clés particuliers est complètement bloqué. Ce filtrage est effectué par le FSI, par les opérateurs réseaux qui contrôlent le trafic Internet dans une juridiction donnée, ou bien par les deux à la fois. Le contenu bloqué existe encore sur Internet mais il est inaccessible pour les utilisateurs du réseau auquel le filtre est appliqué. Cette méthode empêche les utilisateurs de recevoir des informations, mais aussi d'en diffuser sur des sites spécifiques, comme par exemple un réseau social.

    b) ***Arrêt du service*** : un ou plusieurs des services proposés par le ou les fournisseurs peuvent être arrêtés dans une juridiction donnée ou dans une zone géographique. Les utilisateurs ne peuvent donc plus accéder à Internet via une fixe ou mobile, envoyer des SMS etc.

    c) ***Non-neutralité du service*** : l'accès à certains contenus ou applications est ralenti, les utilisateurs y accèdent donc plus difficilement. Ou bien les tarifs appliqués peuvent varier selon les contenus ou les services et certains services spécifiques peuvent être gratuits.

Les deux autres catégories d'intermédiaires couvertes dans ce chapitre, les moteurs de recherche et les réseaux sociaux, sont directement touchées lorsque de telles restrictions sont appliquées au niveau du réseau. Le filtrage au niveau du réseau, ou la menace du filtrage, est d'ailleurs un moyen de pression utilisé pour forcer les moteurs de recherche, les réseaux sociaux et les autres intermédiaires à mettre en place des restrictions au niveau de leurs plates-formes.

2. Les intermédiaires qui agissent **au niveau des plates-formes**, c'est-à-dire les moteurs de recherche et les réseaux sociaux, peuvent supprimer définitivement le contenu, le rendre invisible à certaines catégories d'utilisateurs ou désactiver les comptes de certains utilisateurs. Ces mesures sont appliquées par l'entreprise elle-même, ou bien par des services gouvernementaux qui ont obtenu un accès technique direct aux principales fonctions de la plate-forme. La suppression, le blocage ou la désactivation peuvent être effectués à la demande des autorités, des utilisateurs ou d'une autre partie, ou bien en application du propre règlement de l'intermédiaire.

    Les restrictions décrites ci-dessus sont des outils utilisés auprès de différents types de gouvernance, publique ou privée, pour faire respecter la réglementation/législation nationale, pour identifier les infractions à ces textes réglementaires et pour garantir le respect des conditions de service et autres règlements mis en œuvre par les

entreprises. Elles servent aussi dans certains pays à faire respecter les normes mises en place par des organismes privés ou quasi étatiques.

Les mesures prises par les intermédiaires en ce qui concerne le respect de la vie privée (à la fois au niveau du réseau et des plates-formes) ont aussi des conséquences sur la liberté d'expression. Les internautes qui soupçonnent que leurs communications et leur comportement en ligne sont surveillés ou mis au jour d'une façon qui constitue une infraction à leur droit à la vie privée sont moins susceptibles de s'exprimer librement lorsqu'ils utilisent les services des intermédiaires. Les pratiques suivantes ont un effet néfaste sur le respect de la vie privée et concernent les intermédiaires à tous les niveaux :

a) **la collecte et la surveillance des données** sont présentes à tous les niveaux sur Internet et risquent de restreindre la libre expression en encourageant l'autocensure.

b) **le manque de sécurité dans le stockage des données et leur transmission** peut entraîner des violations du droit au respect de la vie privée, des interceptions non autorisées ou des interceptions par les autorités, sans que l'entreprise n'y prenne part activement.

c) selon les services et des plates-formes, **les internautes ont plus ou moins de contrôle sur leurs informations personnelles**, notamment lorsqu'il s'agit de les préserver ou de les rendre publiques.

Le tableau suivant récapitule les modes de restriction présentés ci-dessus.

Tableau 2 : Manière dont l'expression et le droit au respect de la vie privée peuvent être restreints par les intermédiaires de l'Internet, sur demande ou à l'initiative de l'entreprise

	FSI	Moteurs de recherche	Médias sociaux
Restrictions au niveau du réseau	• Filtrage • Arrêt du service • Non-neutralité du service		
Restrictions au niveau de la plate-forme		• Manipulation de l'ordre d'apparition des résultats des recherches • Retrait ou non-référencement des liens vers des pages ou des types de pages spécifiques	• Suppression du contenu de la plate-forme • Blocage du contenu et de la libre expression, par la restriction de l'accès de certaines catégories d'utilisateurs (notamment en fonction de la localisation) • Limitation ou désactivation des comptes

Effets dissuasifs liés à la vie privée	• Collecte et conservation des données des utilisateurs à des fins commerciales ou pour répondre aux demandes des autorités • Obligation de créer un compte sous son « vrai nom » • Demandes des autorités visant à récupérer les données des utilisateurs • Surveillance en temps réel par les autorités	• Collecte et conservation des données des utilisateurs à des fins commerciales • Demandes des autorités visant à récupérer les données des utilisateurs • Catalogage des informations sur les utilisateurs par des recherches de leur nom	• Collecte et conservation des données des utilisateurs à des fins commerciales • Obligation de donner son vrai nom • Demandes des autorités visant à récupérer les données des utilisateurs

Le caractère international d'un grand nombre de ces entreprises complique encore davantage le rôle des intermédiaires dans la protection ou la limitation de la liberté d'expression. Les entreprises multinationales et les fournisseurs de services Internet dont les utilisateurs se trouvent dans plusieurs juridictions peuvent être soumis à toute une mosaïque de régimes juridiques et réglementaires. Certaines entreprises ont tenté de régler ce problème en créant des filtres spécifiques pour chaque pays et en mettant en place des politiques de gestion des demandes de restrictions des contenus ou de récupération des données, qu'elles émanent des autorités ou des utilisateurs. Quand une entreprise n'a pas de locaux ou de personnel dans une juridiction donnée, il est difficile pour un État de la forcer à appliquer la législation nationale ou à répondre à ses demandes de restrictions de contenus. Par conséquent, certains gouvernements en sont venus à filtrer – ou à menacer de filtrer – certains contenus ou des services entiers. Dans ce contexte très complexe, les normes sur la liberté d'expression sont souvent mal comprises, mal protégées, mal respectées ou ne font pas suffisamment l'objet de réparations.

1.2.3 Engagement en matière de liberté d'expression

Face à ce paysage mondial de plus en plus complexe, on a vu apparaître ces dernières années un certain nombre d'initiatives, menées par les acteurs du secteur ou par les autorités, afin d'aider les intermédiaires de l'Internet à respecter autant que possible la vie privée et la liberté d'expression de leurs utilisateurs. Par exemple, en 2013, la Commission européenne a publié un guide expliquant aux entreprises du secteur des TIC comment mettre en œuvre les Principes directeurs relatifs aux entreprises et aux droits de l'homme, développés avec la participation d'acteurs de l'industrie, du monde universitaire, de la société civile et des gouvernements. Certains intermédiaires ont rendu publics leurs engagements en matière de respect des droits des utilisateurs. Depuis sa création en 2008, plusieurs entreprises d'Internet ont rejoint l'organisation Global Network Initiative (GNI), qui rassemble plusieurs parties prenantes et au sein de laquelle les principaux intermédiaires collaborent avec des membres de la société civile, des investisseurs responsables et des universitaires pour mettre en œuvre un ensemble de principes de

base relatifs à la liberté d'expression et à la vie privée. Google, l'un des intermédiaires étudiés dans le présent rapport, est l'un des membres fondateurs de GNI. En janvier 2014, Google s'est soumis à un processus d'évaluation afin de vérifier que les principes de GNI avaient correctement été appliqués dans le cadre des demandes émises par les gouvernements en matière de restriction des contenus et d'accès aux données des utilisateurs. Facebook a adhéré à GNI en mai 2013, mais en septembre 2015 l'entreprise n'avait pas encore passé d'évaluation permettant de vérifier qu'elle en respectait bien les principes. En 2012, un groupe d'entreprises de télécommunications, parmi lesquelles Vodafone, a formé l'organisation Industry Dialogue on Freedom of Expression and Privacy, dont le but est de mettre au point des principes et des meilleures pratiques pour ce secteur.

Dans ce contexte, on constate également qu'un nombre croissant d'entreprises d'Internet et du secteur des télécommunications ont commencé à publier régulièrement des « rapports de transparence », ainsi appelés car ils informent sur le volume et la nature des demandes de suppression de contenus – aussi bien par des gouvernements que par des entités privées – et de communication de données concernant les utilisateurs. Cette transparence permet aux utilisateurs et au grand public de comprendre quelles restrictions sont mises en œuvre et qui en est à l'origine. Parmi les entreprises examinées dans ce rapport, Facebook, Google, Twitter et Vodafone ont toutes publié des rapports de transparence. Il convient cependant de noter que ces derniers sont très différents, par leur portée, leur degré de précision et la méthodologie employée. Il est donc difficile de tirer des conclusions pertinentes sur le respect de la liberté d'expression et de la vie privée dans une entreprise par rapport aux autres. Les spécialistes ont appelé les entreprises à collaborer avec des universitaires et des militants connaissant bien ces questions afin de créer des approches plus standardisées pour la rédaction de ces rapports de transparence. D'après eux, une enquête vraiment transparente ne doit pas seulement indiquer le nombre de requêtes reçues et traitées, mais également des informations sur les politiques et les pratiques utilisées pour gérer ses demandes, ainsi que sur les mécanismes d'exécution privés.

1.3 MÉTHODOLOGIE

Ce chapitre examine les études de cas présentées dans *Promouvoir la liberté en ligne : le rôle des intermédiaires de l'Internet*, portant sur trois types d'intermédiaires et 11 entreprises :

1. **FSI et fournisseurs de services de télécommunications** : Vodafone, Vivo/Telefônica Brasil, Bharti Airtel, Safaricom
2. **Moteurs de recherche** : Google, Baidu, Yandex
3. **Réseaux sociaux** : Facebook, Twitter, Weibo, iWiW

Ces études de cas contiennent chacune une description et une analyse des cadres juridiques et réglementaires en constante évolution auxquels sont soumis les

intermédiaires, ainsi que les tendances observées dans les entreprises en matière de politiques et de pratiques. Les deux Priorités de l'UNESCO, l'Afrique et l'Égalité des genres, font l'objet de sections dédiées. Le chapitre se termine par des recommandations générales à l'intention de toutes les parties prenantes.

Le choix des trois types d'intermédiaires a été éclairé par la classification en cinq catégories proposées par l'OCDE et ils étaient également les trois types mis en avant comme exemples dans le rapport publié en 2011 par l'ancien Rapporteur spécial des Nations Unies Frank La Rue sur le droit à la liberté d'opinion et d'expression sur Internet. Les entreprises et les pays sélectionnés dans chaque cas l'ont été car l'ensemble représente la variété des environnements culturels, régionaux, politiques et juridiques dans lesquels de puissants intermédiaires de l'Internet ont vu le jour.

Pour chaque pays concerné par cette recherche, une équipe de recherche a été envoyée sur place pour compléter un questionnaire détaillé élaboré au début de l'année 2014. Ces questionnaires contenaient en moyenne 61 questions sur le contexte juridique et politique et son impact sur la régulation d'Internet, les politiques et les pratiques des entreprises sélectionnées dans les pays en question et la manière dont les politiques spécifiques des entreprises et le contexte juridique influaient sur le comportement des utilisateurs, ainsi que quelques questions spécifiques liées au genre. Ces questionnaires ont été remplis en mars et avril 2014, grâce aux entretiens menés par les chercheurs avec des représentants de l'industrie, du monde universitaire et de la justice. Pour répondre aux questions portant sur les utilisateurs dans chaque pays concerné par les études de cas, les chercheurs ont utilisé le contenu des recherches universitaires disponibles, des rapports sur les médias et les forums d'utilisateurs pertinents. Les résultats de ces questionnaires ont ensuite été analysés et distillés par les auteurs de l'étude qui ont collaboré avec les chercheurs pour clarifier et actualiser toutes les données jusqu'en juillet 2014.

2. LÉGISLATION ET RÉGLEMENTATION

Si les plates-formes et les services en ligne peuvent être utilisés pour servir des objectifs légitimes, notamment l'expression personnelle, l'éducation, l'emploi et le commerce, ils peuvent tout aussi bien être utilisés à des fins illégitimes : vol, fraude, harcèlement, violation du droit d'auteur et diffusion de propos diffamatoires, par exemple. La frontière qui sépare les pratiques légitimes et illégitimes dépend en grande partie des contextes politiques, religieux et culturels. À travers le monde, il y a donc de multiples conceptions de ce qui est légitime et de ce qui ne l'est pas. Reconnaissant ce phénomène, particulièrement en ce qui concerne les propos, la Déclaration universelle des droits de l'homme (DUDH), le Pacte international relatif aux droits civils et politiques et d'autres instruments internationaux concernant les droits de l'homme contiennent des dispositions permettant de limiter dans certains cas le droit à la liberté d'expression, tout en préservant l'essence de ce droit. Comme l'a souligné l'ancien Rapporteur spécial des Nations Unies Frank La Rue dans son rapport de 2011, de telles limitations ne sont compatibles avec les normes internationales sur les droits de l'homme que lorsqu'elles sont :

- fondées sur des règles, fixées par la loi et appliquées dans le respect des principes de transparence et de prévisibilité ;
- nécessaires et proportionnelles, en faisant appel aux moyens les moins restrictifs d'atteindre l'objectif recherché ;
- conformes aux objectifs énoncés dans le Pacte international relatif aux droits civils et politiques : nécessaires pour protéger la réputation ou les droits d'autrui ; la sécurité nationale ou l'ordre public ; la santé ou la moralité publiques.

En 2011, le Comité des droits de l'homme, dans son Observation générale n°34, affirme que les restrictions visant à protéger la morale « [doivent être interprétées] à la lumière de l'universalité des droits de l'homme et du principe de non-discrimination. » Les restrictions appliquées par les intermédiaires doivent être évaluées en fonction de ces normes internationales.

Bien que la responsabilité limitée et l'autorégulation soient la norme, il existe des exceptions dans lesquelles les intermédiaires sont tenus responsables des contenus créés par les utilisateurs que d'autres perçoivent comme étant contraires aux lois sur la vie privée et la diffamation, entre autres. Une décision rendue en 2015 par la Cour européenne des droits de l'homme dans l'affaire *Delfi* c. *Estonie*, portant sur des propos diffamatoires, a confirmé cette responsabilité et a estimé qu'un portail d'informations devait connaître ce qu'il contient en tout temps, et non pas seulement supprimer les contenus litigieux qui lui sont signalés. Les juges opposés à cette décision dans cette affaire ont affirmé que cette position n'était pas si différente d'une censure appliquée avant publication.

Dans les cas où une telle responsabilité incombe aux intermédiaires, ils sont obligés d'effectuer eux-mêmes des activités de filtrage et de surveillance, afin d'éviter d'éventuelles répercussions. Cela donne lieu à un processus de contrôle avant publication, qui peut conduire certains gouvernements à compter sur les entreprises du secteur privé pour réguler les contenus en ligne, sans que leur propre responsabilité ne soit engagée ou que les procédures soient respectées. D'un autre côté, une véritable autorégulation conforme aux normes internationales sur les droits de l'homme permet parfois de préserver la liberté d'expression et de respecter les critères précis encadrant les restrictions, tels que définis dans la DUDH et le Pacte international relatif aux droits civils et politiques.

2.1 ENGAGEMENTS DES ÉTATS ET LIMITATIONS DE L'EXPRESSION

Alors que la technologie utilisée, les modèles commerciaux et la portée des activités des intermédiaires de l'Internet ont radicalement évolué ces 20 dernières années, les objectifs réglementaires poursuivis par les États sont pratiquement inchangés, bien que les moyens employés pour y parvenir ne soient plus tout à fait les mêmes. Dans de nombreux cas, la conformité de la réglementation étatique avec les normes définies dans le Pacte international relatif aux droits civils et politiques fait débat, ainsi que la mise en œuvre de ces normes. Si les limitations appliquées sont conformes en termes de légitimité, elles ne correspondent pas toujours pleinement aux critères de nécessité, de proportionnalité et de respect de la procédure. La tendance dominante veut que les limitations sont outrepassées par la calomnie, la sécurité nationale et publique, les propos haineux, les élections, la protection de l'enfance, le blasphème et la propriété intellectuelle.

Même dans les cas où les limitations sont légitimes, la situation reste complexe sur plusieurs points. Si le droit au respect de la vie privée est établi, il n'est pas pour autant défini en détails, particulièrement à l'ère numérique. C'est pourquoi les limitations à la liberté d'expression visant à protéger la vie privée n'accordent pas suffisamment d'importance aux exceptions à mettre en place au nom de l'intérêt du public, qui donnent la priorité au droit à l'information. D'un autre côté, *l'Étude mondiale sur le respect de la vie privée sur l'Internet*, publiée par l'UNESCO en 2012, a démontré que les lois sur le respect de la vie privée offrant une trop faible protection avaient un effet négatif sur la liberté d'expression.

Autre exemple de la difficulté à trouver un équilibre, le cas des acteurs qui tentent de restreindre la liberté d'expression sous couvert de protéger la réputation de certains citoyens, en renvoyant à une conception particulière du respect de la vie privée. Cela à résonance particulière dans l'union européenne d'aujourd'hui, comme l'illustre l'affaire *Google Espagne c. AEPD* qui, en résumé, introduit le « droit à l'oubli », qui s'appuie lui-même sur « le droit de ne plus être référencé » dans les moteurs de recherche, et ce dans tous les pays de la zone. Comme cela sera évoqué dans la suite de ce chapitre, la décision rendue par la Cour européenne de justice en mai 2014 montre que la volonté d'une personne de faire disparaître des informations négatives à son sujet peut aller à l'encontre du droit d'autrui à recevoir de partager des informations. Des critiques comme

Jonathan Zittrain, professeur à Harvard, ont proposé le droit de réponse comme une alternative préférable pour équilibrer protection de la réputation et liberté d'expression.

Dernier cas de figure mettant en avant la complexité des situations : comment garantir le droit à la vie, à la liberté et à la sécurité d'un individu tout en préservant l'essence des droits au respect de la vie privée et à la liberté d'expression ? Cette question est au cœur des débats sur la surveillance numérique. En 2014, le Haut-Commissaire aux droits de l'homme des Nations Unies a appelé à réformer les lois sur la surveillance et s'est appuyé sur des recommandations de la société civile mondiale pour demander l'application des principes de nécessité et de proportionnalité, en insistant sur la responsabilité, la transparence et la réparation. Toutefois, une enquête menée par des experts dans 18 pays en 2014 a montré que ces lois n'ont été que très peu réformées. De fait, dans de nombreux pays, de nouvelles lois ont même renforcé les pouvoirs de l'État en termes de surveillance. Il est prouvé que la surveillance a un effet dissuasif sur la liberté d'expression dans un grand nombre de juridictions.

2.2 RESPONSABILITÉ DES INTERMÉDIAIRES

Comme cela a été signalé plus haut, la responsabilité juridique des intermédiaires est un aspect important du rôle qu'ils ont à jouer pour promouvoir la liberté d'expression : que se passe-t-il quand un individu utilise les services d'un intermédiaire pour publier, partager ou consulter un contenu qui enfreint les lois d'un pays donné ? Dans quelle mesure les intermédiaires peuvent ou doivent-ils être tenus juridiquement responsables des activités de leurs utilisateurs ? Voici les questions essentielles. Les dispositions juridiques prises pour y répondre définissent la manière dont les gouvernements attendent que les intermédiaires gèrent le contenu et les communications des tiers. Dans un grand nombre de juridictions, ces dispositions légales définissent des circonstances dans lesquelles les intermédiaires bénéficient d'une responsabilité limitée, en établissant des critères que ces intermédiaires doivent respecter pour éviter une sanction civile, voire pénale, pour les actions de leurs utilisateurs.

2.2.1 Les différents types de responsabilité des intermédiaires

Plusieurs états dans différentes régions du monde, dont l'Europe et l'Amérique du Nord, ainsi que dans certaines zones de l'Asie du Sud-Est et de l'Amérique latine, ont élaboré des lois spécifiques sur la question de la responsabilité des intermédiaires. Dans d'autres régions, et notamment en Afrique, des états envisagent désormais d'adopter des dispositions juridiques dans ce domaine. De manière générale, dans le pays où elles existent, on peut distinguer trois types de responsabilité aux intermédiaires : la responsabilité stricte, la responsabilité conditionnée et l'exemption presque totale de responsabilité. Les critères exacts et les nuances varient d'une juridiction à l'autre, les modèles de responsabilité sont définis par le gouvernement puis précisés par les tribunaux. Certains intermédiaires respectent explicitement les mandats qui leur sont

juridiquement accordés en termes de responsabilité, en prenant par exemple des mesures d'autorégulation garanties par le respect strict de leurs conditions de service.

- **Responsabilité stricte ou globale** : L'intermédiaire est responsable du contenu publié par des tiers, même lorsqu'il ne connaît pas le caractère illicite du contenu en question (ni même son existence). Le seul moyen d'éviter d'être tenu responsable dans de telles circonstances est de surveiller, de filtrer et de supprimer de manière proactive et avant la publication, s'il y a un risque que le contenu enfreigne la loi. En tous les cas, la surveillance et la suppression du contenu ne suffit pas à dégager l'intermédiaire de sa responsabilité si un contenu illicite passe au travers des contrôles. De tels régimes de responsabilité ne font pas de différence entre les intermédiaires, ils sont tous tenus pour responsables quelles que soient leur taille ou leur fonction.

- **Responsabilité conditionnée** : L'intermédiaire est potentiellement exempt de responsabilité sous certaines conditions – telles que la suppression du contenu après notification (système « d'avis et de retrait »), la notification du créateur du contenu illicite après avoir été informé de son existence (système « d'avis ») ou la suppression de la connexion des contrevenants récidivistes. Si un intermédiaire ne respecte pas ces critères, il peut avoir à rendre des comptes et à verser des dommages et intérêts. Contrairement au système de responsabilité stricte, celui-ci n'oblige pas les intermédiaires à contrôler et à filtrer en amont les contenus pour se dégager de toute responsabilité. Le système « d'avis et de retrait » a été critiqué car il est facile d'en abuser. En outre il encouragerait à l'autocensure en faisant de l'intermédiaire une sorte de juge chargé de déterminer si le contenu est licite ou non. Ce système est d'autant plus susceptible de faire l'objet d'abus lorsqu'il ne respecte pas certains éléments de procédure, comme la possibilité de faire appel de la décision de retrait. En effet, dans ce cas de figure, les intermédiaires sont incités à retirer le contenu immédiatement après qu'il a été signalé, plutôt que d'investir des ressources pour vérifier la validité de la demande et de risquer un procès. Par conséquent, des contenus licites peuvent être censurés.

- **Exemption presque totale de responsabilité** : Dans ce système, l'intermédiaire n'est pas responsable d'une variété de contenus créés par des tiers, quels que soient sa fonction ou le type de contenu.

Étant donné le rôle essentiel des intermédiaires – et des lois qui régissent leurs activités – pour la liberté d'expression en ligne, de plus en plus d'initiatives émergent au niveau international pour établir des principes communs et les meilleures pratiques à appliquer dans ce domaine. Par exemple, en décembre 2011, le Conseil de l'OCDE a inclus la limitation de la responsabilité des intermédiaires parmi les 14 Principes recommandés pour la prise de décisions politiques sur Internet, visant à « promouvoir et protéger partout dans le monde la libre circulation des informations en ligne ». Ces Principes soulignent aussi l'importance de la transparence, du respect des procédures, de la responsabilisation et de la prise de décisions inclusives et impliquant plusieurs parties prenantes. Un conseil consultatif ressemblant des groupes de la société civile a soutenu cette recommandation.

On constate de plus en plus que les systèmes de responsabilité des intermédiaires deviennent des mécanismes juridiques qui permettent aux gouvernements de transposer

sur Internet leurs propres interprétations des limitations de la liberté d'expression, même au-delà de leur juridiction nationale. En fonction des contextes nationaux, sociaux et historiques, les gouvernements restreignent plus ou moins tel ou tel type de contenu et les intermédiaires qui ne respectent pas les limites fixées risquent des sanctions pénales (emprisonnement), des sanctions civiles (amendes) ou la révocation de leur licence d'exploitation. Sur ce point, la difficulté tient au fait que les contenus, les auteurs et le siège de l'intermédiaire se trouvent dans des lieux différents.

2.2.2 Remarque spéciale : responsabilité des intermédiaires en Afrique

Bien que l'utilisation d'Internet se développe rapidement dans les pays en développement, il n'existe que peu de dispositions légales relatives à la responsabilité des intermédiaires en Afrique. Cette absence créé une incertitude réglementaire et procédurale. En 2014, un rapport de l'Association pour le progrès des communications (APC), une ONG internationale qui tient un rôle consultatif auprès du Conseil économique et social des Nations Unies, estimait que le manque de protection pour les intermédiaires dans les pays africains les pousse à restreindre de manière proactive les contenus de leurs réseaux et plates-formes, ce qui peut constituer une restriction indue de la liberté d'expression des utilisateurs.

Dans le même temps, de nombreux pays africains suivent la tendance émergente de concevoir des régimes de responsabilité ; d'une part en réponse aux approches des organismes internationaux et des principaux partenaires commerciaux et organismes d'aide, d'autre part pour protéger les droits de propriété intellectuelle et veiller à ce que les intermédiaires prennent des mesures contre les contenus non respectueux des droits d'auteur sur leurs réseaux et plates-formes. Des groupes de la société civile défenseurs de la liberté d'expression, comme l'APC, ont exprimé leur crainte de voir les autres pays sélectionner dans ces régimes de responsabilité des intermédiaires les éléments qui les intéressent pour mettre en place leurs propres régimes restrictifs et sélectifs. Étant donné que la surveillance, par les intermédiaires, des contenus potentiellement illégaux pourrait compromettre la liberté d'expression et la vie privée des internautes, il conviendra de mettre en œuvre des lois rigoureuses en matière de protection des données et de respect de la vie privée, pour veiller à ce que les régimes de responsabilité des intermédiaires ne servent pas à effectuer une surveillance ou un suivi arbitraire. En effet, si l'absence de régime de responsabilité des intermédiaires nuit à la liberté d'expression, la simple existence d'un tel régime ne garantit pas une meilleure protection des intermédiaires, ni de la liberté d'expression en ligne en général. De plus, les conditions de service des intermédiaires peuvent également ne pas être conformes aux normes régissant la liberté d'expression. La compétence des tribunaux et l'existence d'entités capables de défendre les normes internationales en matière de droit de l'homme en ligne sont essentielles pour assurer la protection des intermédiaires et de la liberté d'expression en ligne.

2.3 AUTORÉGULATION ET CORÉGULATION

Les lois ne sont pas les seules sources de restrictions des contenus en ligne : les règles internes des entreprises, par exemple leurs « conditions de service », peuvent également avoir un impact néfaste sur la liberté d'expression. En 2011, les quatre rapporteurs internationaux sur la liberté d'expression ont déclaré que « l'autorégulation peut être un moyen efficace de réparation pour des discours préjudiciables et elle doit être promue ». Dans certaines juridictions, les systèmes d'élaboration et d'application des lois relatives à la liberté d'expression en ligne combinent des éléments issus des autorités publiques et privées, résultant en des mécanismes d'autorégulation et de corégulation. La portée et le pouvoir de ces mécanismes sont à leur tour grandement modelés par les contextes juridiques et réglementaires des états. Les règlementations privées et publiques sont donc étroitement liées. La tendance dominante est l'engagement, dans une certaine mesure, des intermédiaires dans des actions d'autorégulation et d'application privées des règles. Les cadres constitutionnels, juridiques et réglementaires spécifiques d'une juridiction donnée, notamment son régime de responsabilité des intermédiaires, modèlent à leur tour la portée et la nature de l'autorégulation et de la corégulation. Dès 2003, l'autorégulation et la corégulation ont reçu un accueil favorable ; une déclaration du Conseil de l'Europe stipule en effet que les « États membres devraient encourager l'autorégulation ou la corégulation à l'égard des contenus diffusés sur l'Internet ». De tels systèmes ne doivent pas servir de censure, mais doivent respecter des critères et processus conformes aux normes internationales relatives à la liberté d'expression. De nombreuses options sont pour cela envisageables :

- **Autorégulation de l'entreprise** : Pour l'entreprise, il peut s'agir de prendre des mesures pour bloquer ou supprimer les spams et les virus, ou d'élaborer et d'appliquer des « conditions de service », des règles que les utilisateurs doivent accepter pour utiliser le service. Les conditions de service d'une entreprise peuvent être très proches de dispositions légales et réglementaires, alors qu'une autre entreprise peut choisir d'interdire certains contenus licites, mais jugés indésirables ou incompatibles avec le but ou la nature de ses services. Dans le cadre juridique d'au moins une juridiction, les entreprises du secteur privé sont normalement autorisées à établir leurs propres conditions sur ce qui constitue du contenu indésirable. Néanmoins, comme les plus grandes entreprises s'approchent dans les faits de la sphère publique, certains défenseurs soutiennent que celles-ci ont la responsabilité d'évaluer l'implication de leurs propres règles sur les droits de l'homme afin d'en minimiser l'impact négatif sur les droits des utilisateurs. Ces critères doivent être pris en considération lors de l'élaboration de leurs pratiques et politiques. Certains gouvernements encouragent activement les entreprises privées à s'autoréguler, l'alternative étant la mise en place de réglementations et de législations officielles, par nature moins flexibles et plus obtuses que les règlements privés.

- **Autorégulation collective** : Un groupe d'entités privées peut créer conjointement des codes de conduite pour son secteur ou définir des normes techniques communes auxquelles tous les membres devront se plier.

- **Corégulation**: Cette tendance est en train d'apparaitre comme une alternative aux mesures réglementaires traditionnelles, tout particulièrement dans les pays de l'Union européenne. La corégulation désigne un régime réglementaire impliquant une régulation privée activement encouragée ou même soutenue par l'État par le biais de législations, de financements ou d'autres moyens de soutien étatique ou de participation institutionnelle. Ce modèle permet de mieux responsabiliser les intermédiaires de l'Internet en ce qui concerne leurs décisions. Il peut cependant également coopter ces entreprises dans un rôle dans lequel leurs décisions suivent des normes qui ne satisfont pas les principes internationaux sur la limitation de l'expression libre et de la vie privée.

Les trois études de cas de ce chapitre examinent différents modèles d'autorégulation et de corégulation. Les défenseurs de l'autorégulation de l'industrie affirment qu'elle est préférable aux réglementations gouvernementales, car une telle coordination est plus flexible et plus efficace, décourage les comportements licites mais indésirables dans le contexte d'un service particulier, aide les consommateurs dans leur évaluation et leur choix d'un produit ou d'un service, et peut également diminuer les coûts. Mais d'autre part, des détracteurs soutiennent que les lacunes fréquentes de l'autorégulation en ce qui concerne la responsabilisation du public et les procédures officielles peuvent ne pas protéger les valeurs démocratiques et négliger les règles élémentaires de la justice.

2.4 INTRODUCTION DES ÉTUDES DE CAS

À la lumière de ces problématiques relatives aux contextes réglementaires et juridiques, les trois prochaines sections analysent les FSI, les moteurs de recherche et les réseaux sociaux, en examinant dans quelle mesure les droits des personnes sont respectés lorsque leur liberté d'expression dépend d'intermédiaires du secteur privé. Ces trois études de cas permettent d'illustrer en quoi la liberté d'expression des utilisateurs dépend de l'interaction entre les pratiques et politiques d'une entreprise, la politique gouvernementale et les problématiques juridictionnelles. Les questions clés abordées sont : *Dans quelles mesures les entreprises font-elles des efforts concertés pour respecter les droits des utilisateurs quand elles font face à des requêtes gouvernementales et des cadres juridiques qui ne respectent pas toujours les normes internationales relatives aux droits de l'homme ? Quel est l'impact des conditions de service privées sur la liberté d'expression ? Outre les limitations de contenus, dans quelle mesure les pratiques et politiques privées de protection des données des entreprises, combinées aux exigences de surveillance des gouvernements, affectent la capacité des personnes à s'exprimer librement ?*

Une meilleure compréhension de ces points par toutes les parties prenantes peut favoriser la liberté d'expression en ligne : en encourageant les gouvernements à élaborer des lois qui protègent les droits en ligne ainsi qu'en facilitant le respect des droits des utilisateurs par les intermédiaires ; en aidant les entreprises à améliorer leurs politiques et pratiques pour promouvoir la liberté d'expression par le biais de leurs services ; et en aidant la société civile à tenir pour responsables les gouvernements et les entreprises.

