Nations Unies A/HRC/32/38

Assemblée générale

Distr. générale
11 mai 2016
Français
Original : anglais

Conseil des droits de l'homme
Trente-deuxième session
Point 3 de l'ordre du jour
Promotion et protection de tous les droits de l'homme, civils, politiques, économiques, sociaux et culturels, y compris le droit au développement

Rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression*

Note du secrétariat

Le secrétariat a l'honneur de transmettre au Conseil des droits de l'homme le rapport que le Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, David Kaye, a établi en application de la résolution 25/2 du Conseil. Ce rapport est le premier d'une série d'études sur des questions touchant à la fois à la réglementation publique, aux activités du secteur privé et à la liberté d'expression à l'ère du numérique. Le Rapporteur spécial y étudie le cadre juridique de la liberté d'expression et les principes applicables au secteur privé, recense les principaux acteurs du secteur des technologies de l'information et de la communication (TIC) dont le mode d'action a des incidences sur la liberté d'expression et décrit les questions juridiques et les questions de fond qu'il étudiera au cours de son mandat.

* Le présent rapport a été soumis après la date limite afin que les faits les plus récents puissent être pris en compte.

GE.16-07644 (F) 090616 130616
1607644

Rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression

Table des matières

I. Introduction

1. À l'ère du numérique, le secteur privé occupe un rôle de plus en plus considérable ; il est en effet devenu le fer de lance de la plus grande expansion de l'accès à l'information de l'histoire. Les grands forums de médias sociaux où s'expriment les usagers appartiennent à des sociétés privées. Les principales plateformes, qui regroupent et indexent les connaissances mondiales, et qui élaborent les algorithmes qui déterminent les informations qui apparaissent en ligne, sont issues d'initiatives privées. Les infrastructures de technologie mobile qui permettent à des milliards de personnes de communiquer et de consulter Internet dépendent d'investissements privés, de services de maintenance privés et, en définitive, des décisions d'actionnaires du secteur privé. Les outils employés par les forces de l'ordre et les services de renseignement sont souvent issus de produits utilisés par les professionnels de la surveillance privée et du traitement des données. Ce sont souvent des sociétés privées qui mettent au point, fabriquent et assurent la maintenance des dispositifs ou services de stockage des données personnelles les plus importantes, données qui vont des renseignements financiers et médicaux aux courriels, en passant par les textos, l'historique des recherches, les photographies ou encore les vidéos.

2. L'exercice de la liberté d'opinion et d'expression à notre époque doit pour beaucoup sa force au secteur privé, qui exerce un pouvoir considérable sur l'espace numérique, parce qu'il joue le rôle de portail d'information et d'intermédiaire de l'expression. On ne peut éluder les importantes questions qui se posent dans les environnements numériques, relatives au droit applicable, à la portée de l'action de l'autorité privée et au champ d'application de la réglementation publique. Ces acteurs privés doivent-ils avoir les mêmes responsabilités que les autorités publiques ? Leurs responsabilités doivent-elles être fondées sur le droit des droits de l'homme, les conditions d'utilisation, les dispositions contractuelles ou d'autres éléments ? Comment les rapports entre les acteurs privés et les États doivent-ils se structurer ? Quelles mesures les acteurs privés doivent-ils prendre lorsqu'ils subissent des pressions et qu'ils sont incités à conduire leurs affaires d'une manière contraire à la liberté d'expression ? Doivent-ils refuser d'entrer sur ces marchés ? Doivent-ils s'en retirer ? Doivent-ils informer leurs clients des pressions qu'ils subissent ? Au moment où le monde s'engage de plus en plus dans l'espace numérique, et où « l'Internet des objets » est pour demain, il est essentiel de se doter d'orientations qui garantissent la promotion, la protection et l'exercice des droits.

3. Dans le présent document, le Rapporteur spécial poursuit plusieurs objectifs[1]. Dans un premier temps, il dresse un tableau des catégories d'acteurs privés qui exercent une forte influence sur la liberté d'expression à l'ère du numérique. Dans un second temps, il définit les questions qui se posent au sujet de la protection de la liberté d'opinion et d'expression par le secteur privé et de la responsabilité des autorités publiques en matière de protection de l'espace d'expression. Enfin, il dégage plusieurs domaines dans lesquels les orientations normatives semblent le plus nécessaire. Il analysera et étudiera ces domaines dans des rapports thématiques, à l'occasion de visites de pays et de réunions avec des entreprises, ainsi que dans le cadre d'échanges et de consultations avec les autorités publiques, le secteur marchand et la société civile. En résumé, le présent rapport est le premier d'une série de rapports que le Rapporteur spécial présentera et dans lesquels il formulera des orientations sur la façon dont les acteurs privés devraient protéger et promouvoir la liberté d'expression à l'ère du numérique.

[1] Le Rapporteur spécial remercie son conseiller juridique, Amos Toh, et ses étudiants de la faculté de droit d'Irvine (Université de Californie), qui l'ont aidé à élaborer le présent rapport.

4. Le présent rapport a été élaboré notamment à partir des idées recueillies auprès du grand public lors de consultations. Le 3 décembre 2015, le Rapporteur spécial a lancé un appel à contributions pour le présent rapport. À la date de publication de ce dernier, il avait reçu 15 contributions d'États[2] et 15 contributions d'organisations[3], qui figurent toutes sur son site[4]. Les consultations qu'il a menées lui ont également été très utiles. Les 25 et 26 janvier 2016, il a rencontré 25 membres de la société civile à la faculté de droit d'Irvine (Université de Californie). Le 29 février 2016, il a rencontré 20 représentants du secteur privé et de la société civile au Haut-Commissariat aux droits de l'homme, à Genève. Le résumé de ces réunions est également consultable sur son site.

II. Liberté d'expression, États et secteur privé à l'ère du numérique

5. Le présent rapport d'inventaire repose sur une question fondamentale : dans quelle mesure le secteur des technologies de l'information et de la communication doit-il être responsable de la promotion et de la protection de la liberté d'opinion et d'expression ? Avant de répondre à cette question, il convient de dresser un bref aperçu des dispositions du droit international des droits de l'homme qui imposent aux États de promouvoir et de protéger la liberté d'expression, ainsi que des principes relatifs aux responsabilités du secteur privé en matière de droits de l'homme.

A. Cadre juridique international

6. L'article 19 du Pacte international relatif aux droits civils et politiques et l'article 19 de la Déclaration universelle des droits de l'homme protègent le fait que chacun peut exercer son droit à la liberté d'opinion sans être inquiété pour ses opinions et celui de chercher, de recevoir et de diffuser des informations et des idées de toute espèce, sans considération de frontières, par quelque moyen d'expression que ce soit. Il est devenu courant d'insister sur le fait que les individus jouissent des mêmes droits en ligne que hors ligne. Le précédent titulaire du mandat a mis en évidence le nombre croissant de formes de restrictions au droit à l'information en ligne (voir A/HRC/17/27) et démontré les conséquences de la surveillance numérique élargie sur la liberté d'expression (voir A/HRC/23/40). En 2015, le Rapporteur spécial a souligné le rôle important que le codage et l'anonymat jouaient dans la protection et la promotion de la liberté d'expression (voir A/HRC/29/32). Dans des déclarations conjointes, le Rapporteur spécial et ses homologues régionaux ont mis l'accent sur les questions relatives à la responsabilité des intermédiaires, à l'accès, aux restrictions de contenu et à d'autres sujets majeurs en matière de liberté d'expression en ligne.

[2] Arménie, El Salvador, Estonie, États-Unis d'Amérique, Grèce, Jordanie, Koweït, Maurice, Mexique, Pays-Bas, Pérou, République de Moldova, Roumanie, Slovaquie et Turquie.

[3] Article 19 ; Association pour le progrès des communications ; Center for Democracy and Technology ; Center for Technology and Society ; Centre for Communication Governance at National Law University, New Delhi ; Institut danois pour les droits de l'homme ; Derechos Digitales ; European Digital Rights ; Freedom Online Coalition Working Group on Privacy and Transparency Online ; Global Network Initiative ; Institute for Human Rights and Business ; International Centre for Not-for-Profit Law ; Internet Society ; Korean Progressive Network Jinbonet ; Privacy International ; Ranking Digital Rights ; New America.

[4] Consultable à l'adresse suivante : www.ohchr.org/FR/Issues/FreedomOpinion/Pages/Annual.aspx.

7. Le paragraphe 3 de l'article 19 du Pacte international relatif aux droits civils et politiques autorise certaines restrictions à la liberté d'expression (le paragraphe 1 de ce même article dispose en revanche que nul ne peut être inquiété pour ses opinions). Aux termes du paragraphe 3 de l'article 19 du Pacte, pour être légitimes, les restrictions imposées doivent être expressément fixées par la loi et nécessaires au respect des droits ou de la réputation d'autrui, ou à la sauvegarde de la sécurité nationale, l'ordre public, de la santé ou de la moralité publiques. Toute restriction doit être libellée avec suffisamment de précision et elle doit être accessible pour le public afin de limiter le pouvoir discrétionnaire des autorités et de conférer aux individus suffisamment d'indications (voir l'observation générale n° 34 (2011) du Comité des droits de l'homme sur l'article 19 : liberté d'opinion et liberté d'expression). Pour qu'une restriction soit nécessaire, elle doit être plus que simplement utile, raisonnable ou opportune[5]. Il est également largement établi que le critère de nécessité passe par une évaluation du critère de proportionnalité (voir A/HRC/29/32). Il y a proportionnalité s'il peut être établi que les mesures restrictives constituent le moyen le moins perturbateur parmi ceux qui pourraient permettre d'obtenir le résultat recherché et qu'elles sont proportionnées à l'intérêt à protéger (voir observation générale n° 34). Lorsque les restrictions ne répondent pas à la norme fixée au paragraphe 3 de l'article 19, les individus jouissent du droit à un recours utile consacré au paragraphe 3 de l'article 2 du Pacte.

8. Les personnes peuvent aussi exercer en ligne tout l'éventail de leurs autres droits, notamment le droit à la vie privée, le droit à la liberté de religion, le droit d'association et de réunion pacifique, le droit à l'éducation, le droit à la culture et le droit d'être protégé contre la discrimination. Les États ont pour obligation négative de s'abstenir de contrevenir aux droits et pour obligation positive d'assurer l'exercice de ces droits, ce qui peut les amener à devoir prendre des mesures pour protéger les individus contre les agissements de tiers privés[6].

