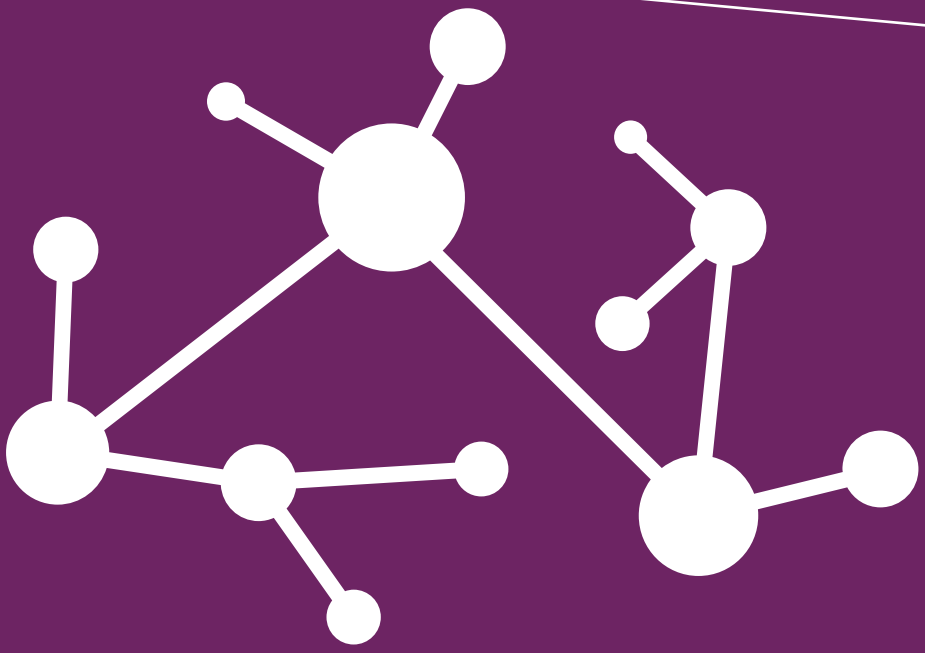
ARTICLE 19



Rester connecté : liberté d'expression, opérateurs télécoms et FAI

Juin 2017

ARTICLE 19
Free Word Centre
60 Farringdon Road
London,
EC1R 3GA
United Kingdom
T: +44 20 7324 2500
F: +44 20 7490 0566
E: info@article19.org
W: www.article19.org
Tw: @article19org
Fb: facebook.com/article19org

The Principles were developed as a part of the Civic Space Initiative financed by the Swedish International Development Cooperation, Sida. Sida does not necessarily share the opinions here within expressed. ARTICLE 19 bears the sole responsibility for the content of the document.

Résumé

Dans ce document d'orientation, ARTICLE 19 examine les obligations des opérateurs de télécommunications (opérateurs télécoms) et des fournisseurs d'accès à Internet (FAI) de protéger et respecter les droits humains, en particulier le droit à la liberté d'expression, et de remédier aux violations de ces droits.

ARTICLE 19 considère que l'étendue des responsabilités des opérateurs télécoms et des FAI en matière de droits humains témoigne du rôle essentiel que jouent ces entreprises en permettant à des individus d'exercer leur droit à la liberté d'expression. Ce document d'orientation explore les contours de ces responsabilités. Notre analyse trouve son origine dans les Principes directeurs des Nations Unies relatifs aux entreprises et aux droits de l'homme (« Principes directeurs »), qui contraignent les opérateurs télécoms et les FAI à intégrer les garanties des droits humains dans leurs activités et à atténuer les impacts de celles-ci sur les droits humains.

Pour garantir que les opérateurs télécoms et les FAI assument pleinement leurs responsabilités en matière de droits humains, en particulier au regard des Principes directeurs, nous recommandons qu'ils mettent en œuvre dans leurs activités les principes fondamentaux d'une approche fondée sur les droits humains, à savoir :

- **Le respect des droits humains** : les conditions d'utilisation devraient être disponibles et accessibles au grand public, formulées avec suffisamment de précision pour permettre aux utilisateurs de comprendre leurs implications et d'adapter leur conduite en conséquence, et ne restreindre l'exercice des droits humains des utilisateurs que lorsque la restriction est nécessaire pour atteindre un objectif légitime, et proportionnée à cet objectif ;

- **La participation** : les usagers devraient avoir le droit de participer aux décisions affectant leurs droits humains. Les conditions d'utilisation des fournisseurs doivent être conditionnées à l'obtention du consentement exprès, libre et éclairé des utilisateurs, et garantir que les usagers seront informés des mesures qui enfreignent leurs droits humains ;

- **L'autonomisation** : les usagers devraient être suffisamment informés pour être capables de comprendre et utiliser les conditions d'utilisation et de pouvoir les contester dans certaines circonstances. Les usagers devraient pouvoir contrôler leurs données personnelles de façon conforme au droit à la liberté d'expression ;

- **La non-discrimination et l'égalité** : Les internautes devraient bénéficier d'un accès sans discrimination à Internet ; leurs contenus et leurs données en ligne devraient être traités sur un pied d'égalité et sans discrimination ;

- **La redevabilité** : Les conditions d'utilisation devraient être transparentes et précises sur les conditions dans lesquelles les droits humains des usagers peuvent être limités. En particulier, les conditions d'utilisation devraient préciser comment et dans quelles circonstances les opérateurs télécoms et les FAI répondront aux injonctions du gouvernement et aux demandes de divulgation de données à caractère personnel. Les conditions d'utilisation devraient fournir aux individus des recours efficaces pour contester ces décisions.

