MCM(2013)007

LIBERTÉ D'EXPRESSION DE RÉUNION ET D'ASSOCIATION EN LIGNE ET LIBERTÉ DES MÉDIAS EN EUROPE

RAPPORT

Ian Brown

Université d'Oxford, Royaume-Uni

Les vues exprimées dans cet ouvrage sont de la responsabilité de l'auteur
et ne reflètent pas nécessairement la ligne officielle du Conseil de l'Europe

« La révolution numérique a été bénéfique pour la liberté d'expression parce qu'elle a accru la diversité des voix dans la sphère publique. Elle a été bénéfique pour la liberté d'information, parce qu'elle a permis à davantage de personnes d'accéder directement aux données et aux documents publics et favorisé l'exigence de transparence envers les institutions au pouvoir. Mais elle a à la fois dynamisé et affaibli la liberté de la presse ». – Paul Starr[1]

Ce rapport offre un aperçu des défis et des menaces qui pèsent actuellement sur la liberté d'expression, de réunion et d'association en ligne et sur la liberté des médias en Europe et analyse les rôles et les responsabilités des acteurs publics et privés dans la protection de ces libertés. Il s'appuie sur les recherches du Conseil de l'Europe[2], sur la jurisprudence de la Cour européenne des droits de l'homme[3], sur des enquêtes et analyses d'institutions telles que l'Organisation pour la sécurité et la coopération en Europe (OSCE) et la Commission européenne et sur les rapports d'organes spécialisés de l'ONU. Les aspects de surveillance et de vie privée sur Internet sont abordés dans un autre rapport.

[1] « An Unexpected Crisis: The News Media in Postindustrial Democracies », *The International Journal of Press/Politics 17*(2), p. 234, 2012

[2] Conseil de l'Europe, *Protecting freedom of expression and information*, http://hub.coe.int/protecting-freedom-of-expression-and-information

[3] Cour européenne des droits de l'homme, Division de la recherche, *Internet : la jurisprudence de la Cour européenne des droits de l'homme*, 2011 ; Unité de la presse, *Fiche thématique – Nouvelles technologies*, 2013 ; arrêts et décisions de recevabilité pertinents.

Table des matières

Liberté d'expression 5

Accès universel et neutralité du réseau 5
Surveillance des communications 7
Expression et produits culturels 7
Autorégulation et protections contre les poursuites 9
Discours de haine et incitation à la violence 11
Autres questions 13

Liberté des médias 13

Protection des sources et des lanceurs d'alerte 14
Diffamation 16
Diversité des médias et éducation aux médias 16

Liberté de réunion et d'association 17

Réunions en ligne sur des sites privés 19
Surveillance des communications et analyse des réseaux sociaux 19
Faut-il protéger les attaques par déni de service distribué ? 20

Réactions envisageables 21

Réponses et actions des États 22
Participation des entreprises et des autres acteurs clés 26

Remerciements 28

Liberté d'expression

Dans son célèbre arrêt *Handyside*, la Cour européenne des droits de l'homme affirme : « Son rôle de surveillance commande à la Cour de prêter une extrême attention aux principes propres à une « société démocratique ». La liberté d'expression constitue l'un des fondements essentiels de pareille société, l'une des conditions primordiales de son progrès et de l'épanouissement de chacun[4] ».

Le droit des internautes à consulter et à partager des données et informations de leur choix est protégé par l'article 10.1 de la Convention européenne des droits de l'homme « sans considération de frontière », les exceptions prévues à l'article 10.2 étant interprétées strictement : « toute « formalité », « condition », « restriction » ou « sanction » imposée en la matière doit être proportionnée au but légitime poursuivi[5] ». Les propos de nature politique, même virulents ou exagérés, sont particulièrement protégés[6].

La portée mondiale d'Internet peut inciter les États à prendre des mesures proportionnées pour restreindre le droit à diffuser des informations, mais aussi offrir un important moyen d'expression face à certaines restrictions[7]. Les droits individuels doivent parfois « s'effacer devant d'autres impératifs légitimes tels que la défense de l'ordre et la prévention des infractions pénales ou la protection des droits et libertés d'autrui[8] ».

Accès universel et neutralité du réseau

Internet offre un grand potentiel de soutien à la liberté d'expression ; encore faut-il y avoir accès. D'après une déclaration du Comité des Ministres, « les États membres devraient favoriser et encourager l'accès de tous aux services de communication et d'information sur Internet de manière non discriminatoire et à un prix raisonnable[9] ». Frank La Rue, Rapporteur spécial de l'ONU sur la liberté d'opinion et d'expression, va dans le même sens : « Assurer l'accès universel à Internet devrait compter parmi les priorités de tous les États[10] ». Pour 2012, Eurostat, l'agence des statistiques de l'UE, a constaté que 72 % des foyers de l'UE disposaient d'un accès Internet à haut débit, avec un pourcentage plus faible dans certains pays d'Europe orientale (50 % ou 51 % en Grèce, en Bulgarie et en Roumanie, bien que beaucoup de foyers roumains disposent d'un accès par modem ou par RNIS). Toujours d'après Eurostat, 39 % des résidents de l'UE se connectent à Internet via des appareils mobiles, comme les smartphones[11].

---

[4] *Handyside c. Royaume-Uni,* série A n° 24, § 49, 7 décembre 1976

[5] *Ibid.*

[6] *Renaud c. France*, n° 13290/07, § 38, 25 février 2010

[7] *Mouvement raëlien suisse c. Suisse*, n° 16354/06, §§ 54-58, 13 janvier 2011

[8] *K.U. c. Finlande*, n° 2872/02, 2 décembre 2008

[9] *Liberté de la communication sur l'Internet*, déclaration adoptée par le Comité des Ministres le 28 mai 2003, lors de la 840e réunion des Délégués des Ministres

[10] A/HRC/17/27 § 85, 16 mai 2011

[11] Données consultables sur http://epp.eurostat.ec.europa.eu/portal/page/portal/eurostat/home/

Comme il ressort de l'analyse de la Cour, « le droit de recevoir et de communiquer des informations entre dans [le] champ d'application [de l'article 10[12]] ». La Cour note également que « le droit d'accès à l'Internet […] est considéré comme inhérent au droit d'accéder à l'information et à la communication protégé par les Constitutions nationales, et qu'il inclut le droit de chacun à participer à la société de l'information et l'obligation pour les États de garantir l'accès des citoyens à Internet. On peut donc déduire de l'ensemble des garanties générales protégeant la liberté d'expression qu'il y a lieu de reconnaître également un droit d'accès sans entraves à Internet[13] ».

Cette analyse est déjà expressément entérinée par la Constitution dans deux des États membres du Conseil de l'Europe. En France, le Conseil constitutionnel a conclu en 2009 que l'accès à Internet était couvert par la Déclaration des droits de l'homme et du citoyen de 1789[14] ; en Grèce, la Constitution affirme que chacun a le droit de participer à la société de l'information et que l'État est tenu de « faciliter l'accès à l'information électronique, aussi bien que la production, l'échange et la diffusion des données[15] ». La Cour d'appel d'Angleterre et du Pays de Galles affirme pour sa part :

> *« L'interdiction générale d'utiliser un ordinateur ou d'accéder à Internet est inadmissible. Elle est disproportionnée, car elle interdit au défendeur l'usage d'un outil qui est aujourd'hui essentiel dans la vie quotidienne d'une grande part de la population et indispensable pour beaucoup d'activités professionnelles. Avant l'apparition d'Internet, si un défendeur possédait des revues contenant des images pédophiles, nul n'aurait songé à lui interdire complètement les livres. La situation est comparable aujourd'hui avec Internet*[16] *».*

Des groupes de la société civile ont été victimes d'attaques techniques contre leur site Internet, susceptibles de nuire à leur droit de diffuser et de recevoir des informations. Ces groupes peuvent aussi avoir plus de mal à trouver un hébergeur pour leur site[17]. La Convention sur la cybercriminalité demande aux États parties d'ériger ce type d'attaque en infraction pénale[18].

Les règles relatives à la discrimination contre certains types ou prestataires de contenus par des fournisseurs d'accès Internet sont aussi importantes pour la liberté d'expression (et d'innovation). Comme l'a déclaré le Comité des Ministres en 2010, « le droit des utilisateurs à accéder à l'information et à la diffuser en ligne, ainsi que le développement de nouveaux outils et services pourraient être défavorablement affectés par une gestion non transparente du trafic, une discrimination à l'égard des contenus et des services ou des entraves à la connectivité des appareils ». Pour empêcher cela, le Comité suggère

[12] Voir la note n° 3, p. 22

[13] *Yildirim c. Turquie*, n° 3111/10, § 31, 18 décembre 2012

[14] *Décision n° 2009-580*, § 12, 10 juin 2009

[15] Article 5A 2., Constitution de la Grèce, telle que révisée par la résolution du 27 mai 2008 de la VIII[e] Chambre révisionnelle

[16] *Regina v. Smith & Others* [2011], EWCA Crim 1772, § 20

[17] Comité des Ministres, *Déclaration sur la protection de la liberté d'expression et de la liberté de réunion et d'association en ce qui concerne les plates-formes Internet gérées par des exploitants privés et les prestataires de services en ligne*, § 4, 7 décembre 2011

[18] STE n° 185, art. 5, 23 novembre 2001

que le Conseil de l'Europe fournisse aux États membres ou aux acteurs du secteur privé des lignes directrices sur la « neutralité du réseau[19] ».

Surveillance des communications

Le Rapporteur spécial de l'ONU sur la liberté d'expression a publié en avril 2013 un rapport prémonitoire, consacré aux conséquences de la surveillance des communications par l'État sur l'exercice des droits fondamentaux à la vie privée et à la liberté d'opinion et d'expression. Constatant « une tendance alarmante à l'extension des pouvoirs de surveillance au-delà des frontières territoriales », il conclut : « La surveillance des communications devrait être considérée comme un acte extrêmement intrusif, qui risque de porter atteinte à la liberté d'expression et au droit à la vie privée et qui menace les fondements d'une société démocratique[20] ».

