Nations Unies A/HRC/35/22

Assemblée générale

Distr. générale
30 mars 2017
Français
Original : anglais

Conseil des droits de l'homme
Trente-cinquième session
6-23 juin 2017
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. Dans ses deux précédents rapports au Conseil, le Rapporteur spécial s'était concentré sur la liberté d'opinion et d'expression à l'ère du numérique, exposant de manière détaillée comment les outils permettant de chiffrer les données et de garantir l'anonymat assuraient la sécurité nécessaire à l'exercice de la liberté d'expression (A/HRC/29/32) et décrivant les incidences des technologies de l'information et des communications sur cette liberté (A/HRC/32/38). Dans le rapport ci-après, le Rapport spécial examine le rôle joué par les prestataires d'accès à Internet et aux services de télécommunication. Il aborde en premier lieu les obligations incombant aux États pour ce qui est de protéger et de promouvoir la liberté d'expression en ligne, puis évalue le rôle joué par les prestataires d'accès à l'espace numérique, et propose enfin un ensemble de principes susceptibles d'aider les acteurs privés à respecter les droits de l'homme.

GE.17-05047 (F) 210417 210417
1705047

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

Table des matières

Introduction

1. Les États font de plus en plus fréquemment appel aux prestataires d'accès au numérique pour contrôler, restreindre ou surveiller l'expression en ligne. Lorsque les autorités veulent que les utilisateurs n'aient plus accès à des sites Web ou à des réseaux sociaux, voire à l'ensemble du réseau Internet, elles sollicitent généralement l'assistance des fournisseurs d'accès à Internet. Ces derniers interviennent sur les points d'échange Internet, qui rendent possible le trafic de données à destination ou à l'intérieur d'un pays, et accèdent aux communications privées et aux autres données personnelles dont disposent les prestataires de services de télécommunication. À l'heure actuelle, bon nombre de ces acteurs sont détenus ou administrés par des sociétés privées. Qu'ils s'y opposent, y consentent tacitement ou y participent volontairement, ils jouent souvent un rôle essentiel dans la censure et la surveillance exercées par les autorités. Ce que les pouvoirs publics demandent à ces acteurs privés et ce qu'ils obtiennent d'eux peut paralyser l'échange d'informations, empêcher les journalistes de mener leurs enquêtes en toute sécurité et exercer un effet dissuasif sur les lanceurs d'alerte et les défenseurs des droits de l'homme. Les acteurs privés peuvent aussi restreindre la liberté d'expression de leur propre initiative, notamment en privilégiant certains contenus ou certaines applications Internet contre rémunération ou en échange d'autres avantages commerciaux, influant ainsi sur l'accès des utilisateurs à l'information en ligne. Les entreprises qui offrent des services de filtrage peuvent quant à elles avoir une influence sur l'éventail de contenus accessibles à leurs abonnés.

2. La liberté d'expression relève tant des États que des acteurs privés. Or, si les obligations des premiers au regard de la protection de cette liberté sont clairement définies, quelles sont celles des deuxièmes vis-à-vis de leurs utilisateurs ? Que devraient faire les acteurs privés pour respecter la liberté d'expression ? Quelles mesures prennent-ils pour évaluer et atténuer les risques que leurs réactions aux initiatives et politiques gouvernementales sont susceptibles de faire peser sur la liberté d'expression et la vie privée ? Quelle quantité d'informations devraient-ils communiquer à leurs clients en ce qui concerne les demandes et exigences de l'État ? Lorsqu'ils sont directement ou indirectement impliqués dans des atteintes aux droits, quels recours faudrait-il offrir aux particuliers et aux autres membres du public dont les intérêts sont menacés ?

3. Les acteurs privés qui rendent possible l'accès à l'espace numérique jouent dans l'exercice de la liberté d'expression un rôle de catalyseur. Certes, l'essentiel des activités de censure et de surveillance sont le fait des États. Cela étant, si ces derniers comptent, sinon systématiquement, du moins fréquemment, sur les prestataires de services pour leur permettre d'exercer leur censure, les utilisateurs − bénéficiaires des formidables progrès de l'ère du numérique − méritent de savoir quels rapports ces acteurs entretiennent les uns avec les autres, quelles sont les conséquences tant de leurs actions que de leurs interactions, et quelles sont les responsabilités des prestataires quant au respect des droits fondamentaux.

4. Le présent rapport est le fruit d'un travail de recherche et de consultation qui s'est étendu sur plus d'une année et a commencé en 2016 par une analyse du secteur des technologies de l'information et des communications (voir A/HRC/32/38)[1]. Par suite de son appel à contributions[2], le Rapporteur spécial a reçu des communications émanant d'États (25), d'entreprises (3), de la société civile (22) et d'universitaires et d'autres personnes, ainsi qu'une communication confidentielle. Le Rapporteur spécial a de surcroît organisé divers événements : une séance de réflexion au siège de l'organisation non gouvernementale Article 19, à Londres, en juillet 2016 ; une réunion d'experts à l'institut des droits de l'homme de l'Université du Connecticut (États-Unis), en octobre 2016 ; des

[1] Je tiens à remercier mon conseiller juridique, Amos Toh, boursier de la Fondation Ford et chargé de cours à la Faculté de droit d'Irvine (Université de Californie), qui a mené des travaux de recherche et d'analyse de grande qualité et a assuré la coordination des importantes recherches sur le fond effectuées par des étudiants en droit suivant le cursus de justice internationale à l'Université d'Irvine.

[2] Voir https://freedex.org/new-call-for-submissions-freedom-of-expression-and-the-telecommunications-and-internet-access-sector/.

consultations régionales avec le Rapporteur spécial sur la liberté d'expression de la Commission interaméricaine des droits de l'homme, à Guadalajara (Mexique), en décembre 2016 ; et des consultations régionales à Beyrouth, en février 2017[3].

II. Obligation de l'État de protéger et de promouvoir la liberté d'expression en ligne

5. Le droit international des droits de l'homme consacre le droit de chacun de ne pas être inquiété pour ses opinions et de rechercher, de recevoir et de diffuser des informations et des idées de toute espèce, sans considération de frontières et par tous les moyens de son choix (voir l'article 19 de la Déclaration universelle des droits de l'homme et l'article 19 du Pacte international relatif aux droits civils et politiques). Le Conseil des droits de l'homme et l'Assemblée générale ont réaffirmé que la liberté d'expression et d'autres droits devaient également être respectés en ligne (voir les résolutions 26/13 et 32/13 du Conseil, la résolution 68/167 de l'Assemblée générale et A/HRC/32/38). Le Comité des droits de l'homme, d'anciens titulaires de mandat et le Rapporteur spécial ont examiné les obligations mises à la charge des États par l'article 19 du Pacte. Pour résumer, les États ne sauraient porter atteinte à la liberté d'opinion ou la restreindre que quelque manière que ce soit (voir l'article 19 du Pacte, par. 1, et A/HRC/29/32, par. 19). Le paragraphe 3 de l'article 19 du Pacte prévoit que les États ne peuvent soumettre la liberté d'expression à d'autres restrictions que celles qui sont expressément fixées par la loi et sont nécessaires au respect des droits ou de la réputation d'autrui ou à la sauvegarde de la sécurité nationale, de l'ordre public ou de la santé ou de la moralité publiques (voir l'observation générale n° 34 (2011) du Comité des droits de l'homme, A/71/373 et A/HRC/29/32).

6. Les États sont de surcroît tenus de prendre des mesures pour préserver les particuliers de toute immixtion d'un acteur privé dans l'exercice de leurs droits (voir le paragraphe 2 de l'article 2 du Pacte et l'observation générale n° 31 (2004) du Comité des droits de l'homme). Le droit des droits de l'homme protège les particuliers contre les violations commises par l'État et par des personnes privées, physiques ou morales (voir l'observation générale n° 31, par. 8)[4]. Conformément aux Principes directeurs relatifs aux entreprises aux droits de l'homme : mise en œuvre du cadre de référence « protéger, respecter et réparer » des Nations Unies, adoptés par le Conseil des droits de l'homme en 2011, les États sont tenus de prendre les mesures qui s'imposent pour empêcher les atteintes aux droits de l'homme et, lorsque pareilles atteintes sont commises, enquêter à leur sujet, en punir les auteurs et les réparer (voir A/HRC/17/31, annexe, principe 1). Il s'agit notamment pour les États de s'assurer, par des moyens d'ordre législatif, judiciaire, administratif, éducatif ou autre, que les entreprises doivent et peuvent respecter la liberté d'expression, et de faire en sorte que lorsque des atteintes sont commises par des acteurs privés, les victimes ont accès à un recours utile (voir l'observation générale n° 31, par. 7, et A/HRC/17/31, annexe, principes 3 et 25).

7. Les mesures prises par les pouvoir publics qui sont exposées plus bas ne sont souvent pas conformes aux exigences du droit des droits de l'homme. De surcroît, les relations des pouvoirs publics avec les prestataires d'accès au numérique sont caractérisées par un manque de transparence, imputable notamment au fait que les lois sont vagues et donnent aux autorités un pouvoir discrétionnaire excessif alors que les tiers se voient imposer des restrictions quant aux informations qu'ils peuvent communiquer concernant l'accès desdites autorités aux données des utilisateurs, voire sont soumis à

[3] Ces communications peuvent être consultées sur le site Web du Rapporteur spécial. On trouvera un résumé des consultations qui se sont tenues et des éléments d'information qui ont été reçus dans le cadre de l'établissement du présent rapport dans une annexe supplémentaire, également consultable sur le site Web du Rapporteur spécial.

[4] Voir aussi Commission africaine des droits de l'homme et des peuples, observation générale n° 3 (2015) sur le droit à la vie, par. 38 ; Cour interaméricaine des droits de l'homme, *Affaire Velásquez Rodríguez*, arrêt du 29 juillet 1988, par. 172 ; et Cour européenne des droits de l'homme, *Özel et atres* c. *Turquie*, arrêt du 17 novembre 2015, par. 170.

l'obligation expresse de garder le silence. Ce manque de transparence compromet l'état de droit et empêche le public d'être dûment informé[5].

A. Coupures de l'accès à Internet et aux services de télécommunication

8. Les coupures de l'accès à Internet et aux services de télécommunication peuvent être expressément destinées à empêcher ou à perturber la consultation ou la diffusion de l'information en ligne, en violation du droit des droits de l'homme (voir A/HRC/32/13, par. 10)[6]. En général, ce sont les pouvoirs publics qui coupent ou font couper cet accès, souvent avec le concours d'opérateurs privés. Les attaques à grande échelle menées contre les infrastructures de réseau par des acteurs privés, telles que les attaques par déni de service distribué (attaques DdoS), peuvent également avoir pour effet d'interrompre l'accès aux services. Les coupures sont souvent liées à des pannes générales de réseau, mais peuvent également survenir lorsque l'accès à la téléphonie mobile, aux sites Web, aux réseaux sociaux et aux applications de messagerie est bloqué, ralenti ou rendu impossible[7]. Elles peuvent survenir à l'échelle d'une ville, d'une région ou d'un pays tout entier, voire de plusieurs pays, et durer de quelques heures à plusieurs mois.