3. ÉTUDE 1 : FSI – VODAFONE, VIVO/TELEFÔNICA BRASIL, BHARTI AIRTEL ET SAFARICOM

3.1 INTRODUCTION

Les FSI permettent d'accéder à l'Internet par le biais de lignes fixes ou de connexions sans fil. Ils permettent la transmission de données dans les deux sens avec d'autres intermédiaires à travers leurs réseaux. Les FSI peuvent être publics, partiellement privatisés ou totalement privatisés. Bon nombre d'entre eux sont exploités par des entreprises dont l'activité de base portait sur les services de téléphonie mobiles ou traditionnels avant l'expansion des services Internet. Les entreprises agissant comme FSI peuvent également proposer d'autres services comme les appels vocaux, l'hébergement de sites, le cloud computing, l'enregistrement de noms de domaines, les e-mails ou d'autres services. Cette étude de cas se concentre sur les principales fonctions d'un FSI en tant que fournisseur d'accès à Internet par lignes fixes ou sans fil.

Comme l'énoncent les principes directeurs de l'organisation Industry Dialogue, les télécommunications peuvent améliorer l'ouverture et la transparence, et sont donc des outils pertinents pour les gouvernements en matière de protection de la sécurité publique. Les FSI jouent un rôle central dans la facilitation du droit à la liberté d'expression, étant donné que l'accès à Internet est un prérequis pour permettre la libre circulation de l'information à l'échelle mondiale. Ils font fonction de « gardes-barrières » sur Internet, grâce à leur accès direct aux transferts de données et de voix sur leurs réseaux et leur capacité technique de les restreindre. Les FSI ont également la capacité de collecter, de stocker et d'accéder aux données personnelles des utilisateurs, au contenu de leurs communications ainsi qu'à des métadonnées telles que l'adresse IP, les détails des appels passés et leurs localisations. Ils peuvent être soumis à des mandats juridiques, et même à des interférences extrajuridiques telles que des pressions informelles, pour donner accès à ces informations, et peuvent également être obligés par la justice de permettre un suivi et une surveillance des données en temps réel. Pour ces raisons, les rôles des FSI sur le réseau peuvent affecter la liberté d'expression des utilisateurs sur d'autres services intermédiaires, comme les moteurs de recherche ou les réseaux sociaux.

Le modèle économique des FSI nécessite généralement d'investir massivement dans des infrastructures physiques, de l'équipement et du personnel dans les juridictions où ils (ou les prestataires de communication) travaillent. Ainsi, leurs politiques et pratiques ayant un impact sur la liberté d'expression sont plus étroitement liées aux contextes juridiques et politiques d'une juridiction que celles de tout autre type d'intermédiaire comme les moteurs de recherche ou les plates-formes de réseaux en ligne, qui opèrent hors des juridictions de leur siège. Les FSI ont néanmoins le contrôle sur de nombreuses décisions

commerciales, politiques et pratiques de l'entreprise, qui ont un impact sur la liberté d'expression en ligne.

3.1.1 Les entreprises

Cette étude de cas se penche sur les FSI suivants :

- **Vivo Telecommunications**, aussi connu sous le nom de Telefônica Brasil, a été créé en 1993. En mai 2014, avec 79 millions de clients mobiles, Vivo est devenu la plus grande entreprise de télécommunication du Brésil. Elle propose des services mobiles, haut débit et par câble.
- **Bharti Airtel** est une entreprise multinationale de télécommunication fondée en 1995. Airtel propose des service sans fil, 2G, 3G et 4G, des services de commerce sur mobile, des services de lignes fixes, des lignes DSL haut débit, la télévision par Internet, des services directs à domicile ou dans l'entreprise, y compris des services longue distance nationaux ou internationaux vers des opérateurs de 20 pays. Airtel est le quatrième opérateur mobile du monde, avec plus de 200 millions d'abonnés.
- **Vodafone** est une entreprise multinationale de télécommunication fondée en 1991. Vodafone est le second plus grand prestataire de communication du monde avec plus de 430 millions de clients. Il opère dans 21 pays, et a formé de joints ventures avec d'autres entreprises, par exemple Safaricom au Kenya, entreprises qu'il appelle ses « opérateurs locaux associés ».
- **Safaricom** est le plus grand opérateur mobile du Kenya, avec 21 millions d'abonnés. Selon Bloomberg Industries, en mars 2014 Safaricom représentait 67 % du marché des téléphones portables dans le pays, ainsi que 79 % du trafic téléphonique et 96 % des SMS. Safaricom est détenu à 40 % par Vodafone, à 35 % par le gouvernement du Kenya et les parts restantes ont été mises sur le marché public à la bourse de Nairobi en juin 2008.

Ci-dessous, un résumé des principales conclusions de cette étude de cas, mettant en valeur les principales problématiques relatives aux expériences de ces entreprises.

3.2 RESTRICTION DIRECTE DE LA LIBERTÉ D'EXPRESSION

Les restrictions réalisées par les FSI se font au niveau du réseau ; elles empêchent ou restreignent l'accès d'un individu à Internet ou à du contenu en ligne, aux opportunités d'expression et aux services proposés par d'autres types d'intermédiaires. Les restrictions au niveau du réseau réalisées par les FSI affectent la nature et la portée des restrictions réalisées par d'autres intermédiaires.

3.2.1 Filtrage au niveau du réseau

Les filtres sont des programmes spécialisés qui peuvent restreindre l'accès à des sites Internet, à des services en ligne, à des pages spécifiques ou à des contenus sur des sites Internet, ou encore à des sites contenant certains mots-clés. Les filtrages demandés par les gouvernements sont habituellement réalisés par les FSI, et peuvent être une condition sine qua non à l'implantation d'une entreprise dans une juridiction. L'État peut également installer des dispositifs centralisés de filtrage aux points d'échange Internet, qui font office de passerelles entre les différentes juridictions et avec les réseaux exploités par différents FSI. Les institutions privées ou locales comme les écoles ou les bibliothèques peuvent placer des filtres dans leur propre réseau local pour interdire l'accès à certains contenus. Des filtres peuvent également être installés au sein même des foyers, la plupart du temps par des parents souhaitant contrôler les contenus visibles par leurs enfants. Compte tenu de la disponibilité de filtres logiciels que les parents peuvent contrôler pour sécuriser leur propre réseau domestique, les experts internationaux se demandent pourquoi les FSI devraient être légalement tenus de filtrer les contenus. Dans le cas de certains types de contenus, comme les discours de haine, l'éducation des utilisateurs aux médias et à l'information et l'autorégulation sont parfois considérés comme plus propices au respect de la liberté d'expression que les règlementations directes ou la voie juridique. Néanmoins, la délégation de trop de pouvoirs répressifs à des intermédiaires privés pose problème. Les paragraphes suivants se concentrent sur les filtrages réalisés par les FSI à la demande des gouvernements ainsi que sur les filtrages mis en place par les FSI pour assurer le respect de leurs propres règles ou pour participer à l'autorégulation ou à la corégulation collective du secteur.

En fonction du contexte juridique, les FSI peuvent recevoir des demandes, recommandations et ordres de filtrage de la part des gouvernements, tierces parties privées et/ou organismes de régulation. De tels ordres peuvent être formulés au cas par cas et communiqués directement au FSI, ou bien prendre la forme d'une « liste noire » générale. Les FSI de certaines juridictions peuvent prendre des mesures autorégulatrices ou corégulatrices, notamment en filtrant des contenus selon les normes de l'entreprise, ainsi qu'en collaborant avec les hotlines, les organismes industriels ou de réglementation pour identifier le contenu contrevenant. Les FSI peuvent proposer aux utilisateurs individuels d'appliquer des filtres aux réseaux de leur domicile ou de leur bureau. La liberté d'expression peut être affectée par les raisons du filtrage et la mise en œuvre pratique de celui-ci ainsi que par la transparence du gouvernement et des entreprises sur les raisons du filtrage et la manière dont il est mis en place. La plupart des entreprises intègrent à leurs conditions de services des types de contenus et d'activités prohibés sur leurs réseaux. Les détails varient, mais la tendance majeure est à l'utilisation de conditions au sens large, qui permettent d'englober de nombreuses formes de contenus interdits.

Les FSI filtrent une large gamme de types de contenus dans le cadre de demandes externes, afin de respecter les lois et leurs propres conditions de service. Dans les pays concernés par cette étude de cas, les types habituels de contenus filtrés par les FSI à la demande des gouvernements ou de mandats juridiques incluent ce qui touche aux contenus non respectueux des droits d'auteur, à la pornographie, aux images d'enfants maltraités, à la diffamation, aux discours de haine, aux interventions en lien à des élections

et aux documents sensibles pour la sécurité nationale. En général, les accords de licence et les lois limitent largement les capacités des FSI de ne pas accéder aux demandes de filtrage du gouvernement. Cela inclut les décisions suivantes : 1) faut-il répondre ou non à la requête ; 2) quel type d'avis public et d'explication de la restriction choisir, et 3) faut-il retirer les filtres sur certains contenus et si oui, quand. L'imprécision des lois ou leur application irrégulière peuvent entrainer des incohérences dans le filtrage au sein d'un pays, comme le filtrage de sites Internet entiers plutôt que du contenu contrevenant spécifique au sein des sites, contredisant ainsi les principes de proportionnalité et de nécessité. La portée excessive du filtrage est également connue sous le nom de « filtrage collatéral », à cause des dommages collatéraux qu'il peut provoquer sur la liberté d'expression.

Les efforts d'autorégulation et de corégulation impliquant des FSI varient grandement en fonction du contexte national. Les mesures autorégulatrices, sous forme de filtres adaptés à la famille mis à la disposition des utilisateurs par les FSI, risquent de placer le prestataire de service dans un rôle qui tient à la fois du juge, du jury, et du policier : le FSI est responsable du choix des critères à inclure au filtre, de sa mise en place et du traitement des plaintes relatives aux sites Internet mal catégorisés. Parfois, les mesures entreprises sous forme de principes autorégulateurs peuvent devenir par la suite des règlements ou être formalisées dans la législation.

ENCADRÉ : Tendance émergente : « le filtrage en amont »

La pratique du « filtrage en amont » par les FSI peut nuire à la liberté d'expression. Lorsque les entreprises commencent à appliquer un filtre dans une juridiction, d'autres juridictions dans lesquelles opère le prestataire peuvent également être affectées par ces pratiques. Le filtrage en amont désigne les répercussions d'un filtre (ou d'autres composants techniques) en place sur le réseau d'un FSI sur un autre réseau. Un contenu considéré comme illicite et donc restreint dans une juridiction peut ainsi être également restreint dans une autre juridiction, où il pourrait être licite.

3.2.2 Arrêts et restrictions de service

Les gouvernements peuvent parfois demander des arrêts du réseau ou des restrictions de service Internet au niveau national ou régional, en invoquant des raisons relatives à la prévention du terrorisme, l'ordre public ou la prévention du désordre public. La restriction peut affecter l'intégralité du réseau ou un service spécifique. Dans de nombreuses juridictions, les FSI doivent respecter ces requêtes sous peine de poursuites judiciaires. Ils peuvent également restreindre ou empêcher l'accès au réseau ou à un service pour cause d'entretien ou de problème technique. L'interruption d'un réseau entier ou la restriction d'un service dans une grande zone est une disposition d'ordre générale qui impacte tous les contenus, au risque de ne pas respecter les principes de nécessité et de proportionnalité, reconnus internationalement. Des mesures plus ciblées peuvent également être prises, comme un ordre du gouvernement ou du FSI de couper ou de suspendre l'accès d'un utilisateur individuel à Internet ou aux services mobiles.

Les entreprises de télécommunication mobiles reçoivent également des ordres des gouvernements leur demandant d'envoyer des messages par le biais de leurs réseaux, ce qui peut nuire à la liberté d'expression, notamment si le message n'est pas envoyé au nom du gouvernement, car de telles mesures, bien qu'elles ne limitent pas l'information, « forcent » au contraire la transmission d'informations aux utilisateurs.

Les FSI ne restreignent généralement l'utilisation de leurs réseaux dans son ensemble qu'en cas de maintenance ou pour des raisons échappant à leur contrôle, mais ils ont fréquemment à couper ou à suspendre les comptes de certains utilisateurs. Les circonstances dans lesquels le service ou le réseau peut être affecté par les politiques des entreprises diffèrent. Tous les FSI se réservent le droit de couper, de suspendre ou de ralentir les services en cas d'abus de leurs services ou de non-respect des Conditions générales de l'entreprise. Les FSI doivent prendre des décisions difficiles en ce qui concerne les demandes externes et la communication en la matière avec le public.

3.2.3 Neutralité du réseau

La « neutralité du réseau » est le principe selon lequel les FSI doivent traiter toutes les données de manière équitable et ne donner la priorité à aucun service ni à aucune donnée, quelle qu'en soit la raison, y compris politique ou commerciale. La neutralité du réseau est importante pour la liberté d'expression, car elle préserve le droit et le choix d'un individu d'accéder à un contenu web, à des applications, à des services ou à des ressources matérielles. Les FSI ont accès à des technologies qui leur permettent d'analyser, de bloquer ou de ralentir certains contenus ou services. Ces pratiques – qui découlent de raisons économiques, de restrictions de contenu ou de volontés de réguler la bande passante – peuvent menacer la neutralité du réseau. Les spécialistes recommandent une plus grande transparence des entreprises sur la manière dont leurs services haut débit fonctionnent, sur les types d'activités de gestion réseau auxquels ils participent et sur la mesure dans laquelle ces activités peuvent impacter les consommateurs. D'une juridiction à l'autre, les gouvernements et régulateurs peinent à comprendre si la neutralité du réseau doit être protégée par la loi, comment mettre en place cette protection et quelles responsabilités doivent assumer les entreprises en la matière. Malgré une tendance émergente des juridictions à proposer des législations à ce sujet, il existe toujours à l'heure actuelle des lacunes en matière de réglementation sur la neutralité du réseau. Par conséquent, les pratiques varient grandement selon les entreprises. Une controverse est née des cas où un certain service ou un ensemble de contenu est « fourni gratuitement », au sens où les coûts de connexions ont été supprimés, par exemple l'initiative Internet.org de Facebook. L'argument en faveur d'une telle option est que fournir un accès gratuit à une partie (subventionnée) d'Internet est toujours mieux que de n'avoir aucun accès. Quoi qu'il en soit, il convient de prendre en considération certaines problématiques liées à la liberté d'expression et au droit à l'information.

3.3 VIE PRIVÉE

Les FSI ont accès à un large panel d'informations au sujet de leurs abonnés, y compris les métadonnées et le contenu de leurs communications. Selon le Rapport de 2014 du Haut-Commissaire des Nations Unies aux droits de l'homme sur le droit à la vie privée à l'ère du numérique, les FSI « devraient adopter une déclaration de principe dans laquelle [ils] s'engagent à respecter les droits de l'homme dans le cadre de toutes leurs activités » et devraient également « avoir en place des politiques de diligence raisonnable appropriées pour identifier, évaluer, prévenir et atténuer toute incidence néfaste ». Le rapport estime en outre que « la possibilité qu'une information relative à des communications soit interceptée constitue même à elle seule une immixtion dans la vie privée et peut être attentatoire à des droits, y compris ceux relatifs à la liberté d'expression et d'association ».

Seules quelques entreprises parmi celles étudiées dans cette étude de cas ont publié des Politiques de confidentialité applicables aux services dédiés proposés localement, ou expliquant clairement et de manière exhaustive quelles données personnelles ils collectent, et ce qu'ils en font. Malgré l'existence, dans de nombreuses juridictions, de mandats juridiques définissant la période pendant laquelle les données peuvent être conservées, les entreprises étudiées ne précisent pas dans leurs conditions de service ou leurs politiques de confidentialité la durée exacte de conservation des données. Dans la plupart des pays étudiés, des exigences légales obligent les utilisateurs à présenter un moyen d'identification remis par le gouvernement lors de l'inscription aux services. Ces exigences s'appliquent habituellement aussi bien aux services prépayés que post-payés et sont à distinguer des demandes d'informations personnelles faites par les FSI pour réaliser des transactions commerciales. Certaines juridictions obligent légalement les FSI à vérifier ces informations avant de fournir le service à l'utilisateur. Cela réduit énormément la capacité de participation anonyme en ligne, le comportement en ligne de l'utilisateur pouvant être relié à son identité réelle sans que la protection de la vie privée garantie par les normes internationales en matière de limitation légitime des droits ne soit appliquée.

3.4 TRANSPARENCE

Dans son rapport de 2012 *Des lignes ouvertes : un appel à la transparence des gouvernements et des entreprises du secteur des télécommunications*, le Global Network Initiative recommande que les FSI et les gouvernements soient transparents en ce qui concerne les lois et les licences d'exploitation, les demandes de filtrage des gouvernements et les demandes gouvernementales de récupération des SMS envoyés via le réseau du FSI. La transparence sur les lois, politiques, pratiques, décisions, raisons et conséquences qui concernent la vie privée et les restrictions de la liberté d'expression permet aux utilisateurs d'agir et de s'exprimer en ligne de manière éclairée. La transparence est en outre importante pour permettre aux utilisateurs d'appliquer leurs droits au respect de la vie privée et à la liberté d'expression.

La pratique et la portée de la transparence des gouvernements et des entreprises en ce qui concerne les pratiques de surveillance, de filtrage et de restriction de services varient

en fonction des juridictions. Dans aucun des pays étudiés les FSI ne sont légalement obligés d'être transparents sur leurs politiques ou pratiques de filtrage, de restriction de service et de surveillance. La capacité des FSI et des services de télécommunication à être transparents vis-à-vis des clients et des consommateurs dépend énormément de la transparence des gouvernements et de l'existence de cadres juridiques permettant un niveau adéquat de transparence de la part des entreprises. Dans les juridictions étudiées, les gouvernements font preuve de peu de transparence en ce qui concerne la nature et la quantité des requêtes officielles de filtrage et de restriction de service faites aux FSI. Les gouvernements de donnent pas une vue d'ensemble ou des statistiques officielles sur le nombre et le type d'ordres de restriction formulés. Parfois les gouvernements reconnaissent les restrictions ou répondent aux accusations de restriction dans les médias, ou aux demandes d'autres branches du gouvernement, bien que ces cas de figure ne soient ni classiques ni réguliers. La tendance prédominante des FSI ici étudiés est le manque de transparence sur l'étendue des filtrages, sur les politiques de filtrage ou sur les exigences légales du filtrage. Certaines lois n'empêchent pas explicitement les FSI de divulguer des informations sur la surveillance et le filtrage, mais quand elles sont interrogées à ce sujet, les autorités ont fait des déclarations qui contredisent la réalité des pratiques existantes.

3.5 RÉPARATION

Les FSI des juridictions étudiées dans cette recherche peuvent proposer réparation à un utilisateur individuel ou un groupe entier d'utilisateur dont le droit à la liberté d'expression a été violé. Le processus peut comprendre une enquête, un rapport public/une explication, le rétablissement du contenu ou de la connexion, ou la mise en place de moyens alternatifs par lesquels les utilisateurs peuvent s'exprimer. Il est donc possible pour les cours ou les tribunaux, les entreprises et les organismes de réglementation d'accorder des réparations. La forme de réparation disponible pour l'utilisateur dépend des juridictions de l'entreprise et de l'utilisateur. Des mécanismes de plainte et de résolution des litiges peuvent éventuellement compléter les systèmes de réparation et de recours fournis par le gouvernement (ou servir d'alternative). Certains gouvernements demandent que les entreprises mettent en place des mécanismes de réclamation et de recours privés, car obtenir réparation auprès d'un tribunal peut être à la fois couteux et long dans certains pays. Il n'existe que peu de recherches internationales sur les meilleures pratiques des organismes de protection des consommateurs pour les affaires qui touchent aux télécommunications.

3.6 CONCLUSIONS

Les FSI jouent un rôle fondamental dans la connexion des utilisateurs à cette mine de connaissances, d'opportunités et de possibilités d'expression qu'est l'Internet. Cependant, certains utilisateurs affirment que les entreprises ne protègent pas assez la

liberté d'expression. Des entreprises comme Vodafone ont fait remarquer que certaines requêtes gouvernementales représentent de grands risques pour la sécurité de leurs employés locaux ou pour leurs intérêts commerciaux. D'autre part, le respect de ces requêtes peut également ébranler la confiance que les utilisateurs leur prêtent.

Plusieurs observations générales peuvent être tirées des conclusions de cette étude de cas :

- ***Les gouvernements et les entreprises ne sont que peu, ou pas du tout, transparents en ce qui concerne les restrictions de l'expression faites par et à travers les FSI.*** Le manque grave de transparence des gouvernements et entreprises, dans de nombreuses juridictions, sur les aspects fondamentaux des pratiques de filtrage est une tendance dominante. Suite aux révélations faites en 2013 par Edward Snowden, des dialogues publics et des initiatives de recherche se sont concentrés sur la transparence en matière de vie privée et de requêtes de surveillance, mais sans accorder beaucoup d'importance aux pratiques qui affectent directement la liberté d'expression des utilisateurs.

- ***En ce qui concerne la surveillance, la transparence des gouvernements est limitée, et seules quelques entreprises se font les porte-parole de leurs utilisateurs.*** Deux pays diffusent publiquement des rapports annuels sur l'étendue de la surveillance gouvernementale. Vodafone publie des lignes directrices claires sur ses politiques en matière de gestion des requêtes gouvernementales de données personnelles, mais les abonnés aux autres services restent dans le noir le plus complet en ce qui concerne la manière dont leurs données sont protégées des gouvernements et d'autres types de pressions. Cette incertitude est amplifiée par le manque d'informations sur les requêtes gouvernementales de données personnelles. En 2014, Vodafone était la seule entreprise à communiquer sur la quantité de demandes de données reçues de la part d'agences gouvernementales. Bien qu'une quantité significative de demandes soit adressée, aucune statistique n'est disponible sur le nombre de requêtes auxquelles les entreprises ont répondu. Vodafone est également la seule entreprise étudiée ici à demander ouvertement aux gouvernements d'être plus transparents et d'entreprendre des réformes juridiques qui permettraient à l'entreprise de communiquer plus d'informations sur les demandes de surveillance et de données personnelles.

- ***Les pratiques des entreprises en matière de protection des données et de respect de la vie privée varient grandement en fonction des lois existantes sur la protection des données***, qui sont en constante évolution dans tous les pays du monde. La tendance majeure est à l'affaiblissement des lois sur le respect de la vie privée et à un affaiblissement parallèle des politiques des FSI en la matière. Dans les pays où la législation est faible ou naissante, les FSI transmettent beaucoup moins d'informations sur leurs pratiques en matière de respect de la vie privée.

- ***Il est difficile pour les individus de tenir les entreprises ou les gouvernements responsables des actions réalisées par le biais des FSI qui restreignent la liberté d'expression des utilisateurs d'une manière incompatible avec les normes internationales relatives aux droits de l'homme.*** Dans certaines juridictions, des

organismes de règlementation du secteur peuvent proposer des moyens par lesquels les utilisateurs peuvent signaler des contenus illicites ou des pratiques de FSI qui violent leurs droits. Néanmoins, les réparations de ces violations de la liberté d'expression en ligne des utilisateurs par les FSI ou les agences gouvernementales se limitent à des amendes, ce qui prouve bien que la reconnaissance et les conséquences de ces violations ne sont que limitées.

- ***L'engagement public de certaines entreprises à respecter les principes internationaux en matière de droit de l'homme est une première étape importante, mais il reste encore beaucoup de chemin à parcourir.*** Comme indiqué précédemment, en 2013 un groupe de vendeurs et d'opérateurs de télécommunication, dont des FSI, ont lancé l'association « Telecommunications Industry Dialogue » sur la liberté d'expression et la vie privée et proposé un ensemble de « principes directeurs » inspirés des Principes directeurs des Nations Unies relatifs aux entreprises et aux droits de l'homme. Vodafone et Telefónica font partie des 9 membres de l'association, et leurs rapports 2014 sont décrits sur le site de l'association comme un résultat de l'engagement des entreprises à proposer des rapports annuels sur les « progrès dans la mise en œuvre des principes directeurs et, le cas échéant, des principaux évènements dans ce domaine ».

Industry Dialogue a dit s'engager dans une étude collective des meilleures pratiques en matière de transparence des entreprises dans leur secteur, ainsi que sur « la manière de mettre en œuvre des mécanismes de réclamation au niveau opérationnel ». Ses membres ont également agi collectivement pour collaborer avec les gouvernements. Comme le stipulent son premier rapport annuel, Industry Dialogue est de « continuer à plaider en faveur d'une plus grande transparence des gouvernements sur l'utilisation et l'étendue de la surveillance des communications et sur les mesures qui ont pour effet de réduire le contenu des communications, conformément à nos Principes ». L'impact concret de ces activités et engagements sur les internautes doit maintenant être étudié de manière systématique. Néanmoins, les activités réalisées par les membres d'Industry Dialogue à ce jour indiquent que ces actions collectives, combinées avec un plus grand engagement des parties prenantes, ont permis aux FSI de prendre des mesures qu'ils ne voulaient pas prendre de leur propre chef. Industry Dialogue n'a pas encore reconnu qu'elle gagnerait en crédibilité en mettant en place un processus de vérification du respect des engagements des entreprises, par exemple par le biais d'une évaluation externe réalisée par GNI.

4. ÉTUDE 2 : MOTEURS DE RECHERCHE – GOOGLE, BAIDU ET YANDEX

4.1 INTRODUCTION

Les **moteurs de recherche** sont le principal moyen par lequel les internautes trouvent des informations. Ils sont importants pour la liberté d'expression, car ils font office d'intermédiaires entre les personnes cherchant des informations et les personnes publiant des informations en ligne. La plupart des pages web ne sont pas indexées par les moteurs de recherche et ne peuvent donc pas être trouvées par leur biais. Même Google, le plus grand et plus populaire moteur de recherche du monde, n'a indexé qu'un faible pourcentage des pages web du monde. Il existe à cela trois principales raisons : a) les pages web n'ont pas encore été trouvées ou ne peuvent pas être trouvée par les robots d'indexation, car aucun autre site Internet ne pointe vers elles ; b) elles sont « invisibles » pour les robots d'indexation, car le propriétaire des pages web ou de la base de données a choisi de les bloquer ; c) la structure de la base de données derrière la plupart des sites Internet « cache » les pages au regard des robots d'indexation.

Tous les moteurs de recherche utilisent leur propre algorithme de recherche, une formule mathématique complexe qui décide quel résultat afficher, et dans quel ordre, en réponse à la requête spécifique de l'utilisateur. La décision de l'algorithme au sujet de ce qui est important ou non pour la personne effectuant la requête dépend en partie des informations contenues dans l'URL, l'en-tête, et d'autres parties de la page web. Les personnes souhaitant que leurs contenus soient diffusés auprès du maximum de personnes peuvent « optimiser » leurs sites Internet, par exemple en déclinant une version du site propre à chaque appareil mobile, augmentant ainsi les chances que leur page apparaisse parmi les premiers résultats du moteur de recherche. Deux moteurs de recherche ne proposeront jamais les mêmes résultats à la même requête, à moins que leurs algorithmes, robots d'indexation et index soient identiques.

En ce qui concerne les moteurs de recherche, la liberté d'expression implique trois parties potentielles : 1) l'utilisateur individuel qui effectue la recherche ; 2) les créateurs et les administrateurs des sites Internet indexés, ou potentiellement indexés, par les moteurs de recherche ; 3) le moteur de recherche en lui-même, dont les algorithmes sont considérés par les spécialistes et quelques jurisprudences comme une sorte de processus éditorial, bien que de manière beaucoup moins directe que dans le cas d'un organe de presse. Cette section examine en quoi les juridictions, et dans une certaine mesure les lois et règlements des autres juridictions, modèlent les politiques des moteurs de recherche et les pratiques en matière de restriction et de manipulation de contenus. Elle examine également comment trois entreprises différentes installées dans trois contextes nationaux différents ont géré les problèmes relatifs à la liberté d'expression en ligne.

Les entreprises

Cette section se concentre sur trois moteurs de recherche, détenus par des entreprises qui proposent également d'autres services :

Baidu est le numéro 1 chinois, avec entre 60 et 70 % de part de marché sur la plus grande base d'internautes du monde (plus de 600 millions).

Yandex détient plus de 60 % de la part de marché en Russie, pays qui compte 84,4 millions d'internautes.

Google est le moteur de recherche le plus utilisé au monde. Sa part de marché aux États-Unis (qui compte environ 280 millions d'internautes) est de 67,5 %. La part de marché de Google est bien supérieure là où il n'y a pas de concurrent local majeur, comme en Inde (97 %) ou en Europe (90 %). La part de marché de Google en Russie est d'environ 25 % et elle est inférieure à 2 % en Chine.

Les principaux points émergeant de cette étude de cas sont présentés ci-dessous.

4.2 IMPACT DU FILTRAGE RÉSEAU SUR LES MOTEURS DE RECHERCHE

La liberté d'expression des utilisateurs de moteurs de recherche peut être affectée par le filtrage des moteurs de recherche par les FSI. Si la page d'accueil d'un moteur de recherche est filtrée, le service est indisponible dans son intégralité pour les utilisateurs y accédant depuis ce FSI ou le réseau national filtré. Il est également possible pour le FSI de filtrer uniquement certaines URL ou certains mots-clés des résultats du moteur de recherche, ce qui rend le service partiellement utilisable – tant que l'utilisateur ne cherche pas du contenu filtré par le FSI.

L'exploitant du moteur de recherche ne joue habituellement aucun rôle et n'a aucun contrôle sur le filtrage par les FSI. Néanmoins, la nature et l'étendue du filtrage par FSI dans une juridiction donnée influencent la manière dont les moteurs de recherche mettent en place leurs propres restrictions. Ainsi, avant de discuter des politiques, pratiques et mises en œuvre des restrictions par ces trois moteurs de recherche, il est nécessaire de décrire l'étendue et la nature du filtrage des moteurs de recherche par les FSI dans chaque pays concerné par cette étude de cas. Dans les quatre juridictions étudiées, quatre approches différentes du filtrage par les FAI ont été identifiées :

- Aucun filtrage des moteurs de recherche
- Filtrage des sites Internet, mais pas des moteurs de recherche
- Filtrage limité des moteurs de recherche
- Filtrage intensif des moteurs de recherche à caractère international avec déconnexion temporaire pour en décourager l'utilisation

4.3 MESURES PRISES PAR LES MOTEURS DE RECHERCHE

Le cadre légal appliqué dans la juridiction du siège des entreprises modèle leurs politiques et pratiques en matière de restriction de contenu. Dans toutes les juridictions, les exploitants d'un moteur de recherche peuvent restreindre ou manipuler les contenus par l'une ou l'ensemble des actions suivantes :

1. Retirer certaines pages spécifiques ou même des sites Internet entiers des index des moteurs de recherche ;
2. Programmer le robot d'indexation pour qu'il n'ajoute pas certaines pages, sites, ou sites contenant certains contenus ;
3. Programmer l'algorithme du moteur de recherche pour qu'il ne renvoie pas de résultat à certaines requêtes ;
4. Programmer l'algorithme pour qu'il donne plus de poids à certains types de pages web par rapport à d'autres ;
5. Influencer la compréhension des utilisateurs de certains résultats de recherche en ajoutant des notes explicatives, avertissements ou déclarations.

Tout comme pour les prestataires de service analysés dans la précédente étude de cas, les moteurs de recherche peuvent restreindre le contenu à la demande des autorités gouvernementales ou d'autres parties externes, ou restreindre des contenus pour respecter leurs propres conditions de services ou toute autre règle ou procédure privée.

4.3.1 Personnalisation

En 2005, Google a commencé à adapter les résultats des recherches de tous les utilisateurs enregistrés en fonction de leurs préférences et intérêts personnels probables, déduits à partir de leurs précédentes recherches. En 2009, la personnalisation a été étendue à toutes les recherches Google, même si l'utilisateur n'est pas connecté, en fonction des cookies de son navigateur Internet. L'effet de cette personnalisation sur la liberté d'expression a fait naître des inquiétudes, car celle-ci rend un même site Internet plus ou moins visible selon les utilisateurs en fonction de leurs habitudes de navigation. L'ensemble des répercussions de la personnalisation sur la liberté d'expression reste flou. Certaines personnes avancent que le problème est moins le degré de personnalisation que l'étendue dans laquelle l'utilisateur est capable de comprendre et de contrôler les facteurs jouant un rôle dans ses propres recherches. Une étude universitaire récente sur les recherches Google a découvert que la personnalisation varie grandement en fonction des requêtes, et qu'elle est bien plus difficile à mesurer lorsque l'utilisateur est déconnecté. Des systèmes de personnalisation existent également chez Baidu et Yandex.

4.3.2 L'Europe et le « droit à l'oubli »

Même lorsqu'ils évoluent dans des environnements où la liberté d'expression est correctement protégée, les moteurs de recherche ne sont pas des arbitres entièrement neutres de l'information. Des ajustements de l'algorithme de recherche sont réalisés au niveau mondial en vue de protéger les utilisateurs des spams, malwares et vols d'identité, pour protéger les enfants de l'exploitation sexuelle, et pour respecter les lois relatives à la propriété intellectuelle. De nombreux autres ajustements sont réalisés pour répondre à des demandes privées ou gouvernementales dans certaines juridictions spécifiques. Les moteurs de recherche font également face à d'autres défis en Europe – et potentiellement dans le reste du monde – avec la décision judiciaire mettant en place le « droit à l'oubli » dans l'Union européenne.