Depuis juin 2013, les révélations d'Edward Snowden, ancien consultant de la NSA (les services de renseignement américains), ont montré que les États-Unis, le Royaume-Uni et leurs alliés avaient mis en place des systèmes de surveillance d'Internet à très grande échelle, en coopérant avec la Suède, le Danemark et d'autres États membres du Conseil de l'Europe[21]. Vingt-trois membres de l'Assemblée parlementaire ont réagi en déposant une proposition de résolution sur « Les opérations massives de surveillance en Europe », exprimant leur vive préoccupation face aux « allégations récentes de surveillance et de collectes étendues de données à caractère personnel par les services de renseignements[22] ». Ils rappellent l'arrêt de la Cour selon lequel les États « ne sauraient prendre, au nom de la lutte contre l'espionnage et le terrorisme, n'importe quelle mesure jugée par eux appropriée », étant donné « le danger, inhérent à pareille loi, de saper, voire de détruire la démocratie au motif de la défendre[23] ». Le Bureau a transmis cette proposition à la Commission des questions juridiques et des droits de l'homme pour qu'elle rédige un nouveau rapport et le présente dans un délai de deux ans. Le texte invite aussi « le Secrétaire général à ouvrir une enquête en vertu de l'article 52 » de la Convention[24].

Expression et produits culturels

L'article 10 protège l'accès des individus à l'expression culturelle et aux loisirs[25]. Afin de protéger la création, l'innovation et la production de biens culturels, la Cour a reconnu

[19] Comité des Ministres, *Déclaration sur la neutralité du réseau*, 29 septembre 2010

[20] A/HRC/23/40, §§ 64 et 81, 17 avril 2013

[21] Caspar Bowden, *The US National Security Agency (NSA) surveillance programmes (PRISM) and Foreign Intelligence Surveillance Act (FISA) activities and their impact on EU citizens' fundamental rights*, Commission des Libertés civiles du Parlement européen, 24 septembre 2013

[22] Doc. 13288, 6 août 2013

[23] *Klass et autres c. Allemagne*, n° 5029/71, § 49, 6 septembre 1978

[24] CEDH, art. 52 : « Toute Haute Partie contractante fournira sur demande du Secrétaire Général du Conseil de l'Europe les explications requises sur la manière dont son droit interne assure l'application effective de toutes les dispositions de cette Convention ».

[25] *Khurshid Mustafa et Tarzibachi c. Suède*, n° 23883/06, § 33, 16 décembre 2008

que l'article 1 du Protocole n° 1 protégeait les droits de propriété intellectuelle (comme les brevets et les marques déposées), tout en soulignant que ces droits de propriété devaient parfois s'effacer devant d'autres aspects d'intérêt général[26].

En Europe, l'équilibre entre ces droits soulève deux défis spécifiquement liés à Internet. Le premier concerne l'utilisation de marques commerciales, en particulier dans le système de noms de domaine utilisé pour convertir des adresses lisibles (par exemple hub.coe.int) en adresses numériques. Ce système est géré par l'ICANN (Internet Corporation for Assigned Names and Numbers), société californienne à but non lucratif. Le Comité des Ministres a reconnu « la nécessité d'appliquer à la gestion des noms de domaine des garanties de respect des droits fondamentaux » et invité les organes du Conseil de l'Europe à coopérer avec l'ICANN pour que ses décisions tiennent pleinement compte du droit international des droits de l'homme.

Ce point est crucial compte tenu du programme de nouveaux domaines génériques actuellement mené par l'ICANN : des milliers de demandes de création de nouveaux domaines, comme par exemple « .book », ont été déposées par des entreprises. Des groupes de la société civile ont cependant critiqué certains aspects de la gestion de ce programme. Un expert accuse l'ICANN de beaucoup trop privilégier la protection des marques commerciales, ajoutant : « Le processus réel a été déconnecté du processus formel d'orientation du programme. Il a consisté en interactions chaotiques et politisées entre le personnel, le gouvernement étasunien, le Comité consultatif gouvernemental et le lobby d'une entreprise commerciale qui ciblait délibérément les superviseurs de l'ICANN au sein du gouvernement étasunien[27] ».

Deuxièmement, plusieurs États membres ont mis en place la possibilité de sanctions rapides, pouvant aller jusqu'à la coupure de l'accès à Internet, contre des internautes accusés (sans que cela ne soit forcément avéré) d'avoir enfreint les droits d'auteur, ainsi que des procédures permettant de demander à un FAI de bloquer l'accès aux sites qui facilitent les atteintes au droit d'auteur. La loi française « HADOPI » prévoyait qu'un tribunal puisse ordonner la suspension de l'accès Internet d'un particulier au bout de trois accusations d'infraction[28]. Cette disposition a été récemment abrogée[29], à la suite de controverses politiques et de doutes quant à sa rentabilité. En Irlande, des détenteurs de droits ont demandé une injonction imposant le même type de « sanction à la troisième infraction ». Ils ont obtenu gain de cause, puisqu'un tribunal a validé un accord amiable entre ces détenteurs et Eircom, le principal fournisseur d'accès Internet du pays[30]. Cependant, d'autres FAI irlandais ont refusé d'appliquer cette règle. Au Royaume-Uni, la loi de 2010 sur l'économie numérique demande aux FAI d'envoyer des

[26] Voir la note n° 3, p. 20

[27] M. Mueller, « Meltdown III: How top-down 'implementation' replaced bottom-up policymaking », blog du projet Gouvernance de l'Internet, 14 septembre 2013. Voir aussi la page de l'Autorité étasunienne des télécoms et de l'information sur le contrat concernant les fonctions de l'IANA : http://www.ntia.doc.gov/page/iana-functions-purchase-order

[28] Loi n° 2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet, 30 octobre 2009

[29] Décret n° 2013-596 du 8 juillet 2013 supprimant la peine contraventionnelle complémentaire de suspension de l'accès à un service de communication au public en ligne et relatif aux modalités de transmission des informations prévue à l'article L. 331-21 du Code de la propriété intellectuelle

[30] *EMI Records & Others v. Eircom Ltd* [2010], IEHC 108

courriers d'avertissement aux clients accusés d'enfreindre le droit d'auteur. Les détenteurs des droits peuvent demander aux FAI une liste de tous les clients ayant dépassé un certain seuil d'avertissements, afin de déposer plainte. Le gouvernement peut demander aux FAI d'imposer des « mesures techniques » à ces clients, dont le ralentissement ou la suspension de leurs connexions. Cependant, en raison d'une forte opposition politique, aucune de ces mesures n'a encore été appliquée. Le Rapporteur spécial de l'ONU a affirmé en 2011 : « Refuser à un usager l'accès à Internet, quel que soit le motif avancé, y compris l'atteinte aux lois sur la propriété intellectuelle, est disproportionné et constitue donc une violation de l'article 19.3 du Pacte international relatif aux droits civils et politiques[31] ».

Autorégulation et protections contre les poursuites

Aux termes de la directive de l'UE sur le commerce électronique, un prestataire d'hébergement n'est pas responsable des informations stockées à la demande d'un utilisateur, à moins qu'il n'ait « effectivement connaissance de l'activité ou de l'information illicite » ou qu'il manque d'agir « promptement pour retirer les informations » dès qu'il en a connaissance. Les prestataires sont ainsi encouragés à agir lorsqu'un détenteur de droits leur signale une atteinte aux droits d'auteur[32]. Le Rapporteur spécial de l'ONU et d'autres acteurs ont pointé le risque que les prestataires ne vérifient pas dûment ces signalements et ne soient pas en mesure de peser les différents intérêts en jeu (dont l'impact sur la liberté d'expression du client) avant de retirer les informations[33].

Le Comité des Ministres a souligné l'importance que les services de réseaux sociaux s'accompagnent de garanties procédurales, « conformément au droit à être entendu et au droit à contester ou faire appel des décisions rendues, y compris, lorsque cela s'avère nécessaire, au droit à un procès équitable, dans un délai raisonnable, à commencer par la présomption d'innocence ». Il recommande aussi d'« informer clairement les utilisateurs sur la politique éditoriale du fournisseur de service de réseau social en ce qui concerne ses modalités de traitement de contenus apparemment illicites et ce qu'il considère comme un contenu ou un comportement inapproprié sur le réseau[34] ». Le Comité a également recommandé que les fournisseurs de moteurs de recherche n'écartent certains résultats de recherche que conformément à l'article 10.2 de la Convention ; la désindexation et le filtrage devraient être « transparents, étroitement ciblés et réexaminés à intervalles réguliers[35] ».

Les tribunaux peuvent assez facilement ordonner le retrait de données enfreignant le droit d'auteur sur des sites Internet de leur ressort territorial (ou le retrait d'autres types de données illégales, comme les images pédophiles, presque partout considérées comme un crime). Lorsque ces données sont hébergées hors de leur ressort territorial,

[31] Voir la note n° 10, § 78

[32] § 14, JO L 178, 17 juillet 2000, pp. 1-16

[33] Voir la note n° 10, § 42

[34] Comité des Ministres, *Recommandation CM/Rec(2012)4 sur la protection des droits de l'homme dans le cadre des services de réseaux sociaux*, paragraphes 5 et I.3, 4 avril 2012

[35] Comité des Ministres, *Recommandation CM/Rec(2012)3 sur la protection des droits de l'homme dans le contexte des moteurs de recherche*, paragraphe 8, 4 avril 2012

les tribunaux ordonnent de plus en plus souvent aux FAI de bloquer l'accès à ces sites. Par exemple, la Haute Cour d'Angleterre et du Pays de Galles a prononcé de telles injonctions concernant deux sites qui facilitaient à grande échelle l'atteinte au droit d'auteur : Newzbin2[36] et The Pirate Bay[37]. En Russie, les détenteurs de droits peuvent obtenir du Tribunal de Moscou qu'il ordonne aux responsables d'un site Internet de retirer dans les trois jours une vidéo constituant une infraction. S'ils n'obtempèrent pas, le tribunal peut ordonner aux FAI russes de bloquer l'accès au site[38].