9. Les coupures qui sont ordonnées secrètement ou ne reposent sur aucun fondement juridique manifeste contreviennent à l'impératif énoncé au paragraphe 3 de l'article 19 du Pacte, qui veut que les restrictions soient « expressément fixées par la loi ». Au Tchad, le fait que les autorités n'aient pas pu justifier les coupures répétées de l'accès à Internet et aux réseaux sociaux survenues entre février et octobre 2016 a conduit certains à penser que ces coupures étaient illégales[8]. Au Gabon, l'accès au réseau aurait été totalement coupé tous les soirs pendant près de deux semaines durant la période électorale de 2016 alors que le Gouvernement avait fourni l'assurance qu'il n'y aurait pas de perturbation[9].

10. Les coupures ordonnées conformément à des lois et règlements libellés en des termes flous ne répondent pas non plus à l'impératif de légalité. Au Tadjikistan, la nouvelle loi sur l'état d'urgence autorise les autorités à bloquer l'accès aux services de téléphonie mobile et à Internet sans décision de justice en cas d'état d'urgence[10], mais ne dit pas quand ni pour quelles raisons l'état d'urgence peut être déclaré. Ce silence de la loi donne aux autorités toute latitude pour bloquer l'accès aux services. Dans certains pays, les autorités invoquent des lois obsolètes pour justifier les coupures[11]. Les lois et règlements adoptés et appliqués secrètement contreviennent aussi à l'impératif de légalité. Aux États-Unis, le *National Coordinating Center for Telecommunications* (Centre national de coordination des télécommunications) n'a publié qu'une version très expurgée de la directive générale 303, dans laquelle sont établies des procédures détaillées d'interruption des services de communication mobile[12]. Ces procédures n'ont encore pas été invoquées, mais elles offrent la possibilité aux autorités de se soustraire à la surveillance de la justice et à l'obligation de rendre compte de leurs actes, ce qui est contraire aux dispositions de l'article 19 du Pacte.

11. Pour être conformes aux dispositions du paragraphe 3 de l'article 19 du Pacte, les restrictions à la liberté d'expression doivent être nécessaires ; en outre, ce type de restriction ne doit jamais être utilisé pour museler les défenseurs des droits démocratiques (voir l'observation générale du Comité des droits de l'homme n° 34, par. 23, et A/71/373,

[5] Freedom Online Coalition, *Report of Working Group 3: Privacy and Transparency Online*, novembre 2015.

[6] Access Now a dénombré 15 interruptions en 2015 et 56 en 2016. La première à avoir été signalée aurait eu lieu au Népal en février 2005.

[7] Communication d'Access Now, partie I, p. 1.

[8] Communication d'Internet sans Frontières, TCD 3/2016, p. 2.

[9] Ibid., GAB 1/2016.

[10] HCDH, « Preliminary observations by the United Nations Special Rapporteur on the right to freedom of opinion and expression, Mr. David Kaye, at the end of his visit to Tajikistan », communiqué de presse (9 mars 2015).

[11] Inde, Code de procédure pénale, art. 144 ; Apar Gupta et Raman Jit Singh Chima, « The cost of internet shutdowns », The Indian Express (26 octobre 2016).

[12] États-Unis, directive 303 du NCC.

par. 26). Il arrive pourtant fréquemment que les autorités bloquent l'accès à Internet lors de manifestations, d'élections et d'autres événements concernant de très près le public, et ce, sans donner d'explication ou presque[13]. À Bahreïn, les coupures de l'accès aux services de téléphonie mobile et à Internet survenues à Duraz auraient coïncidé avec les rassemblements organisés aux abords de la résidence d'une haute autorité religieuse que le Gouvernement avait déchue de sa nationalité[14]. Au Venezuela, l'accès à Internet aurait été bloqué en 2014 lors d'une vague de manifestations contre le Gouvernement[15]. Au Cameroun[16], en Gambie[17], en Inde[18], au Myanmar[19], en Iran[20], en Ouganda[21] et au Monténégro[22], l'accès aux réseaux a été perturbé à l'occasion d'élections ou de manifestations.

12. Lorsqu'une coupure se produit sans être expliquée ni officiellement reconnue, il y a lieu de penser qu'elle a pour but d'empêcher la communication d'informations ou l'expression d'opinions critiques ou dissidentes. D'après certaines informations, des coupures ont été suivies de mesures répressives et de violences commises avec l'aval des autorités, ce qui a fait naître des allégations selon lesquelles des États tiraient parti de ces coupures pour commettre et dissimuler des violations des droits. Au Soudan, par exemple, l'accès à Internet a été suspendu pendant plusieurs heures lors de la répression meurtrière d'une manifestation organisée en septembre 2013 pour protester contre l'augmentation du prix du carburant[23].

13. Des observateurs ont de surcroît constaté que les coupures étaient de plus en plus souvent utilisées comme moyen d'empêcher les étudiants de tricher pendant les examens nationaux. L'Ouzbékistan pourrait être le premier pays à avoir invoqué cet argument, ce qu'il a fait en 2014 lors des examens d'entrée à l'université[24]. En 2016, les autorités indiennes, algériennes, éthiopiennes et iraquiennes auraient fait bloquer l'accès à Internet pendant des examens[25].

14. Les coupures de l'accès aux réseaux ne satisfont jamais à l'exigence de nécessité. En effet, pour établir que ces coupures sont nécessaires, il faut démontrer qu'elles vont permettre d'atteindre l'objectif visé ; or, dans bien des cas, elles sont contre-productives. Certains États soutiennent qu'il est important d'interdire la diffusion d'informations sur les attaques terroristes, même si elles sont conformes à la réalité, afin d'éviter que la population ne panique et que certains ne s'inspirent de ces attaques pour en commettre d'autres[26]. On a toutefois pu constater que le maintien de la connexion au réseau pouvait atténuer les problèmes de sécurité publique et contribuer au rétablissement de l'ordre public. Lors des émeutes survenues à Londres en 2011, par exemple, les autorités ont utilisé les réseaux sociaux pour identifier les auteurs, diffuser des informations sur ce qui s'était vraiment passé et mener des opérations de nettoyage. Au Cachemire, les forces de police

[13] Communication d'Access Now, partie I, p. 5 à 7.
[14] Centre des droits de l'homme de Bahreïn, *Digital Rights Derailed in Bahrain* (2016), p. 13 et 14.
[15] Danny O'Brien, « Venezuela's Internet crackdown escalates into regional blackout », Electronic Frontier Fundation (20 février 2014).
[16] HCDH, « UN expert urges Cameroon to restore Internet services cut off in rights violation », communiqué de presse du 10 février 2017.
[17] Deji Olukotun, « Gambia shuts down Internet on eve of elections », Access Now (30 novembre 2016).
[18] Software Freedom Law Center, « Internet shutdowns in India, 2013-2016 ».
[19] Freedom House, « Freedom on the Net: Myanmar » (2011).
[20] Center for Democracy and Technology, « Iran's Internet throttling: unacceptable now, unacceptable then » (3 juillet 2013).
[21] Article 19, « Uganda: Blanket ban on social media on election day is disproportionate », (communiqué de presse du 1er février 2016).
[22] Global Voices, « WhatsApp and Viber blocked on election day in Montenegro » (17 octobre 2016).
[23] Human Rights Watch, « Sudan: Dozens killed during protests » (27 septembre 2013)
[24] Note d'Access Now, partie I ; voir aussi Freedom House, « Freedom on the Net: Uzbekistan » (2016).
[25] Communication d'Access Now, partie I.
[26] Voir, par exemple, HCDH « Preliminary conclusions and observations by the UN Special Rapporteur on the right to freedom of opinion and expression to his visit to Turkey, 14-18 November 2016 », communiqué de presse (18 novembre 2016).

ont signalé que c'était grâce aux téléphones portables qu'elles avaient pu localiser des personnes prises au piège lors d'attaques terroristes[27].

15. Quelle que soit leur durée et leur portée géographique, les coupures sont généralement disproportionnées. Les utilisateurs qui en pâtissent se voient dans l'impossibilité d'accéder à une large gamme de contenus et de services (services d'urgence, informations sanitaires, services bancaires par téléphonie mobile, commerce électronique, transports, matériel pédagogique, scrutins et suivi des élections, informations sur les crises et les grands événements, enquêtes sur le respect des droits de l'homme[28]. Étant donné le nombre d'activités et de services essentiels sur lesquels elles ont des conséquences, les coupures restreignent la liberté l'expression et nuisent à l'exercice d'autres droits fondamentaux.

16. Les coupures ont également une influence sur d'autres domaines que ceux abordés ici[29]. En 2015, dans les heures qui ont précédé le défilé de la fête nationale du Pakistan, l'accès aux réseaux de communication mobile aurait été coupé non seulement dans le périmètre du défilé, mais aussi dans des zones alentours dans lesquelles la sécurité n'était pas supposée être menacée[30]. La même année, pendant la visite du pape aux Philippines, l'interruption de l'accès aux réseaux de communication mobile imposée pour des raisons de sécurité a touché des zones largement très éloignées de l'itinéraire de Sa Sainteté[31]. Lorsque les interruptions visent certains services ou certaines plateformes, les autorités ciblent généralement ceux qui sont les plus efficaces, les plus sécurisés ou les plus utilisés[32].

B. Accès des pouvoirs publics aux données des utilisateurs

17. Aujourd'hui, la surveillance exercée par les pouvoirs publics repose sur l'accès aux communications et aux données appartenant aux utilisateurs des réseaux privés. Si un tel accès nécessite souvent le concours des acteurs du secteur privé, il peut néanmoins également être obtenu à leur insu ou sans leur participation. Comme d'autres formes de surveillance, l'accès des autorités aux données personnelles peut constituer une immixtion dans la vie privée et restreindre, à la fois directement et indirectement, la liberté de concevoir et d'échanger des idées (voir A/HRC/23/40, par. 24). Le fait que pareilles données puissent être indûment consultées encourage implicitement les utilisateurs à faire preuve de prudence, voire à ne pas émettre d'idées controversées, ni échanger d'informations sensibles ou exercer leur liberté d'expression par d'autres moyens pouvant faire l'objet d'une surveillance des autorités (voir A/HRC/27/37, par. 20).

Demandes d'obtention de données d'utilisateurs

18. Les lois et règlements qui ne sont pas clairement formulés sont contraires au principe de la légalité (voir A/HRC/23/40, par. 50). À titre d'exemple, la loi malaisienne sur les communications et le multimédia autorise les autorités à ordonner la divulgation de toute communication ou type de communications en cas de danger public ou dans l'intérêt de la sécurité publique. Or, la loi ne définit pas les circonstances permettant de conclure à l'existence d'un danger public, une déclaration du Roi étant considérée comme une preuve décisive de l'existence de pareil danger[33]. Au Qatar, les forces de l'ordre jouissent d'une grande latitude pour accéder aux communications des utilisateurs dans les situations d'urgence nationale ou en cas de menace à la sécurité publique[34]. Grâce à ce type de

[27] Institute for Human Rights and Business (IHRB), « Security v. Access: The impact of mobile network sutdowns », étude de cas : Telenor Pakistan (Septembre 2015), p. 31-32.
[28] Access Now submission, part I, pp. 11-14; also Global Network Initiative submission.
[29] IHRB, « Security v. Access: The impact of mobile network shutdowns », case study: Telenor Pakistan (Septembre 2015), p. 20.
[30] Ibid., p. 27 et 28.
[31] Deniz Duru Aydin, "Five excuses governments (ab)use to justify Internet shutdowns" Access Now (6 october 2016).
[32] Communication d'Article 19, p. 2.
[33] Malaisie, loi sur les communications et le multimédia (1998), sect. 266.
[34] Qatar, décret-loi n° (34) de 2006.

dispositions, il suffit aux autorités d'invoquer la sécurité nationale pour se faire communiquer des données d'utilisateurs. De ce fait, les utilisateurs ne peuvent pas prévoir avec une certitude raisonnable les circonstances dans lesquelles leurs communications et données peuvent être transmises aux autorités.