B. Cadre relatif aux responsabilités du secteur privé

9. De façon générale, le droit des droits de l'homme ne régit pas directement les activités ou les responsabilités des entreprises privées. Divers textes indiquent aux entreprises comment respecter les droits fondamentaux. Le Conseil des droits de l'homme a adopté les Principes directeurs relatifs aux entreprises et aux droits de l'homme : mise en œuvre du cadre de référence « protéger, respecter et réparer » des Nations Unies (voir A/HRC/17/4 et A/HRC/17/31). Inspirés par le droit des droits de l'homme en vigueur, ces principes directeurs réaffirment que les États doivent veiller à ce que tant les organismes publics que les entreprises relevant de leur compétence respectent les droits de l'homme[7].

10. Les Principes directeurs constituent un cadre d'examen des responsabilités des entreprises privées dans le secteur des technologies de l'information et de la communication dans le monde entier, quelles que soient les obligations des États ou les modalités de leur respect. Selon l'un de ces principes, les entreprises ont pour responsabilité, à l'échelle mondiale, d'éviter d'avoir des incidences négatives sur les droits de l'homme ou d'y contribuer par leurs propres activités, et doivent remédier à ces incidences lorsqu'elles se produisent ; elles doivent aussi s'efforcer de prévenir ou

[5] Cour européenne des droits de l'homme, requête n° 6538/74, *Sunday Times* c. *Royaume-Uni* (26 avril 1979), par. 59.

[6] Voir l'observation générale n° 31 (2004) sur la nature de l'obligation générale imposée aux États parties au Pacte. D'autres normes du droit international peuvent directement s'appliquer aux activités des acteurs privés, par exemple celles concernant les crimes contre l'humanité, les crimes de guerre et les actes de génocide, en vertu du droit international humanitaire.

[7] Principes directeurs relatifs aux entreprises et aux droits de l'homme, chap. I (A) (1).

d'atténuer les incidences négatives sur les droits de l'homme qui sont directement liées à leurs activités, produits ou services par leurs relations commerciales, même si elles n'ont pas contribué à ces incidences[8].

11. Selon les Principes directeurs, la diligence raisonnable permet aux entreprises d'identifier leurs incidences sur les droits de l'homme, de prévenir ces incidences et d'en atténuer les effets, et de rendre compte de la manière dont elles y remédient[9]. Dans le contexte du numérique, les incidences sur les droits de l'homme peuvent être le résultat de décisions internes faisant suite à la demande d'autorités nationales qui souhaitent limiter l'accès à un contenu ou accéder aux informations concernant les utilisateurs, concernant l'adoption de conditions d'utilisation, les caractéristiques et les techniques choisies en matière de sécurité et de vie privée, et la fourniture ou la cessation de services sur un marché donné.

12. À des fins de transparence, les Principes directeurs précisent que les entreprises doivent être prêtes à faire connaître la façon dont elles gèrent les incidences de leurs activités sur les droits de l'homme, en particulier lorsque des préoccupations sont exprimées par les acteurs concernés ou en leur nom[10]. Le Haut-Commissaire aux droits de l'homme a instamment prié les sociétés d'information et de communication de divulguer les risques encourus et les exigences des gouvernements en toute transparence (voir A/HRC/27/37). Une telle pratique a notamment mis en lumière le volume des demandes de suppression de contenus et d'accès aux données d'utilisateurs faites par des gouvernements, le contexte dans lequel ces demandes sont faites, la façon dont elles sont traitées et l'interprétation faite des lois, politiques et réglementations applicables. Les obligations de transparence des entreprises pourraient également inclure le devoir de faire connaître les processus et les informations concernant l'application des conditions d'utilisation et les demandes privées de réglementation des contenus et d'accès aux données des utilisateurs.

13. Enfin, la responsabilité de respecter les droits de l'homme va de pair avec l'existence de recours utiles, qui vont de la réparation morale à l'indemnisation et aux garanties de non-répétition, lorsque le mode d'action d'un acteur privé a eu des incidences néfastes sur les droits de l'homme ou qu'il y a contribué[11].

14. Les Principes directeurs constituent un point de départ utile, qui peut contribuer à déterminer les responsabilités des acteurs privés dans le domaine de l'information et de la communication. Toutefois, les responsables de plusieurs autres projets ont également proposé des principes pour régir l'activité de ce secteur. Les Principes de liberté d'expression et de respect de la vie privée de l'Initiative mondiale des réseaux (*Global Network Initiative*) mettent à profit l'expérience et les compétences spécialisées des investisseurs, de la société civile et des milieux universitaires. La Commission européenne a publié le *ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights* (Guide d'application des Principes directeurs des Nations Unies relatifs aux entreprises et aux droits de l'homme à l'intention du secteur des TIC). Parmi les initiatives de la société civile en la matière figurent les Principes de Manille sur la responsabilité des intermédiaires, qui établissent une protection minimale pour les intermédiaires, conforme aux normes relatives à la liberté d'expression, la Déclaration africaine sur les droits et libertés en matière d'Internet, qui promeut les normes relatives aux droits de l'homme et le principe d'ouverture en matière de formulation et de mise en œuvre de décisions concernant Internet sur le continent, ainsi que l'Indice de responsabilité des entreprises en matière de droits numériques (*Ranking Digital Rights Corporate Accountability Index*), qui évalue

[8] Ibid., chap. II (A) (11)-(13).
[9] Ibid., chap. II (A) (17).
[10] Ibid., chap. II (B) (21).
[11] Ibid., chap. II (B) (22).

le respect de la liberté d'expression et des normes relatives à la vie privée appliquées par un ensemble de grands acteurs privés de l'espace numérique. La société civile agit également pour contrôler et équilibrer l'action d'autres acteurs de la gouvernance d'Internet : le Code des bonnes pratiques pour l'information, la participation et la transparence dans la gouvernance d'Internet, par exemple, vise à garantir que le public a réellement connaissance des processus en la matière, que toutes les parties prenantes rendent des comptes et que l'accent est mis sur la participation démocratique.

III. Rôles du secteur privé et réglementation publique/privée

A. Incidences des activités des entreprises privées sur la liberté d'expression

15. L'éventail des rôles du secteur privé dans l'organisation d'Internet, l'accès à Internet, l'insertion de contenus sur Internet et de réglementation d'Internet est vaste et inclut souvent des catégories qui se chevauchent[12].

1. Faciliter la connexion à Internet

16. Il convient d'établir une distinction entre les fournisseurs d'accès à Internet, qui relient leurs abonnés à Internet, et les fournisseurs de services de télécommunication, qui offrent un large éventail de services, dont l'accès à la radio, à la télévision, au téléphone et aux communications mobiles. Les grandes sociétés multinationales offrent ces deux catégories de services, dans leur État d'origine et dans le monde entier. Le prestataire britannique Vodafone, par exemple, possède et exploite des réseaux dans 27 pays, et a des réseaux partenaires dans une cinquantaine d'autres pays. TeliaSonera, installée en Finlande et en Suède, dessert des marchés en Europe et en Asie, et MTS Russie assure des services en Russie et des services de télécommunication en Arménie, au Turkménistan et en Ouzbékistan. Souvent, ces entreprises possèdent et entretiennent des pans importants des infrastructures techniques qui transmettent le trafic de télécommunication et le trafic sur Internet, y compris les câbles à fibre optique des réseaux, les satellites ou les liens sans fil. Il arrive que les fournisseurs d'accès Internet sur les marchés locaux et régionaux exploitent un nombre limité de ces réseaux ou qu'ils louent des capacités sur de grands réseaux afin de relier leurs abonnés à Internet. Il est relativement courant qu'un État soit propriétaire d'un fournisseur d'accès : la Suisse, par exemple, détient 51 % des parts de Swisscom AG[13] et l'Uruguay possède Antel, important fournisseur de services de télécommunication du pays[14]. S'il est vrai que les fournisseurs de services de télécommunication et les fournisseurs d'accès Internet sont actuellement les fournisseurs d'accès Internet les plus courants, un nombre croissant de sociétés hybrides fournissent un accès à Internet et d'autres services liés à Internet[15].

[12] Voir, par exemple, « Strategy panel: ICANN's role in the Internet governance ecosystem » (23 février 2014) ; R. Mackinnon et autres, *Fostering Freedom Online: The Role of Internet Intermediaries* (Paris, UNESCO, 2014) ; et D. A. Hope, *Protecting Human Rights in the Digital Age* (février 2011).

[13] Voir https://www.swisscom.ch/fr/about/investisseurs/action/structure-de-lactionnariat.html.

[14] Voir www.antel.com.uy/antel/ ; http://cs.stanford.edu/people/eroberts/cs181/projects/2006-07/latin-america/uruguayIntro.html.

[15] Google, par exemple, fournira un accès à un service sans fil grâce à son service Google Fiber, en plus de ses fonctions de recherche, d'hébergement de contenu et de réseau social, entre autres fonctions. Voir https://fiber.google.com/about/.

2. Concevoir et assurer la maintenance du matériel et des systèmes d'exploitation qui facilitent le traitement de l'information et l'accès à Internet

17. Les sociétés de matériel informatique conçoivent et fabriquent les dispositifs informatiques qui connectent les particuliers à Internet. Toutefois, l'éventail de dispositifs dotés de fonctions informatiques personnelles est en augmentation constante, augmentation qui ne peut être plafonnée compte tenu de la kyrielle d'objets connectés, généralement appelée « Internet des objets », dans lequel la connexion numérique est facilitée dans tous les aspects de la vie contemporaine. Les automobiles, les réfrigérateurs, les télévisions et les montres ne sont que quelques exemples de dispositifs « intelligents » qui incluent aujourd'hui des fonctions de navigation et de messagerie, entre autres fonctions liées à Internet.

18. Il convient aussi d'ajouter que les fournisseurs de services de télécommunication et les fournisseurs d'accès Internet achètent le matériel et les autres composants de réseau qui constituent l'ossature physique de leurs réseaux auprès de vendeurs d'infrastructures et de fabricants de matériel. Ces produits vont des simples routeurs et commutateurs aux dispositifs d'inspection approfondie des paquets, aux dispositifs de filtrage des réseaux et de blocage d'Internet et aux centres de contrôle et de surveillance. De plus en plus, ces sociétés proposent des services, des conseils d'entreprise, des formations et même des prestations opérationnelles.

3. Attribution des noms de domaine

19. Les adresses Internet (c'est-à-dire les adresses universelles (URL)) sont attribuées et vendues par les registres et registraires de noms de domaine, sous la supervision d'Internet Corporation for Assigned Names and Numbers (ICANN), entité à but non lucratif. Aujourd'hui, le plus grand bureau d'enregistrement du monde héberge plus de 61 millions de noms de domaine.

4. Informations concernant l'hébergement Web

20. Les services d'hébergement sur le Web permettent à leurs utilisateurs de télécharger et de remettre des dossiers et d'autres éléments dans leurs navigateurs à l'intention de leurs propres lecteurs ou clients. Ces sociétés fournissent généralement des services de stockage de données, de messagerie électronique et autres associés aux sites que leurs clients ont achetés.