Cependant, la Cour européenne des droits de l'homme a souligné qu'il fallait soigneusement peser les intérêts en jeu avant d'ordonner un blocage, une telle restriction préalable à l'expression appelant « l'examen le plus scrupuleux[39] ». La Cour examine actuellement une requête qui dénonce comme atteinte à l'article 10 le blocage de l'ensemble des sites comportant des œuvres musicales[40]. Dans deux de ses arrêts, la Cour de justice de l'UE affirme qu'imposer à des fournisseurs d'accès Internet ou à des sites de réseaux sociaux de surveiller toutes les données de leurs clients pour prévenir toute atteinte aux droits est contraire au droit de l'Union pour plusieurs raisons, dont un impact disproportionné sur la liberté individuelle de recevoir et de diffuser des informations garantie par la Charte des droits fondamentaux de l'UE[41]. D'après le Comité des Ministres, les mesures générales de blocage ne peuvent être utilisées que contre « un contenu Internet clairement identifiable » et « si les autorités compétentes ont pris une décision provisoire ou définitive sur son caractère illicite[42] ».

L'adoption de mesures d'autorégulation par les prestataires Internet (FAI, hébergeurs…), souvent encouragée par des règles juridiques qui les protègent des poursuites, a l'avantage d'être souple et de s'appuyer sur les connaissances et sur l'engagement des acteurs du secteur privé. Cependant, ces mesures n'assurent généralement pas la protection des droits individuels et la régularité des procédures. Contrairement à l'article 512 de la loi étasunienne sur les droits d'auteur à l'ère numérique, la directive européenne sur le commerce électronique ne prévoit pas même la possibilité qu'un usager conteste un avertissement pour infraction au droit d'auteur. Au Royaume-Uni, les FAI bloquent l'accès aux pages ou sites Internet jugés pédophiles par l'Internet Watch Foundation (IWF), organisme financé par les industriels du secteur, mais seuls quelques-uns avertissent les internautes qui tentent d'accéder à une page bloquée (les autres affichent un message d'erreur général). De son côté, l'IWF n'avertit pas automatiquement les responsables des sites bloqués ; sa procédure de recours n'a été utilisée qu'une fois, sans succès, au sujet du blocage d'une page Wikipedia. Ce

[36] *Twentieth Century Fox Film Corp & Others v. BT plc* [2011], EWHC 1981 (Ch)

[37] *Dramatico Entertainment Ltd & Others v. British Sky Broadcasting Ltd & Others* [2012], EWHC 268 (Ch)

[38] Loi fédérale de la Fédération du Russie n° 187-FZ. Voir aussi l'analyse juridique d'ARTICLE 19, sur http://www.article19.org/data/files/medialibrary/37202/Russia's-new-legislation-on-online-copyright-enforcement-.pdf

[39] Voir la note n° 13, § 47

[40] *Akdeniz c. Turquie*, n° 20877/10

[41] *Scarlet c. SABAM*, affaire C-70/10, 24 novembre.2011 ; *SABAM c. Netlog*, affaire C-360/10, 16 février 2012

[42] Voir la note n° 9

système de blocage a été mis en place en réponse à de fortes pressions du gouvernement, qui menaçait de légiférer sur le sujet[43].

Plus récemment, le gouvernement britannique a fortement incité les fournisseurs d'accès Internet à haut débit à inviter tous leurs clients, pour protéger leurs enfants, à bloquer l'accès à beaucoup plus de sites, certaines options étant activées par défaut. Parmi les catégories visées figurent la pornographie, les armes et la violence, l'extrémisme, le terrorisme, le partage de fichiers, le jeu, l'anorexie, les troubles de l'alimentation, le suicide et les atteintes à soi-même, l'alcool, le tabac, les messages « ésotériques » et les outils permettant de contourner le blocage d'un site. Certains sites sont déjà bloqués par défaut par les FAI mobiles ; les usagers doivent expressément demander à y accéder et montrer qu'ils sont majeurs[44]. Parmi les « outils de contournement des blocages » figurent des systèmes, tels que Virtual Private Networks, que les responsables allemands de la protection des données (et beaucoup d'autres) recommandent pour protéger sa vie privée en ligne[45].

Discours de haine et incitation à la violence

Lutter contre le discours de haine ou l'incitation à la violence contre des groupes ou des individus sur Internet tout en reconnaissant que la liberté d'expression englobe les propos qui « heurtent, choquent ou inquiètent[46] » représente un défi de taille. Les messages de haine ne sont pas protégés par l'article 10 de la Convention[47]. La marge d'appréciation des États est plus grande lorsqu'il s'agit de prendre des mesures contre des propos qui incitent à la violence[48], et il existe une « catégorie de faits historiques clairement établis – tel l'Holocauste – dont la négation ou la révision se verrait soustraite par l'article 17 à la protection de l'article 10[49] ». Bien que les mesures pénales puissent être les mieux adaptées face aux discours de haine « les plus flagrants », d'autres cas appelleraient peut-être davantage des mesures « éducatives, culturelles, informationnelles etc., de nature non réglementaire[50] ».

[43] I. Brown, « Internet self-regulation and fundamental rights », *Index on Censorship* 1 pp. 98-106, 2010

[44] J. Killock, « Sleepwalking into censorship », Open Rights Group blog, 25 juillet 2013

[45] Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, *Keine Umfassende Und Anlasslose Überwachung Durch Nachrichtendienste! Zeit für Konsequenzen*, 5 septembre 2013

[46] Voir la note n° 4

[47] *Gündüz c. Turquie*, n° 35071/97, § 41, CEDH 2003-XI

[48] *Sürek c. Turquie (n° 1)* [GC] (n° 26682/95, § 62, CEDH 1999-IV)

[49] *Lehideux et Isorni c. France*, 23 septembre 1998, § 47, Recueil des arrêts et décisions 1998-VII. Article 17 : « Aucune des dispositions de la présente Convention ne peut être interprétée comme impliquant pour un État, un groupement ou un individu, un droit quelconque de se livrer à une activité ou d'accomplir un acte visant à la destruction des droits ou libertés reconnus dans la présente Convention ou à des limitations plus amples de ces droits et libertés que celles prévues à ladite Convention ».

[50] T. McGonagle, *The Council of Europe against online hate speech: Conundrums and challenges*, contribution à la conférence « Les messages de haine dans le discours politique – Quelles responsabilités ? » organisée à Varsovie les 18 et 19 septembre 2013 par le Conseil de l'Europe et le gouvernement polonais, pp. 4-6, 28-29

Les auteurs de messages de haine sont extrêmement mobiles. Ils peuvent publier sur des sites américains bénéficiant de la large protection constitutionnelle offerte par le Premier amendement. Le blocage ou l'interdiction de tel ou tel site Internet n'est donc pas la bonne solution. Les hébergeurs, y compris les sites de réseaux sociaux, ont chacun leurs clauses contractuelles concernant le discours de haine ; ils sont souvent réticents à exercer eux-mêmes une censure. Les différentes entreprises du secteur peuvent avoir différents niveaux de responsabilité, en fonction de leur rôle éditorial et de divers facteurs contextuels ; « la création et la diffusion de messages de haine peuvent passer par une multiplicité d'acteurs : ceux qui les produisent ou les citent, ceux qui les publient, ceux qui les développent, ceux qui les hébergent ou contribuent à les diffuser ou à les rendre accessibles[51] ».

Vingt États ont ratifié le Protocole additionnel à la Convention du Conseil de l'Europe sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques[52]. Les autorités chargées de poursuivre les auteurs de tels actes doivent trouver un équilibre délicat : jouer un rôle dissuasif sans tétaniser la liberté d'expression. Une législation trop large risque d'être utilisée pour étouffer les critiques[53]. Le parquet d'Angleterre et du Pays de Galles a récemment publié des orientations sur les affaires concernant des messages diffusés via les réseaux sociaux[54].

On peut citer à ce sujet deux exemples récents : une nouvelle loi russe interdisant la « promotion des relations sexuelles non traditionnelles auprès des mineurs[55] », et des messages antisémites sur le site Twitter. Plusieurs groupes de la société civile ont dénoncé les dispositions de la loi russe, qu'ils jugent vagues, subjectives et dépourvues de toute preuve scientifique montrant un lien avec la santé et l'éducation des mineurs[56]. Cette loi fait planer un danger sur les associations qui luttent contre les propos homophobes en Russie. Elle prévoit une amende administrative plus de dix fois plus élevée lorsque les informations visées sont diffusées via les médias et/ou les réseaux d'information et de télécommunication.

En 2012, l'Union des étudiants juifs de France (UEJF) a obtenu du site Twitter qu'il suspende certains des comptes responsables d'un afflux de tweets reprenant les mots-clés « #unbonjuif » et « #unjuifmort ». L'UEJF a également obtenu qu'un tribunal ordonne à Twitter de fournir aux autorités françaises les données permettant d'identifier les auteurs des messages. En 2012, Twitter a instauré une politique permettant de retirer des tweets sur des territoires spécifiques sur réception d'une demande juridique jugée « valide et applicable », politique appliquée pour la première

[51] *Ibid.*

[52] STE n° 189, 28 janvier 2003

[53] Voir la note n° 50, pp. 27-29

[54] http://www.cps.gov.uk/legal/a_to_c/communications_sent_via_social_media/

[55] Loi fédérale du 29 juin 2013, n° 135-FZ, « portant modification de l'article 5 de la loi fédérale de protection des mineurs contre les informations nuisibles à leur santé et à leur développement »

[56] *Russia: Federal laws introducing ban of propaganda of non-traditional sexual relationships*, ARTICLE 19, juin 2013

fois concernant le compte d'un groupe néo-nazi allemand. Twitter s'efforce d'avertir l'auteur des messages retirés et les utilisateurs qui tentent d'y accéder[57].