19. Seule une décision de justice établissant que pareille mesure est nécessaire et proportionnée à la réalisation d'un but légitime devrait pouvoir contraindre un prestataire à communiquer des données d'utilisateurs. Au Canada, le Code pénal prévoit que la police doit faire approuver par un juge les demandes de communication de relevés téléphoniques formulées dans le cadre d'une enquête pénale[35]. Au Portugal, les autorités ont besoin d'une décision judiciaire pour accéder à des données de communication[36]. Toutefois, dans bien des cas, le droit interne autorise les pouvoirs publics à obtenir des données d'utilisateurs sans demander l'autorisation d'un juge. Ainsi, au Bangladesh, dès lors qu'elles invoquent la sécurité et l'ordre publics, les autorités n'ont besoin que de l'approbation du pouvoir exécutif pour accéder aux données de communication appartenant aux abonnés des opérateurs[37].

20. Les lois qui imposent aux acteurs du secteur privé de créer de grandes bases de données d'utilisateurs accessibles par les pouvoirs publics suscitent des préoccupations quant à leur nécessité et leur proportionnalité. Au Kazakhstan, les numéros de téléphone, adresses électroniques et adresses IP doivent être conservés par l'opérateur pendant deux ans, de même que les informations de facturation[38]. En Fédération de Russie, les acteurs du secteur privé sont tenus de stocker le contenu de tous les appels téléphoniques et messages texte de leurs clients pendant six mois, et les métadonnées y relatives pendant trois ans[39]. Dans les deux pays, la loi exige que ces données soient stockées localement[40]. Des pays dans lesquels les téléphones mobiles sont un des principaux moyens de communication sont dotés de lois sur l'enregistrement obligatoire des cartes SIM qui imposent à la majorité de la population de communiquer des informations à caractère personnel (voir A/HRC/29/32, par. 51). La conservation obligatoire de grandes quantités de données d'utilisateurs est contraire aux normes de procédure régulière, et notamment au principe qui veut que seules soient conservées les données de personnes soupçonnées d'avoir commis une infraction.

Affaiblissement du chiffrement

21. Depuis l'établissement du rapport du Rapporteur spécial consacré au chiffrement et à l'anonymat (A/HRC/29/32), de plus en plus de mesures inutiles et disproportionnées visant à affaiblir le chiffrement des données ont été prises dans le monde. Ces mesures menacent tant la liberté d'expression que la sécurité des données numériques. Au Royaume-Uni, par exemple, la loi de 2016 sur les pouvoirs d'enquête autorise le Secrétaire d'État à exiger que les opérateurs lèvent la « protection électronique » des communications, ce qui pourrait contraindre les entreprises à supprimer ou affaiblir le chiffrement, et notamment à permettre l'accès aux données par des portes dérobées[41]. Les États n'ont pas réussi à démontrer que pareilles mesures étaient les moyens les moins contraignants de protéger la sécurité nationale et l'ordre public, d'autant qu'ils disposent de nombreux autres instruments d'enquête (ibid., par. 39).

Accès direct

22. L'accès direct à Internet et aux réseaux de télécommunications permet aux autorités d'intercepter et de surveiller les communications en échappant largement au contrôle de la justice et à l'obligation de rendre compte de leurs actes. Les progrès technologiques ont

[35] Voir la communication du Canada, p. 6.
[36] Portugal, Code de procédure pénale, art. 187 à 190.
[37] Bangladesh, loi sur la réglementation des télécommunications (2001), sect. 97 (Ka).
[38] Kazakhstan, résolution gouvernementale n° 1593 (23 décembre 2011).
[39] HCDH, lettre adressée au Gouvernement de la Fédération de Russie, 28 juillet 2016 (OL RUS 7/2016).
[40] Communication d'Article 19, p. 5
[41] Royaume-Uni, loi sur les pouvoirs d'enquête (2016), art. 253 ; et HCDH, lettre adressée au Gouvernement du Royaume-Uni, 22 décembre 2015 (AL GBR 4/2015).

renforcé les moyens dont disposent les services de police et de renseignement pour se connecter directement aux réseaux sans l'intervention de l'opérateur, voire à l'insu de celui-ci [42]. Lors des élections générales organisées en ex-République yougoslave de Macédoine en 2014, les services de renseignement auraient pu accéder directement aux principaux réseaux de télécommunications du pays, ce qui leur aurait permis d'intercepter les communications de plus de 20 000 personnes, y compris des responsables politiques, des militants, des agents de l'État et des journalistes. Bon nombre de ces personnes ont reçu une transcription de leurs appels téléphoniques[43]. En Inde, les autorités s'emploieraient actuellement à élaborer un dispositif central de surveillance devant leur permettre de se procurer des numéros par voie électronique sans intervention manuelle de l'opérateur sur un réseau sécurisé[44]. Pareilles activités ne sont selon toute apparence pas prévues par la loi, et sont menées sans autorisation judiciaire ni contrôle externe. En outre, elles exposent la sécurité et l'intégrité des infrastructures de réseau à des risques qui mettent en question leur proportionnalité.

C. Neutralité du Net

23. La neutralité du Net − le principe selon lequel tous les contenus publiés sur Internet doivent être traitées de la même manière sans immixtion indue − favorise l'accès le plus large possible à l'information[45]. À l'ère du numérique, la liberté de choisir entre différentes sources d'informations n'a de sens que si tous les types de contenus et d'applications disponibles sur Internet sont communiqués sans discrimination ni interférence de la part d'acteurs non étatiques, y compris de la part des opérateurs. L'obligation positive qu'a l'État de promouvoir la liberté d'expression joue grandement en faveur du maintien de la neutralité du Net, qui facilite l'accès à l'information par le plus grand nombre, sans discrimination.

Hiérarchisation payante

24. La hiérarchisation payante consiste, pour les fournisseurs d'accès, à donner la priorité à certains types de trafic Internet contre rémunération ou en échange d'autres avantages commerciaux. Cette pratique permet aux fournisseurs qui ont les moyens de le faire de payer pour que leurs contenus ou applications soient accessibles rapidement, avec pour résultat que l'accès aux autres services et contenus s'en trouve ralenti [46]. Cette hiérarchisation va à l'encontre de la liberté de choix des utilisateurs, qui soit paient plus cher pour accéder aux contenus et applications disponibles sur la « voie rapide », soit bénéficient d'un service de moindre qualité lorsqu'ils tentent d'accéder à ceux qui sont sur la « voie lente », et peuvent en outre être amenés à consulter des contenus auxquels on a donné la priorité à leur insu.

25. Plusieurs États interdisent la hiérarchisation payante. À titre d'exemple, les Pays-Bas, l'un des premiers pays à adopter le principe de la neutralité du Net, interdisent aux fournisseurs de faire dépendre le tarif des services d'accès à Internet des services et applications proposés ou utilisés au moyen de ces services[47]. La directive sur l'ouverture d'Internet adoptée par la Commission fédérale des communications des États-Unis en 2015 interdit aux prestataires de gérer le réseau des fournisseurs d'accès à Internet haut débit de manière à favoriser directement ou indirectement certains types de trafic au détriment des

[42] Communication de Privacy International et communication du Telecommunications Industry Dialogue, p. 3.
[43] Privacy International, « Macedonia: Society On Tap » (23 mars 2016).
[44] Communication d'Access Now, Part. II, p. 4
[45] Communication de Luca Belli ; communication d'Article 19, p. 7 et 8.
[46] Dawn C. Nunziato et Arturo J. Carrillo, « The price of paid prioritization: The international and domestic consequences of the failure to protect Net neutrality in the United States0160», Georgetown Journal of International Affairs: International Engagement on Cyber V: Securing Critical Infrastructure (2 octobre 2015), p. 103
[47] Pays-Bas, loi sur les télécommunications, art. 7 4a 3).

autres, que ce soit en échange d'une contrepartie, financière ou autre, de la part d'un tiers, ou pour avantager une entité associée[48].

Non-facturation (« zero rating »)

26. La non-facturation consiste à ne pas faire payer les utilisateurs pour les données associées à une application ou à un service Internet particuliers, les autres données étant facturées. Ainsi, certains abonnements permettent aux utilisateurs d'accéder à tels ou tels services sans que cela ne soit déduit de leur forfait, et certains services peuvent être utilisés par des non-abonnés sans que les données correspondantes ne soient déduites de la quantité de données octroyée par l'opérateur[49]. Quelle que soit la forme qu'elle prend, cette pratique privilégie l'accès à certains contenus et risque de faire augmenter le coût des données facturées. En outre, les utilisateurs qui peinent à acheter des données payantes pourraient en venir à utiliser exclusivement des services non facturés, ce qui pourrait pénaliser encore davantage les populations déjà marginalisées en ce qui concerne l'accès à l'information et la participation à la vie publique.

27. La non-facturation peut permettre à des utilisateurs d'avoir un accès limité à Internet dans des domaines qui, autrement, leur seraient totalement inaccessibles[50]. Toutefois, elle peut aussi empêcher certains d'avoir un accès plus large à Internet en les maintenant en permanence dans un « jardin fermé »[51]. L'hypothèse selon laquelle l'accès limité finira par se transformer en connectivité totale nécessite un examen plus approfondi, sa concrétisation pouvant dépendre de facteurs tels que le comportement des utilisateurs, la situation du marché, la situation des droits de l'homme et le cadre réglementaire[52].

28. Ces considérations concurrentes ont donné lieu à des approches réglementaires différentes. En Inde, les préoccupations suscitées par le service « Free Basics » de Facebook ont conduit à l'interdiction de proposer ou de facturer au consommateur des tarifs discriminatoires, c'est-à-dire des tarifs qui diffèrent selon les contenus auxquels ils permettent d'accéder[53]. Le Chili, la Norvège, les Pays-Bas, la Finlande, l'Islande, l'Estonie, la Lettonie, la Lituanie, Malte et le Japon restreignent la non-facturation[54], tandis que les États-Unis, suivis en cela par l'Organe des régulateurs européens des communications électroniques (ORECE), se sont dotés de lignes directrices prévoyant une approche au cas par cas[55]. Les États qui choisissent de se prononcer au cas par cas devraient soigneusement examiner et, au besoin, interdire, tous mécanismes permettant aux prestataires de ne pas facturer les contenus de sociétés affiliées, de subordonner la non-facturation à une rémunération ou de favoriser l'accès à certaines applications d'une catégorie donnée (par exemple en donnant gratuitement accès à tels ou tels services de lecture de musique en continu, mais pas aux autres). De surcroît, les États devraient exiger que les fournisseurs d'accès rendent publiques leurs pratiques de gestion du trafic Internet. À titre d'exemple, le Chili impose à ces sociétés de communiquer les vitesses de connexion à Internet, les

[48] États-Unis d'Amérique, Commission fédérale des communications, *Protecting and Promoting the Open Internet*, FCC 15-24 (12 mars 2015), par. 18. Cette directive, sans doute menacée au moment de l'établissement du présent rapport, reste un modèle utile pour la réglementation de la neutralité du Net.