5. Faciliter l'agrégation, le partage et la recherche d'informations

21. Les moteurs de recherche constituent le lien vital entre les utilisateurs qui recherchent des informations et ceux qui les créent, les agrègent et les publient. En effet, les algorithmes des moteurs de recherche déterminent ce que les utilisateurs voient et dans quel ordre, et peuvent être manipulés de manière à restreindre ou hiérarchiser les contenus. Cependant, les moteurs de recherche n'ont pas l'exclusivité de la recherche d'informations. Les agrégateurs de contenu, les services de recherche spécialisés, les plateformes de médias sociaux et les réseaux professionnels permettent également à leurs utilisateurs de rechercher des contenus.

6. Produire ses propres contenus et en régler l'accès

22. Les entreprises qui créent ou achètent des contenus produits sur leurs plateformes détiennent souvent le droit d'auteur sur ces contenus, ce qui leur permet d'en gérer l'accès et de le monnayer. Certains des détenteurs de droits d'auteur les plus influents sont des médias et des entreprises de divertissement, y compris des organes de presse, des maisons d'édition, des éditeurs de musique, ou encore des studios de cinéma et de télévision.

7. Mettre en contact les utilisateurs et les groupes

23. Les entreprises offrent également une gamme de services qui connectent les utilisateurs au moyen de multiples plateformes, notamment consacrées au courrier électronique, aux dialogues en ligne, aux fils de discussion et au réseautage social et professionnel. Les acteurs les plus importants dans ce domaine sont les fournisseurs de courrier électronique, les médias sociaux et autres plateformes de réseautage, et les tableaux d'affichage en ligne. En outre, les sites d'actualité, les plateformes de commerce électronique et les boutiques d'applications offrent la possibilité de partager des informations et des idées en y affichant des critiques, des commentaires et des discussions. Les systèmes de paiement par Internet intègrent également une fonctionnalité de réseau social.

8. Vendre des marchandises et des services, et faciliter les transactions

24. Le commerce en ligne facilite la vente de biens et services et d'autres transactions commerciales entre entreprises et consommateurs ainsi qu'entre entreprises ou entre consommateurs. La façon dont les entreprises permettent, promeuvent ou organisent ces transactions et dont elles engrangent les grandes quantités de renseignements personnels générés par ces transactions peut avoir des répercussions sur la liberté d'expression et le droit à la vie privée de leurs clients.

9. Recueillir, réutiliser et vendre des données

25. La grande majorité des entreprises énumérées ci-dessus recueillent des informations sur leurs utilisateurs, qui peuvent ensuite être utilisées pour cibler la publicité, personnaliser les services existants, réduire les risques relatifs à la sécurité ou clore les comptes d'utilisateurs abusifs. Des entreprises peuvent cependant aussi s'occuper de la collecte et de l'analyse des informations, et fournir des services tels que la conception, la personnalisation ou la vente de technologies de surveillance et d'analyse de l'information, ou fournir des services de consultation qui facilitent les opérations de maintien de l'ordre, de renseignement, de cybersécurité et de surveillance.

B. La réglementation à l'ère du numérique

26. L'écosystème réglementaire sur Internet est vaste et diversifié, et fait intervenir des acteurs aux niveaux national, régional et international, dans les secteurs public et privé, les milieux universitaires et la société civile. Certains aspects des TIC, telle la fourniture de services de télécommunications et de services en ligne, ont longtemps mobilisé l'activité réglementaire à l'échelle des États et à l'échelle internationale, ainsi que l'attention du public. D'autres domaines, tels que la recherche, les médias sociaux et la vente de technologies de surveillance, font désormais l'objet d'une attention croissante, en rapport avec leur incidence et leur influence croissantes sur l'exercice de la liberté d'expression en ligne.

1. Normes techniques

27. Les normes et processus techniques favorisent le fonctionnement transparent des infrastructures, des réseaux et des applications qui constituent Internet et les réseaux de télécommunications. L'infrastructure physique sur laquelle circule le trafic Internet, comme les câbles et satellites des réseaux, est mise en place et gérée selon diverses prescriptions techniques qui garantissent son bon fonctionnement. Parmi les organisations qui élaborent ces prescriptions, on peut citer l'Union internationale des télécommunications, qui établit des normes pour l'interopérabilité des réseaux de télécommunication ; l'Institute of Electrical and Electronic Engineers, association professionnelle qui élabore des normes pour la transmission par wi-fi ; et la Groupe Speciale Mobile Association, association

internationale privée de l'industrie de la téléphonie mobile qui élabore des normes pour les réseaux de téléphonie mobile.

28. Un autre groupe d'organismes élabore et développe des normes techniques relatives à la façon dont les données sur Internet sont communiquées, stockées, disposées et présentées. Le Groupe de travail d'ingénierie Internet élabore et maintient le protocole de vérification de transmission/protocole Internet (TCP/IP), qui détermine la façon dont les périphériques se connectent à Internet et la façon dont les données sont transmises entre eux. Le World Wide Web Consortium établit des normes relatives à l'affichage des contenus en ligne et à l'interaction avec eux, et s'occupe notamment de représenter les contenus dans diverses langues ou encore d'assurer l'accès aux personnes handicapées. La Société pour l'attribution des noms de domaine et des numéros sur Internet (ICANN) établit les politiques relatives à l'enregistrement des noms de domaine de niveau supérieur, qu'ils soient génériques (par exemple .com, .org, .edu), particuliers à un pays (.cn, .tj, .sg) ou particuliers à une communauté ou une industrie (.aero). Sa filiale, l'Autorité d'attribution des numéros sur Internet (IANA), gère la distribution des adresses de protocole Internet, qui assignent à chaque dispositif qui se connecte à Internet une étiquette numérique particulière qui permet de l'identifier.

29. Les normes techniques ont des incidences importantes sur la liberté d'expression et, pourtant, la Commission de la science et de la technique au service du développement de l'ONU a constaté que le souci du respect des droits de l'homme était rarement pris en compte lors de leur élaboration[16]. À vrai dire, les acteurs intéressés et les membres du public sont autorisés à observer les travaux de la plupart de ces organismes de normalisation ou à y participer. Cependant, ils ne le font guère parce qu'une telle démarche requiert un niveau généralement élevé de compétence technique ; c'est ainsi que la perspective des droits de l'homme n'est pas toujours intégrée dans les discussions, même lorsque les choix et la conception techniques peuvent avoir une incidence considérable sur la liberté d'expression[17].

2. Administration d'Internet et élaboration des politiques

30. Les instruments juridiques internationaux ne traitent pas explicitement de la manière dont les États et les autres acteurs doivent préserver le caractère libre et ouvert d'Internet, et la réglementation par la voie législative n'est pas toujours la méthode appropriée. En effet, l'administration d'Internet n'est pas du ressort exclusif d'organes spécialisés ou des États. Tout récemment, le Sommet mondial sur la société de l'information a souligné qu'il convenait d'adopter une méthode de gestion d'Internet qui intègre les États, la société civile et les entreprises ainsi que les universitaires, les techniciens et les autres parties concernées (voir la résolution 70/125 de l'Assemblée générale). Dans le cadre du commerce mondial,

[16] Voir Groupe intersessions de la Commission de la science et de la technique au service du développement, « The mapping of international Internet public policy issues » (novembre 2014), téléchargeable à l'adresse électronique suivante : http://unctad.org/meetings/en/SessionalDocuments/CSTD_2014_Mapping_Internet_en.pdf.

[17] Un petit nombre d'organisations se sont néanmoins employés à intégrer une démarche soucieuse des droits de l'homme aux débats techniques. L'ICANN, par exemple, a mis en place un Groupe de travail intercommunautaire sur sa responsabilité de respecter les droits de l'homme. Ce groupe a pour objectif de déterminer et comprendre les enjeux et les solutions possibles, s'agissant de la responsabilité sociale et entrepreneuriale de l'ICANN (voir à l'adresse électronique suivante : https://community.icann.org/display/gnsononcomstake/CCWP+on+ICANN's+Corporate+and+Social+Responsibility+to+Respect+Human+Rights). Quelques organisations non gouvernementales ont également produit des contributions axées sur les droits de l'homme dans des débats techniques. Voir par exemple Neils ten Oever, « Research into human rights protocol considerations », téléchargeable à l'adresse électronique suivante : https://datatracker.ietf.org/doc/draft-tenoever-hrpc-research/.

les principes de non-discrimination établis en vertu des accords internationaux administrés par l'Organisation mondiale du commerce peuvent exiger que les États restreignent ou réglementent des services non neutres. L'Organisation mondiale de la propriété intellectuelle a également vu croître le nombre d'États membres qui demandent des conseils sur les cadres législatifs à mettre en place pour respecter leurs obligations conventionnelles dans l'univers numérique. Des organismes régionaux tels que l'Union africaine, la Commission européenne et l'Organisation des États américains veulent que la politique d'Internet soit formulée et mise en œuvre au niveau mondial d'une manière qui prenne en compte les lois, particularités et préoccupations propres à leurs régions respectives[18].

31. Certaines organisations qui établissent les normes techniques jouent, elles aussi, un rôle dans l'élaboration des politiques. L'Union internationale des télécommunications, par exemple, élabore et coordonne les politiques mondiales en matière de télécommunications. L'ICANN prend, en concertation avec les États, le secteur privé, la société civile et les autres acteurs concernés, des décisions d'ordre stratégique sur les types de noms de domaine de niveau supérieur qu'il est possible d'enregistrer et sur ceux qui peuvent en revendiquer la propriété.

32. Divers secteurs de l'économie prennent aussi des initiatives pour relever des questions relatives à la gestion d'Internet qui ne sont pas suffisamment prises en compte dans la réglementation juridique existante. Le Copyright Alert System, par exemple, rassemble des associations professionnelles des secteurs du cinéma et du disque, et des fournisseurs de services Internet, et vise à élaborer et à mettre en œuvre une stratégie unifiée de lutte contre les violations du droit d'auteur en ligne. Le Telecommunications Industry Dialogue regroupe des opérateurs et des fournisseurs du secteur des télécommunications qui souhaitent traiter des préoccupations concernant la liberté d'expression et le droit à la vie privée qui se font jour dans leur secteur.

33. Bon nombre de ces initiatives sont privées, mais leurs membres collaborent parfois avec des États ou reçoivent leur soutien. Par exemple, l'Internet Watch Foundation (Royaume-Uni) offre aux fournisseurs de services Internet et aux plateformes d'hébergement un service de « notification et retrait » qui les alerte sur les contenus qui pourraient être illégaux circulant sur leurs réseaux, et fournit également aux organes chargés du maintien de l'ordre des « données exclusives » dans le cadre de leurs enquêtes sur ce type de contenu.