Autres questions

Certains États membres, en prenant des mesures non justifiées par la Convention, mettent sérieusement à mal la liberté d'expression en ligne. En Azerbaïdjan, pour citer un exemple récent, des blogueurs ont été emprisonnés pour avoir exprimé leur opinion. Trois organisations intergouvernementales européennes estiment que leurs dossiers devraient faire l'objet d'un contrôle juridictionnel plus poussé[58]. Un collectif de la société civile a vivement critiqué les nouvelles lois étendant aux messages en ligne les dispositions pénales sur l'injure et la diffamation[59]. Freedom House a également critiqué les récentes lois russes qui érigent à nouveau la diffamation en infraction pénale et élargissent les critères d'interdiction de sites Internet, dont des sites politiques parfois victimes d'une « définition floue de la notion d'extrémisme » ; des blogueurs sont visés par des « poursuites pénales douteuses », des tribunaux régionaux ordonnent « le blocage de sites Internet qui révèlent des affaires de corruption locale ou contestent les pouvoirs locaux[60] ».

Liberté des médias

Le rôle de « chien de garde » joué par les médias rend particulièrement important leur droit, garanti par l'article 10, de recevoir et de communiquer des informations, notamment lorsqu'elles alimentent des débats sur des questions d'intérêt général[61]. L'accès du public à de telles informations ne saurait être limité que pour des raisons particulièrement impérieuses[62]. Comme l'observe la Cour, « grâce à leur accessibilité ainsi qu'à leur capacité à conserver et à diffuser de grandes quantités de données, les sites Internet contribuent grandement à améliorer l'accès du public à l'actualité et, de manière générale, à faciliter la communication de l'information[63] ».

Dans une déclaration, le Comité des Ministres constate que nous comptons de plus en plus sur les médias en ligne « pour obtenir et échanger des informations, publier des contenus, interagir, communiquer et [nous] associer les uns avec les autres », conférant à ces médias un précieux rôle de sentinelle sociale[64]. En particulier, les moteurs de recherche « permettent au public du monde entier de rechercher, de recevoir et de

[57] Twitter, « Tweets still must flow », *The Twitter Blog*, 26 janvier 2012

[58] *Joint statement on media freedom by European Commission, Council of Europe and Organisation for Security and Cooperation in Europe*, 9 novembre 2012

[59] International Partnership Group for Azerbaijan, *New legislative amendments further erode rights to freedom of expression and peaceful assembly*, 16 mai 2013

[60] *Freedom on the Net 2012: A Global Assessment of Internet and Digital Media*, 24 septembre 2012, p. 13

[61] *Observer et Guardian c. Royaume-Uni*, série A n° 216, § 59, 26 novembre 1991

[62] *Timpul Info-Magazin et Anghel c. Moldova*, n° 42864/05, 27 novembre 2007

[63] *Times Newspapers Limited (n^os^ 1 et 2) c. Royaume-Uni*, n^os^ 3002/03 et 23676/03, § 27, 10 mars 2009

[64] Voir la note n° 17, § 2

communiquer des informations, des idées et d'autres contenus, en particulier d'avoir accès au savoir, de prendre part à des débats et de participer aux processus démocratiques[65] », et les médias sociaux contribuent « à promouvoir l'exercice et la jouissance des droits de l'homme » et offrent de multiples occasions de « renforcer la possibilité pour les individus de participer à la vie politique, sociale et culturelle[66] ».

Les cadres réglementaires nationaux doivent assurer une protection effective de la liberté d'expression journalistique en ligne[67]. Comme l'explique la Cour, « compte tenu du rôle joué par l'Internet dans le cadre des activités professionnelles des médias et de son importance dans l'exercice du droit à la liberté d'expression en général, […] l'absence d'un cadre légal suffisant au niveau interne permettant aux journalistes d'utiliser des informations tirées de l'Internet sans crainte de s'exposer à des sanctions entrave gravement l'exercice par la presse de sa fonction vitale[68] ».

Les agressions et les emprisonnements de journalistes constituent un sérieux problème en Europe ; des blogueurs et des journalistes en ligne en ont aussi été victimes. Le Conseil de l'Europe, l'OSCE et la Commission européenne ont appelé à la libération de « tous les journalistes, blogueurs et citoyens qui ont été privés de liberté pour avoir exprimé leur opinion » en Azerbaïdjan[69]. Pour citer d'autres cas récents, un blogueur slovène a été emprisonné six mois pour injure et diffamation[70], et la rédactrice en chef d'un site Internet de Bosnie-Herzégovine a été victime d'une violente agression deux jours après la première projection de son documentaire sur la guerre de 1991-1995[71].

Protection des sources et des lanceurs d'alerte

La protection des sources et des lanceurs d'alerte est vitale pour tous les médias, traditionnels ou en ligne. L'Assemblée parlementaire affirme dans une recommandation 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 », que chacun devrait pouvoir transmettre des informations à un journaliste à titre confidentiel et que « les fournisseurs d'accès Internet et les entreprises de télécommunication ne devraient pas être tenus de divulguer des informations pouvant permettre d'identifier les sources des journalistes au mépris de l'article 10 de la Convention[72] ».

L'importance de ce problème a été soulignée par les révélations d'Edward Snowden sur la vaste surveillance d'Internet mise en place par les services de renseignement britanniques et étasuniens. Si les gouvernements persistent à surveiller une part substantielle des communications sur Internet (et à collecter les « métadonnées » les

[65] Voir la note n° 35, § 1

[66] Voir la note n° 34, §§ 1-2

[67] *Comité de rédaction de Pravoye Delo et Shtekel c. Ukraine* , n° 33014/05, 5 mai 2011

[68] Voir la note n° 67, § 64

[69] Voir la note n° 58

[70] Reporters sans frontières, « Un blogueur condamné à six mois de prison pour diffamation », 16 mai 2013

[71] Reporters sans frontières, « La rédactrice en chef d'un site Internet passée à tabac », 23 juillet 2012

[72] Recommandation 1950 (2011)

concernant), les journalistes auront beaucoup plus de mal à protéger leurs sources, en particulier celles qui révèlent des activités gouvernementales contestables ou potentiellement illégales. Comme l'a déclaré le rédacteur en chef du *Guardian*, qui a publié plusieurs des déclarations de Snowden : « La collecte des métadonnées compromet très gravement la capacité des journalistes à présenter des informations[73] ». Ethan Zuckerman, expert en médias au MIT, renchérit : « J'ai franchement peur pour les journalistes. Il est extrêmement difficile de leur promettre que leurs sources resteront anonymes[74] ».

La Commission des questions juridiques et des droits de l'homme de l'Assemblée parlementaire a adopté un rapport intitulé « La sécurité nationale et l'accès à l'information », qui souligne l'importance de « la protection de signalements en bonne foi d'abus[75] ». Elle va dans le sens des experts selon lesquels « les intérêts légitimes de la sécurité nationale sont en pratique mieux protégés lorsque la population est bien informée des activités de l'État, dont celles qui visent à assurer cette sécurité[76] ». Vingt membres de l'Assemblée parlementaire ont signé une proposition de recommandation en faveur d'un Protocole additionnel à la Convention sur la protection des donneurs d'alerte qui révèlent des agissements des pouvoirs publics constituant une violation du droit international et des droits fondamentaux[77].

Le tableau se noircit encore quand on sait que le gouvernement britannique a ordonné au *Guardian* de détruire l'ordinateur de ses bureaux londoniens où étaient stockés les documents d'Edward Snowden et que David Miranda, compagnon du journaliste du *Guardian* Glenn Greenwald, a été arrêté alors qu'il était en transit dans le pays[78]. Voici ce qu'un membre de l'Assemblée parlementaire a demandé au Comité des Ministres : « Les autorités britanniques ont exercé des pressions sur le journal *The Guardian* afin qu'il leur remette les dossiers qu'Edward Snowden avait confiés au journal. En outre, les autorités ont retenu pendant plusieurs heures David Miranda à l'aéroport d'Heathrow […]. Le Comité des Ministres considère-t-il que le comportement des autorités britanniques dans ces deux affaires est conforme aux engagements du Royaume-Uni concernant la garantie de la liberté de la presse ? Le Comité des Ministres s'accorde-t-il à reconnaître qu'une législation antiterrorisme ne saurait violer des libertés fondamentales telles que la liberté de la presse et la liberté d'expression[79] ? ». D'après la Cour européenne des droits de l'homme, « le droit des journalistes de taire leurs sources ne saurait être considéré comme un simple privilège qui leur serait accordé ou retiré en fonction de la licéité ou de l'illicéité des sources : c'est un véritable attribut du droit à l'information, à traiter avec la plus grande circonspection ». Les enquêteurs doivent tenir dûment compte de « l'intérêt du public à ce que la liberté d'expression

[73] @JeffJarvis, 20 septembre 2013, sur https://twitter.com/jeffjarvis/status/380838240913461248

[74] @TowCenter, 20 septembre 2013, sur https://twitter.com/TowCenter/status/380837947891007488

[75] Doc. 13293, 3 septembre 2013

[76] *Global Principles on National Security and the Right to Information*, 12 juin 2013, rédigés par dix-sept ONG et cinq pôles universitaires

[77] Doc. 13278, 5 juillet 2013

[78] « A Rusbridger, David Miranda, schedule 7 and the danger that all reporters now face », *The Guardian*, 19 août 2013

[79] Question écrite n° 643 au Comité des Ministres, doc. 13298, 9 septembre 2013

journalistique soit protégée, y compris à travers la protection des sources et la protection contre la remise forcée des documents recueillis[80] ».