[49] Erik Stallman et R. Stanley Adams, IV, « Zero Rating: A framework for assessing benefits and harms », Center for Democracy and Technology (janvier 2016).

[50] Ibid., p. 4 et 11.

[51] Barbara van Schewick, « Network neutrality and zero-rating », document soumis à la Commission fédérale des communications des États-Unis (19 février 2014), p. 7.

[52] Erik Stallman et R. Stanley Adams IV, « Zero Rating: A framework for assessing benefits and harms » (janvier 2016), p. 15.

[53] Inde, autorité de réglementation des télécommunications, « TRAI releases the Prohibition of Discriminatory Tariffs for Data Services Regulations, 2016 », communiqué de presse (8 février 2016).

[54] Emily Hong, « A zero sum game? What you should know about zero-rating », New America Weekly, éd. 109 (4 février 2016).

[55] États-Unis, Commission fédérale des communications, *Protecting and Promoting the Open Internet*, FCC 15-24 (12 mars 2015), par. 21. ORECE, *Guidelines on the Implementation by National Regulators of European Net Neutrality* Rules (août 2016) (BoR 16) 127).

différences de prix ou de débit entre les connexions aux niveaux national et international et les garanties de service afférentes[56].

III. Les fournisseurs d'accès au numérique et la liberté d'expression

29. S'il est bien établi que les États sont tenus de respecter et de protéger la liberté d'expression, les acteurs du secteur privé qui fournissent, exploitent et entretiennent l'accès au numérique ont eux aussi un rôle de premier plan à jouer à cet égard.

A. Opérateurs de réseaux de télécommunication et fournisseurs d'accès à Internet

30. Les opérateurs de réseaux de télécommunication et les fournisseurs d'accès à Internet (ensemble, les « prestataires ») offrent une vaste gamme de services. Leurs activités consistent principalement à exploiter les différents réseaux Internet et à en commercialiser l'accès, mais elles permettent également aux utilisateurs de communiquer et de partager des informations par l'intermédiaire des services de téléphonie mobile et fixe (voir A/HRC/32/38, par. 16). Si, dans bien des régions, les prestataires restent des entités publiques, ce sont de plus en plus souvent des sociétés créées et administrées par des acteurs privés qui, de surcroît, sont multinationales : certains des plus grands prestataires au monde exploitent des réseaux dans plusieurs pays et régions, souvent grâce à des partenariats noués avec des entreprises locales ou avec leurs propres filiales.

31. En tant que de contrôleurs de l'accès à de vastes réseaux d'information, les prestataires subissent de fortes pressions de la part des autorités pour se conformer à la censure et aux activités de surveillance. Exploiter un réseau dans un pays donné nécessite une infrastructure considérable, notamment commerciale, et requiert un matériel de réseau et des effectifs importants. Les prestataires sont généralement soumis à la législation nationale et à d'autres obligations en ce qui concerne les licences, obligations qui sont énoncées dans les accords conclus avec l'État. De surcroît, il est arrivé qu'ils fassent l'objet de mesures d'intimidation prises en dehors de tout cadre légal, notamment qu'ils voient la sécurité de leurs employés et de leurs infrastructures menacée en cas de non-respect de leurs obligations[57].

32. Si plusieurs prestataires tentent de résister à la censure et aux demandes de surveillance, nombre d'entre eux prêtent assistance aux autorités sans opposer de véritable résistance. Aux États-Unis, l'un des principaux prestataires aurait créé un « super moteur de recherche » afin de faciliter l'accès des services de police aux appels téléphoniques des abonnés, alors qu'il n'était pas juridiquement tenu de le faire[58]. Au Royaume-Uni, selon une plainte déposée auprès de l'Organisation de coopération et de développement économiques, les principaux prestataires autorisaient les services nationaux de renseignement à accéder à leurs réseaux et aux données de leurs clients dans une mesure bien plus large que celle prévue par la loi de l'époque[59].

33. De plus en plus de prestataires concluent avec des sociétés de médias et d'autres fournisseurs de contenus des accords qui menacent la neutralité du Net et multiplient les pressions pour affaiblir les normes qui garantissent cette neutralité. Ainsi, tandis que les régulateurs européens s'employaient à élaborer des lignes directrices relatives à la neutralité du Net, 17 des principaux prestataires de la région ont publié un « manifeste pour le déploiement de la 5G », dans lequel ils préviennent que l'adoption de lignes directrices

[56] Chili, loi n° 20 453, art. 24 H (D).
[57] Communication du Telecommunications Industry Dialogue, p. 10.
[58] Dave Maass et Aaron Mackey, « Law enforcement's secret "super search engine" amasses trillions of phone records for decades », Electronic Frontier Foundation (29 novembre 2016).
[59] Privacy International, « OECD complaint against BT, Verizon Enterprise, Vodafone Cable, Viatel, Level 3, and Interoute ».

« excessivement contraignantes » retarderaient leur investissement dans la 5G, prochaine génération de la norme de connexion à Internet par réseau mobile[60].

B. Points d'échange Internet

34. Les points d'échange Internet permettent l'échange de trafic Internet entre réseaux gérés par différents prestataires au sein d'un pays ou d'une région donnés[61]. Cette forme d'interconnexion évite au trafic Internet local ou régional de devoir emprunter un itinéraire international, long et détourné, améliorant ainsi la rapidité et l'efficacité de la connexion. Les points d'échange Internet peuvent être mis en place par des opérateurs d'infrastructures Internet et faire partie d'un éventail de services vendus aux prestataires, ou bien être exploités par des organisations à but non lucratif ou à titre bénévole[62].

35. Les points d'échange Internet gèrent un énorme volume de trafic Internet, qui peut être filtré ou intercepté à la demande des autorités. Le fait que la censure et la surveillance soient de plus en plus souvent exercées à partir des points d'échange Internet montre que ceux-ci sont les principaux points de passage des données, même si leur rôle n'est pas clairement défini. Ainsi, en 2013, au Pakistan, l'accès à YouTube a été bloqué d'une manière qui a montré qu'il était filtré depuis des points d'échange Internet, et non par les fournisseurs d'accès, grâce à une méthode appelée « injection de paquets »[63]. La divulgation d'un mémorandum intérieur d'un fournisseur multinational d'accès à Internet exerçant des activités en Équateur a révélé que les utilisateurs n'avaient pas eu accès à Google et à YouTube en mars 2014 parce que l'association des fournisseurs d'accès à Internet équatoriens, organisme privé qui gère deux des principaux points d'échange Internet du pays, bloquait l'accès à certains sites à la demande des autorités[64]. Les informations selon lesquelles l'Office national de sécurité des États-Unis s'est livré à des activités de surveillance de masse font craindre à certains spécialistes que l'Office n'intercepte une grande partie du trafic Internet national et étranger depuis les points d'échange Internet situés aux États-Unis[65]. En septembre 2016, le plus grand point d'échange Internet au monde, situé en Allemagne, a contesté les injonctions qui lui étaient faites par les services allemands de renseignement de surveiller les communications internationales transitant par lui[66].

C. Réseaux de diffusion de contenu

36. Les réseaux de diffusion de contenu sont des réseaux de serveurs déployés à travers le monde pour permettre une diffusion efficace des pages Web et des autres contenus Internet. Les gros producteurs de contenu s'appuient sur ces réseaux pour atteindre le plus grand nombre d'utilisateurs le plus rapidement possible[67]. Les réseaux de diffusion de contenus stockent des copies des contenus hébergés sur les plateformes des producteurs et réorientent les demandes d'accès des utilisateurs depuis ces plateformes vers les serveurs de son réseau qui se trouvent le plus près de l'utilisateur[68]. Ce processus accélère la vitesse de diffusion des contenus, en particulier pour les utilisateurs situés loin des serveurs de la

[60] Communication d'Article 19, p. 9.
[61] Voir www.bgp4.as/internet-exchanges/.
[62] Jason Gerson et Patrick Ryan, « A primer on Internet exchange points for policymakers and non-engineers », Social Science Research Network (12 août 2012), p. 10.
[63] Zubair Nabi, « The anatomy of web censorship in Pakistan» (2013), p. 4.
[64] Katitza Rodriguez, « Leaked documents confirm Ecuador's Internet censorship machine », Electronic Frontier Foundation (14 avril 2016).
[65] Andrew Clement et Jonathan Obar, « Canadian Internet "boomerang" traffic and mass NSA surveillance: Responding to privacy and network sovereignty challenges », dans Law, Privacy and Surveillance in Canada in the Post-Snowden Era, Michael Geist (dir. publ.) (Les Presses de l'Université d'Ottawa, 2015).
[66] De Cix, « Information on the lawsuit against the Federal Republic of Germany » (16 septembre 2016).
[67] Geoff Huston,« The death of transit? », Asia Pacific Network Information Centre (27 octobre 2016).
[68] Vangie Beal, « CDN − Content Delivery Network », *Webopedia*.

plateforme. Les réseaux de diffusion de contenu sont considérés comme un garde-fou efficace contre le blocage des sites Web, les mesures de censure qui visent les serveurs hébergeant un site Web ou une plateforme particulière n'ayant pas d'incidence sur la fourniture aux utilisateurs de copies des contenus recherchés[69]. Les réseaux de diffusion de contenu sont également devenus un garde-fou important contre les perturbations de réseaux. L'accès rapide à Internet a poussé ces réseaux à investir des ressources considérables dans les infrastructures et les services capables de résister aux attaques par déni de service distribué et aux autres attaques malveillantes[70].

37. Parce qu'ils ne sont pas touchés par la censure, les réseaux de diffusion de contenu sont la cible de restrictions disproportionnées de la liberté d'expression. En Égypte, le blocage du site Internet *The New Arab* en août 2016 a perturbé l'accès au contenu d'autres sites qui n'étaient pas affiliés à celui-ci mais utilisaient le même réseau de diffusion de contenu, ce qui a amené les chercheurs à penser que les autorités visaient ce réseau en particulier[71]. En Chine, un filtre national aurait bloqué le réseau de diffusion de contenu EdgeCast, qui gère les contenus d'un certain nombre de grands sites Web du pays[72].

38. De surcroît, étant donné qu'ils traitent de grands volumes de demandes envoyées par des utilisateurs depuis de nombreux sites Web et plateformes, les réseaux de diffusion de contenu sont vulnérables à la surveillance exercée par les autorités. En 2016, par exemple, Amazon Web Services, qui héberge l'un des plus gros réseaux de diffusion de contenu au monde[73], a signalé que le nombre de demandes d'accès à des données présentées par des organismes gouvernementaux avait plus que doublé par rapport à l'année précédente[74]. Selon des chercheurs, les activités de surveillance de masse visent expressément les réseaux de diffusion de contenu, l'objectif étant de recueillir le maximum d'informations, mais on ne sait pas précisément comment cette surveillance s'effectue ni dans quelle mesure les réseaux de diffusion de contenu y participent, le cas échéant[75].