IV. Questions juridiques et politiques

34. La multiplicité des rôles du secteur des technologies de l'information et de la communication soulève des questions juridiques et politiques qui méritent que les mécanismes internationaux des droits de l'homme leur accordent attention et réflexion.

A. Réglementation des contenus

35. De nombreuses questions concernant les acteurs privés de l'ère du numérique portent sur la réglementation des contenus, par exemple sur la manière dont les États facilitent ou exigent la suppression de contenus, sur la censure et les restrictions inutiles ou disproportionnées imposées au droit de rechercher, de recevoir et de diffuser des contenus sur Internet par l'intermédiaire de plateformes et de réseaux privés. Comment les

[18] Voir, par exemple, Commission européenne, *ICT Sector Guide* (par. 14 ci-dessus) et Cour interaméricaine des droits de l'homme, Bureau du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, *Freedom of Expression and the Internet* (2013).

entreprises privées réagissent-elles à ces exigences et à d'autres pressions extérieures ? Lorsque le secteur privé se développe et applique ses propres politiques et normes internes en vue de protéger et promouvoir les droits en ligne, quelles incidences ont celles-ci sur l'expression individuelle et l'accès à l'information ?

36. Les contenus numériques transmis sur des réseaux privés et hébergés sur des plateformes également privées sont de plus en plus fréquemment soumis à des réglementations prises par l'État ainsi que par les entreprises. L'univers des contenus créés par les utilisateurs ne cesse de s'étendre − blogs, SMS, fils de discussion, photographies, vidéos et messages affichés sur les médias sociaux ne sont qu'un échantillon des types de contenus que les utilisateurs créent et échangent chaque jour. Les entreprises qui gèrent les réseaux et les plateformes adaptés à ces contenus, connues sous le nom d'intermédiaires, peuvent « donner accès aux contenus, produits et services créés par des tiers, les héberger, les transmettre et les indexer », même si elles n'ont ni créé ni produit ces contenus[19].

37. Les exigences des États visant à ce que des contenus soient retirés reposent souvent sur des motifs tels que la diffamation, le blasphème, la réglementation électorale, le harcèlement, le discours de haine, l'incitation à commettre des actes illicites, la propriété intellectuelle, l'obscénité et l'indécence, le recrutement de terroristes, l'apologie du terrorisme, la protection de la sécurité nationale et de la sécurité publique, la protection des mineurs et la prévention des agressions sexistes. Des questions longtemps liées à la liberté d'expression mais devenues de plus en plus complexes à l'ère du numérique ont également fait l'objet de l'activité réglementaire de l'État, notamment celles du droit à l'oubli, du pluralisme et de la diversité (y compris la neutralité du réseau). Les entreprises jouant le rôle d'intermédiaires, elles aussi, établissent et font respecter des conditions d'utilisation conçues de manière à répondre à bon nombre de ces préoccupations, pour des raisons d'ordre juridique, commercial et autre. Beaucoup de ces questions posent à leur tour des problèmes ayant trait à l'équilibre entre la liberté d'expression et d'autres droits de l'homme (par exemple le droit à la vie privée ou l'interdiction de la discrimination). Les règlements relatifs aux contenus sont souvent de nature restrictive, mais peuvent également exiger la transmission de messages mandatés ou approuvés par les autorités[20], ou interdire l'application de prix différenciés pour les contenus et les services de diffusion de contenus[21].

1. Réglementation par l'État

38. Les États réglementent les contenus numériques par divers moyens juridiques, politiques et techniques. Les principaux sujets de préoccupation sont énumérés ci-après.

Caractère trop vague de la législation

39. Les réglementations ayant trait aux contenus sont généralement exposées dans des lois, des ordonnances judiciaires, des directives ou des arrêtés émanant d'organes administratifs habilités à gérer les questions relatives aux télécommunications et à Internet. Par exemple, la Chine a récemment modifié sa loi sur la cybersécurité de manière à interdire aux personnes physiques et morales d'utiliser Internet pour « renverser l'ordre social » ou « nuire à l'intérêt général »[22]. De même, un projet de loi à l'étude au Nigéria

[19] R. MacKinnon et al., *Fostering Freedom Online*, p. 19 ; K. Perset, *The Economic and Social Role of Internet Intermediaries* (OCDE, 2010).

[20] Voir Vodafone Group PLC, « Response on issues relating to mobile network operations in Egypt » (2011).

[21] L'Inde, par exemple, interdit aux fournisseurs de services d'offrir ou de pratiquer des tarifs discriminatoires pour les services de données en fonction des contenus (Prohibition of Discriminatory Tariffs for Data Services Regulations, 2016).

[22] Chine, loi relative à la cybersécurité (2015), art. 9.

interdit à quiconque de publier des contenus, dans « tout média », avec « l'intention malveillante de susciter dans le public discrédit ou opposition à l'encontre de » toute personne, groupe ou institution publique[23]. Pareille formulation donne aux autorités un large pouvoir discrétionnaire pour déterminer les modes d'expression constitutifs d'infraction dans l'univers numérique. Il peut en découler que les particuliers et les entreprises, afin d'éviter de lourdes sanctions, soient tentés de faire preuve d'un excès de prudence en filtrant les contenus au statut juridique incertain et en se livrant à d'autres formes de censure et d'autocensure.

Responsabilité excessive des intermédiaires

40. Les États exigent souvent des intermédiaires qu'ils coopèrent pour faire respecter les règlements sur les réseaux et plateformes privés. Les fournisseurs de services Internet et de télécommunications, par exemple, sont tenus de se conformer aux lois et réglementations locales aux termes des conditions d'octroi de leurs licences d'exploitation. Il s'agit là d'une exigence légitime, mais elle devient problématique lorsque les lois locales ou leur mise en œuvre sont elles-mêmes incompatibles avec le droit des droits de l'homme. Les entreprises moins étroitement tributaires de cette exigence, notamment les plateformes de réseaux sociaux, les moteurs de recherche et les bureaux d'enregistrement de noms de domaine, sont néanmoins soumis au risque que les États perturbent leur infrastructure locale, menacent la sécurité de leurs employés locaux ou bloquent localement l'accès à leurs plateformes.

41. Les acteurs privés peuvent eux aussi demander aux intermédiaires de restreindre la diffusion de contenus ou d'en supprimer d'autres. Par exemple, de fréquentes plaintes relatives à des violations de la propriété intellectuelle reposent sur les allégations d'une partie privée, selon lesquelles un individu aurait partagé ou utilisé un contenu en violation de son droit d'auteur, ou aurait créé un nom de domaine en violation de sa marque déposée. Il est possible d'invoquer le droit à l'usage loyal et d'autres moyens de défense contre ces plaintes, mais il n'en reste pas moins que les cadres de la propriété intellectuelle peuvent inhiber l'expression culturelle et artistique (voir A/HRC/28/57).

42. Dans l'affaire *Google Spain* c. *Mario Costeja González*, la Cour de justice européenne, a contraint Google, en vertu de la Directive de l'Union européenne sur la protection des données, à retirer de la liste des résultats de recherche fondés sur des pages Web qui identifiaient González, même si la publication originale de ces pages n'était elle-même pas soumise au retrait[24]. Cette décision a fait tache d'huile bien au-delà du cadre européen[25]. La portée et la mise en œuvre de cette méthode soulèvent des questions sur l'équilibre approprié entre le droit à la vie privée et à la protection des données personnelles, d'une part, et le droit de rechercher, de recevoir et de diffuser des informations contenant ces données d'autre part.

43. On demande de plus en plus souvent aux intermédiaires d'évaluer la validité des demandes de l'État et des plaintes privées en fonction de critères juridiques généraux, et de supprimer tel ou tel contenu ou les liens qui y conduisent en fonction de ces évaluations. Par exemple, la loi de 2015 sur la cybercriminalité de la République-Unie de Tanzanie n'exonère les fournisseurs de liens hypertextes de leur responsabilité concernant des informations accessibles à partir de tels liens qu'à condition qu'ils « retirent l'information ou désactivent l'accès à celle-ci dès qu'ils en reçoivent l'ordre de l'autorité compétente »[26].

[23] Parlement du Nigéria, projet de loi visant à interdire les pétitions frivoles et autres questions s'y rapportant, sect. 3 3).

[24] Arrêt de la Cour européenne de justice (Grande Chambre), affaire C-131/12 (13 mai 2014).

[25] Voir la contribution d'Article 19.

[26] Par. 43 a).

Dans le contexte du droit d'auteur, le Digital Millennium Copyright Act des États-Unis d'Amérique n'exonère les fournisseurs « de services en ligne et d'accès au réseau » de toute responsabilité à l'égard des contenus de tiers que s'ils réagissent « dans les meilleurs délais pour supprimer tout contenu ou désactiver l'accès à tout contenu qui constituerait une infraction ou en serait l'objet » lorsqu'ils sont notifiés d'une telle infraction[27]. Il a été reproché à ces cadres de notification et de retrait d'encourager les réclamations douteuses et de ne pas assurer une protection adéquate aux intermédiaires qui cherchent à appliquer des normes loyales et soucieuses des droits de l'homme à la réglementation des contenus.

44. Un autre sujet important de préoccupation est que les intermédiaires privés sont en général peu qualifiés pour déterminer quels contenus sont illégaux. La Commission interaméricaine des droits de l'homme a fait observer que les acteurs privés « n'ont pas la capacité d'évaluer les droits et d'interpréter la loi en tenant dûment compte de la liberté d'expression et d'autres normes relatives aux droits de l'homme »[28]. Cela peut tenir à un manque de ressources, de supervision ou de responsabilisation, ou encore à d'éventuels conflits d'intérêts. Face au risque d'une éventuelle responsabilité, les entreprises peuvent être enclines à s'autocensurer et à censurer les contenus.

Restrictions extralégales

45. Les États cherchent également à limiter les contenus numériques en dehors du cadre de la loi. Certains États ont tenté de pousser les entreprises de médias sociaux et d'autres hébergeurs de contenus à surveiller et à retirer de leur propre initiative des contenus créés par les utilisateurs plutôt que d'attendre que les pouvoirs publics leur transmette des demandes juridiquement fondées. Des représentants des pouvoirs publics ont également tenté de convaincre les entreprises d'adopter des initiatives du type du « contre-discours », par l'intermédiaire de forums, de campagnes et de discussions privées. Les gouvernements signalent aussi de plus en plus souvent que des contenus figurant sur des médias sociaux ne respectent pas les termes des conditions d'utilisation de la plateforme concernée, afin d'inciter celle-ci à les supprimer ou à désactiver le compte ayant servi à les mettre en ligne.