Diffamation

Les informations publiées par les médias peuvent significativement nuire à la réputation de certaines personnes. La plupart des pays disposent donc de lois sur la diffamation, applicables en cas de « besoin social impérieux » ; mais si les droits ne sont pas soigneusement pesés, ces lois peuvent porter atteinte à la liberté d'expression et aux médias, en particulier lorsque des journalistes sont menacés d'emprisonnement. L'Assemblée parlementaire a demandé aux États membres d'abolir « sans attendre » les peines d'emprisonnement pour diffamation et de fixer un délai maximal pour le dépôt de plaintes pour diffamation, hors circonstances exceptionnelles[81]. Ce point est important pour les archives des médias en ligne, qui sont expressément protégées par l'article 10, bien que les journalistes soient encore plus tenus de vérifier l'exactitude des informations publiées lorsque la situation n'est pas urgente[82].

La liberté d'expression et la liberté des médias peuvent être limitées pour protéger la vie privée des individus, même lorsque les informations ont déjà été mises en ligne. Cependant, les médias n'ont pas à avertir les individus concernés avant de publier des informations à leur sujet[83].

Diversité des médias et éducation aux médias

Internet a eu un énorme impact sur la diversité et le pluralisme des médias. Beaucoup plus d'individus, d'institutions et d'acteurs médiatiques peuvent désormais s'exprimer via des sites à faible coût, financés par la publicité (sites personnels hébergés par des FAI, blogs, micro-blogs et autres types de médias sociaux). Les moteurs de recherche facilitent l'accès à l'information, mais peuvent poser des problèmes de respect des droits de l'homme, découlant « de la conception des algorithmes, de la désindexation et/ou du traitement partial ou des résultats biaisés, de la concentration du marché, du manque de transparence, aussi bien pour ce qui est de la sélection que du classement des résultats[84] ». Les nouveaux services en ligne ont aussi entraîné une forte baisse des revenus qui alimentaient traditionnellement les journaux, les journalistes de presse et dans une moindre mesure les services de radio et de télévision. Cela a « affaibli la capacité de la presse à attirer l'attention sur les questions d'intérêt public, en sapant les bases économiques du journalisme professionnel et en fragmentant le public. La détresse de ce secteur pourrait affaiblir la démocratie même, si l'on accepte l'idée qu'une presse indépendante assure une fonction démocratique essentielle[85] ».

---

[80] *Nagla c. Lettonie*, n° 73469/10, §§ 97 et 101, 16 juillet 2013

[81] Résolution 1577 et Recommandation 1814 de l'Assemblée parlementaire, *Vers une dépénalisation de la diffamation*, 2007

[82] Voir la note n° 63

[83] *Mosley c. Royaume-Uni*, n° 48009/08, 10 mai 2011

[84] Voir la note n° 35, § 4

[85] Voir la note n° 1, p. 235

L'aptitude de tous, toutes origines confondues, à participer à l'environnement médiatique en ligne est cruciale pour tirer le maximum des avantages individuels et sociaux d'Internet. Les programmes en faveur de la maîtrise d'Internet peuvent encourager la participation citoyenne, favoriser des prises de décision éclairées et réduire le risque que les jeunes soient exposés à certains contenus (violence envers soi-même et les autres, pornographie, discrimination et racisme) et à certains comportements (sollicitation, intimidation, harcèlement ou persécution[86]). D'après la Conférence des ministres responsables des médias et des nouveaux services de communication, l'éducation aux médias est « un outil indispensable pour optimiser, en particulier chez les enfants et les jeunes, la compréhension des médias, l'esprit critique, la citoyenneté, la créativité et la vigilance[87] ». Le Comité des Ministres recommande de promouvoir l'éducation aux médias concernant le fonctionnement des moteurs de recherche, « en particulier pour ce qui est des procédures de sélection, de classement et d'ordre de priorité des résultats de recherches », et la diversification des moteurs de recherche[88].

Liberté de réunion et d'association

L'article 11 de la Convention protège le droit à se réunir, à protester et à s'organiser. Les marches, les manifestations, les occupations de lieux ont joué un rôle central dans l'histoire politique de l'Europe moderne. Des foules se sont rassemblées pour protester, unies autour d'un objectif commun, et pour attirer l'attention par le biais des médias[89] ; tout cela peut être facilité par Internet. Les syndicats (expressément protégés par l'article 11.1) et les autres organisations sociales/politiques, au cœur des mouvements sociaux qui ont renversé les régimes totalitaires en Europe orientale et mis fin à la Guerre froide, ont à la fois protégé et fait progresser les droits individuels.

La plupart des mouvements sociaux s'appuient aujourd'hui sur les outils en ligne pour recruter et organiser leurs membres. L'article 11 s'étend aux associations apolitiques, telles que celles qui « protègent le patrimoine culturel ou spirituel, poursuivent divers buts socio-économiques, proclament ou enseignent une religion, valorisent une identité ethnique ou affirment une conscience de minorité ». D'après l'analyse de la Commission européenne des droits de l'homme, qui a eu à se pencher sur la question, il protège même le droit du personnel des services de renseignement à faire partie d'un syndicat[90]. Les ingérences doivent remplir des conditions aussi strictes que celles prévues pour l'article 10[91].

---

[86] Comité des Ministres, *Recommandation Rec(2006)12 sur la responsabilisation et l'autonomisation des enfants dans le nouvel environnement de l'information et de la communication*, 27 septembre 2006

[87] Première Conférence du Conseil de l'Europe des ministres responsables des médias et des nouveaux services de communication, *Une nouvelle conception des médias ?*, 29 mai 2009, MCM(2009)011

[88] Voir la note n° 35, § 8

[89] D.J. Harris, M. O'Boyle, E.P. Bates et C.M. Buckley, *Law of the European Convention on Human Rights,* 2e édition, 2009, Presses universitaires d'Oxford, p. 516

[90] *Ibid*., p. 547

[91] *Ibid.*, p. 531

Les principaux thèmes des affaires portées devant la Cour au titre de l'article 11 sont « la tolérance envers les protestations pacifiques, le pluralisme de l'opinion même s'il dérange autrui dans une certaine mesure et la légalité de l'ingérence des pouvoirs publics[92] ». D'après le Comité des Ministres, le droit à la liberté de réunion et d'association est, au même titre que la liberté d'expression, « essentiel à la participation de la population au débat public et à l'exercice de sa citoyenneté démocratique, et il doit être garanti dans le plein respect de l'article 11 de la Convention […] (sans distinction entre les environnements en ligne et hors ligne[93]) ». Le Comité souligne en particulier que les réseaux sociaux peuvent « contribuer à la démocratie et à la cohésion sociale » et recommande que les fournisseurs de réseaux sociaux assurent « l'accessibilité à leurs services pour les personnes handicapées, ce qui permettra d'améliorer l'intégration de ces personnes et leur pleine participation à la société[94] ».

Les ingérences dans la liberté d'expression (et dans la vie privée) en ligne ont souvent un impact sur la liberté de réunion et d'association, qui a pourtant fait l'objet de beaucoup moins d'écrits et de décisions que la première[95]. Quand la liberté de réunion est abordée, l'accent est mis sur le rôle et l'impact des nouvelles technologies de communication comme outils de débat et de participation politique (dont la participation des personnes vulnérables et défavorisées), de protestation et d'expression d'un mécontentement en général.

La liberté d'association protège le droit des individus à former des groupes pour défendre leurs intérêts – y compris des partis politiques, « même ceux qui remettent en cause le mode d'organisation actuel d'un État, pourvu qu'ils ne visent pas à porter atteinte à la démocratie elle-même[96] ». D'après le Comité des Ministres, « les obstacles à l'interaction de certaines communautés d'intérêt spécifique devraient être examinés au regard des normes internationales relatives au droit à la liberté de réunion et d'association[97] ». Bloquer l'accès aux sites Internet d'associations ou à des outils de communication (courrier électronique, réseaux sociaux...) peut fortement entraver la liberté de réunion et d'association. Frank La Rue, Rapporteur spécial de l'ONU, souligne le danger des blocages « opportunistes », « à des moments politiques clés : élections, périodes de troubles sociaux ou anniversaires d'événements historiques ou politiques marquants[98] ».

La réaction des autorités turques aux mouvements de protestation qui ont traversé le pays à partir de mai 2013 illustre certains de ces points. Des procureurs d'Istanbul ont ouvert des enquêtes contre des manifestants accusés d'avoir insulté le Premier ministre

[92] *Ibid*., p. 547

[93] Voir la note n° 17, § 1

[94] Voir la note n° 34, §§ 2 et 6

[95] Pour une analyse des liens entre les articles 10 et 11 dans un litige portant sur une action syndicale, voir *Palomo Sanchez et autres c. Espagne* (requêtes n^{os} 28955/06, 28957/06, 28959/06 et 28964/06). On trouvera un intéressant examen du droit de réunion en ligne à la lumière de la Constitution étasunienne dans J.D. Inazu, « Virtual Assembly », *Cornell Law Review* 98, pp. 1093-1142, 2012. Dans ses *Remarks on Internet Freedom*, l'ancienne Secrétaire d'État étasunienne Hillary Clinton estime que « la liberté de se connecter est l'équivalent de la liberté de réunion, dans le cyberespace ». Voir http://www.state.gov/secretary/rm/2010/01/135519.htm

[96] *Parti socialiste et autres c. Turquie*, § 47, Recueil 1998-III

[97] Voir la note n° 17, § 6

[98] Voir la note n° 10, § 30

et d'autres personnalités sur Twitter ou sur Facebook, et le gouvernement a proposé des mesures (jusqu'ici refusées par les deux entreprises) pour demander la transmission des données d'utilisateurs aux enquêteurs[99]. La Turquie a déjà bloqué des sites énormément utilisés par les groupes de la société civile, comme YouTube et Google Sites ; la Cour européenne des droits de l'homme estime que le « blocage de l'accès en général » n'est pas autorisé par la législation turque[100].

Lors de la campagne électorale d'octobre 2013, l'Azerbaïdjan a été largement critiqué par des organisations intergouvernementales et par la société civile pour avoir étendu aux messages et aux manifestations publiques en ligne les dispositions pénales contre la diffamation et l'injure. Des blogueurs et des militants actifs sur les réseaux sociaux ont été arrêtés et condamnés à des peines d'internement administratif. Certains acteurs de la campagne notent que « les entraves au militantisme politique et le manque de diversité des médias faisaient [jusqu'ici] d'Internet le principal refuge de la liberté d'expression et de l'opposition politique en Azerbaïdjan[101] ».