D. Fournisseurs d'équipements de réseau

39. Les fournisseurs d'équipements de réseau fournissent le matériel et les logiciels qui forment la base des réseaux Internet et des réseaux de télécommunications. Les équipements de réseau sont généralement constitués de routeurs, de commutateurs et de points d'accès, qui permettent à plusieurs appareils et réseaux de se connecter les uns aux autres (voir A/HRC/32/38, par. 18). Les fournisseurs d'équipements de réseau ont diversifié leurs activités pour fournir aussi du matériel de voix par le protocole Internet (qui permet d'effectuer des appels sans fil) et un accès à la technologie de l'Internet des objets (qui permet de connecter entre eux des appareils intelligents)[76]. Ils s'adressent rarement au consommateur : leurs principaux clients sont des opérateurs de réseaux, comme les États, les fournisseurs d'accès à Internet et les réseaux de diffusion de contenu. Ils doivent donc configurer les réseaux selon les caractéristiques techniques spécifiées par ces opérateurs, et notamment celles imposées par la législation locale (par exemple en ce qui concerne l'ordre public et la sécurité nationale). Cela étant, ils peuvent concevoir ou modifier le matériel et la technologie afin de les rendre conformes aux exigences des acteurs privés ou des États.

[69] John Holowczak et Amir Houmansadr, « CacheBrowser: bypassing Chinese censorship without proxies using cached content » (2015).

[70] Geoff Huston, « The death of transit? », Asia Pacific Network Information Centre (27 octobre 2016).

[71] Leonid Evdokimov et Vasilis Ververis, « Egypt: Media censorship, Tor interference, HTTPS throttling and ads injections? », Open Observatory of Network Interference (27 octobre 2016).

[72] Joss Wright, « A quick investigation of EdgeCast CDN blocking in China », blog, Oxford Internet Institute (18 novembre 2014).

[73] Au moment de la rédaction du présent rapport, Amazon Cloudfront hébergeait le plus grand nombre de domaines de site Internet au monde.

[74] Amazon Information Request Report (juin 2016).

[75] Voir par exemple, Harrison Weber, « How the NSA & FBI made Facebook the perfect mass surveillance tool », *Venture Beat* (15 mai 2014).

[76] Michael E. Raynor et Phil Wilson, « Beyond the dumb pipe: The IoT and the new role for network service providers », Deloitte University Press (2 septembre 2015).

40. Compte tenu de la manière dont ils fonctionnent, les fournisseurs d'équipements de réseau doivent tenir compte des problèmes que leurs clients ont créés ou auxquels ils font face en ce qui concerne le respect des droits de l'homme. Pour ce qui est de la surveillance, ils sont souvent visés par des mesures « d'interception légale », qui les contraignent à configurer les réseaux de manière à ce que les autorités puissent accéder aux donnés des utilisateurs [77]. En outre, ils peuvent se voir demander de créer des « systèmes d'administration et de médiation » facilitant le partage des données interceptées entre l'opérateur réseau et les autorités, ainsi que de concevoir les systèmes utilisés par ces dernières pour traiter les données interceptées[78]. Lorsqu'ils gèrent les réseaux qu'ils ont créés, les fournisseurs d'équipements de réseau peuvent aussi être chargés de répondre, pour le compte de l'opérateur, aux demandes d'accès aux données d'utilisateurs présentées par les autorités[79].

41. La conception de technologies et d'équipements de réseau à usages multiples soulève des questions au regard de la liberté d'expression et du respect de la vie privée. Les dispositifs d'inspection des paquets en profondeur, par exemple, sont utilisés à des fins techniques anodines, comme la gestion des encombrements sur les réseaux, mais peuvent également être employés pour filtrer des contenus Internet, intercepter des communications et bloquer des flux de données. Les réseaux mobiles sont configurés pour localiser les téléphones portables en temps réel afin que les services mobiles soient accessibles partout, mais cette capacité de localisation peut aussi être utilisée au détriment des utilisateurs[80].

42. Certaines informations permettent de penser que les fournisseurs d'équipements de réseau peuvent aider les autorités à censurer et à surveiller le trafic. Dans une affaire jugée aux États-Unis, Cisco est accusé d'avoir conçu et mis en place et d'avoir contribué à opérer un réseau de surveillance et de sécurité intérieure chinois baptisé *Golden Shield* [81] (La société conteste ces allégations[82]). En Éthiopie, des groupes de défense des droits de l'homme ont constaté que la société ZTE avait conçu et installé, pour le compte d'Ethio Telecom, une base de données clients permettant une surveillance intrusive[83].

E. Autres acteurs privés

43. Les constats et recommandations formulés dans le présent rapport s'appliquent à toute entité fournissant un accès numérique de l'une des manières décrites plus haut. Un nombre croissant de sociétés Internet ajoutent la fourniture d'importants services numérique et services d'infrastructure à leurs prestations. Par exemple, Alibaba et Tencent, deux des plus grands fournisseurs de services Internet chinois, proposent à présent des services de diffusion de contenus [84]. Google teste actuellement des procédés devant permettre d'accéder à des réseaux sans fil sans passer les fournisseurs d'accès traditionnels ; en 2010, dans certaines villes des États-Unis, la société a mis à la disposition des particuliers et des entreprises un service de connexion à Internet à grande vitesse[85]. Google travaille en outre avec Facebook et Microsoft à la construction de réseaux câblés

[77] Voir, par exemple, la résolution du Conseil de l'Union européenne du 17 janvier 1995 relative à l'interception légale des télécommunications, Journal officiel n° C 329 ; et communication de *Privacy International*, p. 2 et 3.

[78] IHRB, « Human rights challenges of telecommunications vendors: addressing the possible misuse of telecommunications systems: case study: Ericsson (novembre 2014), p. 16.

[79] Ibid., p. 17.

[80] Ibid., p. 13.

[81] United States District Court for the Northern District of California, San Jose Division, *Doe et al. v. Cisco Systems, Inc. et al.*, affaire n° 5:11-cv-02449-EJD-PSGx (18 septembre 2013).

[82] John Earnhardt, « Cisco Q&A on China and censorship », blogs Cisco (2 mars 2006).

[83] Human Rights Watch, « They know everything we do: telecom and Internet surveillance in Ethiopia » (25 mars 2014).

[84] Tencent Cloud CDN et Alibaba Cloud CDN.

[85] Klint Finley, « Google eyes blazing-fast wireless as a way into your home », *Wired* (12 août 2016).

sous-marins qui leur permettraient de relier les utilisateurs sans avoir besoin de matériel ou de systèmes appartenant à des tiers[86].

44. Bien qu'ils ne soient pas à proprement parler des acteurs du secteur, ce sont les organismes de normalisation qui établissent les protocoles et les normes techniques qui permettent l'interopérabilité des infrastructures des télécommunications et des infrastructures Internet. Or, les normes ne tenant pas compte des impératifs liés aux droits de l'homme peuvent porter atteinte à la liberté d'expression. Ainsi, le fait que le protocole HTTP ne soit pas toujours sécurisé au moyen du protocole TLS a rendu le trafic sur le Web vulnérable à la censure et à la surveillance. Les efforts déployés par le secteur des technologies pour prendre toutes les précautions qui s'imposent à l'égard des droits de l'homme lors de l'élaboration de normes constituent donc un pas dans la bonne direction[87].

IV. Responsabilités des fournisseurs d'accès numérique en matière de droits de l'homme

45. Les Principes directeurs relatifs aux entreprises et aux droits de l'homme posent que les entreprises doivent respecter les droits de l'homme indépendamment des obligations faites aux États et du respect de ces obligations (voir A/HRC/17/31, annexe ; et A/HRC/32/38, par. 9 et 10). Ils définissent le seuil de responsabilité des entreprises en ce qui concerne le respect des droits de l'homme, encourageant celles-ci à s'engager publiquement à respecter ces droits en publiant une déclaration de principe approuvée par leurs hauts responsables, à se doter de procédures de diligence raisonnable visant à déceler, prévenir et atténuer les conséquences réelles et potentielles de leurs activités sur les droits de l'homme et à faire en sorte qu'il en soit tenu compte, et à remédier aux incidences négatives de leurs activités sur les droits de l'homme ou à contribuer aux efforts déployés à cet effet (voir A/HRC/17/31, annexe, principes 16 à 24).

A. Considérations contextuelles

46. Les Principes directeurs mettent l'accent sur le fait que, pour s'acquitter de leurs responsabilités en matière de droits de l'homme, les entreprises doivent tenir compte des particularités du contexte dans lequel elles exercent leurs activités (ibid.). Dans le secteur de l'accès numérique, ce contexte peut varier et il convient donc d'examiner différentes situations.

Les fournisseurs d'accès fournissent un service public

47. Le secteur de l'accès numérique relève du domaine de l'expression numérique ; sa viabilité commerciale dépend des utilisateurs qui cherchent, reçoivent et diffusent des informations et des idées sur les réseaux qu'il crée et exploite. Les réseaux appartenant à des acteurs privés étant aujourd'hui des outils indispensables à l'exercice de la liberté d'expression, leurs opérateurs ont une fonction sociale et publique éminemment importante. Qu'elles répondent à une demande des pouvoirs publics ou à des intérêts commerciaux, les décisions prises par les acteurs du secteur peuvent avoir un effet direct, positif ou négatif, sur la liberté d'expression et les droits qui y sont associés.

Les restrictions à l'accès à Internet ont des incidences mondiales sur la liberté d'expression

48. Les conséquences que les activités des entreprises du secteur ont sur les droits de l'homme sont souvent d'envergure mondiale en ce qu'elles touchent même des utilisateurs

[86] Joon Ian Wong, « Google and Facebook are doubling down on Internet infrastructure with a new Pacific cable », *Quartz* (17 octobre 2016).

[87] Internet Research Task Force, « Research into human rights protocol considerations 》(25 février 2017), disponible à l'adresse https://datatracker.ietf.org/doc/draft-irtf-hrpc-research/?include_text=1. L'annexe supplémentaire contient une analyse plus détaillée des rôles et responsabilités des organismes de normalisation.

qui sont en dehors des marchés sur lesquels l'entreprise concernée est présente. Par exemple, la surveillance d'un point d'échange Internet situé aux États-Unis peut permettre de capter de vastes flux de communications échangées entre des personnes se trouvant aux États-Unis et des personnes se trouvant dans d'autres pays, voire seulement entre des personnes se trouvant dans d'autres pays. Dans le même ordre d'idées, les failles dans la sécurité d'un réseau ont une incidence sur tous les utilisateurs qui utilisent ce réseau, y compris ceux qui se trouvent loin de celui-ci. Les entreprises devraient donc recenser les conséquences que leurs activités ont sur la liberté d'expression dans le monde et trouver des solutions pour y faire face, sans se limiter aux activités ayant un effet sur les clients et les titulaires de droits présents sur les marchés sur lesquels elles interviennent. Cela étant, les mesures à prendre à cet effet varient en fonction de la taille, des ressources, du régime de propriété, de la structure et du cadre de fonctionnement de l'entreprise (ibid., principe 14). Par exemple, tous les fournisseurs devraient vérifier que les demandes de données d'utilisateurs satisfont à un minimum de conditions, indépendamment de leur origine ou de l'utilisateur concerné. Mais, si une multinationale peut disposer d'équipes expressément chargées de ces vérifications, un fournisseur de petite ou moyenne taille confiera peut-être celles-ci à ses juristes ou à son groupe chargé des relations avec les pouvoirs publics.