Filtrage

46. Il est fréquent que les États bloquent ou filtrent les contenus, avec l'aide du secteur privé. Les fournisseurs d'accès à Internet peuvent bloquer l'accès à des mots de passe, à des pages Web ou à des sites Web entiers. La technique de filtrage utilisée dépend de la nature du contenu et de la plateforme qui l'héberge. Dans certains cas, les bureaux d'enregistrement refusent d'enregistrer les noms de domaine qui figurent sur une liste noire établie par les autorités ; des entreprises du secteur des médias sociaux retirent des informations que les utilisateurs ont placées, ou bloquent des comptes ; dans d'autres cas encore, les moteurs de recherche écartent les résultats qui orientent vers des contenus illégaux. La question de la nécessité et de la proportionnalité de la méthode de restriction imposée par les États ou utilisée par les entreprises peut se poser, en fonction de la valeur des motifs invoqués pour le retrait des informations et du risque de retrait d'expressions légales ou protégées.

47. Les ambiguïtés de la réglementation étatique et les obligations onéreuses liées à la responsabilité des intermédiaires risquent d'entraîner un filtrage excessif. Même si la réglementation sur le contenu était adoptée et dûment appliquée, les utilisateurs pourraient tout de même faire face à des restrictions d'accès inutiles. Par exemple, le filtrage fait dans un État peut avoir des effets sur l'expression numérique des utilisateurs d'autres États. Si les sociétés peuvent configurer des filtres qui ne s'appliquent qu'à un État ou à une région

[27] Code des États-Unis, titre 17, sect. 512 c) 1) C).

[28] Cour interaméricaine des droits de l'homme, *Freedom of Expression and the Internet*, p. 47 et 48.

donnée, il est arrivé que ces filtres se propagent sur d'autres réseaux ou dans d'autres espaces de la plateforme. Par exemple, en 2013, un filtrage demandé par l'État indien et exécuté par Airtel India a abouti à des restrictions portant sur le même contenu sur plusieurs réseaux appartenant au partenaire d'Airtel India, Omantel, à Oman[29].

Fermeture de réseaux ou de services

48. La fermeture de services et les restrictions qui en découlent sont un moyen particulièrement pernicieux de faire respecter la réglementation relative au contenu. De telles mesures sont fréquemment justifiées par la sécurité nationale, le maintien de l'ordre public ou la prévention des troubles à l'ordre public. En 2015, en collaboration avec des représentants de l'Organisation pour la sécurité et la coopération en Europe, de l'Organisation des États américains et de la Commission africaine des droits de l'homme et des peuples, le Rapporteur spécial a jugé illicites les « coupe-circuits » (« kill switches ») de trafic Internet[30]. En une seule année, des fermetures ont été signalées au Bangladesh, au Brésil, au Burundi, en République démocratique du Congo, en Inde et au Pakistan[31]. Le Rapporteur spécial a confirmé, lors de sa visite officielle au Tadjikistan en mars 2016, qu'il avait constaté des cas de fermeture de services de télécommunications et de fournisseurs d'accès[32].

Réseaux non neutres

49. Les États ne doivent pas seulement s'abstenir de toute restriction d'accès aux données numériques inutile ou disproportionnée ; ils sont également tenus de protéger le caractère libre et ouvert d'Internet. Le principe de neutralité des réseaux exige que toutes les données, tout le contenu et tous les services figurant sur Internet soient traités avec égalité, sans discrimination indue. Cependant, les fournisseurs d'accès à Internet peuvent recourir à des technologies qui accélèrent ou favorisent l'accès à certains contenus et services, tout en ralentissant l'accès à d'autres contenus ou services, pratique qualifiée d'« étranglement » (« throttling »). La collaboration croissante entre les fournisseurs d'accès à Internet et les plateformes d'hébergement de contenus, qui offrent des données gratuites sans fil pour accéder à du contenu en ligne ou à des services fournis par ces dernières (pratique connue sous le nom de « zero rated services »), a suscité la controverse. Si de telles mesures dérogent au principe de la neutralité de la toile, la question de savoir si elles sont acceptables dans les zones où l'accès à Internet est réellement défaillant fait toujours débat.

50. La réglementation des États est dans ce domaine inégale et incertaine. Quelques États ont reconnu que la neutralité des réseaux était importante, d'une manière générale. La Roumanie, par exemple, a déclaré qu'elle était « favorable à toutes les initiatives permettant de garantir que les informations en ligne puissent être véritablement consultées par la population tout entière »[33]. D'autres États, moins nombreux encore, ont prévu une protection juridique particulière[34]. Au début de 2016, l'autorité indienne de réglementation des télécommunications a établi une règle portant interdiction, pour les fournisseurs d'accès, de proposer ou de facturer « des tarifs discriminatoires pour des services de

[29] Citizen Lab, « Routing gone wild: documenting upstream filtering in Oman via India » (2012).
[30] Déclaration conjointe sur la liberté d'expression et les réponses aux situations de conflit (2015).
[31] Contribution de l'Institute for Human Rights and Business, p. 3.
[32] Observations liminaires du Rapporteur spécial des Nations Unies sur la promotion et la protection du droit à la liberté d'opinion et d'expression, M. David Kaye, à l'issue de sa visite au Tadjikistan (9 mars 2016).
[33] Contribution du Gouvernement roumain.
[34] R. Mackinnon and others, *Fostering Freedom Online*, p. 80.

données proposés ou facturés aux consommateurs, en fonction de leur contenu »[35]. Certains pays, dont le Brésil, Chili, les États-Unis et les Pays-Bas ont adopté une certaine forme de neutralité du réseau, dans la loi ou dans des politiques menées.

2. Politiques et pratiques internes

51. Les politiques menées concernant les intermédiaires et la réglementation de leur activité peuvent avoir un effet considérable sur la liberté d'expression. Si les conditions d'utilisation constituent la source principale de réglementation, les choix en matière de conception et d'ingénierie peuvent également avoir un effet sur la livraison du contenu.

Conditions d'utilisation

52. Les conditions d'utilisation, que les particuliers doivent en général accepter pour pouvoir accéder à une plateforme, contiennent souvent des restrictions sur le partage des contenus. Ces restrictions varient en fonction des lois et réglementations locales et contiennent des interdictions récurrentes, parmi lesquelles celles relatives au harcèlement, aux discours de haine, à l'incitation aux activités délictueuses, à la violence gratuite et aux menaces directes[36]. Les conditions d'utilisation sont souvent formulées d'une manière tellement générale qu'il peut être difficile de savoir à l'avance avec une certitude raisonnable quel contenu peut faire l'objet d'une restriction. L'application incohérente des conditions d'utilisation suscite aussi des commentaires des usagers. Pour certains, les plateformes les plus populaires à l'échelle mondiale ne répondent pas comme il se doit aux besoins et aux intérêts des groupes vulnérables ; d'aucuns ont par exemple accusé des plateformes de se montrer réticentes « à s'attaquer directement à la violence à l'égard des femmes véhiculée au moyen des technologies de l'information, tant que cette violence ne devient pas un problème de relations publiques »[37]. Ces plateformes ont aussi fait l'objet de critiques visant la censure excessivement zélée qu'elles exercent sur une vaste gamme d'expressions légitimes mais « gênantes » (peut-être pour certains publics)[38]. Ces préoccupations sont renforcées par l'absence de mécanismes de recours et par le fait que les plateformes communiquent piètrement sur les raisons qui les amènent à supprimer un contenu ou à désactiver un compte. Dans les sociétés fermées, les conditions d'utilisation qui exigent l'enregistrement sous le vrai nom d'un particulier ou des preuves de la validité d'un pseudonyme peuvent également dissuader très fortement les groupes vulnérables ou les acteurs de la société civile d'avoir recours à des plateformes en ligne pour s'exprimer, exercer leur droit à la liberté d'association ou mener leurs activités militantes.

53. Les États utilisent de plus en plus fréquemment les conditions d'utilisation pour retirer les contenus qu'ils jugent douteux. Le Rapporteur spécial sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste a constaté que plusieurs États avaient créé des mécanismes qui visaient souvent le retrait de contenus qui étaient licites mais qui pouvaient être considérés comme extrémistes (voir A/HRC/31/65). Le service chargé de la lutte contre l'utilisation d'Internet à des fins terroristes du Royaume-Uni, par exemple, se consacre à retirer les contenus en ligne de « nature extrémiste, violente ou terroriste », notamment en recourant à « des mécanismes de signalement des contenus des sites Web, qui lui permettent de déterminer que tel ou tel contenu constitue une violation des [conditions d'utilisation] du site »[39]. De telles pratiques

[35] Prohibition of Discriminatory Tariffs for Data Services Regulations, 2016.

[36] Voir, par exemple, modalités d'utilisation de Facebook, art. 3 7) ; modalités d'utilisation de Twitter ; Règlement de la communauté YouTube et Reddit.

[37] Voir https://ourinternet-files.s3.amazonaws.com/publications/no24_web_2.pdf.

[38] Voir onlinecensorship.org.

[39] Conseil des chefs de la police nationale, service chargé de la lutte contre l'utilisation d'Internet à des fins terroristes ; observations du Center for Technology and Democracy.

peuvent laisser penser que les États pourraient s'appuyer sur les conditions d'utilisation du secteur privé pour contourner les droits de l'homme ou les lois nationales relatives aux restrictions de contenu.

54. La censure exercée par le secteur privé est compliquée par l'immense volume de réclamations et de contenus signalés que les intermédiaires identifient quotidiennement. Certaines grandes plateformes externalisent la modération des contenus, ce qui accroît encore la distance entre les modérateurs de contenus et les décideurs en interne, et exacerbe les incohérences dans l'application des décisions. Les intermédiaires qui opèrent sur des marchés divers font inévitablement face à des « jugements de valeur complexes », à des problèmes dus à la diversité des sensibilités culturelles et à la « difficulté de trancher face aux conflits de lois »[40].

Choix de conception et d'ingénierie

55. La manière dont les intermédiaires préservent, catégorisent et classent le contenu a une incidence sur les informations auxquelles les utilisateurs ont accès − et sur celles qu'ils consultent − sur leurs plateformes. Par exemple, les plateformes utilisent la méthode des prédictions algorithmiques des préférences de l'utilisateur pour orienter les annonces publicitaires que les particuliers peuvent voir, la manière de présenter les données que ceux-ci affichent sur les médias sociaux et l'ordre dans lequel les résultats de recherche apparaissent[41]. D'autres mesures d'autorégulation, comme les initiatives de « contre-discours » (« counter speech ») destinées à soutenir les messages de lutte contre le terrorisme ou le harcèlement[42], ont également une incidence sur la façon dont les utilisateurs peuvent consommer et traiter des contenus Internet concernant des sujets sensibles. La question de savoir comment concilier les préoccupations concernant la liberté d'expression, suscitées par les choix de conception et d'ingénierie, et la liberté des entités privées de concevoir et de personnaliser leurs plateformes demeure d'actualité.