Réunions en ligne sur des sites privés

S'agissant de protéger les libertés sur Internet, le fait qu'une très grande part des infrastructures nécessaires à l'activité en ligne appartienne à des acteurs privés représente un défi majeur pour les États. Comment équilibrer d'une part l'obligation positive qu'ont les pouvoirs publics de protéger les réunions et associations sur des sites de réseaux sociaux privés, et d'autre part le droit de ces sites à la propriété, garanti par l'article 1 du premier Protocole additionnel à la Convention ? Jusqu'ici, la Cour s'est montrée très réticente à protéger les réunions physiques équivalentes, comme par exemple la distribution de tracts ou la collecte de signatures dans des centres commerciaux privés. Elle juge que l'article 10 et par conséquent l'article 11 ne donnent pas la « liberté de choisir un forum » et que l'évolution des modes d'interaction sociale n'exige pas « automatiquement la création d'un droit de pénétrer dans des propriétés privées ». Elle n'exclut pas que l'État ait à réglementer le droit de propriété dans « une ville appartenant à une entreprise, dans laquelle la municipalité [serait] contrôlée par un organisme privé[102] ». Il serait intéressant de se demander à partir de quelle part de marché un site de réseau social remplirait cette condition.

Surveillance des communications et analyse des réseaux sociaux

Voici ce qu'écrit Martin Scheinin, ancien Rapporteur spécial de l'ONU sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste :

> *L'exercice d'une surveillance menace aussi les droits relatifs à la liberté d'association et à la liberté de réunion. Pour jouir de ces libertés, les personnes*

[99] S. Fraser, « Turkey Investigates Social Media Postings That Allegedly Insult Officials », *The Huffington Post*, 27 juin 2013

[100] Voir la note n° 13, § 62

[101] Voir la note n° 59

[102] Voir la note n° 89, pp. 518-519

doivent souvent se réunir et communiquer en privé afin de s'organiser face aux pouvoirs publics ou à d'autres acteurs puissants. L'extension des pouvoirs de surveillance a eu parfois des effets insidieux, lorsque des services de police ou de renseignements ont qualifié de terroristes certains groupes afin de pouvoir exercer des pouvoirs de surveillance qui ne leur étaient accordés qu'au titre de la lutte contre le terrorisme. Aux États-Unis, des militants écologistes et d'autres contestataires pacifiques ont été placés sur des listes de personnes à surveiller par la police de l'État du Maryland avant les conventions électorales de New York et de Denver. Au Royaume-Uni, des caméras de surveillance sont fréquemment utilisées lors de manifestations politiques et les images conservées dans une base de données. D'après un récent sondage effectué au Royaume-Uni, un tiers des personnes sont réticentes à participer à des manifestations car elles s'inquiètent pour leur vie privée[103].

Comme l'ont montré les révélations d'Edward Snowden, les services de renseignement étasuniens analysent massivement les réseaux sociaux pour collecter des informations sur les citoyens, s'appuyant sur les traces électroniques de leurs communications et autres activités pour dresser la carte détaillée de leurs « connexions sociales » et identifier « leurs fréquentations, les lieux où ils se sont trouvés à tel ou tel moment ou leurs compagnons de voyage ». La NSA reçoit chaque jour 20 milliards de « traces d'activité », comprenant les données des sites de réseaux sociaux, 700 millions de traces d'appels sur téléphones fixes et 1,1 milliard de traces d'appels sur téléphones portables[104].

Si des pays européens (comme probablement le Royaume-Uni, et peut-être la Suède et la France) procèdent au même type de collecte et d'analyse de données, la proportionnalité d'une telle ingérence sera cruciale pour savoir si l'article 11 est respecté. Selon les observations de Maina Kiai, Rapporteur spécial de l'ONU sur le droit de réunion pacifique et la liberté d'association, à la suite d'une visite au Royaume-Uni, « la surveillance et les bases de données des services de renseignement ont un effet indéniablement tétanisant sur les protestataires, qui craignent d'organiser de nouvelles manifestations[105] ». La Cour qualifie le refus d'enregistrer une association et la dissolution définitive d'un parti politique respectivement de « mesure radicale » et de « mesure draconienne », ne se justifiant que dans des circonstances exceptionnelles. Cependant, la restriction des financements en provenance de l'étranger n'a pas été interdite[106]. À cet égard, il est difficile de savoir sur quel point du spectre situer l'enregistrement et l'analyse de toutes les associations et réunions électroniques (et des données physiques associées, comme le lieu d'un appel sur téléphone portable).

Faut-il protéger les attaques par déni de service distribué ?

Autre question encore ouverte : les attaques en ligne par déni de service distribué, utilisées par des protestataires pour rendre certains sites Internet indisponibles,

[103] A/HRC/13/37, § 36

[104] J. Risen et L. Poitras, « NSA Gathers Data on Social Connections of US Citizens », *The New York Times*, 28 septembre 2013

[105] A/HRC/23/39/Add.1, 29 mai 2013

[106] Voir la note n° 89, p. 534

devraient-elles être protégées au même titre que les sit-in ou les manifestations sur des terrains publics ou privés ? D'après la Convention sur la cybercriminalité, ces attaques devraient constituer une infraction pénale[107]. Pour donner un exemple, le collectif en ligne Anonymous a lancé une attaque contre les sites Internet de Visa et de Mastercard parce qu'ils avaient bloqué des dons à WikiLeaks[108].

Même si la Cour acceptait cette analogie, l'article 11 demande aussi aux États d'éviter les rencontres entre protestataires rivaux et autorise une large marge d'appréciation pour limiter les rassemblements qui interrompent volontairement des activités. La Cour examine de plus près la nécessité des interdictions s'agissant des réunions pacifiques visant à exprimer une opinion sur une question d'intérêt général. Cependant, il est de toutes manières peu probable que les auteurs d'actes entrant dans le champ du droit pénal soient protégés contre les poursuites et les condamnations, même s'ils ont cherché à attirer l'attention sur leur cause[109].

Réactions envisageables

Comme l'observe le Conseil de l'Europe dans sa Stratégie 2012-2015 sur la gouvernance de l'Internet, « la liberté d'expression et d'information, sans considération de frontières, constitue une exigence première car elle sert de catalyseur à l'exercice d'autres droits[110] ». Comme nous l'avons vu au chapitre précédent, la liberté de réunion et d'association en ligne est étroitement liée à la liberté d'expression. La première partie du présent chapitre est consacrée aux mesures que les États devraient adopter en priorité pour protéger ces droits, là où l'action de la Cour risque d'être difficile ou de prendre de nombreuses années.

La Stratégie souligne aussi l'importance d'intégrer les diverses parties prenantes pour garantir qu'Internet demeure universel, ouvert et novateur et continue à servir les intérêts des usagers[111]. Dans un second temps, ce chapitre abordera l'engagement des entreprises, de la société civile, des chercheurs et de la communauté technique en vue de cet objectif. Cela soulève d'autres questions épineuses, relatives aux responsabilités des acteurs privés dans la protection des droits de l'homme.

L'UE mène des travaux importants dans ces deux domaines. Son adhésion à la Convention européenne des droits de l'homme devrait l'amener à participer plus encore aux activités du Conseil de l'Europe.

[107] Voir la note n° 18

[108] E. Addley et J. Halliday, « WikiLeaks supporters disrupt Visa and MasterCard sites in 'Operation Payback' », *The Guardian*, 9 décembre 2010

[109] Voir la note n° 89, pp. 517/21/24

[110] CM(2011)175 final, § 3, 15 mars 2012

[111] *Ibid*., § 4

Réponses et actions des États

Comme nous l'avons déjà vu, le Comité des Ministres et l'Assemblée parlementaire du Conseil de l'Europe ont adopté plusieurs déclarations, résolutions et recommandations importantes pour la protection de la liberté d'expression, de réunion et d'association.

Pour progresser encore, le premier défi qui se pose au Conseil consiste à définir le meilleur moyen d'encourager l'accès de tous les Européens à Internet. Cette question est étudiée par la Commission de la culture, de la science, de l'éducation et des médias de l'APCE et par le Comité d'experts sur les droits des usagers d'Internet. L'UE a intégré une obligation de service universel à son règlement de 2009 sur les communications électroniques[112]. Il a déjà été suggéré que le Conseil traite l'accès à Internet comme faisant partie des droits de l'homme[113]. Cette vision très intéressante créerait un engagement pour les États membres, même si une bonne part des investissements dans la mise en place des nouvelles infrastructures est venue du secteur privé.

Le deuxième défi consiste à décider jusqu'à quel point garantir aux internautes la neutralité du réseau ou l'accès aux contenus et aux services sans discrimination. Le Conseil a organisé une rencontre multipartite de deux jours sur ces questions en mai 2013, et participé à la création d'une « coalition dynamique » au sein du Forum de l'ONU sur la gouvernance d'Internet pour détailler les garanties de neutralité, importantes pour la gestion et la sécurité du réseau. La Commission européenne a proposé en septembre 2013 de nouvelles règles sur la neutralité du réseau[114], critiquées toutefois par la société civile comme « une mainmise des entreprises qui relèguerait le reste des citoyens et les nouveaux arrivants dans un Internet de seconde zone, avec des effets désastreux sur la liberté et l'innovation en ligne[115] ». Le Conseil de l'Europe pourrait jouer un rôle important pour élargir ce débat et pour aider à résoudre les tensions entre la promotion des droits de l'homme et la facilitation des investissements privés nécessaires à l'accès universel.

L'environnement en ligne a donné plus d'importance encore aux travaux du Conseil de l'Europe sur la dépénalisation de la diffamation, car les blogueurs et militants indépendants sont encore plus vulnérables que ceux soutenus par une organisation face aux actions des pouvoirs publics visant à les dissuader d'exercer leur liberté d'expression.