Un rapport de 2012 de l'UNESCO a souligné les tensions inhérentes entre le respect de la vie privée et la liberté d'expression. L'une des nombreuses tensions potentielles concerne la volonté d'un individu de faire disparaître d'Internet des informations négatives à son sujet et le droit d'autrui de recevoir et de diffuser des informations. Le 13 mai 2014, la Cour de justice de l'Union européenne a statué dans l'affaire *Google Espagne c. AEPD* intentée contre Google par un Espagnol estimant que la présence d'une annonce de vente aux enchères de sa maison saisie constituait une violation de son droit à la vie privée. Selon la décision de la Cour, les internautes européens ont maintenant le droit de demander aux moteurs de recherche de retirer des liens les concernant si tant est « qu'elles sont inadéquates, non pertinentes ou excessives au regard des finalités du traitement ». De plus, le droit à la vie privée prévaut, « en règle générale » sur l'intérêt des internautes potentiellement intéressés par l'information. Mais l'intérêt du public peut parfois être prépondérant, par exemple dans le cas des personnalités publiques.

Cette décision a été vivement critiquée par des groupes de défense de la liberté d'expression, notamment ARTICLE 19, le Comité pour la protection des journalistes et Index on Censorship, qui ont déclaré qu'une protection excessive de la vie privée pourrait empiéter sur la liberté de la presse. Cette position coïncide avec celle qui estime que la liberté de la presse représente le droit à la libre expression pour communiquer avec le grand public, et que, bien que la suppression de liens vers des contenus ne viole pas en soi l'expression originale, elle diminue de beaucoup l'intérêt même de publier des informations à l'ère numérique. D'autres défenseurs des droits numériques ont estimé que les médias et la communauté de défenseurs de la libre expression ont réagi de manière excessive, en soulignant que Google n'a pas supprimé de données, mais uniquement bloqué les liens dans ses résultats de recherche. De plus, Google a accordé une grande attention à la confidentialité en répondant aux requêtes individuelles, et n'est pas tenu de supprimer du contenu avant le jugement d'un tribunal.

Fin mai 2014, Google a mis en place un cadre rudimentaire lui permettant de respecter ce jugement, et de se protéger contre les affaires qui y font référence. Une page web a donc été créée, pour permettre aux utilisateurs européens de demander à ce que leur nom n'apparaisse pas dans certains résultats de recherche. Le retrait n'est alors effectif que sur les sites Google de l'Union européenne, mais l'information reste visible sur la page mondiale du moteur de recherche, Google.com. De plus, les pages de résultats intègrent une notification du retrait.

En tant que membre de Global Network Initiative, Google a dû concilier le respect de la décision de la Cour avec son engagement auprès de GNI d'être transparent sur la manière dont le contenu est restreint, ainsi que d'interpréter les demandes officielles relatives aux restrictions de contenu de la manière la plus précise possible. Le 11 juillet 2014, Google a annoncé avoir reçu 70 000 demandes de restriction concernant 250 000 sites Internet depuis la mi-mai. Les demandes ont été analysées à la main, et l'entreprise a également mis en place une politique de notification des sites Internet lorsqu'un lien vers une de leur page est supprimé. Le journal *The Guardian* a été l'un des premiers organismes à recevoir des notifications indiquant que des liens vers ses articles avaient été retirés des résultats de recherche en Union européenne. Le fondateur de Wikipedia, Jimmy Wales, a qualifié le processus de « censure », après que son organisation a reçu des notifications de suppression de lien vers des contenus Wikipédia à la demande des personnes sur lesquelles ils portaient.

Google a également mis en place un conseil consultatif dont le rôle est d'étudier la meilleure manière d'équilibrer vie privée et liberté d'expression. David Drummond, Vice-président et Directeur juridique de Google, a déclaré que certaines requêtes étaient clairement illégitimes, comme celles de politiques cherchant à faire disparaitre des écarts passés, mais que bon nombre d'entre elles étaient vues d'un œil favorable. Pendant le troisième trimestre 2014, l'entreprise a organisé des sessions de consultation publique en Europe et mis en ligne un questionnaire visant à collecter les commentaires du public. Les questions incluaient entre autres : *Comment se définit et se délimite le droit à la vie privée d'une personne ayant ou ayant eu une activité publique ? Comment distinguer un contenu d'intérêt public des autres types de contenu ? Le public dispose-t-il d'un droit à l'information sur la nature et le volume des demandes de suppression de contenu soumises aux moteurs de recherche, ainsi que sur la suite qui leur a été donnée ?*

En parallèle à cela, une tendance similaire a émergé partout dans le monde, suite à l'arrêt de la Cour de justice de l'Union européenne. Par exemple, les autorités de régulation du respect de la vie privée membres présentes en juin 2014 à un forum de l'APPA (Autorités de protection de la vie privée de la zone Asie-Pacifique) en Corée ont discuté de la possibilité d'« amorcer le dialogue avec Google et les autres moteurs de recherche » avant de débattre des sujets à aborder lors la réunion suivante de l'APPA en décembre 2014. Les implications de la mise en œuvre de règles similaires dans d'autres juridictions ont commencé à faire débat. Un tribunal français a également débattu du fait que le retrait des liens dans les versions nationales du site Google (p. ex. Google.fr, Google.es) n'était pas suffisant si Google.com – disponible en Europe – les conserve. La conséquence en serait de devoir bloquer Google.com en Europe, ou de faire bloquer par l'entreprise les informations pour toutes les recherches provenant d'adresses IP européennes. L'alternative, faire appliquer l'arrêt européen à l'ensemble des opérations mondiales de Google.com, constituerait l'application excessive d'une décision d'une juridiction extraterritoriale, qui ne serait pas valable à l'échelle mondiale. Comme noté précédemment, une solution encore à prendre en considération serait la création d'un dispositif mis en place par les moteurs de recherche pour donner un « droit de réponse » sur des liens jugés problématique par une personne.

Ce que ce cas particulier, ainsi que l'affaire *Delfi c. Estonie*, pourrait indiquer, c'est l'apparition d'une tendance des tribunaux de créer, plutôt que d'appliquer, des politiques et précédents, du fait de l'absence de politiques et de lois définies par les autorités publiques en réponse aux développements technologiques.

4.4 COLLECTE, RÉTENTION ET SURVEILLANCE DES DONNÉES

La rétention des données personnelles par les moteurs de recherche, combinée à la connaissance accrue des pratiques de surveillance gouvernementale, semble avoir ébranlé la confiance du public envers les moteurs de recherche. Une analyse des Tendances des recherches Google, disponibles publiquement, avant et après juin 2013 (date à laquelle Edward Snowden a commencé à révéler les pratiques gouvernementales de surveillance par Internet) a tenté de découvrir « des preuves empiriques d'un effet dissuasif sur la propension des utilisateurs à saisir des termes de recherche [sensibles] ». Pour cela, les données relatives à 282 termes dans 11 pays ont été analysées. Une diminution du trafic pour les termes de recherche jugés « susceptibles d'attirer des ennuis avec le gouvernement des États-Unis » a été constatée dans neuf pays, alors que les termes plus « sûrs » ont été en augmentation. Aux États-Unis, cette diminution atteint 2,2 %. Les études de ce genre indiquent que dans certaines sociétés au moins, la connaissance d'un manque de confidentialité et l'existence, dans une certaine mesure, d'une surveillance généralisée peuvent commencer à avoir un certain effet dissuasif sur la liberté d'expression des utilisateurs de moteurs de recherche. Les inquiétudes sur la collecte des données par les moteurs de recherche ont entrainé l'apparition de services alternatifs qui déclarent ne pas recueillir et stocker de données numériques des utilisateurs.

4.5 TRANSPARENCE

Les membres de Global Network Initiative se sont explicitement engagés à « respecter et protéger la liberté d'expression de leurs utilisateurs » dans leur réponse aux requêtes gouvernementales de suppression ou de transmission de données. Ils se sont également engagés à assumer les responsabilités de leur engagement. La responsabilité publique des membres de GNI est double : « l'analyse et l'évaluation indépendantes » du fait que les entreprises respectent on non leurs engagements aux principes de GNI et également la « transparence auprès du public ». Deux ans après la création officielle de GNI, composé en 2008 de trois entreprises membres, la pratique dite du « rapport de transparence » tend à se généraliser.

4.6 RÉPARATION

Il existe deux parties potentielles dont les droits à la liberté d'expression peuvent être affectés par les moteurs de recherche : les internautes dans leur ensemble, mais également les créateurs et administrateurs de sites Internet, y compris les personnes possédant un blog ou un site Internet personnel, les organismes de la société civile et les organismes d'information. D'autres parties peuvent avoir des réclamations au sujet d'autres droits – par exemple les créateurs de contenus concernés par des liens vers des sites de partage de données qui violent leur propriété intellectuelle. Cette section se concentre sur les solutions et mécanismes de réclamation relatifs uniquement à la liberté d'expression et non aux mécanismes traitant d'autres droits. Aucun des moteurs de recherche étudiés ne dispose de mécanismes de plainte, de réclamation ou de réparation utilisables par les internautes pensant que leur liberté d'expression a été bafouée par la manière dont les moteurs de recherche gèrent leurs contenus.

Google propose un mécanisme à l'intention des propriétaires de sites Internet pour qu'ils demandent le retrait de leur site Internet des résultats de recherche, dans le respect du Digital Millenium Copyright Act (DMCA) des États-Unis, la loi de protection des droits d'auteur. Depuis que l'entreprise applique la réglementation européenne relative au droit à l'oubli, Google a rétabli des liens vers des articles informatifs qui avaient dans un premier temps été supprimés. Néanmoins le processus de traitement des recours demandant rétablissement reste flou. Avant que Google ne mette en ligne son formulaire de « droit à l'oubli », suite à la décision de la Cour européenne, aucun des moteurs de recherches étudiés n'avait mis en place de mécanisme permettant aux utilisateurs pensant être victimes d'une violation de leurs droits au respect de la vie privée et à la protection de leur réputation de demander réparation. Bien que des Européens aient fait appel avec succès aux tribunaux pour demander réparation pour des violations potentielles du respect à la vie privée par les moteurs de recherche, les plaignants n'ont pas réussi à obtenir gain de cause auprès des tribunaux en ce qui concerne les restrictions des moteurs de recherches appliquées aux liens vers leurs sites Internet.

4.7 CONCLUSIONS

Les politiques et pratiques des moteurs de recherche en ce qui concerne la restriction et la manipulation de contenu sont modelées par leurs juridictions respectives, et dans une moindre mesure par les lois et réglementations des autres juridictions. L'analyse de trois entreprises différentes installées dans trois contextes nationaux très différents permet de tirer les conclusions suivantes :

- ***Les régimes de filtrage des FSI ont une forte influence sur la manière et la mesure dont les moteurs de recherche restreignent leurs propres résultats de recherche.***

- ***Plus le régime de responsabilité est strict dans une juridiction, plus il y a de chance qu'un contenu soit retiré, soit de manière proactive par l'entreprise, soit suite à une demande et sans qu'il n'y ait de contestation.***

- ***Si la restriction de contenu existe sur les moteurs de recherche à la demande des autorités, elle peut également exister pour d'autres raisons dans toutes les juridictions, y compris pour des raisons que les moteurs de recherche jugent être dans leur intérêt, dans celui de l'utilisateur ou dans celui du public.*** Ceci contredit une opinion largement répandue auprès du public que les moteurs de recherche sont des arbitres neutres de l'information. Certains consensus sont apparus entre ces entreprises et les défenseurs de la liberté d'expression sur les meilleures pratiques que devraient appliquer les moteurs de recherche pour traiter les demandes gouvernementales et refuser certaines requêtes au nom du principe de liberté d'expression, comme le montrent les principes et lignes directrices de mise en œuvre adoptés par Global Network Initiative. Il n'existe néanmoins aucun consensus clair entre les parties prenantes sur la manière dont les moteurs de recherche doivent respecter la liberté d'expression lors de la conception de leurs algorithmes et lorsqu'ils restreignent des contenus de leur propre chef, sans demande gouvernementale.

- ***La transparence des entreprises et des gouvernements joue un rôle crucial pour favoriser la confiance du public envers les pratiques d'un moteur de recherche et pour garantir que la liberté d'expression n'est pas limitée pour des raisons illégitimes ou accidentelles.*** Il existe de nombreux exemples prouvant en quoi il est important que les gouvernements soient transparents avec leurs citoyens en ce qui concerne les demandes de restriction faites auprès des moteurs de recherche ainsi que sur les mesures de filtrage au niveau du réseau qui ont un impact direct sur eux. Il est tout aussi important que les entreprises soient transparentes vis-à-vis des utilisateurs sur les contenus supprimés à la demande du gouvernement ou d'autres parties et les raisons de ces suppressions.

- ***Les inquiétudes relatives à la vie privée prennent de plus en plus d'ampleur, mais seule l'une des entreprises – Google – y a répondu de manière publique et directe.*** Bon nombre d'utilisateurs aimeraient que les entreprises auxquelles ils se fient pour effectuer des recherches, ou faire trouver leurs propres contenus, communiquent de manière plus directe en ce qui concerne les droits. Cela couvre aussi bien les informations sur les pratiques de collecte, de stockage et de partage des données dans le cadre prévu par la loi, que la protection des données dans la mesure du possible, au regard des réalités de leurs contextes juridiques et politiques.

- ***L'engagement des parties prenantes, le respect des principes et les moyens de réparation sont importants pour les intermédiaires mondiaux, afin de surmonter les tensions entre la liberté d'expression et les autres droits, et d'opérer dans des contextes réglementaires difficiles.*** L'engagement de Google au sein de GNI depuis la création de l'organisation en 2008, et sa contribution au développement des principes de GNI depuis 2006, a renforcé la capacité de l'entreprise à respecter la liberté d'expression et à contester les requêtes gouvernementales ne respectant pas, selon elle, les normes en matière de droits de l'homme. Néanmoins, sur les autres questions de la liberté d'expression et du respect de la vie privée non liées à des demandes gouvernementales, un cadre de principe doit encore faire l'objet d'un consensus des parties prenantes du monde entier.

5. ÉTUDE 3 : PLATES-FORMES DE RÉSEAUX SOCIAUX – FACEBOOK, TWITTER, WEIBO ET IWIW.HU

5.1 INTRODUCTION

Les réseaux sociaux en ligne jouent un rôle vital dans les interactions sociales et l'expression, en fournissant une plate-forme qui permet de démocratiser la publication de contenus et d'informations. En permettant l'échange et l'agrégation de contenus générés par les utilisateurs, les réseaux sociaux sont perçus par certains comme un moyen de transformer les auditeurs en producteurs d'informations, en fournissant de nouveaux outils pour la cohésion sociale et en donnant les moyens aux citoyens de rendre les gouvernements responsables. Les réseaux sociaux, comme la plupart des entreprises Internet qui proposent des services gratuits, tirent leurs revenus de la publicité. Les entreprises tierces achètent des encarts publicitaires sur les réseaux sociaux, car elles espèrent que ceux-ci sont capables d'identifier les acheteurs potentiels parmi leurs utilisateurs, grâce au traitement de leurs données. Les utilisateurs « paient » ainsi leur droit d'utilisation des services avec leurs informations personnelles et leur vie privée. Ces plates-formes sont en pleine évolution et proposent toujours plus de moyens de créer et de partager des données. Les réseaux sociaux ont également amélioré la visibilité et la portée de certains médias traditionnels, par exemple en permettant de « retweeter » des liens ou en partageant d'autres contenus en ligne, assurant une diffusion de l'information beaucoup plus rapide que par les moyens conventionnels.

De nombreux systèmes juridiques considèrent les réseaux sociaux comme des « hébergeurs de contenus », car les utilisateurs créent des contenus sur leurs plates-formes et les tierces parties sont autorisées à publier et partager l'information. En permettant aux contenus privés d'être partagés publiquement, les réseaux sociaux estompent la démarcation entre les sphères publiques et privées, soulevant ainsi des questions sur les attentes appropriées à avoir vis-à-vis de l'expression sur de telles plates-formes. Compte tenu de la portée et de l'impact de l'expression et des activités générées par les utilisateurs sur les réseaux sociaux, il n'est pas facile pour les entreprises de trouver un équilibre entre la libre expression, le respect des lois, les attentes des utilisateurs et leur obligation fiduciaire de générer des bénéfices. Cette section examine les politiques et pratiques de plusieurs plates-formes des réseaux sociaux dans différents contextes nationaux. Elle conclut que la capacité des plates-formes des réseaux sociaux à respecter la liberté d'expression de leurs utilisateurs est fortement influencée par les contextes réglementaires et juridiques nationaux, notamment le contexte du pays où siège l'entreprise. Dans le même temps, les entreprises ont de nombreuses possibilités en matière de gestion et de conception de plate-forme. Leurs choix ont un impact énorme sur la liberté d'expression des utilisateurs.

Entreprises étudiées :

Facebook (www.facebook.com) est un réseau social fondé en 2004 et basé aux États-Unis. En août 2015, l'entreprise comptait 1,49 milliard d'utilisateurs actifs par mois, dont 83,1 % sont situés hors de l'Amérique du Nord. La plate-forme permet aux utilisateurs enregistrés de tenir à jour un profil personnel à travers lequel ils peuvent partager des données personnelles, des contacts, des photos, des articles, et leur emplacement actuel ; communiquer avec d'autres personnes par le biais de messages publics ou privés ; rechercher et « devenir ami » avec d'autres utilisateurs qu'ils peuvent « taguer » (identifier) dans des photos ou dans des endroits ; rejoindre des groupes et interagir avec les autres membres. Il est possible d'accéder à Facebook par Internet ou par des applications dédiées disponibles sur de nombreux systèmes d'exploitation.

Twitter (www.twitter.com) est une plate-forme de microblogging fondée en 2006 et basée aux États-Unis. En août 2015, elle comptait 316 millions d'utilisateurs actifs par mois, qui envoient 500 millions de messages (« tweets ») par jour. Soixante-dix-sept pour cent des utilisateurs de Twitter résident en dehors des États-Unis. Les utilisateurs enregistrés sur Twitter peuvent échanger des messages de 140 caractères (ou moins) depuis le site Internet, les applications mobiles ou par SMS. Les utilisateurs peuvent diffuser ces messages en les « retweetant », effectuer des recherches sur les messages existants et « suivre » d'autres utilisateurs. Même les utilisateurs non enregistrés peuvent lire les tweets des autres utilisateurs, si tant est que ceux-ci aient un profil public (le réglage par défaut). Twitter est accessible depuis Internet ou depuis de nombreuses applications mobiles. Les tweets peuvent être organisés par hashtag (ou mot-dièse) –le symbole « # » suivi d'un mot ou d'une phrase) qui permettent aux utilisateurs de regrouper les messages traitant du même sujet. Si un hashtag bénéficie d'un grand nombre de « retweets », il est qualifié de « tendance ». Twitter « n'exige pas des utilisateurs qu'ils fournissent leur véritable nom, ne vérifie pas leurs adresses e-mail et n'authentifie pas leur identité ».

Weibo (www.weibo.com) est une plate-forme chinoise de microblogging fondée en 2009, issue de la plate-forme Sina avant l'inscription de ses actions à la bourse américaine en avril 2014. En mai 2015, elle comptait 198 millions d'utilisateurs actifs par mois. Les utilisateurs ont des profils personnels, peuvent poster des messages de 140 caractères (appelés weibo, ce qui signifie « microblog » en chinois) et commenter les weibo des autres utilisateurs, une fonctionnalité qui permet « au peuple chinois et aux organisations de s'exprimer publiquement et en temps réel ».

iWiW (anciennement www.iwiw.hu, « international who is who ») est un réseau social hongrois qui a cessé d'exister en juillet 2014 faute d'un nombre suffisant d'utilisateurs. Fondé en avril 2002 sous le nom de wiw.hu (« who is who »), il est devenu iWiW en octobre 2005, lors d'une tentative infructueuse d'expansion consistant à proposer la plate-forme en plusieurs langues. En avril 2006, il a été racheté par la division T-Online de Magyar Telekom, avant de fusionner en 2008 avec Origo.hu. Jusqu'en 2011, seuls les utilisateurs invités pouvaient rejoindre la plate-forme. En janvier 2013, il comptait 4,7 millions d'utilisateurs enregistrés.

Les réseaux sociaux sont populaires partout dans le monde, mais ils sont utilisés de différentes manières selon les contextes politiques et culturels. Facebook et Twitter sont

deux des réseaux sociaux les plus populaires, avec de nombreux utilisateurs dans de nombreux pays, et une étude de ces services permet donc de mieux comprendre les problématiques liées à la liberté d'expression dans un environnement transnational. iWiW et Weibo se limitent quant à eux à une utilisation principalement nationale. Le cas de Weibo est particulièrement intéressant, car le marché chinois des réseaux sociaux est soumis à une forte compétition tout en restant isolé des concurrents étrangers. iWiW a été sélectionné car il représente un service de réseau social évoluant dans une langue nationale et un contexte culturel local; et ayant à faire face aux concurrents internationaux.

Les conclusions des études de cas de ces entreprises sont présentées ci-dessous.

5.2 IMPACT DU FILTRAGE DES FSI SUR LES PLATES-FORMES DES RÉSEAUX SOCIAUX

Les gouvernements peuvent demander aux FSI de filtrer les plates-formes des réseaux sociaux en bloquant l'accès soit au site dans son ensemble, soit à certains contenus, groupes ou pages. Un tel filtrage peut également être mis en place au niveau des points d'échange Internet nationaux. Les entreprises qui exploitent des plates-formes des réseaux sociaux n'ont aucun contrôle sur les actions des gouvernements et des FSI. Certains réseaux sociaux, comme Facebook, Twitter et Google, se sont déjà prononcés contre le filtrage au niveau du réseau en général. Les entreprises ont par contre le contrôle sur leurs propres conditions de services et sur la manière dont elles répondent aux gouvernements et aux autres requêtes de suppression de contenu ou de désactivation de compte sur leurs plates-formes. Les décisions des entreprises en ce qui concerne ces restrictions au niveau de la plate-forme affectent à leur tour le choix des gouvernements de réaliser ou non un filtrage au niveau du réseau.

Les gouvernements peuvent décider de restreindre ou de bloquer l'accès aux réseaux sociaux par filtrage réseau dans plusieurs cas de figure :

- ***Normes différentes selon les juridictions*** : À la différence des FSI, les réseaux sociaux ne nécessitent pas de présence physique sur un territoire pour atteindre les utilisateurs qui s'y trouvent. Certains gouvernements utilisent néanmoins la menace du filtrage réseau pour contraindre les entreprises internationales à respecter leurs lois.
- ***Au nom de la sécurité ou de l'unité nationale***
- Dans les pays considérant ***qu'il est nécessaire de contrôler et de maintenir l'ordre public en temps réel***.

5.3 SUPPRESSION DE CONTENU ET DÉSACTIVATION DE COMPTE

Si les plates-formes des réseaux sociaux peuvent être la cible de filtrage par les FSI, sur lequel elles n'ont aucun contrôle, elles disposent par contre de leurs propres dispositifs pour bloquer ou restreindre les contenus des utilisateurs. En effet, elles demandent en effet en général aux utilisateurs de créer un compte pour pouvoir partager des contenus. Les administrateurs de ces plates-formes peuvent restreindre le contenu que les utilisateurs partagent sur la plate-forme de plusieurs manières : en les supprimant, en les empêchant d'être vus par les utilisateurs de certaines juridictions, ou en désactivant le compte des utilisateurs postant certains types de contenus. Ces actions peuvent être des mesures d'autorégulation qui visent à garantir le respect de la vie privée ou des mesures prises pour répondre aux requêtes d'un gouvernement ou d'un tiers, ou à tout autre impératif juridique, par exemple dans le cadre d'un ordre d'un tribunal dans une affaire civile. Dans certains cas, les utilisateurs peuvent être pénalisés pour leur expression légitime en ligne. La potentielle responsabilité juridique du réseau ou de l'utilisateur peut également entraîner une autocensure.

Le tableau ci-dessous résume les différents modes de restriction des contenus, leurs raisons et les parties affectées.

Tableau 3 : Principaux facteurs affectant les restrictions de contenus sur les plates-formes des réseaux sociaux :

Raison de la restriction :	Le contenu enfreint-il les conditions de service ?	Mode de mise en œuvre :	Qui est affecté :
• demandes du gouvernement	• possible	• suppression complète de certains contenus	• tous les utilisateurs
• demandes à caractère juridique (p. ex. notification pour atteinte aux droits d'auteur, ordre d'un tribunal dans les affaires civiles)	• possible	• blocage de certains contenus pour des groupes d'utilisateurs ou juridictions spécifiques (les contenus restent accessible pour les autres)	• seulement les utilisateurs de certaines juridictions
• autorégulation à leur propre initiative (conditions de service et autres règles privées)	• habituellement	• filtrage automatisé (proactif) des types de contenus préidentifiés	• seulement certains groupes d'utilisateur (p. ex. en fonction de l'âge)
• signalement d'un utilisateur (pour violation des conditions de service par un autre utilisateur)	• habituellement		

5.4 VIE PRIVÉE

Les réseaux sociaux sont de véritables mines d'informations personnelles, où on révèle tout, des opinions politiques à l'orientation sexuelle. Les utilisateurs confient implicitement aux réseaux sociaux leurs données personnelles, et les gouvernements peuvent demander l'accès à ces informations dans le cadre d'enquêtes civiles, criminelles ou même touchant à la sécurité nationale. Toutes les entreprises examinées ont une politique de respect de la vie privée qui explique comment les informations des utilisateurs sont utilisées, mais ces politiques sont rarement explicites ou complètes. De plus, les réglages par défaut ont des conséquences significatives car la plupart des utilisateurs ne les modifient pas. Les entreprises étudiées ne communiquent pas beaucoup d'informations au sujet de la rétention des données.

En 2014, le Haut-Commissaire des Nations Unies aux droits de l'homme, puis en 2015 le Rapporteur spécial des Nations Unies sur la promotion et la protection du droit à la liberté d'opinion et d'expression, ont souligné l'importance de l'anonymat, dans le cadre du droit au respect de la vie privée, pour l'exercice et la protection des droits de l'homme à l'ère de l'Internet. De nombreuses plates-formes des réseaux sociaux, mais pas toutes, demandent à ce que les utilisateurs s'inscrivent sous leurs vrais noms, et veillent à l'application de ces politiques à des degrés variables et de différentes manières.

5.5 TRANSPARENCE

5.5.1 Transparence sur les demandes gouvernementales et juridiques

Facebook et Twitter ont publié des rapports connus sous le nom de « rapports de transparence ».

Le Rapport des demandes gouvernementales de Facebook a révélé des informations sur la restriction de contenu pour la première fois en avril 2014. Facebook n'indique que le nombre de requêtes gouvernementales que l'entreprise a acceptées, sans toutefois préciser le nombre de requêtes déposées. Le rapport n'indique pas non plus le nombre d'ordres issus de tribunaux ou de notifications pour atteinte aux droits d'auteur. Le rapport de transparence de Facebook donne des informations sur les requêtes gouvernementales concernant les données des utilisateurs – y compris les informations sur le taux d'application et les types de requêtes. Il ne fournit cependant que des informations basiques et incomplètes sur les demandes de restriction de contenu.

Twitter communique sur les demandes de suppression de contenu depuis son premier rapport de transparence, publié en 2012. En plus des informations incluses dans le rapport de Facebook, le rapport de Twitter contient le taux de réponse aux requêtes, le contenu supprimé et les notifications pour atteinte aux droits d'auteur. Twitter se distingue de Facebook en publiant des copies des demandes de retrait et de restriction

de contenu que l'entreprise reçoit, sur le site Internet Chilling Effects. En ce qui concerne la communication sur les demandes de données par les gouvernements, Twitter fournit des informations sur les types de demandes et le taux d'acceptation de ces demandes, ainsi que des données sur les informations transmises aux autorités en cas d'urgence.

Weibo n'est pas en mesure, par contrainte juridique, de publier de rapport de transparence, et il semble que les médias en ligne comme hors ligne ne mentionnent que rarement les restrictions de contenu appliquées au niveau de l'État.

iWiW ne publiait pas de rapports de transparence du temps de son activité.

5.5.2 Transparence sur l'autorégulation

Si Facebook et Twitter on fait des efforts pour améliorer la transparence sur leurs méthodes de traitement des demandes gouvernementales et juridiques, les deux entreprises ne diffusent toujours que peu d'informations auprès des utilisateurs ou du grand public en ce qui concerne la manière dont elles veillent au respect de leurs propres conditions de service. Aucune des entreprises étudiées ne fournit d'informations sur le contenu restreint en application de la politique de l'entreprise, ni de statistiques sur les signalements externes de violations des règles de l'entreprise. Elles ne communiquent aucune donnée sur le nombre, la source ou le sujet de ces cas.

Si tous les réseaux sociaux proposent une liste des contenus prohibés, aucune des entreprises étudiées n'a fourni d'information au public sur les procédures utilisées pour évaluer ces contenus. Des sources du secteur ont défini des règles et procédures internes d'évaluation des contenus lors de discussions avec les parties prenantes concernées, tenues à la condition qu'elles ne puissent pas leur être attribuées, mais ces procédures ne sont généralement pas rendues publiques. La plupart du temps, le public ne prend connaissance de ces procédures que par des faits anecdotiques rapportés par les médias d'information.

5.5.3 Notification aux utilisateurs

Les entreprises ne procèdent pas toujours de la même façon pour informer les utilisateurs quand elles restreignent leur contenu ou transmettent leurs données personnelles. Si du contenu est retiré pour cause de violation des droits d'auteur, Facebook et Twitter sont légalement obligés par le DMCA des États-Unis d'en avertir l'utilisateur et de l'informer de la procédure de contestation. En outre, les deux entreprises s'engagent à informer les utilisateurs des requêtes faites concernant leurs données personnelles, à moins que la situation soit une urgence ou qu'il soit légalement interdit que l'entreprise agisse de la sorte.

En ce qui concerne les contenus supprimés par Facebook dans le cadre de ses Standards de la communauté et de sa Déclaration des droits et responsabilités, l'entreprise s'engage à avertir les utilisateurs avant la suppression. Twitter n'est pas clair en la matière. Dans les cas de restriction de contenu suite à une requête extérieure, Twitter avertit le public de la restriction par un avis de « Tweet bloqué », qui sert aussi aux suppressions pour cause

de droits d'auteur. Comme déjà mentionné, Twitter ne restreint les comptes que dans les juridictions où les autorités lui transmettent des requêtes valides. Facebook affiche un message plus générique, indiquant que « ce contenu n'est actuellement pas disponible », qui peut signifier de nombreuses choses et ne donne aucune précision sur une situation particulière. Lorsque Weibo restreint du contenu, les autres utilisateurs essayant d'y accéder peuvent lire un message les informant que le contenu a été supprimé, et sont redirigés vers un lien pour obtenir plus d'informations. Weibo a été accusé par ses utilisateurs de « camoufler » des messages, pour que ceux-ci ne restent visibles que de l'auteur, sans qu'il ne sache que son contenu a été restreint.

5.6 RÉPARATION

Aucune des entreprises étudiées ne propose de voie de recours claire pour les utilisateurs dont une image ou du texte a été supprimé, ou subissant des restrictions fonctionnelles, comme l'incapacité de publier des photos. Facebook peut supprimer des pages en cas de violation présumée des règles sur les spams, mais les utilisateurs peuvent faire appel. Tout comme Facebook, Twitter donne la possibilité de contester la suspension d'un compte. Lorsque des comptes sont désactivés pour cause de violation des conditions de Facebook, les utilisateurs peuvent faire appel en remplissant un formulaire spécifique. Aucune information n'est transmise quant à la durée de traitement de la requête, à la procédure de prise de décision, ou à la sévérité des violations susceptibles d'entrainer la suspension de compte. La page d'information de Twitter est également pauvre en informations sur le sujet, mais fournit plus de détails sur la procédure d'appel. La seule exception est le droit d'auteur, car la loi des États-Unis en la matière oblige Facebook et Twitter à en notifier la première personne à avoir publié le contenu et à l'informer de la manière de contester la décision. Les voies de recours proposées à l'époque par iWiW sont méconnues, si tant est que la plate-forme en proposait. Weibo ne propose pas de voie directe de recours ou de formulaire en ligne ; en revanche les utilisateurs sont invités à envoyer un e-mail à l'entreprise en indiquant si 1) ils sont en désaccord avec les interventions des administrateurs ; 2) ils ne sont pas satisfaits des réponses de l'administrateur après la communication ; 3) ils ont des questions sur d'autres aspects administratifs. Sur Weibo, le manque d'information sur les possibilités de réparation oblige les utilisateurs à se fier à des témoignages anecdotiques. Les restrictions de contenus semblent ne pas respecter de règles particulières.