B. Surveillance et sécurité numérique

56. La surveillance par l'État et la collecte ou la rétention de données par les entreprises soulèvent des questions importantes au regard de la liberté d'expression. Par exemple, quelles sont les activités de surveillance que mènent les États en coopération avec le secteur privé, et quel est l'effet de cette coopération sur la liberté d'expression ? Quelles sont les responsabilités des acteurs privés quand ils découvrent que les États accèdent secrètement aux données Internet et aux données de télécommunication transmises ou stockées sur leurs réseaux ou plateformes ? Quelles sont les responsabilités du secteur privé dans la protection de la sécurité et de l'anonymat en ligne ?

57. Les communications et données numériques transmises ou stockées sur des réseaux et plateformes privés sont de plus en plus souvent soumises à une surveillance et à d'autres formes d'ingérence de l'État ou d'acteurs privés. Lorsqu'elle inutile et excessive, la surveillance porte atteinte à la sécurité en ligne et à l'accès à l'information et aux idées (voir A/HRC/23/40). Elle peut avoir un effet paralysant sur l'expression en ligne des citoyens ordinaires, qui risquent de s'autocensurer par peur d'être constamment observés. La surveillance a un effet disproportionné sur la liberté d'expression de nombreux groupes vulnérables, parmi lesquels les minorités raciales, religieuses, ethniques, sexuelles et de

[40] Emily Taylor, *The Privatization of Human Rights: Illusions of Consent, Automation and Neutrality*, GCIG Paper n° 24 (2016).

[41] Observations du Center for Technology and Society ; Ranking Digital Rights.

[42] Voir par exemple, Home Affairs Committee, témoignage oral d'Anthony House, Google Europe, Moyen Orient et Afrique (2 février 2016).

genre, les membres de certains partis politiques, la société civile, les défenseurs des droits de l'homme, des professionnels comme les journalistes, les avocats et les syndicalistes, les victimes de violence et de mauvais traitements, ainsi que les enfants (voir A/HRC/29/32). La capacité de surveillance de l'État peut dépendre de la mesure dans laquelle les entreprises coopèrent ou résistent.

1. Demandes de données relatives aux clients

58. Les quantités de données relatives aux clients que transmettent ou accumulent les fournisseurs de services Internet, les plateformes de réseaux sociaux, les moteurs de recherche, les fournisseurs de services cloud et autres sociétés sont certes énormes, mais le volume des demandes d'informations concernant les utilisateurs présentée par l'État, qui se fonde sur la législation nationale − a également commencé à augmenter. Plusieurs grandes sociétés du Web ont fait état d'une augmentation de ces demandes[43], qui émanent pour une grande part de la force publique et des services de renseignement. La surveillance par l'État de ces demandes varie ; elle peut être inexistante, mais elle peut aussi se traduire par l'exigence de l'autorisation judiciaire préalable[44] ou même l'aval du pouvoir exécutif à un niveau élevé[45]. Les accords de licence et la loi peuvent limiter la capacité du secteur privé de résister à de telles demandes ou imposer la responsabilité. Même les plateformes d'hébergement de contenu qui n'ont pas de présence physique dans certains États où elles fonctionnent peuvent se heurter à un blocage total de leurs services et à des tentatives d'intimidation des employés de leurs filiales. Cela dit, les sociétés de l'ensemble du secteur des technologies de l'information et des communications sont capables de créer et d'exercer une pression, à des degrés qui varient, dans leurs relations avec les États, si elles souhaitent résister ou réduire le préjudice causé par une application abusive de la loi. Parmi les stratégies efficaces de résistance, on peut citer : l'ajout de garanties concernant les droits de l'homme dans les accords de licence et autres contrats pertinents, l'interprétation restrictive des demandes formées par les États, les négociations avec les représentants de l'État sur la portée de telles demandes, la mise en cause, au niveau judiciaire, de demandes ou de lois d'une portée excessivement large, la fourniture d'informations pertinentes aux individus, aux médias ou au public touchés et, enfin, la suspension du service sur un marché donné ou la décision de ne pas entrer sur le marché ou de s'en retirer.

2. Vente d'équipements de surveillance et de censure

59. Le secteur privé fournit du matériel informatique, des logiciels et d'autres technologies permettant aux États d'intercepter, de stocker ou d'analyser des communications ou d'autres informations. Les fournisseurs d'infrastructures, les fabricants de matériel informatique et les développeurs de logiciels peuvent concevoir ou personnaliser des produits au nom des États, ou fournir des équipements et des technologies à double usage que les États peuvent ensuite adapter à leurs propres besoins. Les fournisseurs d'accès à Internet et de télécommunications peuvent également acheter à ces sociétés des équipements ou des logiciels à installer sur leurs composants réseau afin de respecter les protocoles d'interception légalement autorisés dans les États où ils opèrent. Les États peuvent recourir à de tels produits et services pour cibler, harceler ou intimider des membres de groupes vulnérables.

[43] Voir les rapports récents de Google, Facebook, Dropbox, Twitter et Microsoft sur la transparence.

[44] Suède, loi relative à la surveillance des signaux dans les activités de renseignement, art. 4 3).

[45] Australie, loi de 1979 relative aux télécommunications (interception et accès), art. 9 1).

3. Surveillance discrète

60. Les États peuvent également s'introduire de manière discrète dans les infrastructures techniques appartenant aux prestataires de services et aux plateformes de contenu pour intercepter des informations très diverses, telles que des communications, des informations sur des comptes d'utilisateurs, des relevés téléphoniques ou des relevés de connexion à Internet. Des États interféreraient avec les équipements informatiques dans le parcours des données vers les clients, infiltreraient des réseaux et plateformes privés à l'aide de logiciels malveillants, pirateraient des dispositifs spécifiques et exploiteraient d'autres failles du système de sécurité numérique. Lorsqu'elles prennent connaissance de cette surveillance, les entreprises peuvent se poser des questions quant à leur responsabilité de protéger les droits de l'homme, comme la question de savoir si elles doivent informer leurs clients ou réduire les effets de la surveillance en prenant des mesures de sécurité. Les entreprises qui vendent des équipements et des services aux États afin que ceux-ci puissent mettre en œuvre des techniques de surveillance secrète peuvent être impliquées dans des atteintes aux droits de l'homme découlant de leurs activités commerciales.

4. Traités d'entraide judiciaire et localisation de données

61. Il est important de noter que les autres demandes visant des informations détenues par des opérateurs du secteur privé peuvent avoir un effet sur la surveillance. Par exemple, le fait que le régime conventionnel d'entraide judiciaire ne permette pas de suivre les demandes de données transfrontalières peut amener les États à prendre des mesures de surveillance extraterritoriale invasives. Les lois qui exigent des opérateurs qu'ils retiennent des données concernant leurs clients ou qu'ils les archivent dans des bases de données locales sont également de nature à encourager une telle surveillance.

5. Encodage et anonymat

62. Depuis que le Rapporteur spécial a souligné l'importance de l'encodage et de l'anonymat aux fins de la protection de la liberté d'opinion et d'expression, la pression exercée par les États sur les entreprises pour qu'elles réduisent la sécurité des dispositifs, des communications et des informations numériques de leurs clients, s'est accrue. Toute une série d'acteurs privés, allant des fabricants de matériel informatique aux services de courrier électronique, en passant par les services de messagerie, ont pris des mesures pour élaborer et mettre en œuvre des technologies qui renforcent la sécurité, l'anonymat et la protection de la vie privée des utilisateurs. Parmi ces mesures, on relève l'encodage de bout en bout des communications numériques, l'encodage des disques durs et la mise à jour régulière des logiciels pour combler les failles en matière de sécurité. Les États réagissent à ces mesures en tentent de contraindre les entreprises à créer ou à exploiter, pour eux, des failles techniques dans leurs produits et services. Aux États-Unis, par exemple, le Bureau d'enquête fédéral (FBI) a saisi une cour fédérale dans le but de contraindre Apple à mettre au point des logiciels qui faciliteraient l'accès à l'iPhone d'un suspect dans le cadre d'une enquête pour terrorisme. Le projet de loi sur les pouvoirs d'enquête présenté au Parlement britannique le 1er mars 2016 autoriserait les services de renseignements à demander un mandat visant à contraindre les entreprises privées « à interférer avec un équipement dans le but d'obtenir des communications […] des données sur les équipements ou toute autre information »[46].

[46] Projet de loi sur les pouvoirs d'enquête (*Investigatory Powers Bill* (2015), Cl. 88 2)).

C. Transparence

63. La transparence peut aider ceux auxquels s'applique la réglementation relative à Internet à prévoir avec précision quelles sont leurs obligations juridiques et à les contester lorsque cela est nécessaire. Lorsque les normes ne sont pas respectées, les individus ne savent plus quelles sont les limites imposées à leur liberté d'expression en ligne et s'ils peuvent former un recours si leurs droits ne sont pas respectés. Les questions relatives à la transparence se posent à la fois au sujet de l'État et au sujet du secteur privé, notamment dans les partenariats entre le public et le privé, lorsque le secteur privé mène des négociations commerciales et dans la course au renseignement en ligne/aux armements numériques.

64. En dépit de multiples tentatives de réforme, la transparence, s'agissant des demandes formulées par les États, fait toujours défaut. On constate certes une certaine amélioration de la transparence s'agissant du signalement des demandes, par les États, d'informations sur les utilisateurs, on a beaucoup moins d'informations quant au volume et à la nature des demandes de restriction ou de suppression de contenu[47]. On ne sait même pas si de telles statistiques sont conservées. Les restrictions imposées par les États concernant la divulgation par le secteur privé d'informations pertinentes peuvent constituer un obstacle majeur à la transparence des entreprises. Plusieurs États interdisent la diffusion d'informations concernant les demandes, qu'ils ont formulées, de retrait de contenu ou d'accès à des données relatives à des utilisateurs. L'Inde, par exemple, interdit aux intermédiaires en ligne de divulguer des informations sur les ordres émanant des autorités de bloquer l'accès à un contenu Internet ainsi que sur toute mesure prise pour répondre à de tels ordres[48]. S'il est adopté, le projet de loi britannique sur les pouvoirs d'enquête interdira aux fournisseurs de services de télécommunications de divulguer, entre autres, « l'existence et le contenu » d'ordres, donnés par les autorités, de conserver les données relatives aux communications de clients[49]. Dans d'autres États, des lois et réglementations ambiguës font qu'il est difficile pour les entreprises de savoir quels types d'informations elles sont autorisées à diffuser. En Afrique du Sud, par exemple, le secteur privé ne peut divulguer les demandes officielles de renseignements concernant des clients[50], mais on ne sait pas si cette restriction s'étend aux demandes de retrait de contenu[51].