Les questions de diffamation et de protection de la réputation appellent une étude plus approfondie. La large diffusion des contenus en ligne a amené certaines juridictions à exercer une compétence très large. La Cour suprême de Londres est désormais célèbre pour ses actions en diffamation dans lesquelles ni le requérant, ni le défendeur, ni la publication ne se trouvent au Royaume-Uni[116]. En réaction, le Royaume-Uni a instauré

[112] JO L 337, 18 décembre 2009

[113] A. Mellakauls, *L'accès à Internet – un droit de l'homme ?*, CDMSI(2012)Misc3Rev

[114] Commission européenne, « Proposition de règlement établissant des mesures relatives au marché unique européen des communications électroniques et visant à faire de l'Europe un continent connecté », COM(2013)627 final, 11 septembre 2013

[115] European Digital Rights, « Net Neutrality Threatened By The Commission's Draft Regulation », *EDRi-gram* 11.17, 11 septembre 2013

[116] English PEN et Index on Censorship, *Free Speech is Not For Sale: The Impact of English Libel Law on Freedom of Expression*, 2009

de nouvelles limites de compétences, prévues à l'article 9 de la loi de 2013 sur la diffamation. Le Conseil pourrait s'appuyer sur cet exemple pour étudier les larges (et délicates) questions de compétence soulevées par Internet au regard de la protection des droits de l'homme. Autrement, les recoupements de compétences risquent sérieusement de restreindre la disponibilité transfrontalière de documents légaux en vertu du droit international mais interdits par des règles nationales culturellement spécifiques, sur des sujets tels que l'obscénité par exemple[117]. Comme l'a déjà noté le Comité des Ministres, les États ont la responsabilité de « s'assurer que les activités exercées dans les limites de leur juridiction ne font pas obstacle de manière illégitime à l'accès aux contenus en dehors de leurs frontières territoriales ni n'entravent le flux transfrontalier du trafic Internet » ; le Comité recommande aux États de « coopérer entre eux et avec les parties prenantes concernées, en toute bonne foi, à tous les stades de l'élaboration et de la mise en œuvre des politiques publiques relatives à l'Internet, de manière à éviter tout effet transfrontière qui pourrait porter atteinte à l'accès à l'Internet et à son utilisation[118] ».

La popularité des commentaires sur les médias en ligne pose un problème spécifique, celui de la responsabilité des éditeurs à l'égard des messages de leurs usagers. Une affaire actuellement examinée par la Cour porte sur un site d'actualité estonien condamné à verser des dommages et intérêts pour les commentaires injurieux postés par plusieurs de ses lecteurs[119]. Le Royaume-Uni a renforcé la protection des opérateurs de sites Internet quant aux propos tenus par des tiers sur leur site, même lorsque les commentaires font l'objet d'une modération[120]. Il s'agit d'une mesure intéressante, qui pourrait empêcher – ce que le Rapporteur spécial de l'ONU Frank La Rue considère comme un sérieux problème[121] – que la responsabilité du fait d'autrui ne nuise au potentiel des plates-formes Internet de relayer l'opinion de tierces personnes.

Le Conseil doit étudier plus avant la protection de la diversité culturelle en ligne et l'accès individuel aux expressions et produits culturels selon des modalités compatibles avec la liberté d'expression et la prééminence du droit. Sous l'égide d'ARTICLE 19, organisation de la société civile, un groupe international d'experts a élaboré des principes sur la liberté d'expression et le droit d'auteur, fondés sur le droit international, qui pourraient servir de point de départ. Aux côtés de plusieurs principes généraux, les auteurs recommandent entre autres de ne pas couper l'accès d'un usager à Internet pour des raisons de droit d'auteur, d'encadrer strictement le filtrage et le blocage et de minimiser la responsabilité du fait d'autrui[122].

S'agissant de la protection de la liberté d'expression via le système des noms de domaine, les représentants du Conseil de l'Europe pourraient chercher à affirmer davantage leur rôle dans les réunions de l'ICANN (Internet Corporation for Assigned

[117] D. Korff et I. Brown, « Social media and human rights », *Human rights and a changing media landscape*, Strasbourg : Éditions du Conseil de l'Europe, 2011, pp. 175-206

[118] Comité des Ministres, *Recommandation CM/Rec(2011)8 sur la protection et la promotion de l'universalité, de l'intégrité et de l'ouverture de l'Internet*, 21 septembre 2011

[119] *Delfi AS c. Estonie*, n° 64569/09, communiquée le 11 février 2011

[120] Loi de 2013 sur la diffamation (c. 26), article 5

[121] Voir la note n° 10, §§ 38-48

[122] *Le droit de partager : principes relatifs au droit à la liberté d'expression et au droit d'auteur à l'ère du numérique*, ARTICLE 19, 2013

Names and Numbers), chargée de la gestion de ce système. Pour cela, ils pourraient participer aux structures existantes de l'ICANN, coordonner les positions des États membres sur les questions de droits de l'homme avec le Comité consultatif gouvernemental de l'ICANN ou même inviter l'ICANN à envisager de nouveaux mécanismes pour que les organismes régionaux de droits de l'homme puissent la conseiller sur les questions de droits de l'homme[123].

Concernant la vaste surveillance d'Internet révélée par Edward Snowden, les graves problèmes de droits de l'homme qu'elle soulève appellent une action coordonnée de la part de tous les organes du Conseil de l'Europe. La Commission des questions juridiques de l'Assemblée examine actuellement une proposition de résolution sur les opérations massives de surveillance en Europe qui « invite le Secrétaire Général à ouvrir une enquête en vertu de l'article 52 de la Convention européenne des droits de l'homme[124] ». Dans l'intervalle, la Cour[125], le Commissaire aux droits de l'homme et le Comité des Ministres auront l'occasion d'examiner les épineuses questions soulevées par ces révélations. Quelles limites à la collecte de renseignements par un État sont nécessaires pour réellement protéger la liberté d'expression, de réunion et d'association, ainsi que la vie privée, à l'ère d'Internet ? Alors que presque toutes les activités humaines laissent une forme ou une autre de trace numérique, suffit-il d'adopter des règles effectives de procédure et de contrôle (et des règles spécifiques, comme celles sur la protection des sources et des lanceurs d'alerte) pour dûment protéger les droits de l'homme ?

Les politiques menées par les États pour assurer la sécurité nationale et lutter contre le terrorisme posent d'autres problèmes délicats pour la liberté d'expression, de réunion et d'association. Les principes de droit international résumés par Frank La Rue, Rapporteur spécial de l'ONU, offrent un bon point de départ à la réflexion. Il propose par exemple que l'interdiction de soutenir des activités et organisations terroristes ne soit appliquée que pour restreindre les propos qui appellent sciemment à des actes de violence imminents et sont susceptibles de les provoquer, et jamais aux débats politiques, aux élections, aux informations concernant les droits de l'homme, les actions des pouvoirs publics ou la corruption des agents publics, aux manifestations pacifiques/activités politiques et à l'expression d'une opinion, d'un désaccord, d'une religion ou d'une croyance, y compris de la part de minorités et d'autres groupes vulnérables[126].

Le Comité des Ministres devrait envisager de recommander d'autres normes positives et procédurales concernant la protection contre les poursuites et les autres mécanismes d'autorégulation et de co-régulation (en s'appuyant sur ses recommandations relatives aux filtres, aux réseaux sociaux et aux moteurs de recherche), et d'élaborer des procédures juridiques permettant aux tribunaux d'ordonner un blocage en tenant pleinement compte de son impact sur la liberté d'expression, de réunion et

[123] Un expert a suggéré de faire du Comité consultatif gouvernemental un organisme multi-pouvoirs publics, où seraient représentés plusieurs organismes gouvernementaux et intergouvernementaux et des partis politiques minoritaires (à l'image de l'Assemblée parlementaire du CdE). Voir M. Mueller, « Reform ICANN's Governmental Advisory Committee: Multi-stakeholderize it! », *Internet Governance Project* blog, 8 août 2012

[124] Voir la note n° 22

[125] L'auteur a fourni une déposition de témoin expert pour une requête déposée par Big Brother Watch, Open Rights Group, la section anglaise de PEN et Constance Kurtze contre le Royaume-Uni (requête n° 58170/13).

[126] Voir la note n° 117

d'association. Ces règles pourraient s'inspirer des normes de procédure dérivées par la Cour des articles 6 (droit à un procès équitable) et 13 (droit à un recours effectif) et des limites que la Cour a posées aux ingérences dans les droits garantis aux articles 8, 10 et 11, ingérences qui doivent :

- reposer sur des règles juridiques claires, accessibles et prévisibles (et dans la mesure du possible inscrites dans la loi) ;
- répondre à un « besoin social impérieux » ;
- n'être ni inefficaces, ni disproportionnées par rapport à l'objectif ;
- prévoir un « recours effectif », de préférence judiciaire, si ces critères ne sont pas remplis[127].

Lorsqu'un organisme se voit déléguer le pouvoir d'appliquer ces règles, il doit avoir une latitude limitée, motiver ses décisions et faire l'objet d'un contrôle juridictionnel. Les responsables des sites bloqués devraient être avertis et avoir la possibilité de contester la décision devant un tribunal[128].

Le Comité des Ministres devrait aussi étudier sérieusement la compatibilité avec la prééminence du droit des pressions informelles exercées par des États sur des intermédiaires pour qu'ils imposent aux internautes des filtres « par défaut » susceptibles de bloquer l'accès à un grand volume de données pourtant légales. Frank La Rue a noté en 2011 que les mesures de blocage insuffisamment ciblées rendant inaccessible un large éventail de contenus, y compris légaux, étaient par définition non nécessaires ou disproportionnées[129].