5.7 CONCLUSIONS

Compte tenu des interactions entre les pratiques et politiques des intermédiaires des réseaux sociaux et les contextes juridiques et réglementaires de chaque pays, les entreprises peuvent plus facilement respecter l'ensemble des droits des utilisateurs dans les juridictions où les lois sont relativement conformes aux normes internationales relatives aux droits de l'homme et au respect de la vie privée. Le contexte juridique des pays

où sont situés les sièges des entreprises est particulièrement important pour le respect des droits des utilisateurs. Les entreprises de réseaux sociaux dont les gouvernements n'empêchent pas ce type d'effort ont fait de grands progrès en matière de transparence et de responsabilité face aux demandes gouvernementales. Mais la liberté d'expression reste fortement influencée, en bien ou en mal, par les règles, procédures et mécanismes propres aux entreprises en ce qui concerne, entre autres, l'application des conditions de service, le respect de la vie privée des utilisateurs et la protection de leur identité. Sur ces points les entreprises sont bien moins transparentes et responsables vis-à-vis du public.

Les recherches effectuées sur Facebook, Twitter, Weibo et iWiW permettent de tirer les conclusions suivantes :

- ***Les actions gouvernementales à l'encontre des utilisateurs de réseaux sociaux peuvent limiter l'espace d'expression***. Les utilisateurs sont parfois pénalisés pour leur expression en ligne, que ce soit par des amendes ou même parfois par des arrestations. Un manque de clarté sur les expressions autorisées, ainsi que des politiques restrictives, peut provoquer une forme d'autocensure. Les entreprises qui exploitent les plates-formes des réseaux sociaux peuvent améliorer la situation en étant transparentes sur leurs pratiques de restriction, leurs paramètres de confidentialité et leurs politiques de partage des données. Elles peuvent également soutenir les individus dans les cas où les pénalités ne sont pas conformes aux normes internationales relatives aux droits de l'homme.

- Les réseaux sociaux n'avalisent pas forcément toutes les demandes de suppression de contenus, Twitter a par exemple appliqué 11 % seulement de ces requêtes, prouvant ainsi que l***es réseaux sociaux ont les moyens de contester les demandes de restriction de contenu***. Il peut être plus simple de résister aux pressions des pays autres que celui de leur siège, mais même dans leur pays d'origine, certaines entreprises n'appliquent pas toutes les requêtes. Sur les quatre réseaux sociaux étudiés ici, seuls Twitter et Facebook publient les critères, voire la procédure réelle, de traitement des requêtes de suppression de contenu par des gouvernements et/ou des tierces parties. ***La diffusion publique des politiques de ce type permet aux utilisateurs de comprendre dans quelles circonstances leurs contenus peuvent être supprimés par requête externe, et aux entreprises d'avoir un cadre plus clair pour contester les requêtes de suppression qui ne respectent pas la procédure établie ou les droits internationaux de l'homme.***

- ***Les réseaux sociaux ne font pas preuve du même niveau de transparence en ce qui concerne les requêtes gouvernementales de suppression de contenu***. Sur les quatre plates-formes de réseaux sociaux étudiées, seuls Twitter et Facebook fournissent des informations sur les requêtes gouvernementales, faisant ainsi la lumière sur la manière dont la loi est appliquée sur leurs plates-formes. Twitter diffuse également les requêtes de suppression de contenu en elles-mêmes sur le site Internet « Chilling Effects », et avertit le public par des messages sur la plate-forme lorsqu'un contenu est restreint suite à une requête gouvernementale. Selon les juridictions, les gouvernements ne sont pas complètement transparents sur la nature et l'étendue des restrictions de contenu et des demandes de données personnelles.

- ***Certains réseaux sociaux n'expliquent pas comment ils partagent les données personnelles avec les autorités et les autres tierces parties***. Facebook et Twitter ont publié des lignes directrices sur leur manière de répondre aux demandes de données personnelles provenant des organismes autorisés, aussi bien nationaux qu'étrangers. Les utilisateurs des autres services ne sont pas informés de la manière dont leurs données personnelles sont protégées des requêtes émanant de gouvernements ou d'autres tiers.

- ***Aucune des entreprises étudiées ne publie de données sur les restrictions autorégulatrices***, comme, par exemple, le nombre de comptes désactivés pour cause d'usurpation d'identité, ou le nombre de récidivistes dont le compte a été complètement supprimé. Les réseaux sociaux en ligne devenant des plates-formes de plus en plus centrales pour l'expression en ligne des individus, les utilisateurs et les parties prenantes souhaitent l'apparition de règles et de procédures d'application à la fois claires, prévisibles et dans une certaine mesure surveillées de manière indépendante. L'absence d'une telle responsabilisation nuit à la légitimité de ces intermédiaires en tant que plates-formes garantissant la liberté d'expression de leurs utilisateurs.

- Étant donné qu'ils possèdent de grandes quantités d'informations personnelles, ***les réseaux sociaux ont une responsabilité spéciale en matière de respect de la confidentialité de leurs utilisateurs***, élément indispensable à la liberté d'expression.

- ***La nécessité pour les utilisateurs de s'inscrire en indiquant leur « vrai nom » a un sérieux effet dissuasif sur les discours et doit être mise en œuvre avec plus de souplesse, pour éviter d'avoir un impact négatif sur la liberté d'expression des utilisateurs. La plupart des gouvernements n'obligent pas légalement les réseaux sociaux à vérifier l'identité de leurs utilisateurs***. Les entreprises devraient prendre en considération les conséquences de la mise en place d'une politique d'inscription avec les vrais noms sur la vie privée et la liberté d'expression, en évaluant son impact sur les droits de l'homme.

- Les principes de GNI sur la liberté d'expression et le respect de la vie privée, ainsi que ses lignes directrices de mise en œuvre, ont donné des orientations claires aux membres de GNI et plus largement aux intermédiaires de l'Internet. Les lignes directrices de GNI sur la transparence et les procédures de traitement des requêtes gouvernementales, basées sur les normes internationales relatives aux droits de l'homme, ont eu un impact sur les pratiques des trois types d'intermédiaires étudiés dans ce chapitre. On constate néanmoins une absence flagrante de principes, lignes directrices et normes similaires en ce qui concerne les pratiques autorégulatrices des entreprises, et notamment l'application de leurs conditions de service. Compte tenu du manque de transparence et de cohérence sur la manière dont les entreprises appliquent leurs conditions de services et d'autres règles privées, et de l'impact de celles-ci sur la liberté d'expression des internautes ***il existe un besoin réel de développement de lignes directrices et de « meilleures pratiques » en matière de réparation et de transparence dans le contexte de l'autorégulation des intermédiaires***.

6. PROBLÉMATIQUES LIÉES AU GENRE

Parmi les 81 pays du Web Index 2013 de la Fondation World Wide Web, seule la moitié avait mis en place des politiques nationales traitant de l'égalité des sexes en ligne. Les auteurs du Web Index 2013 ont identifié qu'au « manque d'attention politique s'ajoute l'absence de collecte de statistiques ventilées par sexe ». Ainsi, « la manière dont le genre influe sur l'accès et l'utilisation d'Internet est encore très mal comprise ». Pour comprendre la relation entre cette situation et les rôles des intermédiaires, il convient de présenter brièvement la question de l'accès de base à l'Internet en comparant les situations des femmes et des hommes. Cette présentation est suivie d'un examen de la manière dont la restriction de contenu dans certains pays a limité l'accès des femmes à des informations sanitaires et à des débats en rapport avec le genre. La dernière section traite de questions liées au harcèlement visant les femmes, et de son effet sur la liberté d'expression en ligne des femmes, car il les dissuade de participer à la société de l'information numérique.

6.1 ACCÈS À L'INTERNET

L'accès à l'Internet a autonomisé les femmes, permettant une meilleure égalité des sexes et leur apportant des avantages économiques. Néanmoins, au niveau mondial, il existe une disparité notable entre les deux sexes en ce qui concerne l'accès à l'Internet haut débit. Les facteurs influant sur l'accès des femmes au haut début incluent les écarts d'éducation et de revenus, écarts encore plus prononcés pour les femmes des pays en développement. Les lacunes en termes d'accès et le manque d'infrastructures Internet affectent surtout les zones rurales à faibles revenus, et encore plus gravement les femmes. Dans le même temps, on observe que les femmes accèdent de plus en plus à l'Internet sur leur smartphone. Les interventions politiques pour combler les écarts entre les hommes et les femmes concernent l'accès à des plates-formes économiques, le développement de plans nationaux pour améliorer la pénétration du haut débit, et le traitement des contraintes du marché qui jouent sur accessibilité des plates-formes Internet sur le plan financier.

6.2 GENRE ET RESTRICTION DES CONTENUS

Dans certains pays, les défenseurs des droits de la femme ont demandé des restrictions plus larges des contenus pornographiques et « obscènes », en affirmant qu'il existe un rapport entre la consultation de ces contenus en ligne et les violences faites aux femmes hors ligne. Certaines femmes ont jugé leurs droits bafoués lorsque des intermédiaires n'ont pas restreint des contenus publiés sur Internet manifestement pour leur nuire.

Néanmoins, la capacité des femmes à accéder et à diffuser des informations et des idées sur la sexualité peut également être sujette à restrictions, et les législations mises en place entre autre pour défendre les femmes, peuvent être un détournées et utilisées à d'autres fins. Les entreprises de l'Internet, y compris les moteurs de recherche, ne restreignent généralement pas les informations médicales relatives aux femmes, mais le traitement de la nudité féminine par les réseaux sociaux a fait l'objet de nombreux désaccords. De plus, des lois censées juguler la pornographie ont également été utilisées dans certains pays pour supprimer d'autres contenus. Les entreprises confrontées à des lois vagues et sujettes à de nombreuses interprétations possibles peinent toujours à trouver un juste équilibre.

6.3 HARCÈLEMENT SEXISTE

Compte tenu de la facilité avec laquelle le harcèlement et les menaces peuvent avoir lieu sur les plates-formes des réseaux sociaux, par exemple le harcèlement avec menaces, les propos haineux, la persécution collective, la « vengeance porno », l'attention sexuelle non sollicitée et la contrainte sexuelle, de nouveaux débats voient le jour sur la responsabilité des intermédiaires dans la prévention et la prise en charge du harcèlement sexiste en ligne. Des exemples en la matière sont exposés dans le chapitre précédent sur la lutte contre les discours de haine en ligne.

6.3.1 Réglementations

On peut observer différentes tendances en ce qui concerne les législations sur le harcèlement sexuel en ligne : certains pays ont élaboré des lois spécifiques, d'autres ont des dispositions générales susceptibles d'englober le harcèlement sexuel en ligne, tandis que certains n'ont aucune législation sur le sujet. Une catégorie spécifique de harcèlement en ligne semble être une tendance émergente selon les preneurs de décisions et les défenseurs des droits de la femme, s'appelle la « vengeance porno ». Les auteurs en sont habituellement des ex-époux ou partenaires rancuniers, ou encore des « trolls », qui publient sur Internet ce que la National Conference of State Legislatures (NCSL) des États-Unis a défini comme étant des « photographies ou vidéos de personnes nues ou à caractère sexuellement explicite publiées sur Internet sans leur consentement, même si la photographie a été prise avec leur consentement ». Depuis 2014, au moins cinq pays et 25 états des États-Unis ont interdit la pratique de la vengeance porno, et bon nombre d'autres se sont attaqués au problème avec des lois pénales, anti-pornographie, sur la protection de la vie privée ou sur la responsabilité civile délictuelle.

6.3.2 Politiques et pratiques des intermédiaires

Une couverture médiatique négative et la pression de groupes de la société civile ont poussé certains intermédiaires à mettre en place de façon proactive des dispositifs de prévention et de sanction du harcèlement sexuel. Leurs réceptions et leurs applications

varient néanmoins grandement en fonction du degré d'engagement de l'entreprise et de l'attention qu'elle porte au problème, de la pression publique et de l'application de la loi. Dans une étude de 2014 sur la manière dont Facebook, Twitter et YouTube traitent les violences à l'encontre des femmes, l'APC a conclu que si les approches de ces entreprises en la matière sont différentes et que celles-ci « ont fait des efforts pour répondre aux préoccupations des utilisateurs », les efforts fournis sont toujours insuffisants. Le rapport de l'APC appelle les intermédiaires de l'Internet à trouver un équilibre entre leur engagement envers la liberté d'expression et les autres droits de l'homme, « comme celui de ne subir aucune forme de discrimination ou de violence. » Comme l'a fait remarquer ce rapport, les entreprises ne mettent parfois en place un dispositif de signalement des abus qu'après avoir été exposées à de fortes critiques de la part du public. Dans le même temps, bien que les plates-formes de réseaux sociaux soient des espaces où les hommes et les femmes ont à faire face au harcèlement sexuel et sexiste, elles permettent également aux activistes de le combattre et de sensibiliser le public à son sujet. Dans certains cas, ces campagnes ont réussi à attirer une attention nationale sur les problèmes existants et à motiver des changements, dans les politiques adoptées comme dans l'action politique en général.

6.4 CONCLUSION

Cette section a montré que les entreprises internationales comme Twitter ou Facebook sont bien moins transparentes et responsables sur leur manière de faire appliquer leurs propres conditions de services que sur celle de gérer les requêtes gouvernementales. L'étude de l'APC citée dans cette section souligne la nécessité d'un meilleur dialogue et d'une plus grande communication avec toutes les parties prenantes sur la façon dont les plates-formes des réseaux sociaux élaborent et font appliquer leurs règles. Les entreprises pourraient travailler plus étroitement avec les utilisateurs, tout type de défenseurs des droits de l'homme et les gouvernements pour que le problème de la violence sexiste en ligne soit traité d'une manière qui respecte et protège la liberté d'expression en ligne. En effet, le problème de la violence sexiste en ligne met en avant le besoin urgent de mettre en place une procédure regroupant les parties prenantes pour concevoir des principes, des normes et des lignes directrices en termes de « meilleures pratiques » sur la manière dont les plates-formes des réseaux sociaux peuvent communiquer avec les utilisateurs et être à leur écoute pour élaborer et appliquer leurs conditions de service.

7. CONCLUSIONS GÉNÉRALES

Les conclusions du présent chapitre mettent l'accent sur les défis majeurs à relever pour réaliser le premier principe de l'Universalité de l'Internet : les droits de l'homme. Sur la base des Principes directeurs des Nations Unies relatifs aux entreprises et aux droits de l'homme, selon lesquels le devoir de protéger les droits de l'homme incombe en premier lieu aux États, les entreprises se doivent aussi de respecter les droits de l'homme, et les sphères publiques comme privées ont un rôle à jouer pour garantir réparation à ceux dont les droits ont été bafoués. L'étude de cas souligne les difficultés auxquelles font face les intermédiaires de l'Internet quand ils cherchent à respecter au mieux le droit des utilisateurs à la liberté d'expression dans des contextes où les États n'honorent pas eux-mêmes leurs devoirs en la matière. Ces cas mettent en lumière des manières pour tous les États de s'améliorer. Néanmoins, il est également clair que les intermédiaires de l'Internet ont un pouvoir considérable sur la liberté d'expression des utilisateurs, même quand les environnements juridiques et réglementaires ne lui sont pas pleinement favorables.

7.1 DEVOIR DE PROTECTION INCOMBANT À L'ÉTAT

Le devoir de l'État de protéger les droits de l'homme comprend un rôle de facilitateur et de soutien pour faire respecter les droits de l'homme par les intermédiaires. Les conclusions de ce chapitre illustrent en quoi les politiques, lois et réglementations ne sont pas bien conformes, à des degrés divers, avec cet aspect particulier du devoir de l'État de protéger les droits de l'homme. Les problèmes identifiés par ces études de cas sont entre autres :

1. Les caractéristiques des régimes de responsabilité des intermédiaires, ou le cas échéant leur absence, ainsi que les objectifs réglementaires de ces régimes, affectent la capacité des intermédiaires à respecter la liberté d'expression. Il est essentiel de limiter la responsabilité des intermédiaires vis-à-vis des contenus publiés ou transmis par des tiers pour garantir l'avènement de services Internet qui facilitent l'expression.

2. Souvent, les lois, politiques et réglementations obligeant les intermédiaires à restreindre, bloquer ou filtrer les contenus dans de nombreuses juridictions ne sont pas suffisamment conformes aux normes internationales relatives aux droits de l'homme sur la liberté d'expression.

3. Les lois, politiques et pratiques liées à la surveillance et à la collecte des données à la demande des gouvernements et réalisées par les intermédiaires, lorsqu'elles ne sont pas suffisamment compatibles avec les normes relatives aux droits de l'homme, contribuent à empêcher les intermédiaires de protéger de manière appropriée la vie privée des utilisateurs.

4. Les accords de licence peuvent impacter la capacité des intermédiaires à respecter la liberté d'expression. Ceci s'applique à tous les FSI de tous les pays et aux réseaux sociaux et moteurs de recherche de certains pays.

5. Si la procédure régulière veut que l'application légale et la prise de décision soient transparentes et accessibles au public, les gouvernements sont souvent opaques en ce qui concerne les requêtes faites aux entreprises de restreindre des contenus, de transmettre des données personnelles ou de procéder à toute autre mesure de surveillance. Le public peut ainsi difficilement demander des comptes aux gouvernements et aux entreprises lorsque le droit des utilisateurs à la liberté d'expression est illégitimement restreint, que ce soit directement en interférant sur le contenu ou indirectement en compromettant la vie privée de l'utilisateur.

7.2 RESPONSABILITÉS À FAIRE RESPECTER PAR LES ENTREPRISES

Les politiques et pratiques des entreprises affectent la liberté d'expression des internautes de manière à la fois positive et négative. Les études de cas soulèvent des questions sur l'application des conditions de service, les politiques en matière de divulgation de l'identité, les pratiques de transparence, la mesure dans laquelle les entreprises veulent ou peuvent contester les requêtes gouvernementales, et les politiques liées à la vie privée, à la rétention de données et à la protection de données. Les principales conclusions sont entre autres :

1. Malgré la récente tendance des entreprises à publier des « rapports de transparence », les informations transmises et la manière de communiquer l'information restent très incohérentes. De plus, les entreprises manquent de transparence sur leur manière d'appliquer leurs conditions de services et de traiter les requêtes privées.

2. Les entreprises qui ont des pratiques et politiques de traitement des requêtes de restriction clairement définies sont mieux placées pour contester les lois et réglementations locales qui ne respectent pas les normes internationales sur les limitations légitimes.

3. Les décisions internes à certaines entreprises de restreindre certains types de contenu et d'appliquer leurs propres règles privées sont souvent accueillies par les gouvernements comme un moyen de gérer les problèmes avant qu'ils ne deviennent l'affaire des tribunaux. Dans le même temps, les procédures internes d'élaboration et d'application des règles manquent de transparence ou de dispositifs indépendants de contrôle qui permettraient de veiller à ce qu'elles ne donnent pas lieu à des erreurs ou à des abus. Les utilisateurs de la plupart des pays étudiés ont fait état d'incidents dans le cas desquels des mesures ont été prises par les intermédiaires contre des contenus qui ne semblaient pas contrevenir aux conditions de service, ou pour lesquels les conditions de service ont été appliquées de manière excessivement

littérale, résultant en un impact négatif sur la liberté d'expression, bien souvent sans moyens de recours appropriés.

4. Les entreprises de ces trois études de cas collectent des données similaires, bien que leurs politiques de rétention et de transmission à des tiers diffèrent grandement, tout comme la mesure dans laquelle elles informent les utilisateurs de l'existence et du contenu de ces politiques. La plupart de ces entreprises n'ont pas clairement expliqué comment elles traitent les requêtes gouvernementales de données personnelles, ni communiqué d'informations sur les réelles demandes de données ou sur les demandes acceptées. Si les lois contribuent à certaines de ces différences, des facteurs spécifiques aux entreprises entrent également en jeu.

5. Le fait que les utilisateurs aient le droit d'utiliser un service ou de créer un compte sans avoir à prouver leur identité au moyen d'une pièce fournie par l'État, ou même à utiliser leur vrai nom, impacte la liberté d'expression des utilisateurs dans un grand nombre des juridictions étudiées.

7.3 ACCÈS À DES MOYENS DE RÉPARATION

La réparation est le troisième pilier des Principes directeurs des Nations Unies relatifs aux entreprises et aux droits de l'homme, qui oblige les gouvernements et les entreprises à donner un accès individuel à des moyens de réparation efficaces. Dans ce domaine, les gouvernements comme les entreprises peuvent encore s'améliorer. Quels que soient les types d'intermédiaires, les juridictions ou les types de restrictions, les individus dont le contenu ou l'accès est limité et les individus souhaitant accéder à ces contenus ont accès à des voies de recours inégales, limitées ou inefficaces pour faire appel de ces décisions de restriction, que ce soit en réponse aux ordres gouvernementaux, aux demandes d'une tierce partie, ou dans le cadre de la politique de l'entreprise. Si certaines entreprises ont récemment redoublé d'effort pour mettre en place des dispositifs de réclamation et d'appel et informer les utilisateurs de leur existence, ces règles ont été appliquées de manière incohérente et sans procédure régulière.

7.4 SUJETS D'INQUIÉTUDES

Les politiques et pratiques des entreprises peuvent se combiner aux contextes juridictionnels pour produire des résultats qui ont un impact négatif sur la liberté d'expression. On a distingué plusieurs types de problèmes courants :

- Les lois trop larges et les régimes très responsabilisants amènent les intermédiaires à trop satisfaire aux requêtes gouvernementales en compromettant le droit de l'utilisateur à la liberté d'expression, ou bien à restreindre trop de contenus pour anticiper les requêtes gouvernementales, même si aucune requête n'est jamais reçue ou si le contenu aurait pu être considéré comme légitime par un tribunal national.

- Les intermédiaires peuvent être assujettis à diverses normes juridiques, et risquent parfois un bannissement total de la part des autorités en désaccord avec certains contenus partagés par leurs services. Les services Internet peuvent parfois résister à ces pressions en entretenant des rapports étroits avec les gouvernements, en bloquant des contenus uniquement dans la juridiction en question ou en supprimant à grande échelle ledit contenu.

- Les entreprises décident d'autoriser ou de bannir un contenu en fonction de leurs politiques internes, tout en étant influencés par leurs obligations légales suite à des décisions juridiques, les ordres gouvernementaux, les poursuites civiles, les instructions de tiers, les requêtes des groupes de surveillance avec lesquels l'intermédiaire coopère, et d'autres paramètres. Cette myriade d'acteurs impliqués, à laquelle s'ajoute l'ambigüité des cadres juridiques, empêche parfois les utilisateurs de savoir quel contenu est autorisé, qui décide du contenu autorisé et comment ; et de connaître les potentielles conséquences de leur expression.

- L'existence et la nature des politiques d'entreprise traitant des discours assimilables à du harcèlement sexuel ou à de la violence sexiste, mais aussi à l'exploitation ou à l'objectification des femmes sont variables, même au sein d'un même type d'intermédiaires et de mêmes juridictions. Les entreprises de ces trois études de cas disposent toute de dispositifs permettant aux utilisateurs de signaler des abus à caractère sexiste. Si ces dispositifs peuvent être utilisés à des fins légitimes, comme le signalement de harcèlement sexuel, ils peuvent dans un même temps être utilisés d'une manière excessive qui compromet les droits légitimes des utilisateurs en matière de liberté d'expression.

7.5 INTERMÉDIAIRES ET GOUVERNANCE DE L'INTERNET

En 2005, le Groupe de travail des Nations Unies sur la gouvernance de l'Internet a défini la « gouvernance de l'Internet » comme « l'élaboration et l'application par les États, le secteur privé et la société civile, dans le cadre de leurs rôles respectifs, de principes, normes, règles, procédures de prise de décisions et programmes communs propres à modeler l'évolution et l'utilisation de l'Internet ». Ainsi, si le terme de « gouvernance de l'Internet » est souvent utilisé dans les médias et les débats publics au sens strict pour désigner l'élaboration de politiques et les fonctions de coordination d'organismes comme la Société pour l'attribution des noms de domaine et des numéros sur Internet (ICANN), le concept a été à l'origine créé pour englober un plus large éventail de procédures permettant de déterminer les politiques et pratiques qui modèlent le fonctionnement d'Internet à tous les niveaux. Le rôle politique des intermédiaires de l'Internet – et les politiques jouant un rôle sur leur fonctionnement – est une forme de gouvernance de l'Internet au sens large du terme. Il est donc utile d'inscrire les conclusions de ce chapitre dans le contexte des débats mondiaux sur les principes fondamentaux de l'élaboration de politiques pour Internet qui ont un impact direct sur les intermédiaires.

Le Forum annuel sur la gouvernance de l'Internet (IGF), dont la création a été mandatée par l'Agenda de Tunis pour la société de l'information (2005), offre une plate-forme pour que les parties prenantes débattent de toutes les questions sous-jacentes à la gouvernance de l'Internet. Il n'est néanmoins pas mandaté pour définir des politiques. Plusieurs « coalitions dynamiques » se sont formées pour soutenir les travaux en cours sur la société de l'information, entrainant l'émergence en 2008 de la coalition dynamique Internet Rights and Principles (IRP). L'IRP a élaboré en 2011 une Charte relative aux droits et principes de l'Internet, qui regroupe dix principes fondamentaux, notamment les principes de liberté d'expression et de respect de la vie privée. L'IGF de septembre 2014 à Istanbul a été l'occasion de lancer une nouvelle coalition dynamique sur la « responsabilité des plates-formes », qui se concentre sur certaines catégories d'intermédiaires comme « les réseaux sociaux et les autres services interactifs en ligne » pour discuter « des solutions concrètes et interopérables pour protéger les droits de l'homme des utilisateurs de ces plates-formes ». Cette nouvelle coalition dynamique a un potentiel similaire pour contribuer à des normes sur les services de réseaux sociaux, des moteurs de recherche et des autres types d'intermédiaires qui peuvent être considérés comme des « plates-formes » d'expression. Cela pourrait servir d'axe majeur pour l'élaboration de principes s'appuyant plus sur les droits de l'homme et de dispositifs de responsabilisation pour différentes formes émergentes d'autorégulation et de corégulation.

8. RECOMMANDATIONS

Les recommandations suivantes s'appliquent à différents degrés aux gouvernements, aux entreprises, à la société civile et aux organisations internationales. Pour que la liberté d'expression en ligne soit respectée et protégée de manière adéquate, tous ces acteurs doivent trouver des moyens de travailler ensemble et par-delà les frontières pour améliorer les cadres réglementaires et juridiques, établir et mettre en œuvre des meilleures pratiques institutionnelles, et améliorer la sensibilisation et la participation des internautes et des citoyens. L'élaboration et l'application de règles en rapport aux discours en ligne – qu'elles soient réalisées par les gouvernements ou les entreprises – doivent être compatibles avec les normes internationales relatives aux droits de l'homme et responsables face à elles. Les recommandations suivantes sont une première étape dans cette direction, et elles visent à encourager les discussions et à parvenir à un plus grand consensus international.

8.1 POLITIQUES ET CADRES JURIDIQUES ADÉQUATS

Les objectifs politiques, juridiques et réglementaires qui affectent les intermédiaires doivent être conformes aux normes internationales relatives aux droits de l'homme pour que les États puissent protéger la liberté d'expression en ligne et que les entreprises la respectent autant que possible. Les gouvernements doivent veiller à ce que des cadres juridiques et des politiques soient en place pour répondre aux problèmes relatifs à la responsabilité, ou à l'absence de responsabilité, des intermédiaires. Les cadres juridiques et les politiques qui affectent la liberté d'expression et la vie privée devraient être adaptés en fonction du contexte sans transgresser les normes universelles, et ils devraient être conformes aux normes des droits de l'homme, notamment le droit à la liberté d'expression, et faire mention d'un engagement aux principes de procédure régulière et d'équité. Ils doivent également être précis et basés sur une claire compréhension de la technologie qu'ils sont censés traiter, supprimant l'incertitude juridique qui donnerait autrement l'opportunité de commettre des abus ou qui laisserait les intermédiaires opérer dans des manières qui restreignent la liberté d'expression par crainte d'être tenus responsables.

Afin de mieux éclairer les procédures d'élaboration des règles privées et publiques, il convient de mener des recherches mondiales plus quantitatives et qualitatives sur l'impact des pratiques, politiques, modèles économiques et décisions de conception des entreprises sur la liberté d'expression. Il manque à l'heure actuelle des enquêtes réalisées auprès d'internautes du monde entier, sur la manière dont les intermédiaires ont un impact sur la liberté d'expression des individus dans différents contextes. Plus de recherches sont également nécessaires sur la manière dont les cadres juridiques, réglementaires et politiques affectent la capacité des intermédiaires à respecter les droits des utilisateurs, ainsi que leur impact sur les internautes au sens plus large. Ce chapitre ne fait qu'effleurer la manière dont les politiques et pratiques des entreprises affectent la liberté d'expression dans différentes juridictions. Il serait également nécessaire d'obtenir des informations

plus détaillées sur les relations de cause à effet entre politiques, pratiques et résultats. Ces données donneraient plus de moyens aux parties prenantes pour affiner et ajuster leurs politiques, pratiques et stratégies et ainsi optimiser la protection et le respect des droits à la liberté d'expression des internautes du monde entier.

8.2 ÉLABORATION DE POLITIQUES MULTIPARTITES

Les lois, réglementations et politiques gouvernementales, ainsi que les politiques d'entreprise, ont plus de chance d'être compatibles avec la liberté d'expression si elles sont élaborées en concertation avec toutes les parties prenantes concernées et prennent en compte les intérêts de chacune. Un réel processus multipartite consiste à impliquer dès le début toutes les parties prenantes potentiellement affectées par la politique, plutôt que de simplement demander leurs opinions une fois que les principes de base et les orientations clés en ont été définis.

8.3 TRANSPARENCE

La transparence est importante pour prouver que les actions d'application des règles et de gouvernance respectent les principes, règles et conditions préétablis. Une plus grande transparence des gouvernements sur les requêtes et exigences soumises aux entreprises qui ont le potentiel d'affecter la liberté d'expression et la vie privée des utilisateurs est un prérequis pour la responsabilisation dans la gouvernance publique d'Internet. La transparence des entreprises est un prérequis pour la responsabilisation sur la manière dont les intermédiaires répondent aux requêtes gouvernementales, ainsi que pour leur propre « gouvernance » privée, nécessaire non seulement pour la protection de la liberté d'expression des utilisateurs, mais également pour permettre aux entreprises de gagner et de conserver la confiance du public dans leurs services.

Il existe en la matière deux types de transparence : la transparence qualitative et la transparence quantitative. La transparence qualitative implique que les gouvernements diffusent publiquement les lois, les interprétations juridiques, les procédures administratives et les autres mesures liées aux restrictions de contenu et à la surveillance. Pour les entreprises, la transparence qualitative implique de communiquer avec les utilisateurs sur les processus de réponse aux requêtes gouvernementales et d'application des règles et procédures de l'entreprise. La transparence quantitative appelle à la publication de données agrégées sur les requêtes gouvernementales et les taux de réponse, ainsi que des autres données qui permettraient aux internautes de comprendre quel type de contenu est supprimé, sous quels auspices et pour quelles raisons. GNI et le Center for Democracy and Technology ont élaboré des recommandations de transparence pour les gouvernements en ce qui concerne la restriction de contenu. Des mesures de transparence similaires sont recommandées pour que les gouvernements communiquent des rapports ainsi bien quantitatifs que qualitatifs sur la surveillance. Les entreprises

devraient diffuser, au minimum une fois par an, des informations agrégées sur la quantité de demande d'informations personnelles et de surveillance en temps réel qu'elles reçoivent, et sur leur manière d'y répondre. Les gouvernements devraient engager des réformes qui permettraient clairement une telle transparence, et les entreprises devraient être capables de révéler l'existence des exigences techniques que les gouvernements leur imposent en matière de surveillance, et de fournir des informations de base à ce sujet.

8.4 VIE PRIVÉE

La protection de la vie privée des utilisateurs est essentielle pour permettre à la liberté d'expression de prospérer. Les intermédiaires devraient adopter des meilleures pratiques en matière de respect de la vie privée et disposer de politiques claires et compréhensibles en ce qui concerne les données personnelles collectées et stockées, leurs manières de les traiter, et les circonstances dans lesquelles les autorités peuvent y avoir accès. L'existence de ces politiques devrait être communiquée, et celles-ci devraient être faciles d'accès. En ce qui concerne les gouvernements, les politiques, réglementations, lois et pratiques d'application qui ont un impact sur la vie privée des utilisateurs, notamment la collecte et la surveillance pour faire appliquer de la loi, doivent respecter les principes fondamentaux des droits de l'homme. Les Principes internationaux sur l'application des droits de l'homme à la surveillance des communications, élaborés par une coalition mondiale de groupes de la société civile entre fin 2012 et mai 2014, définissent 13 principes auxquels les gouvernements et les entreprises peuvent faire appel pour veiller à ce que la surveillance des communications soit réalisée dans le respect des normes internationales relatives aux droits de l'homme.