65. Il est fréquent que les fournisseurs d'accès et les plateformes d'hébergement de contenu divulguent au moins certaines informations sur les circonstances dans lesquelles ils retirent un contenu ou communiquent aux autorités, à leur demande, des données relatives à des clients. On observe de grandes variations dans les décisions de divulguer ou non des interprétations ou des explications de la réglementation de l'État et des conditions d'utilisation ainsi que des processus internes de mise en œuvre et d'exécution, et, s'ils décident de divulguer de telles informations, dans la manière dont les fournisseurs d'accès et les plateformes d'hébergement de contenu le font. On constate également des lacunes dans la divulgation par les entreprises de statistiques concernant le volume, la fréquence et le type de demandes de retrait de contenu et de données sur des utilisateurs, dues soit à des restrictions imposées par les États soit à des décisions de politique interne. En tout état de cause, les entreprises sont plus enclines à divulguer des statistiques sur les demandes des autorités que

[47] Observations de Freedom Online Coalition Working Group on Privacy and Transparency Online ; et Telecommunications Industry Dialogue.

[48] Inde, règles de 2009 relatives aux technologies de l'information (procédures et garanties en matière de blocage de l'accès du public à l'information), règle n° 16.

[49] Projet de loi sur les pouvoirs d'enquête, Cl. 84 2).

[50] Afrique du Sud, loi n° 70 (2002) portant réglementation de l'interception des communications et de la mise à disposition d'informations ayant trait aux communications, art. 42 1).

[51] Afrique du Sud, loi n° 102 (1980) sur la protection des sites d'importance vitale, art. 10 c).

sur les demandes émanant du secteur privé. À ce jour, il y a d'ailleurs eu beaucoup moins de recherches sur le volume d'informations divulguées par les autres intermédiaires (par exemple les intermédiaires financiers ou les entreprises de commerce électronique) et les sociétés concernant le retrait de contenu ou les demandes relatives à des clients.

66. Les débats en cours sur les normes minimales de divulgation par les entreprises et sur les meilleures pratiques en la matière traduisent les incertitudes qui entourent le juste équilibre entre la transparence et les valeurs qui entrent en conflit avec celle-ci, comme la sécurité individuelle et le secret commercial. Si l'on s'accorde de plus en plus à dire que les entreprises devraient divulguer des informations sur la manière dont elles interprètent et appliquent les restrictions, on s'entend moins, en revanche, sur les modalités de telles démarches. De même, il est largement admis que la transparence quantitative est importante, mais on n'a pas défini comment il faut contextualiser et présenter ces informations, et les rendre accessibles.

D. Voies de recours

67. Jour après jour, la liberté d'expression en ligne fait l'objet de restrictions dans lesquelles les entreprises jouent souvent un rôle, soit qu'elles y sont contraintes par la loi, soit qu'elles appliquent leur propre politique ou pratique (énoncées, par exemple, dans les conditions d'utilisation). On peut notamment citer les suppressions de contenu illégales ou douteuses, les restrictions de service et les suspensions de compte, ainsi que les atteintes à la sécurité des données.

68. En vertu du paragraphe 3 de l'article 2 du Pacte international relatif aux droits civils et politiques, les États parties doivent garantir que les personnes dont les droits et les libertés reconnus dans le Pacte ont été violés disposent d'un recours utile. Selon les Principes directeurs relatifs aux entreprises et aux droits de l'homme, les entreprises doivent mettre en place des mécanismes de réclamation et de réparation qui soient légitimes, accessibles, prévisibles, équitables, compatibles avec les droits, transparents, fondés sur la participation et le dialogue et source d'apprentissage permanent[52]. Peu d'orientations sont en revanche fournies sur les moyens de mettre concrètement en œuvre ou d'évaluer ces éléments à l'ère des technologies de l'information et des communications (TIC). Par exemple, lorsque des liens hypertextes ont été abusivement supprimés des résultats de recherche, le moteur de recherche pourrait être tenu de les rétablir. Il y a toutefois peu de directives, à ce jour, sur la conception et l'application des mécanismes de plainte ou de recours qui devraient permettre que ces suppressions soient effectivement signalées, évaluées et réparées. Ces questions de conception sont d'autant plus compliquées quand la clientèle du moteur de recherche est très dispersée. On n'a pas encore déterminé non plus s'il conviendrait que les entreprises mettent en place des réparations supplémentaires, comme le versement d'indemnités pour les pertes financières subies pendant la période de suppression, ou l'application de garanties de non-répétition.

69. En ce qui concerne le respect des conditions d'utilisation, les entreprises n'ont pas toujours mis en place les procédures permettant à l'utilisateur de contester des décisions relatives à la suppression de contenus ou à la désactivation de comptes lorsqu'il estime que la mesure appliquée résulte d'une erreur ou de campagnes de signalement abusives. Il pourrait être utile de mener des recherches supplémentaires pour examiner les meilleures pratiques des entreprises lorsqu'elles communiquent les décisions relatives à l'application des conditions d'utilisation et qu'elles mettent en œuvre les mécanismes de recours.

[52] Principes directeurs, chap. III A) 31).

70. L'étendue de la responsabilité de réparer qui incombe à l'entreprise est également contestée. À qui incombe-t-il de réparer le préjudice subi en cas de suppression abusive ou de demande de données inappropriées lorsque les entreprises interprètent ou appliquent la législation nationale pertinente de manière trop stricte ? Lorsque les produits ou les services d'une entreprise sont utilisés pour commettre des violations des droits de l'homme, qu'est-ce qui déclenche l'obligation de réparer ? Lorsqu'elles sont accusées d'actes répréhensibles, les entreprises ont-elles l'obligation de mener des enquêtes internes ? Ces enquêtes doivent-elles répondre à certaines normes ? Lorsqu'une restriction s'applique à des individus au-delà frontières, quel est l'État compétent pour examiner les recours formés ? Ces questions illustrent les incertitudes auxquelles font face les victimes de violations des droits de l'homme lorsque le comportement des entreprises et la conduite des États s'imbriquent.

71. Il convient également d'analyser de plus près le rôle que les États ont à jouer pour compléter ou réglementer les mécanismes privés de réparation. Les consommateurs lésés par les initiatives des entreprises ont souvent la possibilité d'engager des poursuites civiles ou de demander réparation par d'autres voies judiciaires, mais ces procédures sont souvent lourdes et coûteuses. Des mécanismes de plainte et de réclamation établis et administrés par des organes de protection des consommateurs et des organismes de surveillance par secteur sont aussi des solutions intéressantes. Plusieurs États mandatent également des mécanismes de réparation ou de réclamation internes. L'Inde, par exemple, impose aux sociétés qui possèdent, gèrent ou exploitent des données personnelles sensibles de charger des agents de répondre aux réclamations, et d'examiner « tout anomalie et toute réclamation [...] concernant le traitement des informations »[53].

V. Autres questions thématiques

72. Compte tenu de la diversité des activités privées liées aux TIC qui encadrent l'exercice de la liberté d'opinion et d'expression en ligne et exercent une influence sur cet exercice, le Rapporteur spécial a choisi d'examiner les obligations des États et les responsabilités des entreprises dans certains domaines prioritaires. Les questions juridiques et politiques évoquées ci-dessus le guideront pour rédiger des rapports thématiques, communiquer avec les gouvernements, se rendre dans les pays et dans les entreprises, mener des consultations régionales et des consultations d'experts et autres tâches.

73. Les paragraphes ci-après présentent quelques-unes des priorités du Rapporteur spécial relatives aux études et aux orientations thématiques :

Restrictions sur l'offre de services de télécommunications et d'Internet

74. Les États exigent de plus en plus des entreprises privées qui fournissent des services de télécommunications et d'Internet de respecter les exigences de censure. En sus des pratiques de filtrage des réseaux, les États forcent ou poussent les entreprises à fermer des réseaux ou à bloquer des services entiers. Il convient d'obtenir des informations supplémentaires sur cette tendance et de l'examiner de près. Dans le cadre de son mandat, le Rapporteur spécial examinera les lois, les politiques et les mesures extralégales qui permettent aux États d'imposer de telles restrictions, ainsi que les coûts et les conséquences qui en découlent. Il examinera également les responsabilités qui incombent aux entreprises de donner suite à ces mesures d'une manière qui respecte les droits, limite les préjudices et offre des voies de recours lorsque des abus sont commis.

[53] Inde, loi sur les technologies de l'information, 2008, section 43 A ; article 5 9) du Règlement de 2011 sur les technologies de l'information (procédures et pratiques raisonnables en matière de sécurité, et informations ou données personnelles sensibles).

Restrictions relatives au contenu en application des conditions d'utilisation et des normes appliquées par les communautés virtuelles

75. Les acteurs privés font face à d'importantes pressions des États et de citoyens qui leur demandent d'imposer des restrictions à l'expression de contenus assimilés à l'extrémisme ou à la haine, à l'hostilité ou au harcèlement. Il arrive aussi que les acteurs privés encouragent d'eux-mêmes ce qu'ils considèrent comme des débats citoyens sur leurs plateformes, réglementent l'accès à leurs services en demandant aux utilisateurs d'utiliser leur vrai nom, entre autres politiques d'enregistrement, et présentent ou hiérarchisent certains contenus à des fins commerciales. Le Rapporteur spécial s'emploiera à évaluer la mesure dans laquelle les États peuvent porter atteinte aux initiatives privées, les conséquences qu'ont les initiatives privées sur la liberté d'expression, ainsi que les obligations et les responsabilités pertinentes en matière de droits de l'homme. Il axera son étude non seulement sur le rôle des médias sociaux et des moteurs de recherche, mais également sur celui d'acteurs moins connus comme les acteurs du commerce électronique et les intermédiaires financiers.

Responsabilité relative à l'hébergement de contenu

76. Il est de plus en plus fréquent que les intermédiaires soient tenus responsables du contenu des tiers qu'ils hébergent, que ce soit par le biais de régimes de responsabilité qui leur sont applicables ou de règles de censure. Ces restrictions sont communément justifiées par les impératifs de la cybersécurité, de la défense du droit d'auteur, ou encore de la lutte contre la diffamation et de la protection des données. Il conviendra d'étudier la légitimité de cette logique, d'évaluer la nécessité des restrictions qui l'accompagnent et de s'intéresser au fait que les cadres existants applicables à la suppression de contenu de tierces parties ne prévoient pas de garanties de procédure. Le Rapporteur spécial examinera les sources et les modalités de la responsabilité des intermédiaires dans certaines situations et régions. Il s'emploiera aussi à dégager les grands principes et pratiques applicables pour garantir la capacité des intermédiaires de promouvoir et de protéger la liberté d'expression.