Ce document d'orientation fournit également des recommandations détaillées sur des mesures spécifiques déployées par les opérateurs télécoms et les FAI – à l'instigation de l'État ou sous sa contrainte (notamment coupures de réseau, surveillance étatique, génération et conservation de certaines données, ou interdictions d'applications ou de services particuliers), ou bien volontairement, notamment pour répondre à des intérêts commerciaux. Des recommandations spécifiques seront proposées afin de déterminer comment le secteur privé devrait mettre en adéquation de telles pratiques avec le droit international des droits humains.

Table des matières

Introduction

L'accès à l'Internet – et plus largement la connectivité numérique[1] – n'est plus le domaine réservé des privilégiés et des mieux lotis. Il est devenu un besoin essentiel pour tous, quel que soit leur niveau économique ou scolaire. C'est par le biais des technologies numériques que la population du XXIe siècle apprend, gagne sa vie, agit et effectue des transactions, et exerce une variété de droits humains, dont les droits à la liberté d'expression et d'information, le droit de réunion et d'association, et le droit à l'éducation.[2] Les technologies numériques sont aussi devenues le moyen par lequel les États fournissent un large éventail de services publics et sociaux. Par conséquent, certains prétendent que le réseau Internet – son épine dorsale de protocoles et d'infrastructures clés – peut être considéré comme un bien public qui procure des avantages à toute la population mondiale.[3]

Bien que les États assument de nombreuses obligations concernant Internet, l'accès à ce dernier passe, dans la plupart des cas, par des acteurs privés. Les opérateurs télécoms et les fournisseurs d'accès Internet (dénommés conjointement « les fournisseurs ») connectent les individus à une infrastructure complexe de fils, câbles et satellites leur permettant d'être « en ligne ». De plus, les fournisseurs communautaires émergents, qui constituent une autre forme d'inclusion numérique, jouent un rôle important dans la diversification du pool d'accès à Internet et contribuent à la pluralité et à la diversité des modèles de connexion à Internet. Les fournisseurs agissent comme une passerelle entre les individus et l'exercice des droits humains, et jouent un rôle essentiel dans l'accès aux services publics et aux informations qui circulent dans le monde.

Les fournisseurs prennent souvent des mesures, à l'instigation des gouvernements, qui menacent les droits humains des individus. Cela inclut la coupure de réseau, la restriction de l'usage de certains services et applications, la déconnexion punitive pour infraction au droit d'auteur, la surveillance étatique, et l'interdiction du chiffrement et de l'anonymat en ligne. Les changements et les défis émergents – de l'avènement des réseaux 5G aux débats intenses sur l'accès des autorités policières aux appareils cryptés – constituent des enjeux encore plus importants.

Des fournisseurs prennent aussi de plus en plus fréquemment – au nom de la conformité avec leurs conditions d'utilisation (également appelées « termes et conditions ») – des mesures qui sapent et mettent en péril les droits humains, dont le droit à la liberté d'expression et d'information. Ces mesures comprennent des actions unilatérales telles que la restriction de l'accès à des contenus en

ligne, la génération, la conservation et la vente d'informations personnelles des usagers, et la priorisation de certains types de contenus sur la base de leur origine, leur destination ou fournisseur de service.

L'asymétrie de pouvoir entre les fournisseurs et les internautes est aggravée par l'absence de transparence et de redevabilité dans la façon dont les conditions d'utilisation sont interprétées et appliquées. Un langage fastidieux, complexe et légaliste obscurcit souvent l'intention des conditions d'utilisation, et la relation « à sens unique » entre les fournisseurs et les usagers empêche un examen ou une négociation authentique des termes de cette relation. Dans la plupart des conditions d'utilisation, les individus ont rarement le droit de contester – voire d'être informés sur – les décisions négatives des fournisseurs visant, par exemple, à faciliter la surveillance étatique, à divulguer des données à des tiers, à saper la neutralité du Net ou couper l'accès. Les conditions d'utilisation ressemblent trop souvent à une boîte noire qui, sous couvert du consentement des utilisateurs, brouille le rôle des fournisseurs et leurs obligations contractuelles envers les utilisateurs.