8.5 ÉVALUATION DE L'IMPACT SUR LES DROITS DE L'HOMME

La protection de la liberté d'expression en ligne pourrait être renforcée si les gouvernements réalisaient des évaluations de l'impact sur les droits de l'homme, pour déterminer en quoi les propositions de lois, de réglementations et de politiques pourraient affecter la liberté d'expression des internautes et/ou leur vie privée, aussi bien au niveau national que mondial, et publier les résultats de ces évaluations. Les entreprises devraient réaliser des évaluations de l'impact sur les droits de l'homme pour déterminer en quoi leurs politiques, pratiques et activités commerciales affectent la liberté d'expression des internautes, et adapter leurs activités en fonction des résultats, avec des stratégies pour limiter les préjudices potentiels identifiés. Afin d'obtenir les meilleures informations possibles pour mener à bien ce genre d'évaluation, il convient de s'engager auprès des parties prenantes dont les droits à la liberté d'expression sont les plus vulnérables en ligne, y compris les médias et les groupes de la société civile qui sont capables de représenter leurs intérêts.

8.6 L'AUTORÉGULATION DOIT SUIVRE LES PRINCIPES DE PROCÉDURE RÉGULIÈRE ET DE RESPONSABILITÉ, ET RESPECTER LES NORMES RELATIVES AUX DROITS DE L'HOMME

Les droits nationaux doivent renforcer les procédures judiciaires et l'adhésion aux normes internationales relatives aux droits de l'homme pour protéger les droits des internautes, mais des principes directeurs sont également essentiels pour garantir la légitimité des entreprises dans leur rôle de dépositaire des contenus en ligne. Ils doivent être un point de référence pour les procédures d'application des conditions de service privées. Ceci est conforme aux normes internationales, qui exigent que toute limitation de la liberté d'expression soit définie par des règles et prévisible, et non pas arbitraire ou rétroactive. L'autorégulation devrait également mieux respecter les principes de nécessité, de proportionnalité, et d'objectif légitime internationalement admis. Afin de permettre une expérience sûre pour les utilisateurs, les restrictions de contenu mises en place par les intermédiaires devraient non seulement être aussi minimes que possible, mais également éviter d'entrer en conflit avec le principe fondamental des droits de l'homme de non-discrimination – qui est intimement lié à la question de neutralité d'Internet. Afin d'identifier et de limiter les potentiels impacts négatifs sur la liberté d'expression des utilisateurs, les intermédiaires peuvent réaliser des évaluations de l'impact de leur système d'autorégulation sur les droits de l'homme.

L'Internet Society a proposé en 2014 des principes et recommandations en matière de procédures et d'institutions d'autorégulation, y compris des moyens spécifiques pour que les dispositifs d'autorégulation élaborent des pratiques transparentes et responsables. Les règles proportionnées et équilibrées, les procédures régulières et les garanties judiciaires sont des éléments essentiels. Les systèmes de ce type devraient faire l'objet d'évaluations périodiques.

8.7 RÉPARATION

Les internautes ont le droit d'avoir une voie de recours efficace quand leurs droits sont restreints ou violés par des intermédiaires, par des États ou bien par les deux à la fois. Il devrait être possible pour les particuliers de porter réclamation et d'obtenir réparation de la part des intermédiaires privés comme des autorités gouvernementales, y compris les institutions nationales des droits de l'homme. Lorsqu'ils demandent réparation pour des restrictions ou des violations de leurs droits à la liberté d'expression en ligne, les internautes ne devraient pas nécessairement avoir à engager d'actions juridiques auprès d'un tribunal. Des voies de recours connues, accessibles, abordables et capables de garantir les réparations adaptées devraient être mises à la disposition du public.

En fonction du contexte national, les dispositifs de réclamation et de réparation fournis par les États peuvent inclure des dispositifs fournis par les autorités de protection des données, les institutions des droits de l'homme, les procédures judiciaires et les services

d'assistance. Les dispositifs de réclamation et de réparation fournis par les intermédiaires privés et les mécanismes privés de régulation devraient contenir des dispositifs d'autorégulation pour recevoir les réclamations des internautes et y répondre. Ces dispositifs doivent être accessibles, sécurisés, et appropriés du point de vue linguistique et culturel. La question de savoir si une réparation réelle existe pour les utilisateurs dont les droits à la liberté d'expression ont été restreints ou violés devrait être examinée dans le cadre d'une procédure d'évaluation de l'impact sur les droits de l'homme, réalisée par l'entreprise. En fonction de la réclamation et du dommage identifié, la réparation peut, mais ne doit pas obligatoirement, impliquer des compensations financières. Des mesures compensatoires concrètes peuvent également être la reconnaissance du problème, des excuses ou l'engagement à traiter le problème à l'avenir ; la réalisation d'une enquête indépendante ou la mise en place d'une surveillance permanente ; ou la participation à des groupes multipartites au niveau régional ou du secteur pour clarifier et limiter les potentielles restrictions ou violations des droits des utilisateurs.

8.8 ÉDUCATION ET INFORMATION PUBLIQUES, ET ÉDUCATION AUX MÉDIAS ET À L'INFORMATION

Le concept composite d'éducation aux médias et à l'information couvre toutes les compétences nécessaires aux citoyens pour participer aux sociétés du savoir. Dans leur relation avec les intermédiaires de l'Internet, les citoyens nécessitent un ensemble de connaissances sur la question de la libre expression. Les entreprises et les gouvernements ont un rôle à jouer dans la promotion, formelle comme informelle, de ces connaissances. Les États ont l'obligation de fournir des informations claires et accessibles au public pour que les internautes non seulement comprennent et exercent efficacement leurs droits, mais reconnaissent également quand leurs droits ont été restreints, violés ou perturbés. Les restrictions de la libre expression par les États ne doivent pas uniquement être réalisées dans un but légitime et respecter les droits de l'homme, elles doivent également être rendues publiques. L'information du public devrait également inclure des instructions concrètes sur les dispositifs officiels de réclamation et de réparation.

Le respect des droits des internautes par les intermédiaires privés nécessite également d'informer les utilisateurs et de communiquer avec eux sur leurs droits, sur la manière dont leur expression peut être restreinte en fonction des conditions de service de l'intermédiaire, sur les raisons de ces restrictions et leur nécessité, et sur toute autre information pertinente, pour qu'ils décident de manière éclairée d'utiliser ou non le service. Les institutions éducatives devraient être encouragées et incitées à inclure des informations sur les droits des internautes dans les cursus en rapport aux droits de l'homme, aux gouvernements ou à l'instruction civique. De même, les médias devraient être encouragés et incités à inclure des contenus qui encouragent des discussions publiques éclairées sur les droits des internautes, et sur l'obligation des États et des entreprises de respecter et de protéger ces droits.

8.9 MÉCANISMES GLOBAUX DE RESPONSABILISATION

Les entreprises comme les gouvernements peuvent s'engager à mettre en œuvre les principes fondamentaux de liberté d'expression et de respect de la vie privée. Dans notre environnement mondial numérique et interconnecté, ces principes devraient être mis en œuvre d'une manière responsable, aussi bien localement que mondialement. Une autre approche de responsabilisation des entreprises est leur évaluation et leur accréditation par des organisations indépendantes multipartites. GNI, une coalition multipartite, demande à ses membres de réaliser des évaluations périodiques dans le cadre d'un dispositif de responsabilisation pour l'adhésion à ses principes et la mise en œuvre de directives sur la manière dont les entreprises traitent les requêtes gouvernementales. Néanmoins, les directives de mise en œuvre et les évaluations de GNI n'incluent pas à l'heure actuelle la question de la vie privée des consommateurs ou celle de l'application des conditions de service. D'autres organisations et dispositifs devraient peut-être voir le jour, pour améliorer la responsabilisation et la transparence dans ces domaines si GNI est incapable de les intégrer à l'avenir.

En ce qui concerne les États, une coalition de 27 gouvernements a rejoint la Freedom Online Coalition, dont les membres ont accepté de travailler ensemble pour faire avancer « la liberté d'expression, d'association, et de rassemblement ainsi que la vie privée en ligne à l'échelle mondiale ». En avril 2014, les membres de la coalition ont publié la déclaration de Tallinn, un ensemble de « Recommandations pour la liberté en ligne ». Trois groupes de travail multipartites ont été mis en place. La coalition organise une conférence annuelle où sont invités des représentants d'entreprises et de la société civile. Il reste néanmoins à voir si des dispositifs vont émerger pour pouvoir évaluer les gouvernements et permettre aux parties prenantes mondiales de les tenir responsable de la mesure dans laquelle ils ont répondu à ces recommandations. Les intermédiaires de l'Internet vont subir d'intenses pressions pour être à la hauteur de leur responsabilité en matière de respect les droits de l'homme, à moins que les gouvernements ne remplissent leurs propres obligations de protection des droits de l'homme, y compris la liberté d'expression et le respect de la vie privée en ligne.

9. CONCLUSION

Ce chapitre s'est concentré sur le rôle de trois types d'intermédiaires de l'Internet pour la promotion de la liberté d'expression, en prêtant une attention particulière aux contextes normatifs, juridiques et politiques dans lesquels ils évoluent. Cette étude n'a pas pour objectif d'être un échantillon représentatif ou statique d'acteurs, mais plutôt d'extrapoler des perspectives plus générales. Diverses tendances ont été identifiées, dont une amélioration générale de la prise de conscience et du nombre d'actions entreprises par les intermédiaires eux-mêmes ou par les gouvernements pour tenir compte de l'importance des FSI, des moteurs de recherche et des réseaux sociaux pour la liberté d'expression.

Cette analyse cherche à aider toutes les parties prenantes, ainsi que les intermédiaires, à identifier en quoi le rôle de garde-barrière inhérent à la médiation des contenus d'Internet peut être optimisé pour la liberté d'expression et le respect de la vie privée. De cette manière, les intermédiaires de l'Internet peuvent contribuer à l'évolution des sociétés du savoir, qui est elle-même cruciale pour l'avènement de la démocratie, du développement durable et de la paix à l'échelle mondiale.

VI. SÉCURITÉ DES JOURNALISTES

1. PRÉSENTATION

Ce chapitre examine les récentes tendances en matière de sécurité des journalistes, en présentant les statistiques de l'UNESCO pour 2013 et 2014 et en suivant les autres développements jusqu'en août 2015. Il suit le cadre du précédent rapport de l'UNESCO intitulé *Tendances mondiales en matière de liberté d'expression et de développement des médias*, réalisé à la demande des États membres dans la Résolution 53 de la 36e Conférence générale de l'UNESCO, et qui couvrait la période de 2007 à mi-2013. Il traite notamment de la sécurité physique, de l'impunité et de l'emprisonnement des journalistes, et aborde également ces questions sous l'angle du genre.[7] Ce chapitre examine également les récentes tendances en matière de renforcement des normes internationales, d'élaboration de mécanismes pratiques, d'amélioration de la coopération interagences, d'amélioration de la collaboration avec le système judiciaire et les forces de sécurité, et de recherche.

Le présent chapitre note également que les assassinats de journalistes ont connu un pic en 2012, année pour laquelle l'UNESCO a relevé 123 cas, pic suivi d'une légère diminution les deux années suivantes. Le nombre de journalistes tués reste néanmoins très élevé. Au cours de la période étudiée, une faible proportion des États membres où les assassinats de journalistes ont été perpétrés ont répondu aux demandes d'information sur le statut des enquêtes judiciaires. Selon les données reçues, il semble que le taux d'impunité reste également élevé. Dans le même temps, l'attention portée et les efforts conjoints au sujet de la sécurité des journalistes et de l'impunité ont augmenté au niveau international, ainsi que dans certains pays.

7 Voir UNESCO. 2014. *Tendances mondiales en matière de liberté d'expression et de développement des médias*. Paris : UNESCO. http://unesdoc.unesco.org/images/0022/002270/227025f.pdf et Résolution 53, adoptée lors de la 36e Session de la Conférence générale de l'UNESCO en novembre 2011. Disponible à l'adresse suivante : http://unesdoc.unesco.org/images/0021/002150/215084f.pdf

2. SÉCURITÉ PHYSIQUE

L'UNESCO continue d'être l'agence des Nations Unies mandatée spécialement pour défendre la liberté de la presse et la liberté d'expression, et dont le rôle est de sensibiliser aux assassinats de journalistes, d'agents des médias et de producteurs de médias sociaux.[8] Mettre un terme à l'impunité pour les crimes à l'encontre des journalistes a représenté une part importante des travaux réalisés en 2013-2014. Dans ce contexte, la Directrice générale de l'UNESCO, par mandat du Conseil intergouvernemental du Programme international pour le développement de la communication (PIDC) de l'Organisation, a continué à condamner tous les meurtres avérés pendant la période étudiée. Elle a en outre continué de demander aux États membres où ces crimes ont eu lieu de transmettre volontairement des informations sur l'avancement des procédures judiciaires. Par une décision du PIDC en 2012,[9] les États transmettant ces informations peuvent indiquer s'ils souhaitent ou non voir leur réponse mentionnée sur la page Internet de l'UNESCO dédiée à ce sujet[10] , qui répertorie les assassinats et les déclarations de la Directrice générale.

Plus particulièrement, en 2013 et 2014, la Directrice générale de l'UNESCO a publiquement dénoncé les assassinats d'un total de 178 journalistes, agents des médias et producteurs de média sociaux impliqués dans des activités journalistiques.

En 2013, on a dénombré 91 assassinats, soit une diminution d'un quart par rapport à 2012. Néanmoins, ce chiffre représente le second plus grand nombre de meurtres de journalistes depuis 2006. Après plusieurs années de calme relatif en Irak, le nombre de journalistes tués est passé à 15 en 2013, en faisant le pays le plus dangereux pour les journalistes cette année-là. Cependant, pour comparaison, les premiers et seconds plus grands chiffres enregistrés en la matière en Irak sont 33 assassinats en 2007 et 29 en 2006.

En 2014, la Directrice générale a fait des déclarations publiques sur 87 affaires d'assassinat de journalistes. Le conflit armé en cours en Syrie a couté la vie à de nombreux journalistes, avec dix morts en 2014. Cette même année,[11] huit journalistes ont été tués en Palestine, cinq en Irak, cinq en Libye, et cinq en Afghanistan. Sept journalistes ont également été tués en Ukraine.

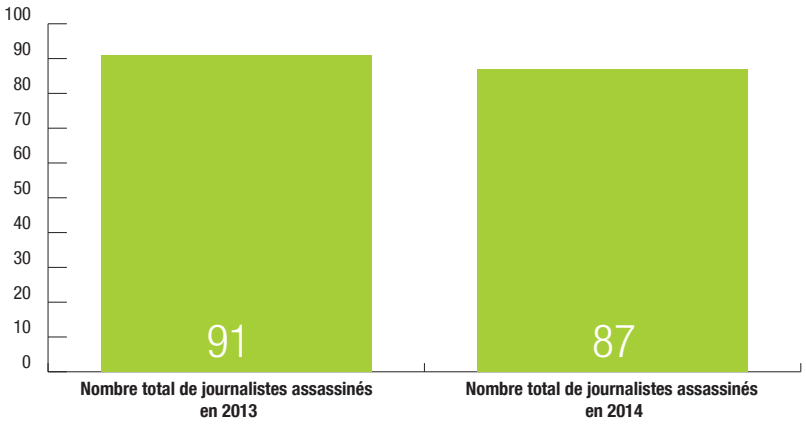
8 Voir la Décision 196 EX/31 sur la sécurité des journalistes et la question de l'impunité adoptée lors de la 196e session du Conseil exécutif de l'UNESCO. Disponible à l'adresse suivante : http://unesdoc.unesco.org/images/0023/002323/232337f.pdf

9 La 28e session du Conseil PIDC a demandé à la Directrice générale « de mettre sur le site Internet de l'UNESCO, à la demande des États membres concernés, les informations fournies officiellement pour chacun des décès de journalistes condamnés par l'Organisation ».

10 Voir le site Internet dédié « L'UNESCO condamne l'assassinat de journalistes » à l'adresse suivante : www.unesco.org/new/fr/condemnation

11 Ces zones ont été identifiées dans le rapport 2013 du Secrétaire général des Nations Unies sur la protection des civils dans les conflits armés, soumis au Conseil de sécurité des Nations Unies tous les 18 mois.

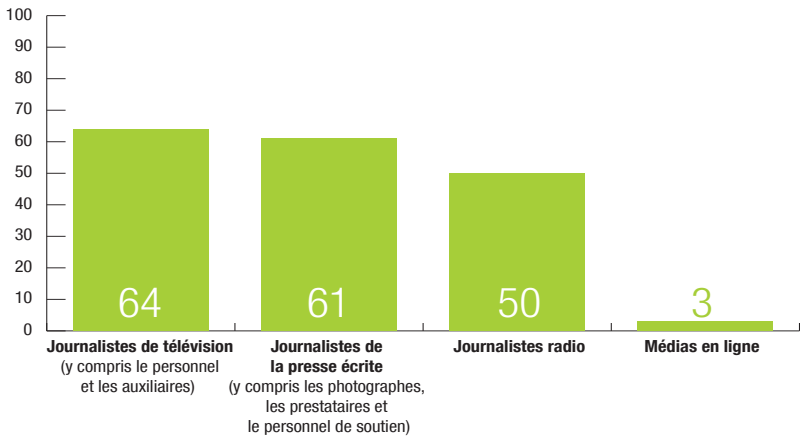
Nombre total de journalistes assassinés en 2013 et 2014



Les années précédentes, la grande majorité des journalistes assassinés était des locaux. En 2013, sept des 91 journalistes assassinés (8 %) venaient de pays étrangers. En 2014, le nombre de correspondants étrangers tués a grandement augmenté en passant à 20 % (17 cas sur 87). Douze de ces affaires ont eu lieu en Syrie et en Ukraine.

En ce qui concerne les types de média, les journalistes de télévision (y compris le personnel et les auxiliaires) ont été les plus touchés, avec 64 morts pendant la période 2013-2014. Viennent ensuite les journalistes de la presse écrite (y compris les photographes, les prestataires et le personnel de soutien), avec 61 morts. On compte également 50 morts parmi les journalistes radio. Trois journalistes travaillant essentiellement pour les médias en ligne ont également été tués pendant cette période. En tout, 98 % de ces assassinats ont touché des personnes travaillant pour les médias « traditionnels ».

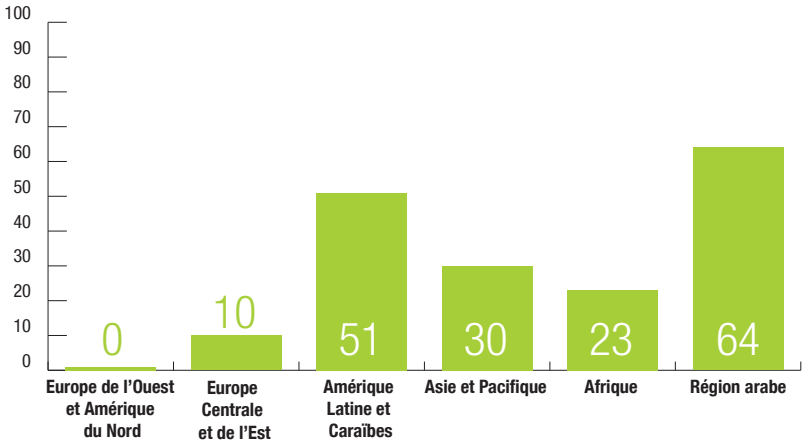
Nombre total de journalistes tués par type de média au cours de la période 2013-2014



En ce qui concerne les régions où ces crimes ont été perpétrés, 64 ont eu lieu dans la région des États arabes (36 %), ce qui en a fait la région la plus dangereuse pour les journalistes en 2013 et 2014. Au total, 10 assassinats de journalistes ont été commis en Europe centrale et en Europe de l'Est, 23 dans la région Afrique, 30 dans la région Asie et Pacifique, et 51 dans

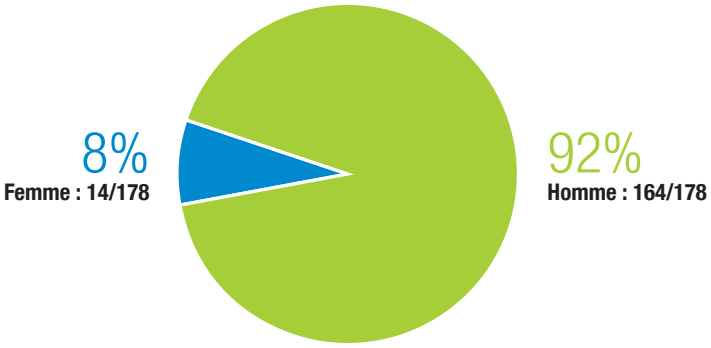
la région Amérique latine et Caraïbes. Pendant les deux années étudiées, aucun assassinat de journaliste n'a été identifié en Europe de l'Ouest et en Amérique du Nord.[12]

Nombre total de journalistes tués par région au cours de la période 2013-2014



Entre 2013 et 2014, la très grande majorité des journalistes tués étaient des hommes, avec un total de 164 meurtres sur 178 (92 %).

Nombre de journalistes tués par genre au cours de la période 2013-2014



La sécurité numérique des journalistes, pouvant également mener à des menaces physiques à l'encontre des journalistes et de leurs sources, est devenue un problème bien plus important au cours de cette période. Un certain nombre de médias ont du faire face à des attaques sur leurs sites internet, à des intrusions dans leurs communications électroniques et à la saisie de leurs dispositifs numériques.[13]

12 Les attaques perpétrées à l'encontre de l'hebdomadaire français *Charlie Hebdo* ont eu lieu peu de temps après cette période.

13 Celles-ci sont identifiées dans les publications 2015 de l'UNESCO *Construire une sécurité numérique pour le journalisme : enquête sur une sélection de questions*, et *Des clés pour la promotion de sociétés du savoir inclusives*, ainsi que dans la recherche menée pour l'UNESCO par l'Association Mondiale des journaux (WAN-IFRA) sur le thème de la protection de la confidentialité des sources dans le monde numérique.

3. IMPUNITÉ

Une demande d'information sur l'avancement des enquêtes de l'ensemble des assassinats de journalistes non résolus et condamnés par l'UNESCO est envoyée chaque année à tous les États membres sur les territoires desquels des meurtres ont été commis. Selon les données reçues, il semble que la tendance reste à l'impunité : en effet, peu d'auteurs d'assassinats de journalistes ont été traduits en justice.

L'impunité désigne l'absence de sanction contre les personnes qui commettent un crime. Elle est le symbole de l'échec des systèmes judiciaires et de la création d'un environnement dans lequel les crimes contre la liberté d'expression restent impunis, ce qui alimente un cercle vicieux et pose une sérieuse menace à la liberté d'expression. La pratique de l'impunité et l'impunité escomptée pour les crimes commis contre les journalistes ont des implications sur l'impunité de manière plus générale. Les journalistes qui poursuivent leur travail en faisant fi des inquiétudes permettent de veiller à ce que d'autres violations des droits n'aient pas lieu dans l'ombre. Si les crimes à l'encontre de journalistes continuent à rester impunis, cela risque d'encourager les violations de nombreux droits de l'homme autres que la liberté d'expression et la liberté de la presse, tout en favorisant d'autres formes de criminalité. La réduction au silence par des moyens physiques, les arrestations et les détentions arbitraires, les disparitions forcées, le harcèlement et l'intimidation visent souvent non seulement à faire taire les journalistes, mais aussi à intimider la population pour l'amener à pratiquer l'autocensure.

En juin 2012, le Rapporteur spécial des Nations Unies sur la promotion et la protection du droit à la liberté d'opinion et d'expression[14] mettait l'impunité sur le compte du manque de volonté politique à mener des enquêtes, exacerbé par la peur des représailles de la part de puissants réseaux criminels, des faiblesses du cadre juridique, du système judiciaire et des forces de police, du manque de ressources, et de la négligence ou de la corruption.

Le dernier rapport biennal du Directeur général du PIDC sur la sécurité des journalistes et le risque d'impunité, publié en 2014, souligne que dans neuf cas sur dix, les auteurs de ces crimes ne sont jamais poursuivis.[15] Le rapport continue à exhorter les États membres « d'informer la Directrice générale de l'UNESCO, sur base du volontariat, des actions engagées pour mettre fin à l'impunité des auteurs de crimes et de lui indiquer les progrès des enquêtes judiciaires diligentées sur chacun des meurtres de journalistes [...] qui ont été condamnés par l'UNESCO ».

14 Le rapport du Rapporteur spécial des Nations Unies sur la promotion et la protection du droit à la liberté d'opinion et d'expression (A/HRC/20/17) a été présenté à la 20e session du Conseil des droits de l'homme.

15 Ce rapport est réalisé conformément aux décisions adoptées par le Conseil intergouvernemental du PIDC lors de ces 26e, 27e, 28e et 29e sessions, respectivement en 2008, 2010, 2012 et 2014.

Comme par le passé, le taux de réponse des États membres reste faible.[16] En 2013, sur les 57 pays dans lesquels des meurtres de journalistes ont été commis et n'ont pas encore été résolus, 17[17] (30 %) ont répondu à la demande officielle d'information. En 2014, 13 pays sur 59[18] (22 %) ont répondu à la requête officielle. Au 31 août 2015, 24 pays sur 57[19] (42 %) ont répondu à la dernière demande d'information, signe d'une possible tendance à la hausse.

Les réponses reçues en 2015 se réfèrent à 46% des 641 cas non résolus durant la période du 1er janvier 2006 au 31 décembre 2014. Cela représente une augmentation de la portée des informations par rapport à la période précédente. Entre 2006 et 2013 inclus, les informations étaient reçues dans 22% des cas non résolus. Cependant, en dépit d'une couverture plus élargie, il est toujours vrai qu'aucune information n'est reçue dans plus de la moitié des cas.

Parmis les informations reçues par l'UNESCO de la part des Etats Membres, les cas cumulés déclarés comme judiciairement résolus représentent 5% en 2012 et 8% en 2014. Bien que cela représente une faible augmentation dans les pourcentages et malgré l'existence de cas signalés comme perpétuellement en cours, il est évident que l'impunité demeure la tendance prédominante. En extrapolant, ces pourcentages peuvent également s'appliquer aux cas pour lesquels l'UNESCO n'a reçu aucune information, ce qui signifierait que la proportion de cas résolus à tous niveaux serait déterminée comme étant toujours extrêmement faible.

16 En 2011, une demande officielle d'information a été envoyée à 38 pays où des meurtres de journalistes ont été perpétrés, et 19 d'entre eux ont répondu sur la période 2011-2012, soit 50 %. Pour la période de 2007 à 2012, le rapport de l'UNESCO Tendances mondiales en matière de liberté d'expression et de développement des médias de 2014 indique que 42 % des États membres avaient répondu à la mi-2013.

17 En 2013, 17 pays ont répondu à la requête officielle : Bahreïn, Bolivie, Brésil, Colombie, Croatie, Fédération de Russie, Honduras, Kazakhstan, Kenya, Pérou, République démocratique du Congo, République du Congo, Sri Lanka, Tanzanie, Tunisie, Turkménistan, et Vietnam. Cette même année, 40 pays n'ont pas répondu : Afghanistan, Angola, Bangladesh, Bulgarie, Cambodge, Cameroun, Chine, Égypte, El Salvador, Équateur, Érythrée, Géorgie, Grèce, Guatemala, Haïti, Inde, Indonésie, Iran, Irak, Kirghizistan, Liban, Libye, Mexique, Myanmar, Népal, Nigéria, Ouganda, Pakistan, Palestine, Philippines, République dominicaine, Guyana, Rwanda, Somalie, Soudan, Syrie, Thaïlande, Turquie, Venezuela et Yémen.

18 En 2014, 13 pays ont répondu à la requête officielle : Chine, Colombie, El Salvador, Honduras, Indonésie, Irak, Mexique, Pakistan, Pérou, Philippines, République dominicaine, Tanzanie, et Turquie. Cette même année, 46 pays n'ont pas répondu à cette requête dont notamment : Afghanistan, Angola, Bahreïn, Bangladesh, Bolivie, Brésil, Bulgarie, Cambodge, Cameroun, République Centrafricaine, République du Congo, République démocratique du Congo, Equateur, Egypte, Erythrée, Géorgie, Grèce, Guatemala, République de Guinée, Haïti, Inde, Iran, Kenya, Kirghizstan, Liban, Libye, Mali, Myanmar, Népal, Nigéria, Palestine, Paraguay, Fédération de Russie, Rwanda, Somalie, Soudan du Sud, Sri Lanka, Soudan, Syrie, Thaïlande, Tunisie, Turkménistan, Uganda, Venezuela et Yémen.

19 Au 1er septembre 2015, 24 pays ont répondu à la requête officielle : Bahreïn, Brésil, Bulgarie, Colombie, Égypte, El Salvador, Équateur, Érythrée, Grèce, Guatemala, Haïti, Honduras, Indonésie, Mexique, Nigéria, Pakistan, Paraguay, Philippines, République dominicaine, Sri Lanka, Tanzanie, Turquie, Ukraine, et Venezuela. Cette même année, 33 pays n'ont pas répondu : Afghanistan, Angola, Bangladesh, Cambodge, Cameroun, République Centrafricaine, République du Congo, République démocratique du Congo, Géorgie, République de Guinée, République de Guyana, Inde, Iran, Irak, Kenya, Kirghizstan, Liban, Libye, Mali, Myanmar, Népal, Palestine, Pérou, Fédération de Russie, Rwanda, Somalie, Soudan du Sud, Soudan, Syrie, Thaïlande, Tunisie, Uganda et Yémen.

Taux de réponses des Etats membres aux requêtes de la Directrice générale sur le statut des enquêtes judiciaire concernant des journalistes assassinés (1 janvier 2013 – 31 août 2015)

30 %
2013 : 17/57 pays

22 %
2014 : 13/59 pays

42 %
2015 : 24/ 57 pays

4. TENDANCE À LA HAUSSE DU RENFORCEMENT DES NORMES INTERNATIONALES SUR LA SÉCURITÉ DES JOURNALISTES

Bien que les tendances décrites ci-dessus n'aient connu aucun revirement majeur par rapport à la période précédente, de grands progrès ont en revanche été faits au niveau normatif. Ces deux dernières années ont vu un renforcement significatif des normes internationales relatives à la sécurité des journalistes. Cette tendance s'est accrue par la réaction mondiale face aux meurtres de journalistes du magazine satirique *Charlie Hebdo* commis à Paris début 2015, attentat suivi par la décapitation brutale de journalistes en Syrie. Bien que cet attentat ait eu lieu après la période étudiée, il est mentionné dans ce chapitre, car il a eu lieu dans un contexte d'attention internationale accrue qu'il a encore permis de renforcer, notamment grâce à une marche de protestation rassemblant des dirigeants mondiaux. Tout comme les images de décapitation de journalistes par des extrémistes et les meurtres particulièrement violents perpétués par des trafiquants de drogue à l'encontre de reporters pendant la période 2013-2014, l'attentat commis en 2015 à Paris a sensibilisé le monde entier à la gravité de ces crimes.

Les activités des Nations Unies sont un bon indicateur de cette sensibilité accrue. Comme détaillé ci-après, sur la période 2012-2015, le Conseil de sécurité des Nations Unies, l'Assemblée générale, le Conseil des droits de l'homme et l'UNESCO ont adopté d'importantes résolutions et décisions qui condamnent sans équivoque toutes les attaques et violences à l'encontre des journalistes. Bon nombre de ces déclarations incluent des mesures visant à renforcer la surveillance à l'échelle mondiale et les mécanismes de signalement en matière de sécurité, et soulignent également à quel point il est important que les États membres prennent des mesures pour mettre un terme à l'impunité.

L'Assemblée générale des Nations Unies, le plus haut organe décisionnel de l'Organisation des Nations Unies, a adopté les Résolutions A/RES/68/163 (en 2013) et A/RES/69/185 (en 2014), qui condamnent vigoureusement toutes les attaques à l'encontre des journalistes et des agents des médias, y compris la torture, les exécutions sommaires, les disparitions forcées, les détentions arbitraires, le harcèlement et l'intimidation, dans les situations de conflit comme de paix. Ces Résolutions critiquent également fermement l'impunité persistante dans les affaires d'agressions et de violences à l'encontre des journalistes.