S'agissant du discours de haine, une récente contribution à une conférence organisée par le Conseil de l'Europe et le gouvernement polonais note que « l'éventail des dommages à prévenir ou à minimiser est complexe et varié » et que la réglementation contre les messages de haine « les plus flagrants » doit être complétée par des mesures éducatives, culturelles et informationnelles. L'auteur recommande les mesures suivantes :

- revoir les recommandations (97) 20 et 21 du Comité des Ministres pour qu'elles s'appliquent mieux à l'environnement en ligne ;
- mettre le discours de haine en ligne au premier plan du travail normatif du Conseil de l'Europe ;
- fournir des orientations sur le poids respectif des droits, des devoirs et des responsabilités à l'ère numérique, en particulier concernant les messages de haine en ligne ;
- renforcer les capacités et mieux sensibiliser ;
- chercher collectivement des solutions ;

[127] *Ibid.*

[128] *Ibid.*

[129] *Ibid.*

- élaborer et promouvoir activement un « serment anti-discours de haine » pour les responsables et partis politiques[130].

L'un des défis les plus difficiles à relever pour le Conseil consiste à encourager les médias d'actualité à rester aussi divers et dynamiques dans l'environnement en ligne. Les réponses les plus appropriées de la part des différents acteurs dépendront des trajectoires suivies par ces médias. Il pourrait s'avérer nécessaire d'étoffer les règles concernant le pluralisme des médias[131]. De nouvelles formes de règles anti-monopole pourraient être utiles[132]. Les programmes éducatifs et, généralement, le développement de la maîtrise des nouveaux médias chez les enfants et les adultes ont un rôle important à jouer[133]. Paul Starr relève un avantage de la tradition d'après-guerre en Europe : « Il est difficile d'imaginer que la seule philanthropie compense les ressources perdues [...]. Les pays dotés de services publics de radio et de télévision bien établis seront peut-être mieux armés, sur le plan idéologique comme institutionnel, pour relever les défis de la crise des médias[134] ».

Participation des entreprises et des autres acteurs clés

Les entreprises et techniciens qui développent et font fonctionner une bonne part de l'infrastructure Internet, les chercheurs qui étudient les comportements en ligne et les groupes de la société civile qui défendent les droits des usagers ont un rôle crucial à jouer pour protéger les libertés sur Internet. D'après une déclaration du Comité des Ministres, « la libre parole sur l'Internet fait face à de nouveaux défis et pourrait être victime des mesures prises par des plates-formes et des prestataires de services en ligne gérés par des exploitants privés. Il est donc nécessaire de reconnaître le rôle de ces acteurs en tant que facilitateurs de l'exercice de la liberté d'expression et du droit à la liberté de réunion et d'association[135] ». Pour citer Hillary Clinton, ancienne Secrétaire d'État étasunienne, le secteur privé « partage la responsabilité de préserver la libre parole. Et lorsque ses pratiques commerciales menacent cette liberté, il doit se demander ce qui est juste, et non simplement ce qui rapporte[136] ».

D'après Frank La Rue, Rapporteur spécial de l'ONU, les entreprises Internet ont des devoirs pour protéger les droits des usagers[137]. Korff et Brown résument ainsi ces devoirs : « Les intermédiaires ne devraient limiter ces droits que sur intervention de la justice, porter les mesures prises à la connaissance de l'usager concerné et du grand public le cas échéant, avertir les usagers dans la mesure du possible avant d'adopter des

[130] Voir la note n° 50, p. 35

[131] Cette discussion remonte à au moins quinze ans au Conseil de l'Europe. Voir C. Marsden, *Le pluralisme sur le marché multichaînes : pistes à explorer sur le plan de la régulation*, MM-S-PL(1999)012, § 5.1

[132] I. Brown et C.T. Marsden, *Regulating Code: Good Governance and Better Regulation in the Information Age*, Cambridge, MA : MIT Press, 2013

[133] S. Livingstone, T. Papaioannou, M. Mar Grandío Pérez et C. Wijnen, « Critical insights in European media literacy research and policy », *Media Studies 3*(6) pp. 1-13, 2012

[134] Voir la note n° 1

[135] Voir la note n° 17, § 5

[136] Voir la note n° 95

[137] Voir la note n° 10

mesures restrictives et limiter strictement l'impact des restrictions au contenu concerné. Enfin, les usagers touchés doivent disposer de recours effectifs, dont des voies de recours fournies par l'intermédiaire et par une autorité judiciaire compétente[138] ».

En juin 2011, le Conseil des droits de l'homme de l'ONU a adopté à l'unanimité des Principes directeurs relatifs aux entreprises et aux droits de l'homme[139]. Ils énoncent les devoirs qui incombent aux entreprises pour éviter de porter atteinte aux droits, corriger les impacts négatifs de leurs actions et coopérer pour offrir un recours en cas de violation. Un groupe de travail de l'ONU travaille encore à ces principes ; la Commission européenne, de son côté, a récemment soutenu l'élaboration d'un guide destiné au secteur des TIC. Il décrit, à l'attention des entreprises, un processus leur permettant de tenir dûment compte des droits de l'homme sur les marchés où elles opèrent en analysant l'impact potentiel des activités de l'entreprise sur les différents groupes de parties prenantes. Le guide présente six éléments clés du « devoir de respect des droits de l'homme » pour les entreprises, représentés par la figure 1[140].

Dans le cadre d'un projet multipartite, la Global Network Initiative (GNI), des entreprises de technologies, des investisseurs, des chercheurs et des groupes de la société civile ont développé des principes de protection des droits de l'homme qui vont déjà au-delà des Principes directeurs de l'ONU. Les États et les autres acteurs devraient envisager de promouvoir davantage ce type d'initiative d'autorégulation auprès des secteurs clés (comme les entreprises de télécommunications) qui n'ont jusqu'ici joué qu'un rôle limité. Aux États-Unis, le Congrès débat d'un projet de loi sur la liberté en ligne dans le monde, qui demanderait aux opérateurs actifs dans des pays désignés par le Secrétariat d'État comme « imposant des restrictions à Internet » de publier le détail de leurs politiques en matière de respect des droits de l'homme. Les entreprises adhérant à la GNI ou à d'autres initiatives similaires seraient exemptées de certaines des dispositions de la loi[141]. Le Comité des Ministres pourrait envisager de recommander des mesures similaires.

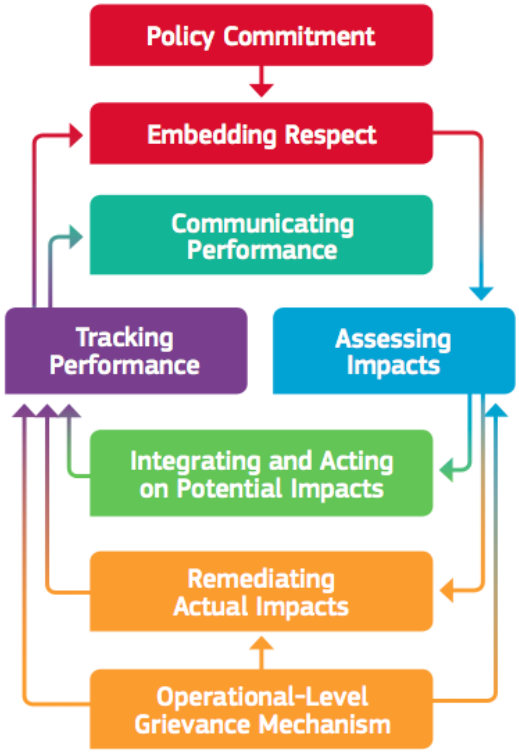

Figure 1 : éléments clés du devoir de respect des droits de l'homme pour les entreprises. Source : Commission européenne

[138] Voir la note n° 117

[139] A/HRC/17/31, 21 mars 2011

[140] Shift et Institute for Human Rights and Business, *ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights*, Commission européenne, 2012

[141] I. Brown, « The Global Online Freedom Act », *Georgetown Journal of International Affairs 14* (1), pp. 153-160, 2013

Légende du schéma

Policy Commitment	**Engagement politique**
Embedding Respect	**Intégrer le respect**
Communicating Performance	**Communiquer les réalisations**
Tracking Performance	**Surveiller les réalisations**
Assessing impacts	**Évaluer les impacts**
Integrating and Acting on Potential Impacts	**Connaître les impacts potentiels et y réagir**
Remediating Actual Impacts	**Remédier aux impacts actuels**
Operational-Level Grievance Mechanism	**Mécanisme de recours opérationnel**

Parmi les éléments des Principes directeurs de l'ONU sur lesquels le Conseil de l'Europe travaille déjà figure l'amélioration de la transparence des parties prenantes concernant, par exemple, le nombre de demandes de retraits de contenu ou de transmission de données d'usagers aux pouvoirs publics et les procédures suivies à cet effet. Des entreprises telles que Google, Microsoft, Yahoo et plus récemment Facebook publient régulièrement des statistiques sur le nombre et l'origine de ces demandes. Tandis qu'auparavant, la législation étasunienne leur interdisait de publier les demandes formulées pour des raisons de sécurité nationale, ces entreprises cherchent aujourd'hui à faire valoir ce droit en vertu du Premier amendement[142] ; à la suite des révélations de Snowden, le gouvernement étasunien les a autorisées à publier des synthèses statistiques. Plusieurs projets de loi actuellement à l'étude au Congrès étasunien visent à protéger ce droit[143]. Le processus multipartite en cours au Conseil de l'Europe pour élaborer des orientations et des engagements en matière de transparence pourrait fortement contribuer à cet effort de transparence au niveau mondial.

Remerciements

Merci beaucoup à Gabrielle Guillemin, Douwe Korff et Chris Marsden pour leurs suggestions et commentaires au fil de la rédaction de ce rapport.

[142] Microsoft Corporation, *In re Motion to Disclose Aggregate Data Regarding FISA Orders*, US Foreign Intelligence Surveillance Court, affaire n° MISC. 13-04, et autres requêtes similaires par LinkedIn Corporation, Facebook, Inc., Yahoo! Inc. et Google Inc.

[143] Voir par exemple S. 1452 (Surveillance Transparency Act, 2013) et H.R. 3035 (Surveillance Order Reporting Act, 2013)