Le secteur est vulnérable aux pressions exercées par l'État pour restreindre la liberté d'expression…

49. Les Principes directeurs ont pour objet de combler les lacunes qui existent dans le respect du principe de responsabilité par les entreprises du fait de l'absence de législation nationale ou de la non-application de la législation existante[88]. Il se peut toutefois qu'une application énergique de la législation interne pose des problèmes en ce qui concerne les droits de l'homme dans le secteur du numérique. Ainsi, les États peuvent tenir les fournisseurs pour responsables des contenus affichés par les utilisateurs sur leurs réseaux, ou encore faire pression sur eux pour qu'ils restreignent ces contenus en vertu de lois destinées à réprimer des infractions allant du discours haineux à la diffamation, en passant par la cybercriminalité et le lèse-majesté. Or, cette responsabilité des intermédiaires incite fortement à la censure, les fournisseurs pouvant estimer qu'il est plus risqué de contester la loi que de limiter les contenus à ce point strictement que l'expression légitime et licite s'en trouve restreinte. La pression exercée sur les entreprises pour qu'elles aident l'État à censurer et à surveiller le trafic prend encore davantage d'ampleur lorsque les autorités harcèlent, menacent ou arrêtent des employés ou tentent de faire intrusion dans les réseaux ou les équipements de l'entreprise[89].

... mais est néanmoins particulièrement bien placé pour faire respecter les droits des utilisateurs.

50. En étant à la fois la porte d'accès au numérique et, donc, la cible de restrictions imposées par les pouvoirs publics, le secteur joue un rôle de garde-fou particulièrement important lorsqu'il s'agit d'empêcher tant les autorités que les acteurs privés d'outrepasser leurs pouvoirs. Ainsi, les prestataires sont généralement les mieux placés pour s'opposer à une interruption de service ou une demande de données d'utilisateurs. Les réseaux de distribution de contenus occupent dans l'infrastructure Internet une place stratégique pour contrer les attaques malveillantes qui perturbent l'accès aux services, et les fournisseurs sont les mieux à même de déterminer si leurs produits sont ou seront utilisés en vue de porter atteinte aux droits de l'homme, notamment lorsqu'ils effectuent des audits préalables de vente et des activités de maintenance.

[88] Yael Ronen, « Big Brother's little helpers: the right to privacy and the responsibility of Internet service providers », *Utrecht Journal of International and European Law*, vol. 31, n° 80 (février 2015), p. 76.

[89] En 2014, une demande de fermeture de réseau adressée à Orange, prestataire multinational de télécommunications, par les autorités de la République centrafricaine aurait été accompagnée de menaces de sanctions individuelles pour le cas où l'entreprise n'obtempérerait pas. Voir la communication du *Telecommunications Industry Dialogue*, p. 11.

B. Responsabilité en ce qui concerne le respect de la liberté d'expression des utilisateurs

51. Pour respecter ses engagements en matière de droits de l'homme, le secteur du numérique devrait allouer les ressources voulues à certaines mesures parmi lesquelles, au minimum, celles décrites ci-après. Bien que les principes qui sous-tendent ces mesures soient envisagés dans le contexte de l'accès numérique, ils s'appliquent aussi aux autres secteurs de l'économie numérique, et notamment aux réseaux sociaux, au commerce en ligne, et à la surveillance et aux recherches électroniques.

1. Diligence raisonnable

52. La diligence raisonnable permet aux fournisseurs d'accès numérique de cerner, de prévenir et d'atténuer les effets de leurs activités sur le respect des droits de l'homme (voir A/HRC/17/31, annexe, principe 19). S'il n'est ni possible ni recommandable d'adopter une démarche unique en ce qui concerne la diligence raisonnable, le fait pour les fournisseurs d'évaluer l'incidence de leurs activités sur le respect des droits de l'homme permet néanmoins d'apprécier les risques auxquels la liberté d'expression et le droit à la vie privée sont exposés et de prendre des mesures pour y remédier[90]. La diligence raisonnable doit répondre aux exigences minimales suivantes.

Règles régissant les procédures de diligence raisonnable

53. Les entreprises devraient élaborer des critères clairs et précis permettant de déterminer quelles activités risquent de porter atteinte à la liberté d'expression et nécessitent une procédure de diligence raisonnable[91]. Les effets − passés et présents − des activités de l'entreprise sur le respect des droits de l'homme sont des indicateurs utiles, de même que la pratique du secteur. Dans le secteur du numérique, les activités en question peuvent être des fusions-acquisitions ; des entrées sur le marché ou des sorties de marché ; des demandes de restriction de contenu ou de données d'utilisateurs émanant des autorités ou d'autres acteurs ; l'élaboration ou la modification des politiques relatives à la restriction des contenus et au respect de la vie privée ; des modifications de produits liées à la modération des contenus ou au cryptage des communications ; le fait de faciliter l'accès prioritaire à certains contenus et certaines applications Internet plutôt qu'à d'autres ; et la conception, la vente et l'achat de matériel et de technologies d'interception et de filtrage du trafic réseau et de services de formation et de conseil y relatifs[92]. Cette liste, loin d'être exhaustive, doit faire l'objet de mises à jour régulières tenant compte de l'évolution des activités commerciales, des technologies et des milieux dans lesquels les entreprises exercent leurs activités[93].

Points à examiner

54. Les procédures de diligence raisonnable devraient comprendre un examen de plusieurs éléments, parmi lesquels, au minimum : les lois et normes locales et internationales applicables, et notamment les éventuels conflits entre les lois locales et les droits de l'homme ; les risques que les produits et services fournis par l'entreprise font peser sur la liberté d'expression et le droit à la vie privée ; les stratégies destinées à atténuer et à prévenir ces risques ; les limites à l'efficacité de ces stratégies qui découlent de

[90] Parmi les principaux fournisseurs de télécommunications, on compte Telia Company et Telefonica. Ibid., p. 7 et 8.

[91] Nokia a intégré à son outil de vente un dispositif automatique qui signale les risques que les ventes potentielles représentent pour le respect des droits de l'homme. Ibid., p. 7.

[92] Commission européenne, *ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights* (2013), p. 32 à 36.

[93] Michael A. Samway, « Business, human rights and the Internet: a framework for implementation », dans *Human Dignity and the Future of Global Institutions*, Mark P. Lagon et Anthony Clark Arend (dir. publ.)(Washington, D.C., Georgetown University Press, 2014), p. 308.

l'environnement juridique, réglementaire et opérationnel de l'entreprise ; les possibilités de promouvoir les droits de l'homme grâce aux activités de l'entreprise[94].

Procédures et formations internes

55. S'il est important pour une société d'être dotée de commerciaux et de spécialistes des questions liées aux droits de l'homme dynamiques, les mesures de diligence raisonnable ne devraient pas être la responsabilité de ces seules personnes ; les différents groupes fonctionnels concernés devraient y participer aussi. Pour cela, il faut établir un dialogue et une collaboration entre les différentes unités de l'entreprise (respect de la vie privée, respect des lois, relations avec les autorités, conformité aux normes, gestion des risques, conception de produits et opérations) et les spécialistes (ingénieurs, chercheurs dans le domaine de l'expérience des utilisateurs, commerciaux et directeurs)[95]. Les chercheurs ont constaté que rendre les chefs d'unité responsables des démarches visant à assurer la protection de la vie privée et les y faire participer, et placer dans les différentes unités des employés dotés de compétences dans ce domaine et personnellement chargés de veiller au respect de la vie privée, avait pour effet de créer un environnement favorable au respect de la vie privée[96]. Ce type de pratique pourrait également favoriser le respect de la liberté d'expression par les entreprises. Dans les petites et moyennes entreprises, cela pourrait nécessiter la participation de l'ensemble du personnel aux procédures de diligence raisonnable[97].

Compétences extérieures

56. Étant donné l'ampleur des connaissances qu'elles exigent, les procédures de diligence raisonnable devraient faire intervenir des entités extérieures et non étatiques, notamment la société civile locale, les organisations internationales des droits de l'homme, les mécanismes des droits de l'homme des organisations internationales et régionales, et les milieux techniques et universitaires. Les forums multipartites sont également l'occasion de partager des connaissances et de veiller à ce que le principe de responsabilité soit mutuellement appliqué. Ainsi, des chercheurs ont constaté que le fait de participer à des projets visant à promouvoir les droits de l'homme dans le cadre d'un secteur donné, comme le *Global Network Initiative* et le *Telecommunications Industry Dialogue*, avait une influence sur la mesure dans laquelle l'entreprise respectait les droits de l'homme[98].

Consultations avec les utilisateurs et les titulaires de droits concernés

57. Tous les fournisseurs d'accès numérique influent, d'une manière ou d'une autre, sur la liberté d'expression des utilisateurs finaux. Par conséquent, même les entreprises qui ne sont pas en contact avec les consommateurs devraient consulter ces utilisateurs aux fins de l'établissement de leur procédure d'évaluation des risques. Il ne s'agit pas de recourir aux larges forums multipartites mentionnés plus haut, mais plutôt d'établir un dialogue à double sens afin de recueillir les avis et conseils particuliers des parties prenantes concernées (ou de leurs représentants), avis et conseils qui seront ensuite pris en compte dans les procédures de prise de décisions et les activités de l'entreprise[99]. On pourrait ainsi, par exemple, consulter des personnes et groupes vulnérables ou marginalisés lors de négociations relatives à l'octroi de licences dans des environnements à haut risque ou lors de la conception, de la mise à l'essai et du lancement de politiques de non-facturation. Pour que les consultations fassent sens, il faudrait qu'elles supposent un dialogue régulier avec

[94] Ibid., p. 310 à 312, pour un aperçu plus complet des domaines que les procédures de diligence raisonnable devraient couvrir.

[95] Commission européenne, *ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights* (2013), p. 36.

[96] Kenneth A. Bamberger et Deirdre K. Mulligan, *Privacy on the Ground: Driving Corporate Behavior in the United States and Europe* (Cambridge, Massachusetts, MIT Press, 2015), p. 177.

[97] Commission européenne, *ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights* (2013), p. 37.

[98] Communication de *Ranking Digital Rights*, p. 5.

[99] Commission européenne, *ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights* (2013), p. 37 et 38.

les organisations de la société civile, qui peuvent exprimer les besoins et défendre les intérêts des utilisateurs finaux dans tel ou tel groupe de population et risquent elles-mêmes d'être exposées à des pressions particulières du fait de leurs activités de sensibilisation.

Évaluations dynamiques continues

58. Les entreprises devraient rapidement adapter leurs procédures de diligence raisonnable en fonction de l'évolution des circonstances ou du contexte dans lequel elles exercent leurs activités. Ainsi, l'évaluation des risques devrait se poursuivre après la phase de conception et avoir lieu à intervalles réguliers tout au long de la vie du produit ou du service, compte étant tenu de facteurs tels que l'évolution des technologies et des infrastructures et les failles qu'elle fait naître en matière de sécurité, les changements dans le comportement des consommateurs et l'évolution de l'environnement juridique, politique et social dans lequel les entreprises travaillent[100].