En outre, par sa Résolution A/RES/68/163, l'Assemblée générale a instauré la Journée internationale de la fin de l'impunité pour les crimes commis contre des journalistes, le 2 novembre, marquant ainsi une étape importante de la reconnaissance du problème à l'échelle internationale. L'UNESCO, qui a été chargée de faciliter les commémorations de cette journée internationale, a organisé entre autres une conférence à la Cour européenne des droits de l'homme à Strasbourg, en France, en collaboration avec le Conseil de l'Europe, le centre pour la liberté des médias de l'université de Sheffield et l'Union des Avocats Européens. Des évènements locaux ont également été organisés à New York, Tunis, Accra et Abuja. Lors de ces événements, l'UNESCO a cherché à

dialoguer avec les acteurs de la justice, à les sensibiliser au rôle qu'ils peuvent jouer pour mettre à terme à l'impunité, et à les informer sur la manière dont les efforts engagés pour résoudre ces crimes à l'encontre de journalistes peuvent contribuer au renforcement des règles de droit et des droits de l'homme dans l'ensemble de la société. L'événement de Strasbourg a également permis une évaluation multipartite du Plan d'Action des Nations Unies sur la sécurité des journalistes et la question de l'impunité. Le Plan a été approuvé par le Conseil des chefs de secrétariat des organismes des Nations Unies en 2012, et salué par l'Assemblée générale des Nations Unies en décembre 2013, dans sa Résolution A/RES/68/163.

Deux Résolutions traitant de la sécurité des journalistes ont également été adoptées : la Résolution historique de 2012 (A/HRC/RES/21/12) adoptée par le Conseil des droits de l'homme, suivie en 2014 par la Résolution A/RES/HRC/27/5. Ces Résolutions appellent toutes les parties à respecter leurs obligations en matière des droits de l'homme et de droit humanitaire international. Elles encouragent également tous les États à promouvoir un environnement sûr et favorable pour que les journalistes puissent travailler de manière indépendante sans ingérence excessive.

Lors de sa 191e session en avril 2013, le Conseil exécutif de l'UNESCO a approuvé le Plan de travail de l'UNESCO sur la sécurité des journalistes et la question de l'impunité. Le Plan de travail, qui met en avant la coopération Sud-Sud, définit l'approche de l'UNESCO en matière de sécurité, dans le cadre du Plan de travail des Nations Unies sur la sécurité des journalistes et la question de l'impunité. Subséquemment, le Conseil exécutif de l'UNESCO a adopté la Décision sur la sécurité des journalistes et la question de l'impunité le 20 avril 2015, lors de sa 196e session. Cette Décision renforce les travaux actuels de l'UNESCO en rapport au Plan d'action des Nations Unies, par une approche multipartite qui implique tous les acteurs pertinents, y compris des autorités nationales, des agences des Nations Unies, des groupes de la société civile, des universitaires et les médias. La Décision a de nouveau confirmé que la mission de veiller à la sécurité du journalisme comprend la sécurité des producteurs de médias sociaux, qui sont parmi les acteurs majeurs du journalisme d'intérêt public.

De plus, le Conseil de sécurité des Nations Unies a adopté la Résolution 2222 (le 27 mai 2015), qui appelle les parties en conflit et tous les États membres à créer un environnement sûr, dans la loi comme dans les faits, pour permettre aux journalistes de faire leur travail. Elle prie également le Secrétaire général des Nations Unies d'inclure systématiquement dans ses rapports sur la protection des civils en période de conflit armé une sous-section sur la sûreté et la sécurité des journalistes, des professionnels des médias et du personnel associé.

Le nombre croissant de signataires de ces résolutions témoigne d'une meilleure reconnaissance de la gravité du problème.

- Résolution A/RES/68/163 de l'Assemblée générale des Nations Unies, adoptée en 2013 : 54 signataires[20]
- Résolution A/RES/69/185 de l'Assemblée générale des Nations Unies, adoptée en 2014 : 82 signataires[21]
- Résolution A/HRC/21/12 du Conseil des droits de l'homme, adoptée en 2012 : 52 signataires[22]
- Résolution A/HRC/27/5 du Conseil des droits de l'homme, adoptée en 2014 : 63 signataires[23]

La décision du Conseil exécutif de l'UNESCO 196 EX/31, adoptée en avril 2015 a également reçu la signature de 47 États.[24] De même, le Conseil de sécurité des Nations Unies a adopté la Résolution UNSC 2222 (le 27 mai 2015) avec les signatures de 49 États.[25]

20 Les 54 pays suivants se sont portés coauteurs de la Résolution A/RES/68/163 : Albanie, Allemagne, Andorre, Argentine, Arménie, Australie, Autriche, Azerbaïdjan, Belgique, Bénin, Bosnie-Herzégovine, Brésil, Bulgarie, Canada, Chili, Chypre, Colombie, Costa Rica, Croatie, El Salvador, Espagne, Estonie, États-Unis d'Amérique, France, Ghana, Grèce, Hongrie, Irlande, Italie, Japon, Lettonie, Luxembourg, Maldives, Mali, Malte, Maroc, Mongolie, Nigeria, Panama, Paraguay, Pays-Bas, Pérou, Pologne, Portugal, Qatar, République de Corée, République tchèque, Roumanie, Saint-Marin, Serbie, Slovaque, Slovénie, Tunisie, Turquie et Uruguay.

21 Les 82 pays suivants se sont portés coauteurs de la Résolution A/RES/69/185 : Allemagne, Andorre, Argentine, Arménie, Australie, Autriche, Azerbaïdjan, Belgique, Bénin, Bosnie-Herzégovine, Brésil, Bulgarie, Burkina Faso, Cap-Vert, Chili, Chypre, Colombie, Costa Rica, Croatie, Danemark, Égypte, El Salvador, Espagne, Estonie, États-Unis d'Amérique, Finlande, France, Géorgie, Ghana, Grèce, Guatemala, Honduras, Hongrie, Irlande, Islande, Israël, Italie, Japon, Jordanie, l'ancienne République yougoslave de Macédoine, Lettonie, Liban, Libye, Liechtenstein, Lituanie, Luxembourg, Maldives, Mali, Malte, Maroc, Mexique, Monaco, Mongolie, Monténégro, Norvège, Nouvelle-Zélande, Panama, Paraguay, Pays-Bas, Pérou, Pologne, Portugal, Qatar, République centrafricaine, République centrafricaine, République de Corée, République de Moldavie, République tchèque, Roumanie, Royaume-Uni de Grande-Bretagne et d'Irlande du Nord, Saint-Marin, Serbie, Slovaquie, Slovénie, Somalie, Suède, Suisse, Tunisie, Turquie, Ukraine et Uruguay.

22 Les 52 pays suivants se sont portés coauteurs de la Résolution A/HRC/21/12 : Albanie, Allemagne, Argentine, Australie, Autriche, Belgique, Bosnie-Herzégovine, Botswana, Brésil, Bulgarie, Chypre, Colombie, Croatie, Danemark, Égypte, Estonie, Finlande, Géorgie, Grèce, Guatemala, Honduras, Hongrie, Irlande, Islande, Kenya, Lettonie, Liban, Libye, Liechtenstein, Lituanie, Luxembourg, Mexique, Monténégro Maroc, Nigéria, Norvège, Palestine, Pays-Bas, Pérou, Pologne, Portugal, Qatar, République de Moldavie, République tchèque, Roumanie, Royaume-Uni de Grande-Bretagne et d'Irlande du Nord, Serbie, Slovénie, Suède, Suisse, Tunisie et Turquie.

23 Les 63 pays suivants se sont portés coauteurs de la Résolution A/HRC/27/5 : Allemagne, Argentine, Australie, Autriche, Belgique, Bénin, Bosnie-Herzégovine, Brésil, Bulgarie, Burkina Faso, Canada, Chypre, Colombie, Costa Rica, Croatie, Danemark, Espagne, Estonie, États-Unis d'Amérique, Ex-République yougoslave de Macédoine, Finlande, France, Géorgie, Grèce, Guatemala, Honduras, Hongrie, Irlande, Islande, Italie, Lettone, Liban, Liechtenstein, Lituanie, Luxembourg, Maldives, Maroc, Mexico, Monténégro, Nigeria, Norvège, Nouvelle-Zélande, Palestine, Paraguay, Pays-Bas, Pérou, Pologne, Portugal, Qatar, République centrafricaine, République de Moldavie, République tchèque, Roumanie, Royaume-Uni de Grande-Bretagne et d'Irlande du Nord, Saint-Kitts-et-Nevis, Serbie, Slovaquie, Slovénie, Suède, Suisse, Tunisie, Turquie et Yémen.

24 Les 47 pays suivants se sont portés coauteurs de la décision du Conseil exécutif de l'UNESCO 196 EX/31 : Albanie, Allemagne, Andorre, Argentine, Australie, Autriche, Brésil, Chypre, Danemark, El Salvador, Espagne, Estonie, États-Unis d'Amérique, Finlande, France, Gabon, Grèce, Honduras, Irlande, Islande, Italie, Japon, Lettonie, Liberia, Malawi, Maroc, Namibie, Nigeria, Norvège, Paraguay, Pays-Bas, Pérou, Portugal, République de Corée, République dominicaine, République tchèque, Royaume-Uni, Saint-Kitts-et-Nevis, Serbie, Slovaquie, Slovénie, Suède, Suisse, Trinité-et-Tobago, Tunisie, Ukraine et Uruguay.

25 Les 49 pays suivants se sont portés coauteurs de la Résolution UNSC 2222 du Conseil de sécurité des Nations Unies : Albanie, Allemagne, Angola, Australie, Autriche, Belgique, Bosnie-Herzégovine, Bulgarie, Canada, Chili, Chypre, Croatie, Danemark, Espagne, Estonie, États-Unis d'Amérique, Ex-République yougoslave de Macédoine, Finlande, France, Grèce, Hongrie, Islande, Israël, Italie, Japon, Jordan, Lettonie, Liban, Liechtenstein, Lituanie, Luxembourg, Malaisie, Monténégro, Nigeria, Norvège, Nouvelle-Zélande, Palaos, Pays-Bas, Pologne, République de Moldavie, République tchèque, Roumanie, Royaume-Uni de Grande-Bretagne et d'Irlande du Nord, Serbie, Slovaquie, Slovénie, Suède, Tchad et Ukraine.

5. ÉLABORATION DE DISPOSITIFS PRATIQUES POUR PROMOUVOIR LA SÉCURITÉ ET METTRE UN TERME À L'IMPUNITÉ

En 2012 et 2013, de grands progrès ont été faits en matière de développement institutionnel sur la sécurité et l'impunité. De nombreux pays de la région Amérique latine ont continué à élaborer des cadres et institutions officiels pour traiter des problèmes de sécurité et de protection, et beaucoup se sont inspirés de l'expérience positive de la Colombie. Ces dispositifs sont entre autres des systèmes de coordination interdépartementale, des forums multipartites avec des représentants des médias et de la société civile, et l'affectation de personnel et de budget. Au Pakistan, une grande coalition a œuvré pour impliquer de nombreuses parties prenantes, notamment des parlementaires et des membres des gouvernements, dans des discussions régulières sur la sécurité et l'impunité. En Serbie, une commission de représentants des médias indépendants, d'un ministère et des services de sécurité a permis de poursuivre en justice quatre personnes accusées du meurtre d'un journaliste il y a 16 ans.

En 2013, le Haut-Commissariat aux droits de l'homme, en collaboration avec le Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, a publié un rapport mettant en valeur les initiatives et les meilleures pratiques relatives à la sécurité des journalistes et à l'impunité. Le rapport présente la situation des journalistes, les lois applicables et les initiatives mises en œuvre par les États membres, les agences des Nations Unies et d'autres organisations pour assurer la sécurité des journalistes. Il identifie également les meilleures pratiques qui pourraient aider à créer un environnement sûr et favorable dans lequel les journalistes pourraient exercer librement leur profession.

Le 2 avril 2015, le Conseil de l'Europe a créé une plate-forme en ligne visant à protéger le journalisme et à favoriser la sécurité des journalistes. La plate-forme est conçue pour faciliter la compilation, le traitement et la diffusion des informations factuelles, vérifiées par les partenaires, en ce qui concerne les menaces physiques sévères à l'encontre des journalistes et des autres professionnels des médias, les menaces relatives à la confidentialité des sources et les formes d'intimidation politique et judiciaire. La plate-forme repose sur un partenariat du Conseil de l'Europe avec ARTICLE 19, l'Association des journalistes européens, la Fédération européenne des journalistes, la Fédération internationale des journalistes et Reporters sans frontières.

La tendance mondiale du journalisme à évoluer de plus en plus en ligne est également reflétée par la quantité croissante de formations et d'outils journalistiques portant sur la sécurité numérique, notamment sur les appareils mobiles. Ceci inclut le développement d'applications pour téléphones mobiles, qui permettent aux journalistes de mieux se protéger. La Fondation internationale des femmes dans les médias (IWMF) a développé une application, *Reporta*, qui intègre des fonctions « présence », « alertes » et « SOS ». De même, le Centre international pour les journalistes (ICFJ) développe *Salama*, une application d'évaluation des risques.

6. COLLABORATIONS INTERAGENCES RENFORCÉES

Pendant la période 2013-2014, la coopération entre les organes des Nations Unies s'est améliorée. Le Haut-Commissariat aux droits de l'homme et l'UNESCO ont contribué au rapport du Secrétaire général des Nations Unies sur la mise en œuvre de la Résolution A/RES/68/163 sur la sécurité des journalistes et la question de l'impunité. Ce rapport, qui a été soumis à l'Assemblée générale des Nations Unies, présente les récentes tendances en matière de sécurité des journalistes et des professionnels des médias, et compile les initiatives mises en œuvre pour assurer leur protection. Il énonce également des recommandations.

L'ONUDC a publié en 2013 l'*Étude mondiale sur l'homicide*, qui cherche à donner un aperçu complet des homicides volontaires à travers le monde. Une sous-section consacrée plus particulièrement aux assassinats de journalistes a été réalisée avec l'aide de l'UNESCO.

Le Département de l'information des Nations Unies (DPI) a quant à lui transmis les informations relatives à l'élaboration du Plan d'Action des Nations Unies sur la sécurité des journalistes et la question de l'impunité à ses 63 Centres d'information des Nations Unies. ONU Femmes et l'UNESCO ont collaboré pendant la période étudiée, sur des questions ayant trait aux femmes journalistes. La question de la sécurité des journalistes a également été mieux incorporée au Plan cadre des Nations unies pour le développement national, notamment en Jordanie, au Népal et au Soudan du Sud.

Le Haut-Commissariat aux droits de l'homme, l'Organisation internationale du travail (OIT) et l'UNESCO ont également collaboré avec le Forum mondial pour le développement des médias pour élaborer le projet d'indicateurs pour les Objectifs de développement durable (ODD). L'Objectif 16.10 est de « Garantir l'accès public à l'information et protéger les libertés fondamentales, conformément à la législation nationale et aux accords internationaux ». Les discussions entre les groupes précités ont permis d'aboutir à un consensus sur une proposition d'indicateur relatif à la sécurité pour cet objectif spécifique. L'indicateur proposé, qui devrait être adopté début 2016, est le suivant : « Nombre de cas vérifiés de meurtres, kidnapping, disparitions forcées, détentions arbitraires et torture de journalistes, personnel associé des médias, syndicalistes et défenseurs des droits de l'homme durant les 12 derniers mois ». Ces indicateurs devraient davantage souligner que la sécurité des journalistes est une liberté fondamentale, au même titre qu'un Objectif de développement durable – et un instrument qui contribue à la réalisation des autres ODD.

7. VERS UNE PLUS GRANDE IMPLICATION DU SECTEUR JUDICIAIRE DANS LA LUTTE CONTRE L'IMPUNITÉ

Ces deux dernières années, la tendance a été d'améliorer l'engagement du système judiciaire dans la lutte contre l'impunité, en réalisant des efforts de renforcement des capacités auprès des juges et des avocats. La conférence sur l'impunité tenue à la Cour européenne des droits de l'homme en novembre 2014 a déjà été mentionnée. En 2014 également, le Knight Center for Journalism in the Americas de l'Université du Texas à Austin a collaboré avec l'ancien Rapporteur spécial des Nations Unies sur la promotion et la protection du droit à la liberté d'opinion et d'expression et l'ancien Rapporteur de l'Organisation des États Américains pour réaliser un cours en ligne ouvert et massif (MOOC) sur la liberté d'expression, qui abordait entre autres la sécurité des journalistes. Ce cours, auquel plus de 800 acteurs du secteur de la justice ont participé en l'espace d'un mois, a initialement été créé pour la Cour suprême du Mexique, et a depuis lors suscité l'intérêt d'autres acteurs judiciaires dans le reste de la région Amérique latine. Il a pu être réalisé grâce au financement accordé par le Programme international pour le développement de la communication (PIDC) de l'UNESCO en 2013. Ce MOOC sera une nouvelle fois proposé en 2015 avec le soutien de l'UNESCO et du gouvernement de l'état de Coahuila au Mexique.

De nombreuses décisions de justice, comme celle de la Cour africaine des droits de l'homme et des peuples qui a ordonné de reprendre l'enquête sur le meurtre du journaliste burkinabé Norbert Zongo et de trois autres personnes en 1998, reconnaissent davantage l'importance d'une application efficace de l'État de droit. Une jurisprudence similaire marque également le jugement rendu en 2014 par la Cour de justice de la Communauté Économique des États de l'Afrique de l'Ouest, en ce qui concerne le meurtre du journaliste gambien Deyda Hydara, commis en 2004.[26]

26 Ces exemples touchent à l'actualité. En 2009, lors de l'affaire *Ríos et al. c. Venezuela*, la Cour interaméricaine des droits de l'homme a estimé que les exécutions extrajudiciaires nécessitent des enquêtes réalisées en temps opportun et d'une manière sérieuse, équitable et efficace.

8. RENFORCEMENT DE LA COLLABORATION AVEC LES FORCES DE SÉCURITÉ NATIONALE

L'interaction avec les forces de sécurité est un élément crucial pour garantir la sécurité des journalistes. C'est notamment vital durant les périodes de tension et de pression intense, comme les élections ou lors de manifestations. L'UNESCO a commencé à favoriser le renforcement des capacités dans ce domaine en 2013, avec une série de formations en Tunisie, en collaboration avec le ministère de l'Intérieur, et avec le soutien des Pays-Bas et de l'Agence Suédoise de Coopération Internationale pour le Développement. Cette série de sessions de formation a formé la base d'un nouveau manuel de l'UNESCO intitulé *Maintien de l'ordre et respect de la liberté d'expression*. En 2015, des formations similaires ont été organisées à Mogadiscio, en Somalie, en coopération avec Relief International et la Mission d'assistance des Nations Unies en Somalie (MANUSOM). Cette tendance émergente d'améliorer l'engagement des forces de sécurité et des professionnels des médias pourrait également renforcer l'ordre public et la liberté d'expression.

9. PROMOTION D'UN PROGRAMME DE RECHERCHE SUR LA SÉCURITÉ DES JOURNALISTES

L'acquisition de nouvelles connaissances a également permis de renforcer la sécurité des journalistes pendant cette période. Lors de l'évaluation du Plan d'action des Nations Unies à Strasbourg en novembre 2014, les connaissances se sont approfondies par des discussions sur la manière dont le contexte dans lequel les journalistes sont tués, y compris en matière de volonté et de capacité politiques, appelle à différents types de soutien, comme le partage de connaissances, le renforcement, la sensibilisation des parties prenantes ou d'un public plus général, des formations en matière de sécurité pour les journalistes, et la création d'une documentation sur les attaques pour que justice puisse être faite à l'avenir.

Pour étayer ces connaissances nuancées acquises durant la période étudiée, les connaissances sur les causes, l'impact et les réparations en lien avec la sécurité et l'impunité se sont améliorées. Citons par exemple la mise en place des Indicateurs sur la sécurité des journalistes de l'UNESCO au Pakistan, au Honduras, au Guatemala et au Libéria, ainsi que le début d'études complètes sur les ISJ au Népal, en Irak et au Kenya.

Un autre développement a été l'intérêt croissant et l'augmentation du nombre d'actions dans le monde universitaire et des chercheurs. La stratégie de mise en œuvre du Plan d'action des Nations Unies a identifié une opportunité significative dans le domaine des recherches universitaires scientifiques sur la sécurité des journalistes et l'impunité. Lors d'une analyse générale des recherches universitaires réalisées ces 20 dernières années, il a été noté que peu d'entre elles ont donné lieu à des publications. Parmi les études disponibles, la plupart se concentrent sur le « reportage de guerre » ou sur la protection des journalistes en situation de conflit armé, bien que plus de la moitié des attaques visant des journalistes aient lieu en temps de paix.

Afin d'encourager les recherches en la matière, l'UNESCO a élaboré en 2014 un programme de recherche en dix points et en a fait la promotion, en juillet 2015 lors de sessions spéciales sur la sécurité des journalistes durant la conférence de l'Association internationale des études et recherches sur l'information et la communication (AIERIC) à Montréal et la conférence de la Global Communication Association à Berlin. Plus de 100 chercheurs ont participé à ces événements. Plusieurs universités ont également exprimé leur intérêt pour une collaboration avec l'UNESCO afin de réaliser des recherches en matière de sécurité.

10. EMPRISONNEMENT DE JOURNALISTES

Comme l'indique le rapport de l'UNESCO *Tendances mondiales en matière de liberté d'expression et de développement des médias*, l'emprisonnement de journalistes dans l'exercice légitime de leur métier provoque un phénomène d'autocensure et affecte le droit de la société d'obtenir des informations. Il ajoute par ailleurs : « Les peines d'emprisonnement motivées par une pratique légitime du journalisme constituent une réponse disproportionnée ne revêtant aucun caractère de nécessité aux termes des normes internationales relatives aux restrictions de l'exercice de la liberté d'expression et aux sanctions y afférant. » Compte tenu de son mandat, l'UNESCO ne réalise pas la collecte et le suivi d'information en rapport avec l'emprisonnement des journalistes de manière systématique.[27] Néanmoins, selon une grande quantité de sources et de données, le taux d'emprisonnement des journalistes à l'échelle mondiale reste élevé en 2013 et 2014. Entre 178 et 211 journalistes ont été déclarés incarcérés en 2013, contre 211 en 2014.[28] Ce chiffre atteignait 232 journalistes en 2012 et 179 en 2011. La disparition forcée ou involontaire de journalistes est toujours considérée comme un problème. Dans ces cas des journalistes portés disparus, qui enquêtaient souvent sur des activités criminelles ou des faits de corruption avant leur disparition, le Groupe de travail des Nations Unies sur les disparitions forcées ou involontaires et le Groupe de travail des Nations Unies sur la détention arbitraire ont été contactés par des acteurs qui cherchent à obtenir réparation ou la réouverture de l'enquête.

27 Comme indiqué dans le premier rapport, de nombreux gouvernements ont maintenu que ces journalistes n'ont pas été emprisonnés pour leur pratique du journalisme, mais pour d'autres raisons, et l'UNESCO n'est pas mandatée pour évaluer la situation.

28 Sur la base des données publiques fournies par les principales organisations internationales pour la liberté de la presse comme le Comité pour la protection des journalistes ou Reporters sans frontières.

11. APPROCHE DE LA SÉCURITÉ DES JOURNALISTES EN FONCTION DU GENRE

Si moins de 8 % des journalistes tués pendant la période 2013-2014 sont des femmes (soit 14 sur 178), ce chiffre est néanmoins en légère hausse.[29] De plus, les femmes journalistes sont toujours sujettes à d'autres formes de harcèlement et d'agressions.

Ces deux dernières années, l'UNESCO a soutenu plus de recherches et réalisé plus de travaux de sensibilisation dans le domaine spécifique de la sécurité des journalistes. En mars 2014, l'UNESCO, en collaboration avec l'Institut international pour la sécurité de la presse (INSI), la Fondation internationale des femmes dans les médias (IWMF) et le gouvernement autrichien, a présenté les résultats d'une étude, intitulée *Violence and Harassment against Women in the News Media: a Global Picture*, à laquelle près de 1 000 personnes ont participé. Cette étude espère susciter de nouvelles recherches sur les problèmes de sécurité rencontrés particulièrement par les femmes journalistes.

En outre, en 2015, l'UNESCO a porté une attention particulière aux questions d'égalité des sexes dans sa nouvelle publication *Construire une sécurité numérique pour le journalisme : Enquête sur une sélection de questions*. Cette enquête, qui traite des menaces numériques faites aux journalistes, a démontré que les femmes sont plus susceptibles que les hommes d'avoir à faire face à des réponses négatives et menaçantes en ligne. Les femmes journalistes sont notamment la cible de « doubles attaques » quand elles sont prises à partie à la fois en tant que journalistes et en tant que femmes.

Durant la période étudiée et dans le cadre d'une volonté de sensibilisation dans ce domaine, l'UNESCO a régulièrement inclus la dimension du genre dans ces principaux événements de sensibilisation, par exemple lors de la Journée mondiale de la liberté de la presse. Ces deux dernières années, cet événement international a intégré des sessions dédiées à la sécurité des femmes journalistes, notamment des ateliers de formations. Il a également été l'occasion de traiter de divers autres problèmes liés au genre dans les médias. En 2015, dans le cadre du 20e anniversaire de la Déclaration et du Programme d'action de Beijing, l'UNESCO a organisé trois sessions dédiées à la question du genre dans les médias durant la Journée mondiale de la liberté de la presse à Riga, en Lettonie.

Afin de souligner encore davantage l'importance de la sécurité des journalistes dans le monde entier, et plus particulièrement le rôle des femmes journalistes, la Directrice générale de l'UNESCO a nommé en 2015, peu de temps avant la Journée mondiale de la liberté de la presse, la correspondante internationale en chef pour CNN Christiane Amanpour Ambassadrice de bonne volonté pour la liberté d'expression et la sécurité des journalistes.

29 Six femmes journalistes ont été tuées en 2013 et huit l'ont été en 2014.

12. CONCLUSION

Ce chapitre a analysé les tendances en matière de sécurité des journalistes ainsi que la question de l'impunité, sur la base de statistiques collectées en 2013 et en 2014 Il a également fait référence à certaines évolutions observées en 2012 et 2015. Si les agressions de journalistes et la question de l'impunité restent un problème sérieux, on peut remarquer des progrès évidents dans plusieurs autres domaines, comme le grand nombre d'États membres des Nations Unies qui s'associent aux Résolutions de Nations Unies, et un meilleur taux de réponses aux enquêtes de l'UNESCO en 2014 par rapport à 2013. D'autres améliorations ont été listées, au niveau par exemple de la sensibilisation, des institutions, du renforcement des capacités et de la production de savoir. Il n'est pas facile d'évaluer si toutes ces nouvelles actions ont eu un impact direct sur les statistiques. Il n'est pas non plus facile d'évaluer si cet impact sera pérenne. Il est par contre clair qu'il existe un réel élan mondial vers l'établissement d'une culture dans laquelle la sécurité des journalistes et la fin de l'impunité seront garanties. Il semble probable que cette tendance continuera à se développer aussi longtemps que le problème persistera, et, si tant est qu'elle soit couronnée de succès, qu'elle œuvrera à l'avènement de sociétés pacifiques du savoir et à la réalisation des Objectifs de développement durable des Nations Unies.

VII. ANNEXES

ANNEXE 1 – PERSONNES INTERVIEWÉES POUR *COMBATTRE LES DISCOURS DE HAINE SUR INTERNET*

Imran Awan, directeur adjoint du centre de criminologie appliquée, École des sciences sociales, Université de la ville de Birmingham, Royaume-Uni de Grande-Bretagne et d'Irlande du Nord

Monika Bickert, responsable mondiale des politiques de contrôle, Facebook, États-Unis d'Amérique

Drew Boyd, directeur des opérations, The Sentinel Project for Genocide Prevention, Canada

Ian Brown, professeur de sécurité de l'information et de respect de la vie privée, Oxford Internet Institute, Université d'Oxford, Royaume-Uni de Grande-Bretagne et d'Irlande du Nord

Laura Geraghty, Mouvement contre le discours de haine, Royaume-Uni de Grande-Bretagne et d'Irlande du Nord

Matthew Johnson, directeur de l'éducation, HabiloMédias, Canada

Myat Ko Ko, administrateur de programme pour le Myanmar, Justice Base, Myanmar

Ciara Lyden, responsable des politiques de contenus et des politiques des produits, Facebook, Irlande

Andre Oboler, PDG, Online Hate Prevention Institute, Australie

Harry Myo Lin, Panzagar, Myanmar

Nanjira Sambuli, responsable de projet, UMATI, Kenya

Christopher Wolf, président, National Committee on the Internet, Anti-Defamation League, États-Unis d'Amérique

ANNEXE 2 – PERSONNES INTERVIEWÉES POUR *PROTÉGER LES SOURCES DES JOURNALISTES À L'ÈRE NUMÉRIQUE*

Rasha Abdulla, professeur agrégé de journalisme et de communication de masse, Université américaine du Caire, Égypte

Ricardo Aguilar, journaliste d'investigation, *La Razón*, Bolivie

Rawda Ahmed, avocat, Réseau arabe d'information sur les droits de l'homme, Égypte

Mahasen Al Eman, directrice, Arab Women's Media Center, Jordanie

Amare Aregawi, propriétaire, Media and Communications Center et Horn of Africa Press Institute, Éthiopie

Hans-Gunnar Axberger, professeur de droit constitutionnel, Université d'Uppsala, Suède

Wendy Bacon, professeur honoraire, Australian Centre for Independent Journalism, Australie

Martin Baron, rédacteur en chef, *The Washington Post*, États-Unis d'Amérique

Peter Bartlett, associé, Minter Ellison, Australie

Katarina Berglund-Siegbahn, conseillère juridique, ministère de la Justice, Suède

Catalina Botero Marino, ancienne Rapporteuse spéciale sur la liberté d'expression, Commission interaméricaine des droits de l'homme

Cliff Buddle, rédacteur en chef, *South China Morning Post*, Chine

Umar Cheema, journaliste d'investigation, *The News*, et fondateur, Center for Investigative Reporting, Pakistan

Zine Cherfaoui, rédacteur en chef, *El Watan*, Algérie

Marites Dañguilan Vitug, co-fondatrice et membre du Conseil d'administration, Philippines Center for Investigative Journalism, Philippines

Yves Eudes, reporter, *Le Monde*, et co-fondateur, Source sûre, France

Tomaso Falchetta, juriste, Privacy International, Royaume-Uni de Grande-Bretagne et d'Irlande du Nord

Javier Gaza Ramos, expert en sécurité des journalistes, Mexique

Carlos Guyot, rédacteur en chef, *La Nación*, Argentine

Silvia Higuera, Knight Center for Journalism in the Americas, Université du Texas à Austin, États-Unis d'Amérique

Daoud Kuttab, journaliste, Jordanie

Fredrik Laurin, directeur de l'unité d'investigation, Swedish Public Radio (SR), Suède

Ronaldo Lemos, directeur, Institute for Technology & Society (ITS), Rio de Janeiro, et professeur, faculté de droit, Université de l'État de Rio de Janeiro, Brésil

Justine Limpitlaw, avocate spécialisée en communication électronique, Afrique du Sud

Henry Omusundi Maina, directeur, ARTICLE 19 Afrique de l'Est et Corne de l'Afrique, Kenya

Susan E. McGregor, directrice et professeure adjointe, Tow Center for Digital Journalism, École de journalisme de Columbia, Université de Columbia, États-Unis d'Amérique

Toby Mendel, directeur, Centre for Law and Democracy, Canada

Gavin Millar, QC, avocat, Matrix International, Royaume-Uni de Grande-Bretagne et d'Irlande du Nord

Peter Noorlander, avocat spécialiste des médias, Media Legal Defence Initiative, Royaume-Uni de Grande-Bretagne et d'Irlande du Nord

Gunnar Nygren, professeur, faculté de Sciences sociales, Université de Stockholm, Suède

Leanne O'Donnell, avocate senior, Legal Policy, Law Institute of Victoria, Australie

Toyosi Ogunseye, rédacteur, *The Sunday Punch*, Nigeria

Julie Owono, présidente du bureau Afrique, Internet Sans Frontières, France

Courtney Radsch, directrice du plaidoyer, Comité pour la protection des journalistes, États-Unis d'Amérique

Marcelo Rech, directeur exécutif du journalisme, RBS Group, Brésil

Alan Rusbridger, rédacteur en chef, *The Guardian*, Royaume-Uni de Grande-Bretagne et d'Irlande du Nord

Gerard Ryle, directeur, International Consortium of Investigative Journalists, États-Unis d'Amérique

Rana Sabbagh, directrice exécutive, Arab Reporters for Investigative Journalism, Jordanie

Josh Stearns, directeur journalisme et développement durable, Fondation Geraldine R. Dodge , États-Unis d'Amérique

Atanas Tchobanov, rédacteur, Bivol.bg, et journaliste, BalkanLeaks, Bulgarie

Charles D. Tobin, associé, Holland & Knight, États-Unis d'Amérique

Pär Trehörning, médiateur, Union suédoise des journalistes, Suède

Pedro Vaca Villarreal, directeur exécutif, Fundación para la Libertad de Prensa (FLIP), Colombie

Anita Vahlberg, conseiller senior, Union suédoise des journalistes, Suède

Dirk Voorhoof, professeur, Faculté de Sciences politiques et sociales et Faculté de Droit, Université de Gand, Belgique

Wei Yongzheng, chargé de cours, Université de communication de Chine, Beijing, Chine

George Williams, professeur, professeur Mason, professeur Scientia, directeur de la fondation Gilbert + Tobin Centre for Public Law, Faculté de droit, Université de Nouvelle-Galles du Sud, Australie

Jillian York, directeur pour la liberté d'expression internationale, Electronic Frontier Foundation, Allemagne

Yuan Zhen (pseudonyme), rédacteur en chef, (journal inconnu), Chine

ANNEXE 3 : ÉTATS MEMBRES DE L'UNESCO ÉTUDIÉS DANS *PROTÉGER LES SOURCES DES JOURNALISTES À L'ÈRE NUMÉRIQUE*[30]

Afrique	Asie et Pacifique	États arabes	Europe et Amérique du Nord	Amérique latine et Caraïbes
Angola	Australie	Algérie	Andorre	Argentine
Bénin	Bangladesh	Égypte	Arménie	Bolivie
Botswana	Cambodge	Mauritanie	Autriche	Brésil
Burkina Faso	Bhoutan	Maroc	Bélarus	Chili
Burundi	Chine	Djibouti	Belgique	Colombie
Cameroun	Timor Oriental	Soudan	Bosnie	Costa Rica
Cap-Vert	Fidji	Syrie	Bulgarie	République dominicaine
Tchad	Inde		Canada	Équateur
Côte d'Ivoire	Indonésie		République tchèque	El Salvador
République démocratique du Congo	Japon		Danemark	Guatemala
Éthiopie	République de Corée		Estonie	Guyana
Zambie	Kiribati		Finlande	Haïti
Gambie	Kirghizistan		France	Honduras
Ghana	Malaisie		Géorgie	Mexique
Kenya	Nouvelle-Zélande		Allemagne	Paraguay
Lesotho	Pakistan		Grèce	Panama
Libéria	Palaos		Hongrie	Pérou
Malawi	Singapour		Islande	Uruguay
Mali	Sri Lanka		Irlande	Venezuela
Maurice	Philippines		Israël	Nicaragua
Mozambique	Ouzbékistan		Italie	
Ouganda	Tadjikistan		Lettonie	
Niger	Turkménistan		Lituanie	
Nigeria	Vanuatu		Luxembourg	
Rwanda			Macédoine	
Sénégal			Monaco	
Zimbabwe			Pays-Bas	
Afrique du Sud			Norvège	
Swaziland			Pologne	
Somalie			Portugal	
Tanzanie			Russie	
Togo			Slovaquie	
			Espagne	
			Suède	
			Suisse	
			Turquie	
			Royaume-Uni et Irlande du Nord	
			États-Unis d'Amérique	

30 États membres sélectionnés sur la base de l'étude de David Banisar en 2007, *Réduire les sources au silence : enquête internationale sur la protection des sources journalistiques et les menaces à leur encontre.*

ANNEXE 4 : QUESTIONS DE L'ENQUÊTE *PROTÉGER LES SOURCES DES JOURNALISTES À L'ÈRE NUMÉRIQUE*

1. Quels sont les défis a) actuels et b) émergents touchant à la liberté d'expression dans un environnement numérique, dans le cadre de la pratique du journalisme d'investigation, qui s'appuie sur des sources confidentielles ?