Censure et secteur de la surveillance

77. Les entreprises jouent un rôle majeur dans la conception, la production et le transfert de logiciels et de matériel que les États peuvent utiliser à des fins de maintien de l'ordre, de renseignement et de sécurité publique. Si ces outils peuvent avoir des objectifs légitimes, ils sont souvent utilisés par les autorités à des fins de censure et de surveillance anormalement élevées. Le Rapporteur spécial étudiera ces questions sous l'angle des droits de l'homme et encouragera l'exercice de la diligence raisonnable s'agissant de recenser les cas où ces technologies sont utilisées pour entraver la liberté d'expression.

Efforts visant à affaiblir la sécurité numérique

78. Les entreprises qui transmettent, stockent ou génèrent des communications et d'autres formes de données sur les utilisateurs − en particulier les fournisseurs de services de télécommunications et d'Internet, et les plateformes d'hébergement de contenu − sont de plus en plus sollicitées par les services de maintien de l'ordre et de la sécurité qui souhaitent accéder aux données de leurs clients. Le Rapporteur spécial s'emploiera à repérer les logiques qui pourraient optimiser le cadre de la liberté d'expression tout en tenant néanmoins compte des intérêts légitimes des États en matière de sécurité nationale et d'ordre public.

Accès à Internet

79. Les milliards d'individus qui sont connectés à Internet jouissent d'un accès à l'information et aux idées dont des milliards d'autres sont privés, faute d'infrastructures, de conditions de sécurité suffisantes ou d'un environnement politique, juridique ou social leur permettant de se connecter. Le secteur privé cherchant de plus en plus à doter ces autres milliards de personnes de moyens d'accès, il sera essentiel que cet accès soit libre, ouvert et sécurisé. Le Rapporteur spécial examinera les problèmes concernant l'accès et étudiera comment le secteur privé peut s'investir dans l'accessibilité à un coût abordable, notamment pour les groupes marginalisés.

Gouvernance d'Internet

80. Les textes issus du Sommet mondial sur la société de l'information ont témoigné du large soutien qui était régulièrement exprimé en faveur d'une gouvernance multipartite d'Internet. Le modèle existant subit néanmoins des pressions croissantes du fait de certaines politiques nationales (en matière de localisation des données par exemple) ou de certaines stratégies comme la « cybersouveraineté ». En outre, il reste nécessaire de respecter ou de mieux intégrer les droits de l'homme à tous les niveaux de la gouvernance, notamment en définissant des normes techniques, et de veiller à ce que les dispositifs de gouvernance d'Internet et les efforts de réforme tiennent compte des besoins des femmes, des minorités sexuelles et d'autres communautés vulnérables.

81. Tout au long de ses futurs travaux, le Rapporteur spécial prêtera une attention particulière aux faits nouveaux survenus sur le plan juridique (législatif, réglementaire et judiciaire) aux niveaux national et régional. Dans cette perspective, il informe toutes les parties prenantes qu'il aimerait rassembler de telles informations pour les communications et rapports qu'il compte établir, et encourage les parties intéressées à réunir ces informations et à les lui fournir au fur et à mesure.

VI. Conclusions et recommandations

82. **Le secteur des technologies de l'information et des communications se développe rapidement, les technologies étant constamment améliorées et la vie quotidienne numérisée. Par conséquent, on ne peut s'intéresser aux questions juridiques et politiques pour déterminer les lacunes normatives actuelles sans prendre le risque de passer à côté des tendances qui se dégagent à peine ou qui n'ont pas encore vu le jour. C'est une caractéristique naturelle de l'ère du numérique. Cependant, en dépit de l'évolution rapide des technologies, l'environnement numérique demeurera la cible des menaces qui continuent de peser sur la liberté d'opinion et d'expression. On peut notamment citer la mainmise, ou les tentatives de mainmise, des pouvoirs publics sur les sources d'information, qui passe par le recours à la censure des services et des infrastructures en ligne ; les efforts considérables que déploient les entreprises pour promouvoir leurs produits et leurs services dans des milieux hostiles à la liberté d'expression ; les manquements de nombreuses entreprises qui ne parviennent pas à concilier la promotion et la protection des droits, et la poursuite de leurs intérêts commerciaux ; et, enfin, les exigences souvent contradictoires des individus qui veulent que les entités commerciales leur assurent non seulement sécurité mais aussi commodité, connectivité et accès à des communautés virtuelles. À mesure que son étude des responsabilités liées aux TIC progressera, le Rapporteur spécial fera appel à des experts de terrain − issus des pouvoirs publics, du secteur privé, de la société civile, de la communauté technique et des milieux universitaires − à qui il demandera de l'aider à réaliser des analyses et à établir des rapports sur des questions d'actualité situées au carrefour des technologies et de la liberté d'expression, et sur les caractéristiques de l'ère du numérique à long terme.**

83. **Le Rapporteur spécial engage vivement toutes les parties prenantes − acteurs étatiques, entreprises du secteur privé, organisations de la société civile ou particuliers − à participer activement à l'élaboration des projets à venir. Il encourage tout particulièrement les parties prenantes des pays les moins avancés et des communautés vulnérables à faire connaître leurs points de vue sur les incidences que le secteur des TIC peut avoir sur l'exercice des droits, et sur le rôle que les État peuvent jouer soit en limitant ces droits soit en les promouvant.**

84. **Même si ce projet n'en est qu'à ses débuts, il n'en reste pas moins essentiel que les État et les acteurs privés prennent dès à présent des mesures pour assurer le respect de la liberté d'opinion et d'expression. Il faudrait, au minimum, qu'ils mettent en place les mesures ci-après, que le Rapporteur spécial analysera plus avant au cours de son mandat.**

États

85. **Les États sont au premier chef responsables de la protection et du respect du droit d'exercer la liberté d'opinion et d'expression. À l'ère des technologies de l'information et des communications, cela signifie qu'ils ne doivent ni exiger du secteur privé qu'il prenne des mesures qui entravent de manière inutile ou disproportionnée la liberté d'expression, que ce soit par le biais de lois, de politiques ou d'autres moyens extralégaux, ni exercer sur lui d'autres formes de pressions à cette fin. Toute exigence, toute demande et toute autre mesure visant à supprimer des contenus numériques ou à accéder aux données de clients doivent être fondées sur des dispositions législatives dûment adoptées, être soumises à un contrôle externe et indépendant, et montrer qu'elles visent à réaliser, de manière utile et proportionnée, l'un ou plusieurs des objectifs énoncés à l'article 19 3) du Pacte international relatif aux droits civils et politiques. S'agissant plus particulièrement de la réglementation du secteur privé, les lois et les politiques élaborées par les États doivent être adoptées et appliquées en toute transparence.**

86. **Les États doivent également adopter et appliquer des lois et des politiques qui protègent les initiatives privées et favorisent la mise en place de mesures techniques et la fourniture de produits et services qui font progresser la liberté d'expression. Ils doivent garantir l'existence de processus législatifs, stratégiques et d'autres processus de normalisation relatifs aux droits et aux restrictions sur Internet afin de réellement permettre au secteur privé, à la société civile, à la communauté technique et aux milieux universitaires d'apporter leur pierre à l'édifice.**

Secteur privé

87. **Les États exercent des pressions indéniables sur les entreprises privées du secteur des technologies de l'information et des communications, qui ont souvent de lourdes répercussions sur la liberté d'expression. Cependant, le secteur privé joue aussi un rôle indépendant qui peut soit promouvoir soit restreindre les droits, élément que le Conseil des droits de l'homme a bien compris en adoptant, en 2011, les Principes directeurs relatifs aux entreprises et aux droits de l'homme, qui tiennent lieu de directives générales dans ce domaine. Les entreprises privées devraient être évaluées à l'aune des mesures qu'elles prennent pour promouvoir ou pour entraver la liberté d'expression, même dans des milieux hostiles et peu favorables aux droits de l'homme.**

88. **Il serait notamment très important que les acteurs privés prennent des mesures visant à établir et à mettre en œuvre des procédures transparentes permettant d'évaluer la situation des droits de l'homme. Ils devraient définir et appliquer des stratégies prenant en compte les incidences potentielles de telles procédures sur les droits de l'homme. De telles évaluations devraient permettre d'examiner d'un œil**

critique tout l'éventail des activités du secteur privé auxquelles ils prennent part, par exemple la formulation et l'application effective de conditions d'utilisation et de normes appliquées par les communautés virtuelles concernant la liberté d'expression des utilisateurs, y compris l'externalisation des activités de contrôle en la matière. Elles devraient aussi permettre d'examiner les incidences des produits, services et autres initiatives commerciales sur la liberté d'expression des utilisateurs à toutes les étapes de leur élaboration, notamment en ce qui concerne les choix de conception et d'application technique. Elles devraient aussi couvrir les incidences des plans pour la tarification différenciée des contenus et services Internet ou pour l'accès à ceux-ci, ainsi que les conséquences des transactions conclues avec des clients publics potentiels sur les droits de l'homme, comme l'exploitation d'infrastructures de télécommunications ou le transfert de technologies relatives à la surveillance ou à la réglementation des contenus.

89. **Il est également essentiel que les acteurs privés assurent la transparence la plus grande possible dans leurs stratégies, normes et activités influant sur la liberté d'expression et d'autres droits fondamentaux. Les évaluations de la situation des droits de l'homme devraient être soumises à un examen transparent, tenant compte des méthodes suivies, de la manière dont les obligations juridiques sont interprétées et du poids que ces évaluations ont sur les décisions des entreprises. La transparence est importante à tous les niveaux, notamment sur le plan de la réglementation des contenus et, à cette fin, les pouvoirs publics devraient établir des rapports concernant leurs demandes de suppression.**

90. **Au-delà de l'adoption de politiques, les acteurs privés devraient aussi tenir compte des engagements pris en faveur de la liberté d'expression dans leurs processus internes d'élaboration de politiques, leurs études techniques sur les produits, le développement commercial, la formation du personnel et autres processus internes pertinents. Le Rapporteur spécial s'emploiera à étudier de différentes façons les politiques et tout l'éventail des mesures de mise en œuvre, notamment en se rendant dans les entreprises.**

Organisations internationales et processus multipartites

91. **Comme le présent rapport l'a montré, nombre d'organisations internationales jouent un rôle dans la gouvernance des technologies de l'information et des communications. Il est essentiel que ces organisations permettent réellement au public d'accéder aux politiques, aux normes, aux rapports et à d'autres informations concernant la gouvernance d'Internet dont elles-mêmes, ou leurs membres, sont à l'origine ou qu'elles produisent, notamment en facilitant l'accès aux ressources gratuites en ligne et aux initiatives d'éducation du public. Plus généralement, le processus multipartite relatif à la gouvernance d'Internet a été un puissant moteur de création de politiques favorables à la liberté d'expression. Les organisations internationales devraient tenir compte de cet élément et garantir une véritable participation de la société civile à l'élaboration des politiques et à d'autres processus de normalisation, notamment en renforçant la participation d'experts techniques sensibles aux problèmes relatifs aux droits de l'homme.**