2. Incorporation de mesures de protection des droits de l'homme dès la conception

59. Comme c'est le cas pour toute évolution technologique de grande ampleur, les choix de conception et de fabrication reflètent les politiques gouvernementales et devraient être guidés par le respect des droits de l'homme. Ainsi, le découpage en tranches, élément clé de la technologie 5G, pourrait permettre aux opérateurs mobiles de gérer plus efficacement le trafic et de répondre aux besoins des consommateurs, qui se diversifient avec le développement de l'Internet des objets. Dans le même temps, les réseaux pourraient aussi être « découpés » en voies plus ou moins rapides afin de faciliter l'accès à certaines applications plutôt qu'à d'autres, au risque d'interférer avec la neutralité du Net. Les entreprises devraient par conséquent veiller à concevoir et déployer les nouveaux équipements et technologies de réseaux − notamment ceux destinés à des usages multiples − dans le respect des normes relatives à la liberté d'expression et à la protection de la vie privée[101].

60. Les entreprises devraient participer activement à la mise en place de mécanismes de protection de la liberté d'expression et de la vie privée. Par exemple, il faudrait faire en sorte que les dispositifs de sécurité numérique servant à détecter et prévenir les attaques par déni de service distribué et le piratage ciblent le trafic malveillant sans compromettre les échanges légitimes entre personnes, organisations et groupes de population. Configurer les équipements de réseau de façon à ce que les informations recueillies sur les utilisateurs soient réduites au strict minimum requis − compte étant tenu de la législation locale et des besoins en ce qui concerne le routage des données − empêche de recevoir des demandes de données dépassant les limites raisonnables, les entreprises ne pouvant pas fournir des informations dont elles ne disposent pas[102]. Même lorsque des données d'utilisateurs sont enregistrées, il est possible de limiter la durée pendant laquelle elles sont conservées, le cas échéant, ce qui restreint la quantité d'informations personnelles et sensibles accessibles à des tiers.

3. Engagement des parties prenantes

61. L'engagement des pouvoirs publics, des entreprises partenaires et des autres parties prenantes en faveur des droits de l'homme peut à long terme permettre de prévenir ou d'atténuer les violations des droits de l'homme. Les entreprises qui traitent directement avec les autorités devraient faire pression pour que les licences d'exploitation et les contrats de vente comportent des dispositions visant à protéger les droits de l'homme, et notamment à garantir que personne ne peut accéder aux équipements de réseau ni les modifier (potentiellement dans le but de faciliter la perpétration de violations des droits de l'homme) à leur insu. Intervenir dans une procédure judiciaire (par exemple à titre d'*amicus curiae*

[100] Business and Social Responsibility, « Applying the Guiding Principles on Business and Human Rights to the ICT industry », version 2.0: *Ten lessons learned, A briefing paper* (septembre 2012), p. 9.

[101] Article 19, « Our 5G future: Light at the end of the tunnel or Internet fast-lane for the elite? » (15 septembre 2016).

[102] Electronic Frontier Foundation, « User privacy for ISPs and accidental ISPs ».

dans un procès engagé par un groupe de la société civile ou une entreprise pour protester contre une loi de surveillance ou de censure) et plaider la cause des droits de l'homme auprès du gouvernement et du parlement peut aussi permettre de renforcer la protection juridique de la liberté d'expression et du droit à la vie privée.

62. Les accords conclus avec des partenaires devraient permettre à toutes les parties de s'acquitter de leurs responsabilités au regard des droits de l'homme. Ils devraient en particulier être conçus de manière à ce que les filiales, les coentreprises partenaires, les fournisseurs et les distributeurs soient tenus de se conformer à toutes les mesures de protection de la liberté d'expression et de la vie privée adoptées par l'entreprise. Par exemple, les entreprises devraient prévoir dans leur règlement que les demandes de censure ou de surveillance adressées aux opérateurs locaux qui n'entrent pas dans le cadre habituel doivent être envoyées à la direction centrale pour examen[103]. Des dispositifs de protection des lanceurs d'alerte devraient être établis à l'intention des employés et des sous-traitants. Les entreprises qui entretiennent des relations commerciales suscitant des préoccupations au regard des droits de l'homme devraient s'attacher à prendre des mesures à long terme visant à prévenir ou atténuer les violations[104].

63. Les entreprises peuvent également promouvoir le respect des droits de l'homme en collaborant avec d'autres entités, notamment en menant des activités de communication et de sensibilisation d'autres entreprises du secteur ; en travaillant avec des entités régionales et internationales, y compris des mécanismes de promotion des droits de l'homme et des organisations économiques ; et en se joignant à des associations professionnelles et en participant à des initiatives faisant intervenir divers partenaires[105]. La tenue de consultations régulières avec les utilisateurs, la société civile et les victimes de violations des droits de l'homme peut permettre de mobiliser le public en faveur des efforts déployés pour lutter contre l'ingérence des autorités. La coopération intersectorielle est aussi utile en ce que les pratiques optimales et normes ont d'autant plus de poids qu'elles sont largement acceptées, ce qui fait que les autorités et les entreprises du secteur sont davantage poussées à les respecter.

4. Stratégies d'atténuation[106]

64. Dans la mesure où elles se voient demander de contrôler les contenus et de communiquer des données d'utilisateurs, les entreprises peuvent adopter des politiques et pratiques visant à atténuer les effets préjudiciables des restrictions imposées par les autorités.

Veiller à ce que les demandes de restriction des contenus et les demandes de communication de données d'utilisateurs soient rigoureusement conformes à la loi

65. Les entreprises devraient veiller à ce que toutes les demandes de restriction de contenus et de communication de données d'utilisateurs respectent non seulement les règles et procédures définies dans la législation locale, mais aussi les garanties internationales d'une procédure régulière[107]. Étant donné qu'elles empiètent sur les droits de l'homme, ces demandes devraient être approuvées par des tribunaux ou d'autres mécanismes juridictionnels indépendants et impartiaux. De plus, les entreprises devraient exiger qu'elles soient formulées par écrit, soient accompagnées d'une description précise du fondement juridique sur lesquelles elles reposent, et portent le nom, la qualité et la signature de la

[103] Communication du Telecommunications Industry Dialogue, p. 13 et 16.

[104] SHIFT, « Using leverage in business relationships to reduce human rights risks » (New York, novembre 2013).

[105] Communication du Telecommunications Industry Dialogue, p. 12; et communication de l'Initiative mondiale des réseaux, p. 7.

[106] Les orientations données dans cette section sont largement inspirées de la communication du Telecommunications Industry Dialogue et des directives de mise en œuvre des principes de liberté d'expression et de respect de la vie privée de l'Initiative mondiale des réseaux.

[107] Voir, par exemple, les Principes de Manille sur la responsabilité des intermédiaires et les Principes internationaux sur l'application des droits de l'homme à la surveillance des communications, établis conjointement par plusieurs organisations non gouvernementales.

personne dont elles émanent. Les entreprises devraient en outre s'assurer que l'agent ou organisme de l'État ayant formulé la demande était habilité à ce faire[108]. Ces formalités devraient être exigées même si elles ne sont pas imposées par la loi. De surcroît, pour toutes les demandes, les entreprises devraient systématiquement conserver une trace écrite de leurs échanges avec l'auteur et un historique de l'accès aux données d'utilisateurs, à condition que cela ne risque pas de compromettre le droit à la vie privée[109].

Interpréter la portée des demandes des pouvoirs publics et le champ d'application de la législation

66. Lorsque les demandes des pouvoirs publics et les dispositions juridiques applicables manquent de clarté, les entreprises ont du mal à déterminer si elles agissent en conformité avec la législation locale. Elles peuvent toutefois atténuer ce problème en adoptant des règlements prévoyant que toutes leurs unités, y compris les filiales locales, doivent faire en sorte que toute ambiguïté dans la loi soient interprétée en faveur de la liberté d'expression et du respect du droit à la vie privée et des autres droits de l'homme. Pareils règlements devraient s'appuyer non seulement sur les responsabilités mises à la charge des prestataires au regard des droits de l'homme, mais aussi sur l'obligation faite aux États de respecter la législation applicable en la matière et les mesures de protection inscrites dans la législation locale (lois constitutionnelles, lois de procédure pénale et lois relatives à la protection des données).

67. Dans la pratique, les entreprises devraient, autant que possible, interpréter les demandes de façon à limiter au minimum les restrictions appliquées aux contenus et l'accès aux données d'utilisateurs. Ainsi, l'Initiative mondiale des réseaux recommande aux entreprises saisies de demandes trop générales de demander des précisions et d'exiger que les modifications qui s'imposent soient apportées[110].

Contester des demandes et les lois sur lesquelles elles reposent

68. Les entreprises ont tout intérêt à exercer leurs activités dans un environnement juridique respectueux des droits de l'homme, des garanties de procédure et de l'état de droit. Elles devraient étudier tous les moyens que la loi met à leur disposition pour contester les demandes dont la portée est excessive, telles que celles visant à faire bloquer l'accès à des plateformes ou des services tout entiers, à faire fermer des sites Web dans le but manifeste de passer sous silence les critiques et les opinions dissidentes, ou à obtenir des données excessivement générales concernant des utilisateurs non spécifiés[111].

69. Comme chaque fois qu'elles décident d'engager une action en justice, les entreprises pourraient tenir compte d'une série de critères tels que « l'impact bénéfique potentiel sur le respect [des droits de l'homme], la probabilité de succès, la gravité du cas, le coût, la représentativité du cas et son éventuelle association à un mouvement plus large[112] ». Cela étant, pour prendre leur décision, elles devraient accorder un grand poids aux considérations relatives aux droits de l'homme et soigneusement apprécier tant les avantages qu'il y aurait à engager une procédure que les risques que cela ferait naître sur le plan des droits de l'homme. Elles pourraient ainsi juger opportun de contester les demandes trop générales lorsqu'elles sont raisonnablement sûres d'obtenir gain de cause, même s'il faut pour cela mobiliser des ressources importantes, mais préférer une autre solution si engager une action en justice risque de créer un précédent négatif, de susciter des protestations ou de nuire au respect de la liberté d'expression et de la vie privée.

[108] Initiative mondiale des réseaux, directives de mise en œuvre des principes de liberté d'expression et de respect de la vie privée, p. 5 et 6 ; voir également communication du Telecommunications Industry Dialogue, p. 8 à 10.

[109] Communication du Telecommunications Industry Dialogue, p. 8 et 9.

[110] Ibid.

[111] Yael Ronen, « Big Brother's little helpers » (février 2015), p. 81.

5. Transparence

70. La transparence est au cœur de la responsabilité qui incombe aux acteurs du numérique en ce qui concerne le respect des droits de l'homme. Le public devrait être informé, dans toute la mesure permise par la loi, des activités des pouvoirs publics qui nécessitent l'assistance ou la participation des entreprises. Les entreprises devraient cependant être conscientes du fait que les informations communiquées sont principalement utilisées par la société civile pour saisir la justice de violations des droits de l'homme, déposer plainte auprès de mécanismes nationaux ou internationaux pour le compte d'utilisateurs, ou faire appliquer le principe de responsabilité de toute autre manière. La communication devrait donc être régulière et constante et se faire d'une manière accessible, les informations étant dûment placées dans leur contexte.