2. Quelles lois/instruments juridiques existent actuellement dans votre pays, ou dans la région où vous travaillez, pour défendre les sources des journalistes ?

3. Quelles lois/précédents juridiques/politiques en la matière ont été révoquées, remplacées ou ajoutées depuis 2007 dans votre pays ou dans la région où vous travaillez ?

4. Dans quelle mesure ces lois protègent-elles le journalisme sur interface numérique et les sources des journalistes ?

5. Comment pourraient/devraient être modifiées les législations qui influent sur la protection des journalistes à l'ère numérique ?

    i) Quels changements sont nécessaires dans ces lois pour assurer une meilleure protection de l'échange d'informations entre les journalistes et leurs sources dans un environnement numérique ?

    ii) Quels changements sont plus particulièrement nécessaires dans votre pays ou la région où vous travaillez ?

    iii) Quels changements seraient mieux adoptés par le biais d'instruments politiques mondiaux (p. ex. les Nations Unies) ?

6. Veuillez identifier un à trois cas de votre pays, ou la région où vous travaillez, qui mettent en avant des problèmes liés à la protection des sources qui mériteraient selon vous un examen plus approfondi. (Note : Nous sommes tout particulièrement intéressés par les études de cas qui soulignent la complexité de l'échange d'information et de la publication dans un environnement numérique, l'émergence des journalistes citoyens, l'impact des législations sur la sécurité nationale, le conflit entre la protection législative des sources des journalistes et les autres protections, telles que le droit au respect de la vie privée.)

7. Existe-t-il un besoin de protection spécifique de la liberté d'expression sur Internet en ce qui concerne la pratique du journalisme d'investigation ? Pourquoi/Pourquoi pas ?

8. Des législations ont-elles été élaborées, ou des jurisprudences ont-elle été adoptées dans votre pays (ou la région où vous travaillez) qui ont défini/testé le droit des blogueurs/journalistes citoyens à invoquer la protection de la loi pour ne pas révéler leurs sources ? Merci de fournir des exemples.

9. Avez-vous connaissance de législations/politiques formelles ou affaires juridiques où la question et le rôle des intermédiaires en ligne (p. ex. Google, Facebook, Twitter) en ce qui concerne la protection des sources journalistiques ont été remis en question ? (p. ex. quand un site tiers a pu avoir accès à des données qui, si elles venaient à être révélées, pourraient permettre d'identifier une source, ou quand une cour de justice a demandé à des tierces parties ce type de données, circonvenant ainsi au droit légal et/ou à l'obligation éthique des journalistes de protéger leurs sources ? Dans l'affirmative, veuillez fournir des informations détaillées.

10. Si cela est pertinent dans votre organisation, avez-vous mis en œuvre des politiques et procédures et/ou campagnes conçues pour informer les journalistes et/ou les lanceurs d'alertes des changements apportés par l'environnement numérique en matière de protection des sources ? Dans l'affirmative, veuillez fournir des informations détaillées.

ANNEXE 5 – QUESTIONS DES ENTRETIENS QUALITATIFS *PROTÉGER LES SOURCES DES JOURNALISTES À L'ÈRE NUMÉRIQUE*

a. Questions pour les avocats, les défenseurs des droits de l'homme, les ONG

1. Dans l'ère du numérique, à quel point la protection juridique des sources des journalistes est-elle sécurisée ?

2. Selon votre expérience, quels sont les principaux défis et les principales menaces qui voient le jour actuellement en ce qui concerne la protection des sources ?

3. À quel point la surveillance de masse (par l'État ou les entreprises) est-elle une menace pour l'efficacité des lois de protection des sources dans votre région/travail ? (Merci de fournir des exemples).

4. Qu'en est-il du rôle des législations relatives à la sécurité nationale/la lutte contre le terrorisme (qui ont un effet limitant sur les lois de protection des sources) dans l'affaiblissement des lois de protection des sources ? Comment ce problème se manifeste-t-il dans votre région ? (Merci de fournir des exemples).

5. Selon vous, quelles sont les pressions émergentes sur la protection des sources journalistiques par des intermédiaires tiers comme Facebook, Twitter, Google, les entreprises mobiles et les FSI, en ce qui concerne la conservation et la transmission des données (aux tribunaux, gouvernements, etc.) ? (Merci de fournir des exemples)

6. À qui les lois de protection des sources devraient-elles s'appliquer à l'ère du numérique ? Aux journalistes professionnels (si oui, comment les définir) ? À tous les acteurs des médias numériques ? Ou devrions-nous limiter la protection aux « actes de journalisme » (ici encore, comment les définir) ?

7. Est-il réellement possible pour les journalistes de promettre à leurs sources qu'elles resteront confidentielles compte tenu de l'impact de la surveillance de masse, de la conservation des données, et du caractère prioritaire des législations relatives à la sécurité nationale/la lutte contre le terrorisme, qui sapent les protections juridiques mises en place normalement pour permettre la confidentialité des sources ?

8. Comment la protection juridique des sources peut-elle être renforcée à l'ère du numérique ? Est-il par exemple possible de réfléchir à l'introduction d'exceptions légales pour les journalistes afin qu'ils puissent les protéger (ou protéger leurs données) de l'exposition par la surveillance de masse ?

9. Que pensez-vous du cadre proposé pour l'évaluation des lois sur la protection des sources à l'ère du numérique ? N'hésitez pas à commenter chaque point. Que voudriez-vous supprimer/ajouter dans cette liste pour lui permettre d'être un outil de mesure de l'efficacité des lois sur la protection des sources ?

   Dans l'idéal, une loi sur la protection des sources parfaite devrait :

   1. Reconnaitre le principe éthique et la valeur pour la société que représente la protection des sources
   2. Reconnaitre que la protection doit s'étendre à tous les actes de journalismes, définis en termes inclusifs
   3. Reconnaitre que la protection des sources ne nécessite pas l'enregistrement ou l'octroi d'une licence aux pratiquants du journalisme
   4. Affirmer que la confidentialité doit s'appliquer à l'utilisation, par n'importe quel acteur, de toute donnée numérique personnelle collectée
   5. Définir des exceptions à tous les points précédents, en définissant précisément la raison justifiant la limitation du principe
   6. Définir des exceptions selon le principe de nécessité, c'est-à-dire quand il n'existe pas d'alternative
   7. Définir un processus judiciaire indépendant, permettant de faire appel, pour les exceptions autorisées
   8. Ériger en infraction pénale toute violation non autorisée de la confidentialité des sources par n'importe quelle tierce partie

10. Quelle action, s'il y en a, voudriez-vous voir dans votre région, ou au niveau international, en ce qui concerne le renforcement de la protection légale des sources des journalistes ?

b. Autre série de questions pour les journalistes

1. Dans quelle mesure faites-vous confiance aux protections légales des sources existantes dans votre pays/votre région en 2014 ?
2. En quoi votre confiance dans les protections légales des sources a-t-elle été affectée par l'apparition de nouvelles problématiques liées au numérique (merci d'expliciter vos réponses) :

   a) La surveillance de masse – les lois qui défendent le droit des journalistes à ne pas divulguer leurs sources sont-elles vraiment utiles si la surveillance de masse les démasque ?
   b) Les lois sur la conservation des données (et les demandes de transmission de données faites aux intermédiaires tiers comme Facebook, Twitter, Google, les FSI) ?

c) Les législations sur la sécurité nationale/la lutte contre le terrorisme (car elles limitent la portée des lois de protection des sources) ?

3. Quels impacts ont eu ces changements sur vos sources confidentielles – y a-t-il des signes d'un effet dissuasif ? Sont-elles plus réticentes à transmettre des informations que par le passé ? (Merci de fournir des exemples).

4. Pensez-vous qu'il soit toujours possible de promettre aux sources qu'elles garderont l'anonymat et bénéficieront de protections légales (s'il y en a dans votre région) ? Lorsque vous le promettez, vous sentez-vous à l'aise sur le plan éthique ? Si oui, pourquoi ? Si non, pourquoi pas ?

5. À qui les lois de protection des sources devraient-elles s'appliquer à l'ère du numérique ? aux journalistes professionnels (si oui, comment les définir) ? à tous les acteurs des médias numériques ? Ou devrions-nous limiter la protection aux « actes de journalisme » (ici encore, comment les définir) ?

6. Dans la pratique, en quoi l'insécurité autour de la protection des sources change-t-elle la manière dont vous pratiquez le journalisme d'investigation (p. ex. avez-vous tendance à publier moins d'articles qui dépendent de sources confidentielles ? Adaptez-vous vos pratiques de reportage d'une autre manière ? Si oui, comment ?).

7. Avez-vous pris part à des partenariats internationaux et collaboratifs de journalisme d'investigation ? Dans l'affirmative, comment les points ci-dessus se sont manifestés lors des investigations transfrontalières ? Comme composez-vous avec les différentes normes et pratiques juridiques internationales lors de telles investigations ? Qu'avez-vous appris globalement sur l'efficacité des lois sur la protection des sources dans ce contexte ?

8. Comment la protection juridique des sources peut-elle être renforcée à l'ère du numérique ? Par exemple, les États devraient-ils réfléchir à l'introduction d'exceptions légales pour les journalistes afin qu'ils puissent être protégé (ou que leurs données soient protégées) de l'exposition par la surveillance de masse ? (Pourquoi/Pourquoi pas ?) L'effet limitant des lois sur la sécurité nationale/la lutte contre le terrorisme sur les lois en matière de protection des sources devrait-il être étudié plus en détail ? (Pourquoi/Pourquoi pas ?)

9. Que pensez-vous du cadre proposé pour l'évaluation des lois sur la protection des sources à l'ère du numérique ? N'hésitez pas à commenter chaque point. Que voudriez-vous supprimer/ajouter dans cette liste pour lui permettre d'être un outil de mesure de l'efficacité des lois sur la protection des sources ?

   Dans l'idéal, une loi sur la protection des sources parfaite devrait :

   1. Reconnaitre le principe éthique et la valeur pour la société que représente la protection des sources
   2. Reconnaitre que la protection doit s'étendre à tous les actes de journalismes, définis en termes inclusifs

3. Reconnaitre que la protection des sources ne nécessite pas l'enregistrement ou l'octroi d'une licence aux pratiquants du journalisme
4. Affirmer que la confidentialité doit s'appliquer à l'utilisation, par n'importe quel acteur, de toute donnée numérique personnelle collectée
5. Définir des exceptions à tous les points précédents, en définissant précisément la raison justifiant la limitation du principe
6. Définir des exceptions selon le principe de nécessité, c'est-à-dire quand il n'existe pas d'alternative
7. Définir un processus judiciaire indépendant, permettant de faire appel, pour les exceptions autorisées
8. Ériger en infraction pénale toute violation non autorisée de la confidentialité des sources par n'importe quelle tierce partie

10. Quelle autre action, s'il y en a, voudriez-vous voir dans votre région, ou à l'international, en ce qui concerne le renforcement de la protection légale des sources des journalistes ?

BIBLIOGRAPHIE SÉLECTIVE

Nations Unies :

Comité pour l'élimination de la discrimination raciale. 2002. Recommandation générale 29 concernant la discrimination fondée sur l'ascendance (soixante-et-unième session, 2002), U.N. Doc. A/57/18 p. 111 (2002), réimprimée dans Compilation des Observations et Recommandations générales adoptées par les organes des traités, U.N. Doc. HRI\GEN\1\Rev.6 at 223 (2003)

Haut-Commissariat des Nations Unies aux droits de l'homme. 5 octobre 2012. Plan d'action de Rabat relatif à l'interdiction de l'appel de la haine nationale, raciale ou religieuse qui constitue une incitation à la discrimination, à l'hostilité ou à la violence. http://www.ohchr.org/Documents/Issues/Opinion/SeminarRabat/Rabat_draft_outcome.pdf

—. 2011. *Principes directeurs relatifs aux entreprises et aux droits de l'homme*. New York et Genève : Nations Unies.

—. 16 décembre 1966. *Pacte international relatif aux droits civils et politiques*. http://www.ohchr.org/fr/professionalinterest/pages/ccpr.aspx

Assemblée générales des Nations Unies. 11 février 2015. *Résolution adoptée par l'Assemblée générale le 18 décembre 2014, 69/185. La sécurité des journalistes et la question de l'impunité*. A/RES/69/185. http://www.un.org/fr/ga/search/view_doc.asp?symbol=A/RES/69/185

—. 23 septembre 2015. *Rapport du Rapporteur spécial sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste* A/69/397. http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N14/545/20/PDF/N1454520.pdf?OpenElement

—. 21 février 2014. *La sécurité des journalistes et la question de l'impunité : Résolution adoptée par l'Assemblée générale le 18 décembre 2013*. A/RES/68/163. http://www.refworld.org/cgi-bin/texis/vtx/rwmain/opendocpdf.pdf?reldoc=y&docid=53a7fad04

—. 20 novembre 2013. *Le droit à la vie privée à l'ère du numérique. (A/C.3/68/167).* http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/68/167&referer=/english/&Lang=F

—. 1979. *Convention sur l'élimination de toutes les formes de discrimination à l'égard des femmes*. http://www.un.org/womenwatch/daw/cedaw/

—. 16 décembre 1966. *Pacte international relatif aux droits civils et politiques*. http://www.ohchr.org/fr/professionalinterest/pages/ccpr.aspx

—. 10 décembre 1948. *Déclaration universelle des droits de l'homme*. http://www.un.org/fr/documents/udhr/

Assemblée générale des Nations Unies, Comité des droits de l'homme. 5 janvier 2015. *Rapport de la Rapporteuse spéciale sur les questions relatives aux minorités, Rita Izsák*. A/HRC/28/64

—. 11-29 juillet 2011. *Observation générale n° 34*. http://www2.ohchr.org/english/bodies/hrc/docs/CCPR.C.GC.34_fr.doc

—. 14 juillet 2011. *Résolution 17/19, sur les droits de l'homme, l'orientation sexuelle et l'identité de genre*. A/HRC/RES/17/19

—. 2000. *Observation générale n° 28: Égalité des droits entre hommes et femmes*, U.N. Doc. CCPR/C/21/Rev.1/Add.10

—. 1993. *Observation générale n° 22, Article 18* (quarante-huitième session). Compilation des Observations et Recommandations générales adoptées par les organes des traités, U.N. Doc. HRI/GEN/1/Rev.1 at 35 (1994)

Conseil des droits de l'homme des Nations Unies. 22 mai 2015. *Rapport du Rapporteur spécial des Nations Unies sur la promotion et la protection du droit à la liberté d'opinion et d'expression, David Kaye.* A/HRC/29/32. http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx

—. 2 octobre 2014. *Résolution adoptée par le Conseil des droits de l'homme, 27/5 : La sécurité des journalistes*. A/HRC/RES/27/5. http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G14/177/81/PDF/G1417781.pdf?OpenElement

—. 23 juillet 2014. *La sécurité des journalistes : Rapport du Haut-Commissariat des Nations Unies aux droits de l'homme*. A/HRC/27/35. http://www.refworld.org/docid/53eb46d34.html

—. 30 juin 2014. *Le droit à la vie privée à l'ère du numérique : Rapport du Haut-Commissariat des Nations Unies aux droits de l'homme.* A/HRC/27/37. www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf

—. 1e juillet 2013. *La sécurité des journalistes : Rapport du Haut-Commissariat des Nations Unies aux droits de l'homme*. A/HRC/24/23. http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G13/153/19/PDF/G1315319.pdf?OpenElement

—. 17 avril 2013. *Rapport du Rapporteur spécial des Nations Unies sur la promotion et la protection du droit à la liberté d'opinion et d'expression*. A/HRC/23/40. http://www.refworld.org/docid/51a5ca5f4.html

—. 9 octobre 2012. *Sécurité des journalistes : Résolution adoptée par le Conseil des droits de l'homme*. A/HRC/RES/21/12. http://www.refworld.org/cgi-bin/texis/vtx/rwmain/opendocpdf.pdf?reldoc=y&docid=50adf4be2

—. 16e juillet 2012. *La promotion, la protection et l'exercice des droits de l'homme sur l'Internet* A/HRC/RES/20/8. http://daccess-dds-ny.un.org/doc/RESOLUTION/GEN/G12/153/26/PDF/G1215326.pdf?OpenElement

—. 4 juin 2012. *Rapport du Rapporteur spécial des Nations Unies sur la promotion et la protection du droit à la liberté d'opinion et d'expression, Frank La Rue.* A/HRC/20/17. http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session20/A-HRC-20-17_en.pdf

—. 16 mai 2011. *Rapport du Rapporteur spécial des Nations Unies sur la promotion et la protection du droit à la liberté d'opinion et d'expression, Frank La Rue.* A/HRC/17/27. http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

—. 20 avril 2010. *Rapport du Rapporteur spécial des Nations Unies sur la promotion et la protection du droit à la liberté d'opinion et d'expression, Frank La Rue.* A/HRC/14/23. http://www2.ohchr.org/english/bodies/hrcouncil/docs/14session/A.HRC.14.23.pdf

—. 16 janvier 2009. *Rapport du Haut-Commissaire des Nations Unies aux droits de l'homme, Additif, Séminaire d'experts sur les relations entre les articles 19 et 20 du Pacte international relatif aux droits civils et politiques*, A/HRC/10/31/Add.3 http://www2.ohchr.org/english/issues/opinion/articles1920_iccpr/docs/A-HRC-10-31-Add3.pdf

—. 10 septembre 2006. *Incitation à la haine raciale et religieuse et promotion de la tolérance : Rapport du Haut-Commissaire des Nations Unies aux droits de l'homme*. A/HRC/2/6. http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G06/139/97/PDF/G0613997.pdf?OpenElement

Office des Nations Unies contre la drogue et le crime. 2013. *Global Study on Homicide*. http://www.unodc.org/gsh/

—. 2003. *Convention des Nations Unies contre la corruption*. https://www.unodc.org/documents/treaties/UNCAC/Publications/Convention/08-50027_F.pdf

Radio des Nations Unies 12e juillet 2013. « Human Rights chief urges respect for right to privacy and protection of individuals revealing human rights violations ». http://www.unmultimedia.org/radio/english/2013/07/human-rights-chief-urges-respect-for-right-to-privacy-and-protection-of-individuals-revealing-human-rights-violations/

Conseil de sécurité des Nations Unies. 27 mai 2015. *Résolution 2222 (2015) : Adoptée par Conseil de sécurité à sa 7450e séance, le 27 mai 2015*. S/RES/2222 (2015). http://www.refworld.org/cgi-bin/texis/vtx/rwmain/opendocpdf.pdf?reldoc=y&docid=558934914

—. 22 novembre 2013. *Rapport du Secrétaire général sur la protection des civils en période de conflit armé* . S/2013/689. http://www.refworld.org/cgi-bin/texis/vtx/rwmain/opendocpdf.pdf?reldoc=y&docid=529f190e4

UNESCO

Daudin Clavaud, P. et T. Mendel. 2015. *Maintien de l'ordre et respect de la liberté d'expression: manuel pédagogique.* Paris : UNESCO. http://unesdoc.unesco.org/images/0022/002279/227977f.pdf

Dutton, W. H. et al. 2011. *Liberté de connexion, liberté d'expression: écologie dynamique des lois et règlements qui façonnent l'internet*. Collection de l'UNESCO sur la liberté de l'Internet. Paris : UNESCO. http://unesdoc.unesco.org/images/0021/002160/216029f.pdf

Gagliardone, I. et al. 2015. *Combattre les discours de haine sur Internet*. Collection de l'UNESCO sur la liberté de l'Internet. Paris : UNESCO. http://unesdoc.unesco.org/images/0023/002346/234620f.pdf

Henrichsen, J. R., M. Betz et J. M. Lisosky 2015. *Construire une sécurité numérique pour le journalisme : A Survey of Selected Issues*. Paris : UNESCO. http://unesdoc.unesco.org/images/0023/002323/232358e.pdf

MacKinnon, R. et al. 2014. *Promouvoir la liberté en ligne : Le rôle des intermédiaires de l'Internet*. Collection de l'UNESCO sur la liberté de l'Internet. Paris : UNESCO / Internet Society. http://unesdoc.unesco.org/images/0023/002311/231162e.pdf

Mendel, T. et al. 2012. *Etude mondiale sur le respect de la vie privée sur l'Internet et la liberté d'expression*. Collection de l'UNESCO sur la liberté de l'Internet. Paris : UNESCO. http://unesdoc.unesco.org/images/0021/002196/219698F.pdf

UNESCO. *L'éducation à la citoyenneté mondiale*. http://www.unesco.org/new/fr/education/resources/in-focus-articles/global-citizenship-education/

—. 2015. *Des clés pour la promotion de sociétés du savoir inclusives : Accès à l'information et au savoir, liberté d'expression, respect de la vie privée et éthique sur un Internet mondial*. Paris : UNESCO. http://unesdoc.unesco.org/images/0023/002325/232564F.pdf

—. 17 mars 2015. *Décision 196 EX/31 sur la sécurité des journalistes et la question de l'impunité*. Adoptée lors de la 196e session du Conseil exécutif de l'UNESCO. http://unesdoc.unesco.org/images/0023/002323/232337f.pdf

—. 2014. *Tendances mondiales en matière de liberté d'expression et de développement des médias*. Paris : UNESCO. http://www.unesco.org/new/fr/communication-and-information/resources/publications-and-communication-materials/publications/full-list/world-trends-in-freedom-of-expression-and-media-development/

—. Juillet 2014. *Universalité de l'Internet : un outil pour la construction des sociétés du savoir et de l'agenda pour le développement durable post-2015*. Projet proposé par le Secrétariat http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/news/internet_universality_fr.pdf

—. Mai 2014. *La Déclaration de Paris appelle à un intérêt renouvelé pour l'éducation aux médias et à l'information (MIL) à l'ère numérique*. http://www.unesco.org/new/fr/communication-and-information/resources/news-and-in-focus-articles/in-focus-articles/2014/paris-declaration-on-media-and-information-literacy-adopted/

—. 2013. *Projet de Stratégie à moyen terme : 2014–2021 (37 C/4)*. Paris : UNESCO. http://unesdoc.unesco.org/images/0022/002200/220031f.pdf

—. Novembre 2013. *Resolution on Internet related issues: including access to information and knowledge, freedom of expression, privacy and ethical dimensions of the information society*. 37e session de la Conférence générale. http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/news/37gc_resolution_internet.pdf

—. 25 octobre – 10 novembre 2011. *Actes de la Conférence générale, 36e session*. Volume 1 : Résolutions. http://unesdoc.unesco.org/images/0021/002150/215084f.pdf

UNESCO, Conseil intergouvernemental du Programme international pour le développement de la communication (PIDC). 20-21 novembre 2014. *Décisions prises par la 29e session du Conseil du PIDC*. Salle X, Siège de l'UNESCO , Paris. http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/IPDC/ipdc29EN_IPDC29_FULL_DECISIONS_FINAL.pdf

—. 22-23 mars 2012. *Rapport final (Vingt-huitième session)*. UNESCO : Paris. http://unesdoc.unesco.org/images/0021/002199/219910F.pdf

—. 24-26 mars 2010. *Rapport final (Vingt-septième session)*. UNESCO : Paris. http://unesdoc.unesco.org/images/0018/001896/189697m.pdf

—. 26-28 mars 2008. *Rapport final (Vingt-sixième session)*. UNESCO : Paris. http://unesdoc.unesco.org/images/0016/001634/163437m.pdf

UNESCO, Programme international pour le développement de la communication (PIDC). 2014. *La sécurité des journalistes et danger d'impunité, rapport de la Directrice générale au Conseil intergouvernemental du PIDC (vingt-neuvième session)*. CI-14/CONF.202/4 Rev2. Paris. http://unesdoc.unesco.org/images/0023/002301/230101F.pdf

Autres organisations intergouvernementales :

Commission Africaine des Droits de l'Homme et des Peuples. 17-23 octobre 2002. Déclaration de principes sur la liberté d'expression en Afrique, 32e Session, Banjul

APEC Cross-Border Privacy Rules System. http://www.cbprs.org/

Association des nations de l'Asie du Sud-Est (ASEAN). 19 novembre 2012. *Déclaration des droits de l'homme de l'ASEAN*. http://www.asean.org/news/asean-statement-communiques/item/asean-human-rights-declaration

Benedek, W. et M. C. Kettemann. Décembre 2013. *Liberté d'expression et internet*. Strasbourg : Conseil de l'Europe. https://book.coe.int/eur/fr/droits-de-l-homme-et-democratie/6317-liberte-d-expression-et-internet.html

Bigo et al. 2013. *Les programmes nationaux de surveillance massive des données à caractère personnel dans les États membres et leur compatibilité avec le droit de l'Union européenne*. Parlement européen. http://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/493032/IPOL-LIBE_ET%282013%29493032_FR.pdf

Botero Marino, C. 22 avril 2014. *Annual Report of the Inter-American Commission on Human Rights 2013: Annual report of the office of the special rapporteur for freedom of expression,* Volume ii. Washington, D.C. : Organisation des États Américains. http://www.oas.org/en/iachr/expression/docs/reports/2014_04_22_%20IA_2013_ENG%20_FINALweb.pdf

—. 31 décembre 2013. *Violence against journalists and media workers: Inter-American standards and national practices on prevention, protection and prosecution of perpetrators*. Bureau du Rapporteur spécial sur la liberté d'expression, Commission interaméricaine des droits de l'homme. http://www.oas.org/en/iachr/expression/docs/reports/2014_04_22_Violence_WEB.pdf

—. 2012. *Annual Report of the Inter-American Commission on Human Rights,* volume II, Report of the Office of the Special Rapporteur for Freedom of Expression

Broadband Commission Working Group on Broadband and Gender. Septembre 2013. *Doubling Digital Opportunities: Enhancing the Inclusion of Women & Girls in the Information Society*. Genève : International Telecommunication Union. www.broadbandcommission.org/Documents/working-groups/bb-doubling-digital-2013.pdf

Conseil de l'Europe. 16 avril 2014. *Recommandation du Comité des Ministres aux États membres sur un Guide des droits de l'homme pour les utilisateurs d'internet*. (CM/Rec(2014)6.) https://wcd.coe.int/ViewDoc.jsp?id=2184807

—. 15 avril 2012. *Mapping study on projects against hate speech online*. Strasbourg. https://www.coe.int/t/dg4/youth/Source/Training/Training_courses/2012_Mapping_projects_against_Hate_Speech.pdf

—. 26 septembre 2007. *Lignes directrices du Comité des Ministres du Conseil de l'Europe sur la protection de la liberté d'expression et d'information en temps de crise,* 1005e réunion. https://wcd.coe.int/ViewDoc.jsp?Ref=CM/Del/c(2007)1005/5.3&Language=lanFrench&Ver=appendix11&Site=COE&BackColorInternet=DBDCF2&BackColorIntranet=FDC864&BackColorLogged=FDC864

—. 28 janvier 2003. *Protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques*

—. 23 novembre 2001. *Convention sur la cybercriminalité*

Conseil de l'Europe, Comité des Ministres. 28 mai 2003. *Déclaration sur la liberté de la communication sur l'Internet*. (Decl-28.05.2003E.) https://wcd.coe.int/ViewDoc.jsp?Ref=Decl-28.05.2003&Language=lanFrench&Ver=original&Site=COE&BackColorInternet=DBDCF2&BackColorIntranet=FDC864&BackColorLogged=FDC864

—. 2000. *Recommandation sur « le droit des journalistes de ne pas révéler leurs sources d'information »*. http://www.coe.int/t/dghl/standardsetting/media/doc/cm/rec(2000)007&expmem_FR.asp?

Conseil de l'Europe, Commissariat aux droits de l'homme. 4 octobre 2011. Protection of journalists from violence: Issue discussion paper. https://wcd.coe.int/ViewDoc.jsp?id=1899957https://wcd.coe.int/ViewDoc.jsp?id=1899957

Conseil de l'Europe, Commission européenne contre le racisme et l'intolérance (ECRI). 15 décembre 2000. *Recommandation de politique générale N° 6 : La lutte contre la diffusion de matériels racistes, xénophobes et antisémites par l'Internet*. http://www.coe.int/t/dghl/monitoring/ecri/activities/gpr/en/recommendation_n6/recommendation_6_FR.asp?