71. Même si la législation locale n'autorise pas une transparence complète, les entreprises devraient rendre publiques toutes les informations pouvant être rendues publiques qui méritent de l'être. Ainsi, si elles ne sont pas autorisées à divulguer l'origine ou le motif d'une demande de fermeture, elles devraient néanmoins tâcher de tenir le public régulièrement informé de toute interruption ou tout rétablissement de services et des mesures prises pour résoudre le problème, et fournir, après coup, des explications sur ce qui s'est passé. Des mesures de transparence innovantes, telles que la publication de données consolidées et la rétention sélective d'informations[113], permettent en outre d'atténuer les effets des lois et décisions interdisant la divulgation d'informations. Les entreprises devraient révéler à quelles lois locales elles se conforment et, lorsque cela est possible, contester toutes lois et tous règlements nuisant à la transparence vis-à-vis des utilisateurs et du public en général[114].

72. Les entreprises devraient rendre publiques les procédures et mesures qu'elles adoptent pour protéger la liberté d'expression, en particulier en ce qui concerne la conservation et l'utilisation des données, la gestion des réseaux et la vente et l'achat de technologies de filtrage et d'interception[115]. Elles devraient également divulguer la fréquence, la portée et l'objet des procédures de diligence raisonnable, ainsi qu'un résumé des conclusions adoptées à haut niveau. De façon générale, elles devraient consulter les ressources toujours plus nombreuses consacrées à l'étude des indicateurs de transparence et des pratiques optimales en ce qui concerne la transparence. Les mesures de transparence devraient être élaborées et mises en œuvre après consultation des utilisateurs, de la société civile et des autres entreprises du secteur.

6. Recours utiles

73. Si certains aspects de la responsabilité des entreprises ont évolué ces dernières années, la question des recours semble néanmoins rarement faire partie des préoccupations du secteur privé. Or, les recours sont un pilier du principe de la responsabilité des entreprises, et doivent être accessibles lorsque les activités d'une société « ont eu des incidences négatives » (voir A/HRC/17/31, annexe, principe 22). C'est aux États qu'il incombe au premier chef de remédier aux violations des droits de l'homme commises par les entreprises, particulièrement lorsqu'ils en sont à l'origine, par exemple parce qu'ils ont imposé des restrictions de contenu excessives, ont illégalement requis la communication de données d'utilisateurs ou ont exercé une surveillance disproportionnée. Cela étant, les entreprises qui n'adoptent pas les procédures de diligence et autres garde-fous voulus peuvent également être à l'origine de violations des droits de l'homme ou contribuer à pareilles violations. Elles devraient alors « prévoir des mesures de réparation ou collaborer à leur mise en œuvre suivant des procédures légitimes » (ibid.).

74. Les voies de recours peuvent permettre d'obtenir une indemnisation ou une autre forme de réparation (ibid., principe 27). En cas de restriction à la liberté d'expression, les

[113] Par exemple, lorsque l'entreprise Telia s'est vue ordonner de suspendre ses services, elle n'a pas indiqué que la suspension était due à des problèmes techniques, communication du Telecommunications Industry Dialogue, p. 14.

[114] Telecommunications Industry Dialogue, « Information on country legal frameworks pertaining to freedom of expression and privacy in telecommunications » (2016).

[115] Communication de Ranking Digital Rights.

réparations peuvent comprendre l'accès à un mécanisme de plainte, la communication d'informations concernant la violation et la formulation de garanties de non-répétition[116]. Il se peut que les utilisateurs dont les comptes ont été fermés abusivement souhaitent avoir la satisfaction d'être entendus et de se voir donner des explications et des garanties de non-répétition[117].

75. De surcroît, les politiques et mécanismes existants pourraient être révisés ou renforcés de façon à limiter les violations de la liberté d'expression. Par exemple, un prestataire pourrait améliorer sa politique de restriction des contenus et mieux former ses équipes de modération afin de réduire les risques de fermeture injustifiée de sites Web ou de restriction excessive des contenus, et notamment de filtrage. Les mécanismes de plainte mis à la disposition des consommateurs pourraient également être améliorés en vue de donner aux utilisateurs la possibilité de mettre en évidence les pratiques de gestion du trafic, les modes de filtrage commercial et les autres restrictions de contenu qu'ils jugent excessifs ou injustes.

V. Conclusions et recommandations

76. **L'exercice de droits individuels fondamentaux tels que le droit à la liberté d'opinion et d'expression, le droit à la vie et divers droits économiques, sociaux et culturels est dépendant de l'accès au numérique. Or, cet accès est régulièrement entravé par des obstacles tels que des coupures de service et l'exercice d'une surveillance. Le présent rapport est essentiellement consacré aux moyens d'empêcher ou de dissuader les particuliers de s'exprimer en pratiquant la censure numérique, et ne traite pas des autres obstacles à la liberté d'expression, tels que l'insuffisance des infrastructures de connexion, l'application par les pouvoirs publics de tarifs d'accès élevés, les inégalités entre les sexes et les barrières linguistiques, qui peuvent aussi s'apparenter à des formes de censure[118]. C'est pourquoi il est largement centré sur le rôle et les obligations des États, qui, pour censurer, recourent toutefois de plus en plus souvent au secteur privé. Le rapport passe en revue non seulement les obligations mises à la charge des États par le droit des droits de l'homme, mais aussi les principes que les acteurs privés doivent respecter en ce qui concerne les droits de l'homme. Les principales recommandations formulées dans le rapport sont reproduites ci-après.**

Concernant les États et le Conseil des droits de l'homme

77. **Dans sa résolution 32/13, le Conseil des droits de l'homme a condamné sans équivoque les mesures visant à empêcher ou à perturber délibérément l'accès à l'information ou la diffusion d'informations en ligne, en violation du droit international des droits de l'homme, et a invité tous les États à s'abstenir de telles pratiques et à les faire cesser. Il conviendrait de compléter et de préciser le sens de cette prise de position, qui est au cœur de l'action menée par le Conseil pour faire respecter les droits de l'homme sur Internet. Empêcher ou perturber délibérément l'accès à l'information est le fait de prendre toute mesure ayant pour résultat d'interrompre ou de bloquer l'accès aux réseaux de télécommunications, aux services mobiles, aux réseaux sociaux et à d'autres services. En s'employant, dans ses travaux futurs, à préciser les règles applicables à l'accès à l'espace numérique telles qu'elles sont décrites dans le présent rapport, le Conseil contribuerait à la promotion du droit à la liberté d'opinion et d'expression sur Internet.**

[116] Communication du Telecommunications Industry Dialogue, p. 17.

[117] Peter Micek and Jeff Landale, « Forgotten pillar: the Telco remedy plan », Access Now (mai 2013), p. 6.

[118] Communication de la Commission mondiale pour la gouvernance d'Internet ; Arco Iris Libre de Cuba, Centro de Información Hablemos Press, Centro de Información Legal CubaLex, Mesa de Diálogo de la Juventud Cubana Plataforma Femenina Nuevo País, "Situación del derecho a la libertad de opinion y expression en Cuba" (Situation du droit à la liberté d'opinion et d'expression à Cuba) (juillet 2016), p. 20.

78. **Il est par de surcroît primordial que le Conseil et les États définissent la corrélation qui existe entre immixtions dans la vie privée et liberté d'expression. Certes, les immixtions dans la vie privée doivent être appréciées à la lumière de l'article 17 du Pacte international relatif aux droits civils et politiques et des autres normes du droit international des droits de l'homme. Toutefois, certaines formes d'immixtion, telles que les demandes de communication de données d'utilisateurs qui sont trop générales et la conservation de ce type de données par des tiers, peuvent avoir des effets dissuasifs à court et long terme en ce qui concerne la liberté d'expression, et il convient par conséquent de les prévenir tant en droit qu'en pratique. Les États devraient à tout le moins faire en sorte que toute surveillance soit autorisée par une instance judiciaire indépendante, impartiale et compétente garantissant que la demande est proportionnée et nécessaire à la poursuite d'un but légitime.**

79. **Le Rapporteur spécial est particulièrement préoccupé par le fait que des entreprises, leurs équipements et infrastructures, et leurs employés, auraient fait l'objet de menaces et d'actes d'intimidation. On retiendra en outre que le Conseil a mis l'accent sur le rôle important joué par le secteur privé et la nécessité de protéger celui-ci. Les États devraient passer en revue toutes les activités menées pour accéder aux réseaux afin de s'assurer qu'elles sont licites, nécessaires et proportionnées, en s'attachant tout particulièrement à déterminer si elles sont le moyen le moins contraignant de poursuivre un but légitime.**

80. **La protection que les États peuvent accorder au secteur privé doit avoir des limites. Les États ne devraient pas faire primer les bénéfices des acteurs privés sur la liberté d'opinion et d'expression des utilisateurs, et devraient par conséquent interdire toute tentative pour rendre certains types de contenus ou d'applications numériques accessibles en priorité contre rémunération ou en échange d'autres avantages commerciaux.**

81. **Le fait qu'à l'ère du numérique, l'action des autorités et celle des entreprises se superposent à certains égards reste une idée relativement nouvelle pour bon nombre d'États. Il serait utile, tant à l'échelon national qu'au niveau international, d'élaborer des plans d'action nationaux consacrés à la question des entreprises et des droits de l'homme et d'y définir des méthodes permettant à tous les acteurs du numérique de mesurer l'incidence de leurs activités sur le respect des droits de l'homme et de prendre des mesures pour y faire face.**

Concernant les acteurs privés

82. **Il y a maintenant des années que les particuliers et les entreprises du secteur du numérique ont compris qu'ils jouaient un rôle essentiel dans l'élargissement de l'accès aux technologies de l'information et de la communication. Le numérique est un secteur d'activité dont le succès devrait reposer sur l'élargissement de l'accès et l'amélioration des performances, de la diversité et de la transparence. Particuliers et entreprises devraient considérer les principes définis dans le présent rapport comme des outils leur permettant de renforcer le rôle qu'ils jouent dans la promotion du droit des utilisateurs à la liberté d'expression. Dans cet esprit, les entreprises devraient venir appuyer les engagements de haut niveau pris en faveur des droits de l'homme en consacrant les ressources voulues à leur concrétisation, notamment en ce qui concerne l'exercice du devoir de diligence, la prise de décisions de conception et de fabrication axées sur le respect des droits, la participation des parties prenantes, les stratégies de prévention et de réduction des risques de violations des droits de l'homme, la transparence et les recours utiles. Dans cette optique, la conception et l'application de mesures visant à faire appliquer le principe de responsabilité des entreprises à l'égard des droits de l'homme devraient s'appuyer sur les compétences nationales et internationales et les contributions des utilisateurs et des autres titulaires de droits concernés, de la société civile et de l'ensemble des acteurs du domaine des droits de l'homme.**

83. **On ne saurait pour autant dire que les entreprises privées ne subissent pas de pressions. Mais lorsque les États leur demandent de participer à des activités de**

censure ou de surveillance, elles devraient s'attacher à prévenir ou atténuer dans toute la mesure prévue par la loi les effets néfastes que leur coopération a sur le respect des droits de l'homme. En tout état de cause, elles devraient prendre toutes les mesures licites voulues pour ne pas causer de violations des droits de l'homme, contribuer à pareilles violations ou en être complices. Les accords avec les entreprises partenaires devraient permettre à toutes les parties de s'acquitter de leurs responsabilités en ce qui concerne le respect des droits de l'homme. Les entreprises devraient en outre s'attacher à introduire, dans les relations commerciales qu'elles ont déjà établies, des mécanismes permettant de prévenir ou d'atténuer les incidences négatives de leurs activités sur le respect des droits de l'homme.