Conseil de l'Europe, Assemblée parlementaire. 25 janvier 2011. *Recommandation 1950 : La protection des sources d'information des journalistes*. http://assembly.coe.int/Mainf.asp?link=/Documents/AdoptedText/ta11/EREC1950.htm

Cour de justice de l'Union européenne. 8 avril 2014. La Cour de justice déclare la directive sur la conservation des données invalide. Communiqué de presse N° 54/14. http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf

Edwards, L. 22 juin 2011. *Role and Responsibility of Internet Intermediaries in the Field of Copyright and Related Rights*. Genève : World Intellectual Property Organisation. (WIPO-ISOC/GE/11/REF/01/EDWARDS). www.wipo.int/export/sites/www/copyright/en/doc/role_and_responsibility_of_the_internet_intermediaries_final.pdf

Commission européenne. 16e juillet 2013. *Overview on Binding Corporate Rules. Data Protection*. http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/index_en.htm

—. 28 novembre 2008. *Framework Decision on Racism and Xenophobia*. http://ec.europa.eu/justice/fundamental-rights/racism-xenophobia/framework-decision/index_en.htm

—. 4 mai 2000. *Directive sur le commerce électronique*. (2000/31/EC). http://ec.europa.eu/internal_market/e-commerce/directive/index_en.htm

Cour européenne des droits de l'homme. 1996. *Goodwin c. Royaume-Uni*. http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-57974

Parlement européen et Conseil de l'Union européenne. 22 mai 2001. *Directive 2001/29/CE du Parlement européen et du Conseil du 22 mai 2001 sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information*. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32001L0029

Union européenne. 2000. *Charte des droits fondamentaux de l'Union européenne*. http://ec.europa.eu/justice/fundamental-rights/charter/index_fr.htm

Horsley, W. 2012. *OSCE Safety of journalists guidebook*. Office of the OSCE Representative on Freedom of the Media. https://www.osce.org/fom/85777?download=true

Hulin, A. (Ed.). 2013. *Joint Declarations of the representatives of intergovernmental bodies to protect free media and expression*. Vienne : Organization for Security and Co-operation in Europe. www.osce.org/fom/99558?download=true

Commission interaméricaine des droits de l'homme. 20 octobre 2000. *Inter-American Declaration of Principles on Freedom of Expression*

—. 13 novembre 1985. *Advisory Opinion OC-5/85*

Cour interaméricaine des droits de l'homme. 2009. 28 janvier. *Case of Ríos et al. v. Venezuela*. http://corteidh.or.cr/docs/casos/articulos/seriec_194_ing.pdf

ISO/IEC. Mars 2015. FDIS 11179-1. 'Information technology - Metadata registries - Part 1: Framework'. http://stats.oecd.org/glossary/detail.asp?ID=4575

Ligue des États arabes. 22 mai 2004. Charte arabe des droits de l'homme. Entrée en vigueur le 15 mars 2008

Ministres de la Freedom Online Coalition. *Recommendations for Freedom Online*. Adoptées à Tallinn, Estonie, le 28 avril 2014. https://www.freedomonlinecoalition.com/wp-content/uploads/2014/04/FOC-recommendations-consensus.pdf

Organisation de Coopération et de Développement Économiques. 13 décembre 2011. *OECD Council Recommendation on Principles for Internet Policy Making*. www.oecd.org/internet/ieconomy/49258588.pdf

—. Septembre 2011. *The Role of Internet Intermediaries in Advancing Public Policy Objectives*. Paris : OECD http://browse.oecdbookshop.org/oecd/pdfs/product/9311031e.pdf

Organisation des États Américains. *American Convention on Human Rights 'Pact of San José, Costa Rica' (B-32)*. http://www.oas.org/dil/treaties_B-32_American_Convention_on_Human_Rights.htm

—. 2011. *Mandatory membership in a professional association for the practise of journalism*. http://www.oas.org/en/iachr/expression/showarticle.asp?artID=154&lID=1

Organisation de la coopération islamique. 5 août 1990. *Déclaration du Caire sur les droits de l'homme en Islam*, préambule

Organisation de la coopération islamique. Décembre 2013. *Sixth OIC Observatory Report on Islamophobia*. Présenté au 40e Conseil des Ministres des Affaires étrangères, Conakry, République de Guinée

Organization for Security and Co-operation in Europe. *Decriminalization of defamation*. www.osce.org/fom/106287

—. 8 juin 2011. *Vilnius Recommendations on Safety of Journalists*. http://www.osce.org/cio/78522

Perset, K. / OCDE. Mars 2010. *The Economic and Social Role of Internet Intermediaries*. (DSTI/ICCP(2009)9/FINAL). Paris : OCDE. www.oecd.org/internet/ieconomy/44949023.pdf

Autres documents et ressources

Access Now. *Telco Remedy Plan*. https://www.accessnow.org/telco-remedy-plan

ARTICLE 19. Avril 2009. *The Camden Principles on Freedom of Expression and Equality*. https://www.article19.org/data/files/pdfs/standards/the-camden-principles-on-freedom-of-expression-and-equality.pdf

Broadband Stakeholder Group (UK). *Voluntary industry code of practice on traffic management transparency for broadband services*. http://www.broadbanduk.org/wp-content/uploads/2013/08/Voluntary-industry-code-of-practice-on-traffic-management-transparency-on-broadband-services-updated-version-May-2013.pdf

The Center for Internet and Society. Juillet 2014. *World Intermediary Liability Map (WILMap)*. Stanford, Calif.: Stanford Law School. http://cyberlaw.stanford.edu/our-work/projects/world-intermediary-liability-map-wilmap

Chilling Effects. http://www.chillingeffects.org

Comité pour la protection des journalistes. 1e décembre 2014. *2014 prison census: 221 journalists jailed worldwide*. https://cpj.org/imprisoned/2014.php

—. 1e décembre 2013. *2013 prison census: 211 journalists jailed worldwide*. https://cpj.org/imprisoned/2013.php

Electronic Frontier Foundation. *Takedown Hall of Shame*. https://www.eff.org/takedowns

—. 2014. *Who Has Your Back? Protecting Your Data From Government Requests*. https://www.eff.org/who-has-your-back-2014

European University Institute, Centre for Media Pluralism and Media Freedom. 2014. *Status of European Journalists*. http://journalism.cmpf.eui.eu/maps/journalists-status/

Facebook. *Standards de la communauté*. https://www.facebook.com/communitystandards/

Global Network Initiative. *Implementation Guidelines*. https://globalnetworkinitiative.org/implementationguidelines/index.php

—. *Principles*. http://www.globalnetworkinitiative.org/principles/

Google. *Rapport de transparence*. http://www.google.com/transparencyreport/

Hatebase. *Most Common Hate Speech*. http://www.hatebase.org/popular

Projet In Other Words. 2013. *Toolbox*. http://www.inotherwords-project.eu/sites/default/files/Toolbox.pdf

Internet Live Stats. 2014. *Internet Users by Country*. www.internetlivestats.com/internet-users-by-country

HabiloMédias *Facing online hate*. http://mediasmarts.ca/tutorial/facing-online-hate-tutorial

Microsoft, Windows Dev Center. 11.0 Content Policies. *Windows apps*. https://msdn.microsoft.com/en-us/library/windows/apps/Dn764940.aspx

Microsoft, Xbox. Janvier 2014. *Code de conduite pour les clients Xbox Live*. http://www.xbox.com/fr-FR/legal/codeofconduct

Necessary and Proportionate. 10 juillet 2013 *Principes internationaux sur l'application des droits de l'homme à la surveillance des communications*. https://fr.necessaryandproportionate.org/text

Mouvement contre le discours de haine 2013. *Campaign tools and materials*. http://nohate.ext.coe.int/Campaign-Tools-and-Materials

—. 2013. *No Hate Ninja Project - A Story About Cats, Unicorns and Hate Speech*. https://www.youtube.com/watch?v=kp7ww3KvccE

Ofcom. 22e juillet 2014. *Report on Internet safety measures - Internet Service Providers: Network level filtering measures*. http://stakeholders.ofcom.org.uk/internet/internet-safety-2?utm_source=updates&utm_medium=email&utm_campaign=filtering-report

Online Hate Prevention Institute. *Fight Against Hate*. http://fightagainsthate.com/

Open Rights Group. Juillet 2014. *Blocked! The personal cost of filters*. https://www.blocked.org.uk/personal-stories

OpenNet Initiative. About Filtering. https://opennet.net/about-filtering

Organisation de Coopération et de Développement Économiques. Mars 2014. *The CleanGovBiz Toolkit for Integrity*. http://www.oecd.org/cleangovbiz/CGB-Toolkit-2014.pdf

Reporters sans frontières. *2014: Journalistes emprisonnés*. http://fr.rsf.org/barometre-de-la-liberte-de-la-presse-journalistes-emprisonnes.html?annee=2014

—. *2013: Journalistes emprisonnés*. http://fr.rsf.org/barometre-de-la-liberte-de-la-presse-journalistes-emprisonnes.html?annee=2013

Telecommunications Industry Dialogue on Freedom of Expression and Privacy. 16 mars 2013. *Guiding Principles*. http://www.vodafone.com/content/dam/sustainability/pdfs/telecom_industry_dialogue_principles.pdf

Tell MAMA (Measuring Anti-Muslim Attacks). 2014. http://tellmamauk.org

Terms of Service; Didn't Read. https://tosdr.org/

Twitter. Règles de Twitter. https://support.twitter.com/articles/75576

—. 18 mai 2015. *Conditions d'utilisation de Twitter*. https://twitter.com/tos?lang=fr

UC Berkeley Library. *Invisible or Deep Web: What it is, How to find it, and Its inherent ambiguity*. http://www.lib.berkeley.edu/TeachingLib/Guides/Internet/InvisibleWeb.html

UNESCO. *L'UNESCO condamne l'assassinat de journalistes*. http://www.unesco.org/new/fr/condemnation

WAM! *WAM Twitter harassment reporting tool*. https://womenactionmedia.wufoo.com/forms/ztaetji1jrhv10/

YouTube. *Community Guidelines*. http://www.youtube.com/yt/policyandsafety/communityguidelines.html

Livres, articles et rapports

African Gender Institute. Décembre 2013. *Feminist Africa*, Vol. 18, « e-spaces: e-politics ». http://agi.ac.za/sites/agi.ac.za/files/fa18_web-1.pdf

Albanian Media Institute. 2014. *Hate speech in online media in South East Europe*. http://www.institutemedia.org/Documents/PDF/Hate%20speech%20in%20online%20media%20in%20SEE.pdf

Alston, P. (Ed.). 2005. *Non-State Actors and Human Rights*. Oxford : Oxford University Press.

Alves, R. 2014. « Trends in global collaborative journalism », *Trends in Newsrooms 2014,* Darmstadt, Allemagne : WAN-IFRA, pp. 83-87

Andrejevic, M. 2014. Wikileaks, Surveillance, and Transparency. *International Journal of Communication*, 8, pp. 2619–2630

Athique, A. 2013. *Digital Media and Society: An Introduction*. Polity.

Banisar, D. novembre 2008. *Speaking of terror: A survey of the effects of counter-terrorism legislation on freedom of the media in Europe*. Conseil de l'Europe, Direction générale des droits de l'Homme et des affaires juridiques division Médias et société de l'information. http://www.coe.int/t/dghl/standardsetting/media/Doc/SpeakingOfTerror_en.pdf

—. 2007. *Silencing Sources: An international survey of protections and threats to journalists' sources*. Privacy International. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1706688 accessed 25/6/2014

Bankston, K., D. Sohn et A. McDiarmid. Décembre 2012. *Shielding the Messengers: Protecting Platforms for Expression and Innovation*. Washington DC: Center for Democracy and Technology. www.cdt.org/files/pdfs/CDT-Intermediary-Liability-2012.pdf

Barton, A. et H. Storm. 2014. *Violence and Harassment against Women in the News Media: A Global Picture*. International Women's Media Foundation and International News Safety Institute. http://www.iwmf.org/wp-content/uploads/2014/03/Violence-and-Harassment-against-Women-in-the-News-Media.pdf

Bauman, Z. et al. 2014. After Snowden: Rethinking the Impact of Surveillance. *International Political Sociology*, 8:2, 121-140

Bayley, E. 16 novembre 2009. *The Clicks that Bind: Ways Users "Agree" to Online Terms of Service*. Electronic Frontier Foundation. https://www.eff.org/wp/clicks-bind-ways-users-agree-online-terms-service

Benesch, S. 2012. Words as Weapons. *World Policy Journal*, vol. 29, no. 1, pp. 7-12

—. 12 janvier 2012. 'Dangerous Speech: A Proposal to Prevent Group Violence'. New York : World Policy Institute. http://www.worldpolicy.org/sites/default/files/Dangerous%20Speech%20Guidelines%20Benesch%20January%202012.pdf

Bently, L. et B. Sherman. 2009. *Intellectual Property Law*, 3e éd. Oxford : Oxford University Press.

Bergman, M. K. août 2001. White Paper: The Deep Web: Surfacing Hidden Value. *Taking License*. Vol. 7, Numéro 1. http://quod.lib.umich.edu/j/jep/3336451.0007.104

Beschastna, T. 2014. Freedom of Expression in Russia as it Relates to Criticism of the Government. *Emory International Law Review*, Vol. 27, No. 2. http://law.emory.edu/eilr/content/volume-27/issue-2/comments/freedom-expression-russia.html

Black, J. janvier 1996. Constitutionalising Self-Regulation. *The Modern Law Review*, Vol. 59, No. 1, pp. 24-55. http://dx.doi.org/10.1111/j.1468-2230.1996.tb02064.x

BSR, avec CDT. Septembre 2014. *Legitimate and Meaningful Stakeholder Engagement in Human Rights Due Diligence: Challenges and Solutions for ICT Companies*. http://www.bsr.org/reports/BSR_Rights_Holder_Engagement.pdf

Budish, R. 19 December 2013. « What Transparency Reports Don't Tell Us ». *The Atlantic*. www.theatlantic.com/technology/archive/2013/12/what-transparency-reports-dont-tell-us/282529

Business and Human Rights Resource Centre. Septembre 2010. *The UN 'Protect, Respect and Remedy' Framework for Business and Human Rights*. www.reports-and-materials.org/sites/default/files/reports-and-materials/Ruggie-protect-respect-remedy-framework.pdf

Buyse, A. 2014. Words of Violence: 'Fear Speech,' or How Violent Conflict Escalation Relates to the Freedom of Expression. *Human Rights Quarterly*, vol. 36, no. 4, pp. 779–97

Castells, M. 2012. *Networks of Outrage and Hope: Social Movements in the Internet Age*. Cambridge : Polity

Chin, Y. C. août 2013. Regulating social media. Regulating life (and lives). *RJR 33 Online*, http://journalism.hkbu.edu.hk/doc/Regulating_social-Media.pdf

Citron, K. D. et H. Norton. 2011. Intermediaries and hate speech: Fostering digital citizenship for our information age. *Boston University Law Review,* vol. 91, pp. 1435-84

Comninos, A. octobre 2012. *The Liability of Internet Intermediaries in Nigeria, Kenya, South Africa, and Uganda: An Uncertain Terrain*. Afrique du Sud : Association for Progressive Communications. www.apc.org/en/system/files/READY%20-%20Intermediary%20Liability%20in%20Africa_FINAL.pdf

—. Octobre 2012. *Intermediary liability in South Africa*. Intermediary Liability in Africa Research Papers, No. 3. Afrique du Sud : Association for Progressive Communications. www.apc.org/en/system/files/Intermediary_Liability_in_South_Africa-Comninos_06.12.12.pdf

Cotter, T. F. 2005. Some Observations on the Law and Economics of Intermediaries. *Michigan State Law Review*, Vol. 1, pp. 1-16. Washington & Lee Legal Studies Paper No. 2005-14. http://ssrn.com/abstract=822987

Das, S. et A. Kramer. 2013. Self-Censorship on Facebook. *Proceedings of the Seventh International Association for the Advancement of Artificial Intelligence (AAAI) Conference on Weblogs and Social Media*, pp. 120-27. www.aaai.org/ocs/index.php/ICWSM/ICWSM13/paper/viewFile/6093/6350

Davies, S. (Ed.). Juin 2014. A Crisis of Accountability: A global analysis of the impact of the Snowden revelations. *Privacy Surgeon*. www.privacysurgeon.org/blog/wp-content/uploads/2014/06/Snowden-final-report-for-publication.pdf

Defeis, E.F., 1992. Freedom of speech and international norms: A response to hate speech. Stan. Journal of International Law, vol. 29, pp. 57-74

Deibert, R. et al. (Eds). Avril 2010. *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*. Cambridge, Mass.: MIT Press. http://mitpress.mit.edu/books/access-controlled

—. 2008. Janvier. *Access Denied: The Practice and Policy of Global Internet Filtering.* Cambridge, Mass.: MIT Press. https://mitpress.mit.edu/books/access-denied

DeNardis, L. août 2013. Internet Points of Control as Global Governance. Internet Governance Papers. No.2. Centre for International Governance Innovation. http://www.cigionline.org/sites/default/files/no2_3.pdf

Diamond, L. juillet 2010. Liberation technology. *Journal of Democracy*, Vol. 21, No. 3, pp. 69-83. www.journalofdemocracy.org/articles/gratis/Diamond-21-3.pdf

Electronic Frontier Foundation. Janvier 2011. *Freedom of Expression, Privacy and Anonymity on the Internet.* https://www.eff.org/Frank-La-Rue-United-Nations-Rapporteur

Epstein, G. 3 mars 2011. Sina Weibo. *Forbes Asia*. www.forbes.com/global/2011/0314/features-charles-chao-twitter-fanfou-china-sina-weibo.html

Foxman, A.H. and C. Wolf. 2013. Viral hate: Containing its spread on the Internet. Macmillan

Ghanea, N. 2013. Intersectionality and the Spectrum of Racist Hate Speech: Proposals to the UN Committee on the Elimination of Racial Discrimination. *Human Rights Quarterly*, vol. 35, no. 4, pp. 935-54. http://dx.doi.org/10.1353/hrq.2013.0053

Gillespie, T. 2010. The Politics of 'Platforms'. *New Media & Society*, vol. 12, no. 3, pp. 347-64. http://dx.doi.org/10.1177/1461444809342738

Giroux, H. 2015. Totalitarian Paranoia in the Post-Orwellian Surveillance State. *Cultural Studies*, vol. 29, no. 2, pp. 108-140

Global Network Initiative. Janvier 2014. *Public Report on the Independent Assessment Process for Google, Microsoft, and Yahoo*. http://globalnetworkinitiative.org/sites/default/files/GNI%20Assessments%20Public%20Report.pdf

Goldsmith, J.L. and T. Wu. 2006. *Who controls the Internet? Illusions of a borderless world*. Oxford : Oxford University Press. http://jost.syr.edu/wp-content/uploads/who-controls-the-internet_illusions-of-a-borderless-world.pdf

Goodman, E. et F. Cherubini. 2013. *Online comment moderation: emerging best practices. A guide to promoting robust and civil online conversation*. World Association of Newspapers and News Publishers (WAN-IFRA). http://www.wan-ifra.org/reports/2013/10/04/online-comment-moderation-emerging-best-practices

Grabowicz, P. A. et al. 2012. Social Features of Online Networks: The Strength of Intermediary Ties in Online Social Media. *PLoS ONE*, Vol. 7, No. 1. http://dx.doi.org/10.1371/journal.pone.0029358

Hannak, A. et al. Measuring Personalization of Web Search. *WWW '13 Proceedings of the 22nd international conference on World Wide Web*, pp. 527-538. http://www.ccs.neu.edu/home/cbw/pdf/fp039-hannak.pdf

Harvey, D., VP, Trust & Safety, Twitter. 29e juillet 2013. *We hear you.* https://blog.twitter.com/en-gb/2013/we-hear-you

Herpai, G. 7 janvier 2013. Unsocial network: the rise and fall of iWiW. *Budapest Business Journal*. www.bbj.hu/business/unsocial-network-the-rise-and-fall-of-iwiw_64418

Hoechsmann, M. and S. R. Poyntz. 2012. *Media Literacies. A Critical Introduction.* Oxford: Wiley-Blackwell

Hope, D. A. février 2011. *Protecting Human Rights in the Digital Age.* BSR. https://globalnetworkinitiative.org/sites/default/files/files/BSR_ICT_Human_Rights_Report.pdf

Howard, P. N. 2010. *The Digital Origins of Dictatorship and Democracy: Information Technology and Political Islam*. Oxford : Oxford University Press

Human Rights Watch. 2014. *Liberty to Monitor All*. https://www.hrw.org/report/2014/07/28/liberty-monitor-all/how-large-scale-us-surveillance-harming-journalism-law-and

iHub Research. 2013. *Umati Final Report*. http://www.research.ihub.co.ke/uploads/2013/june/1372415606__936.pdf

Imre, A. mai 2009. National intimacy and post-socialist networking. *European Journal of Cultural Studies*, Vol. 12, No. 2, pp. 219-33

The Institute for Human Rights and Business and Shift. Juin 2013. *ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights*. Commission européenne. www.shiftproject.org/publication/european-commission-ict-sector-guide

Intel Corporation et Dalberg Global Development Advisors. 2012. *Women and the Web: Bridging the Internet Gap and Creating New Global Opportunities in Low and Middle-Income*

Countries. www.intel.com/content/dam/www/public/us/en/documents/pdf/women-and-the-web.pdf

Internet Watch Foundation. 2013. *Internet Watch Foundation Annual & Charity Report 2013*. Cambridge : IWF, www.iwf.org.uk/assets/media/annual-reports/annual_report_2013.pdf.pdf

Jellema, A. et K. Alexander. 22 novembre 2013. *2013 Web Index Report*. Genève : World Wide Web Foundation. http://thewebindex.org/wp-content/uploads/2013/11/Web-Index-Annual-Report-2013-FINAL.pdf

Johnson, E. J., S. Bellman et G. L. Lohse. 2002. Defaults, Framing, and Privacy: Why Opting In-Opting Out. *Marketing Letters*, Vol. 13, No. 1. https://www0.gsb.columbia.edu/mygsb/faculty/research/pubfiles/1173/defaults_framing_and_privacy.pdf

Kamdar, A. 6 décembre 2012. EFF's Guide to CDA 230: The Most Important Law Protecting Online Speech. *EFF Deeplinks* Blog. https://www.eff.org/deeplinks/2012/12/effs-guide-cda-230-most-important-law-protecting-online-speech

Kohl, U. 2002. Eggs, Jurisdiction, and the Internet. *International and comparative law quarterly*, vol. 51, no. 3, pp. 556-582

KVG Research. Décembre 2013. *TV Market and Video on Demand in the Russian Federation*. Strasbourg : European Audiovisual Observatory. www.obs.coe.int/documents/205595/552774/RU+TV+and+VoD+2013+KVG+Research+EN.pdf/5fbb076c-868e-423a-bfed-dca8b66cac43

Laclau, E. and Mouffe, C. 1985. *Hegemony and Socialist Strategy. Towards a Radical Democratic Politics.* London: Verso

Learner, J. et R. Bar-Nissim. 2014. Law Enforcement Investigations Involving Journalists. *Legal Studies Research Paper Series*, no. 2014-71. School of Law, University of California, Irving

Leo, L. A., F. D. Gaer et E. K. Cassidy. 2011. Protecting Religions from Defamation: A Threat to Universal Human Rights Standards. *Harv. JL & Pub. Pol'y*, vol. 34, pp. 769-95

Limpitlaw, J. 2013. *Media Law Handbook for Southern Africa*, vol. 2. Johannesburg : Konrad-Adenauer-Stiftung Regional Media Programme. http://www.kas.de/wf/doc/kas_35248-1522-2-30.pdf?130825185204

Marquis-Boire, M. et al. Mars 2013. 'You only click twice: FinFisher's Global Proliferation'. Citizen Lab. https://citizenlab.org/2013/03/you-only-click-twice-finfishers-global-proliferation-2/

Meddaugh, P. M. and Kay, J. 2009. Hate Speech or 'Reasonable Racism?' The Other in Stormfront, *Journal of Mass Media Ethics, Vol.* 24, no. 4, pp. 251-68. MediaSmarts.NDa

Lengyel, B. et al. 26 janvier 2013. Distance dead or alive Online Social Networks from a geography perspective. SSRN. http://dx.doi.org/10.2139/ssrn.2207352

Levine, M., VP of Global Public Policy, Facebook. 28 mai 2013. 'Controversial, Harmful and Hateful Speech on Facebook'. https://www.facebook.com/notes/facebook-safety/controversial-harmful-and-hateful-speech-on-facebook/574430655911054

MacKinnon, R. 2012. C*onsent of the Networked: The Worldwide Struggle for Internet Freedom*. New York : Basic Books.

Maireder, A. et S. Schlögl. Décembre 2014. 24 Hours of an #outcry: The Networked Publics of a Socio-Political Debate. *European Journal of Communication*, Vol. 29, No. 6

Marsden, C. T. 2011. *Internet Co-Regulation: European Law, Regulatory Governance, and Legitimacy in Cyberspace*. Cambridge : Cambridge University Press

Marthews, A. et C. Tucker. 24 mars 2014. Government Surveillance and Search Behavior. SSRN. http://ssrn.com/abstract=2412564

McNamee, J. janvier 2011. *The Slide from Self-Regulation to Corporate Censorship*. Bruxelles : European Digital Rights Initiative. www.edri.org/files/EDRI_selfreg_final_20110124.pdf

Moore, M. juin 2007. Public interest, media neglect. *British Journalism Review*, vol. 18, no.2

Morsink, J. 1999. *The universal declaration of human rights: Origins, drafting, and intent*. University of Pennsylvania Press

Mossberger, K., C. J. Tolbert et R. S. McNeal. 2008. *Digital Citizenship. The Internet, Society and Participation.* Londres : The MIT Press

Nash, V. 2013. Analyzing Freedom of Expression Online: Theoretical, empirical, and normative contributions. In Dutton, W.H. (Ed.). *The Oxford Handbook of Internet Studies*. Oxford : Oxford University Press

Natour, F. et J. D. Pluess. Mars 2013. *Conducting an Effective Human Rights Impact Assessment*. BSR. http://www.bsr.org/reports/BSR_Human_Rights_Impact_Assessments.pdf

Noorlander, P. 5 décembre 2014. 'Finding Justice for Whistleblowers'. *Journalism in Europe discussion series,* Centre for Media Pluralism and Media Freedom, European University Institute

Nowak, M. 1993. *UN covenant on civil and political rights: CCPR commentary*. NP Engel Kehl

Nyst, C. juillet 2014. *End violence: Women's rights and safety online project – Internet intermediaries and violence against women online. Executive summary and findings*. Association for Progressive Communications. http://www.genderit.org/sites/default/upload/flow-cnyst-summary-formatted.pdf

Omanovic, E. 20 novembre 2014. *Private Interests: Monitoring Central Asia*. Privacy International. https://www.privacyinternational.org/?q=node/59

Osler, A. and H. Starkey. 2005. *Changing Citizenship.* Berkshire: Open University Press

Palfrey, J. G. Jr. Local Nets on a Global Network: Filtering and the Internet Governance Problem. *The Global Flow of Information.* In Balkin, J. (Ed.). Harvard Public Law Working Paper No. 10-41, p.8. http://ssrn.com/abstract=1655006

Parti, K. et L. Marin. 2013. Ensuring Freedoms and Protecting Rights in the Governance of the Internet: A Comparative Analysis on Blocking Measures and Internet Providers' Removal of Illegal Internet Content. *Journal of Contemporary European Research*, vol. 9, no. 1, pp. 138-59. www.jcer.net/index.php/jcer/article/view/455/392

Pasquale, F. A. 2010. Beyond Innovation and Competition: The Need for Qualified Transparency in Internet Intermediaries. *Northwestern University Law Review*, vol. 104, no. 1, pp. 105-74. www.law.northwestern.edu/lawreview/v104/n1/105/LR104n1Pasquale.pdf

Petrova, D. 9-10 février 2011. 'Incitement to National, Racial or Religious Hatred: Role of Civil Society and National Human Rights Institutions'. 2011 Expert Workshops on the Prohibition of Incitement to National, Racial or Religious Hatred, Vienna

Pew Research Center in association with Columbia University's Tow Center for Digital Journalism. 5 février 2015. *Investigative Journalists and Digital Security: Perceptions of Vulnerability and Changes in Behavior*. http://www.journalism.org/files/2015/02/PJ_InvestigativeJournalists_0205152.pdf

Phillips, G. 10 octobre 2014. *On protection of journalistic sources*. Centre for Media Pluralism and Media Freedom, European University Institute. http://journalism.cmpf.eui.eu/discussions/on-protection-of-journalistic-sources/

Podkowik, J. 2014. 'Secret surveillance, national security and journalistic privilege – in search of the balance between conflicting values in the age of new telecommunication technologies'. University of Oslo. http://www.jus.uio.no/english/research/news-and-events/events/conferences/2014/wccl-cmdc/wccl/papers/ws8/w8-podkowik.pdf

Post, R., I. Hare et J. Weinstein. 2009. Hate speech. In *Extreme speech and democracy*. Oxford : Oxford University Press, pp. 123-38

Ramzy, A. 17 février 2011. Wired Up. *Time*. http://content.time.com/time/printout/0,8816,2048171,00.html

Rosenberg, R. S. 2011. Controlling access to the Internet: The role of filtering. *Ethics and Information Technology*, vol. 3, no. 1, pp. 35-54. www.copacommission.org/papers/rosenberg.pdf

Rotenberg, M. et D. Jacobs. 2013. Updating the Law of Information Privacy: The New Framework of the European Union. *Harvard Journal of Law & Public Policy*, vol. 36, no. 2, pp. 605-52. www.harvard-jlpp.com/wp-content/uploads/2013/04/36_2_605_Rotenberg_Jacobs.pdf

Rowbottom, J., 2012. To Rant, Vent and Converse: Protecting Low Level Digital Speech. *The Cambridge Law Journal*, vol. 71, no. 2, pp. 355-383

Russell, L. 2014. Shielding the Media: In an Age of Bloggers, Tweeters, and Leakers, Will Congress Succeed in Defining the Term "Journalist" and in Passing a Long-Sought Federal Shield Act? *Oregon Law Review*, 93, pp. 193-227

Rustad, M. L. et D. D'Angelo. 2012. The Path of Internet Law: An Annotated Guide to Legal Landmarks. *Duke Law & Technology Review*, vol. 2011, no. 012. Suffolk University Law School Research Paper No. 11-18. http://ssrn.com/abstract=1799578

Ryngaert, C. 2008. *Jurisdiction in international law*. Oxford : Oxford University Press

Samway, M. A. octobre 2014. Business, Human Rights and the Internet: A Framework for Implementation. In Lagon, M. P. et A. C. Arend (Eds.). *Human Dignity and the Future of Global Institutions.* Georgetown University Press

Savin, A. et J. Trzaskowski (eds). 2014. *Research Handbook on EU Internet Law*. Edward Elgar Publishing

Seng, D. et I. Garrote Fernandez-Diez. 2012. *Comparative Analysis of National Approaches of the Liability of the Internet Intermediaries*. Genève : World Intellectual Property Organization. www.wipo.int/export/sites/www/copyright/en/doc/liability_of_internet_intermediaries.pdf

Sieminski, P. 21 novembre 2013. Striking Back Against Censorship. WordPress *Hot Off the Press* Blog. http://en.blog.wordpress.com/2013/11/21/striking-back-against-censorship

Sparas, D. 18 juin 2013. EU regulatory framework for e-commerce. *Atelier de l'OMC sur le commerce électronique*. Genève : Organisation mondiale du commerce. www.wto.org/english/tratop_e/serv_e/wkshop_june13_e/sparas_e.pdf

Stearns, J. 2013. *Acts of journalism: Defining Press Freedom in the Digital Age*. Washington, DC : Free Press. http://www.freepress.net/resource/105079/acts-journalism-defining-press-freedom-digital-age

Sunstein, C. décembre 2013. Deciding by Default. *University of Pennsylvania Law Review*, Vol. 162, No. 1. http://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=1000&context=penn_law_review

Tuppen, C. 2012. *Opening the Lines: A Call for Transparency from Governments and Telecommunications Companies*. Global Network Initiative. https://globalnetworkinitiative.org/sites/default/files/GNI_OpeningtheLines.pdf

Van Hoboken, J. 2012. *Search Engine Freedom: On the implications of the right to freedom of expression for the legal governance of Web search engines.* Thèse de doctorat, University of Amsterdam Faculty of Law. http://dare.uva.nl/document/357527

Viljoen, F., 2012. *International human rights law in Africa.* Oxford : Oxford University Press

Villeneuve, N. janvier 2006. The Filtering Matrix: Integrated mechanisms of information control and the demarcation of borders in cyberspace. *First Monday*, vol. 11. No. 1-2

Waldron, J., 2012. *The Harm in Hate Speech*. Cambridge, MA : Harvard University Press

York, J. C. septembre 2010. 'Policing Content in the Quasi-Public Sphere'. OpenNet Initiative. https://opennet.net/policing-content-quasi-public-sphere

Zingales, N. novembre 2013. *Internet intermediary liability: Identifying best practices for Africa*. Afrique du Sud : Association for Progressive Communications. www.apc.org/en/system/files/APCInternetIntermediaryLiability_BestPracticesAfrica_20131125.pdf

Zittrain, J. printemps 2006. A History of Online Gatekeeping. *Harvard Journal of Law & Technology*, Vol. 19, No. 2, pp. 253-98. http://jolt.law.harvard.edu/articles/pdf/v19/19HarvJLTech253.pdf

Les *Tendances mondiales en matière de liberté d'expression et de développement des médias : Regards sur le numérique 2015* étudie les nouveaux défis et les nouvelles opportunités pour la liberté de la presse à l'ère du numérique. Ce rapport souligne l'importance de nouveaux acteurs dans la promotion et la protection de la liberté d'expression, en ligne et hors ligne, en se focalisant sur les questions liées au discours de haine, à la protection des sources journalistiques, au rôle des intermédiaires Internet dans la promotion de la liberté d'expression et à la sécurité des journalistes. Au sein d'un environnement médiatique transformé par les technologies numériques, cette publication spéciale de la série *Tendances mondiales* représente une référence clé pour les gouvernements, les journalistes, les professionnels des médias, la société civile, le secteur privé et les milieux universitaires.

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

Secteur de la communication et de l'information

9 789232 000798

Tendances mondiales en matière de liberté d'expression et de développement des médias : Regards sur le numérique 2015