ARTICLE 19 est convaincu qu'une meilleure compréhension du rôle et des responsabilités des acteurs privés est essentielle pour protéger la liberté d'expression et d'information, ainsi que d'autres droits humains en ligne. De ce fait, ce document d'orientation explore les contours de ces responsabilités. Nous prenons pour point de départ les Principes directeurs des Nations Unies relatifs aux entreprises et aux droits humains (« Principes directeurs ») – également baptisés Principes de Ruggie –, qui contraignent les fournisseurs à protéger les droits humains et à atténuer les impacts de leurs activités sur ces droits, à publier des rapports de transparence et à proposer des recours efficaces contre les violations de ces droits. Pour s'assurer du respect de ces Principes directeurs, nous recommandons que les conditions de services élaborées par les fournisseurs englobent les principes fondamentaux d'une approche fondée sur les droits humains, la participation, l'autonomisation, l'égalité et la redevabilité.

Portée de cette politique

Le secteur responsable de la construction, la fourniture et l'entretien des composants physiques et techniques d'Internet qui assurent la connectivité est formé d'un réseau complexe d'acteurs. Aux fins de définir les responsabilités en matière de droits à la liberté d'expression et d'information, ARTICLE 19 suggère que ces acteurs privés soient répartis selon les catégories suivantes :[4]

- **Acteurs fournissant des services essentiels pour accéder à Internet :** il s'agit des entreprises de télécommunications, des opérateurs télécoms, des fournisseurs d'accès à Internet (FAI), des opérateurs de réseau, et des points d'échange Internet ;

- **Acteurs fournissant des services essentiels pour accéder à l'information sur Internet** : il s'agit de l'ICANN, des registres et bureaux d'enregistrement de noms de domaines, des services d'hébergement d'Internet, et des moteurs de recherche ;

- **Acteurs facilitant le partage d'information sur Internet** : il s'agit des plateformes de médias sociaux, des blogs, des forums en ligne ainsi que des services de e-commerce offrant ou distribuant des contenus ;

- **Acteurs produisant des contenus** : cela comprend les journaux et d'autres producteurs de contenus, qu'il s'agisse d'auteurs individuels ou d'entreprises ;

- **Autres acteurs** : il s'agit de fabricants d'ordinateurs ou autres matériels informatiques, développeurs de logiciels, entreprises fournissant des services de stockage de données ou des services cloud, et entreprises de cyber sécurité, qui sont essentielles pour la sécurité de la toile.

Nous pourrions également décrire ces acteurs comme des fournisseurs de service au niveau **physique**, **logique**, au niveau des **contenus** et au niveau **social** d'Internet. Les discussions pertinentes sur les politiques relatives à la protection des droits humains, y compris le droit à la liberté d'expression, concernent ces quatre niveaux. Ainsi, un changement de politique à un niveau donné aura un impact direct sur les autres niveaux, d'une façon ou d'une autre.[5]

Dans ce document, nous nous intéresserons plus particulièrement aux opérateurs télécoms et aux fournisseurs d'accès à Internet (FAI), les entités privées ou publiques qui fournissent et entretiennent le niveau technique d'Internet, permettent l'accès au Net via des services de téléphonie fixe ou mobile. Ce document s'applique à la fois aux fournisseurs commerciaux et aux prestataires communautaires.

En raison de la complexité et de la portée de cette seule question, nous n'aborderons pas ici les organes du secteur privé qui hébergent des contenus (par ex. les fournisseurs de services d'hébergement sur Internet) ou les

fournisseurs d'applications et de services en ligne (par ex. les plateformes de médias sociaux ou les applications de messagerie). Nous exclurons également les réseaux de distribution de contenu (content delivery networks - CDN), les points d'échange Internet (Internet exchange points - IXP), et d'autres organes dont les clients sont des entreprises et non des individus ; ainsi que la gamme d'acteurs privés dont les activités ont des impacts sur la liberté d'expression dans le contexte numérique, y compris les fabricants de matériel informatique et les développeurs de logiciels, les producteurs de contenus et les titulaires de droits d'auteur, les entreprises fournissant des services de stockage de données ou des services cloud, ou des entreprises de cybersécurité. Ces acteurs sont abordés dans d'autres documents d'orientation d'ARTICLE 19.

Ce document s'appuie sur des travaux précédents d'ARTICLE 19 relatifs aux rôles et responsabilités des intermédiaires dans le contexte de la liberté d'expression et d'information en ligne ;[6] il propose également des recommandations spécifiques pour les États et les fournisseurs dans les domaines respectifs de cette politique.

Normes internationales en vigueur

Le secteur des télécommunications a évolué de manière diamétralement opposée selon les pays et les contextes. Dans de nombreux pays, ce secteur était initialement un monopole d'État, qui a été depuis partiellement ou totalement privatisé, et les marchés des télécommunications se sont ouverts à des acteurs nouveaux et étrangers.[7] Dans d'autres contextes, les télécommunications ont toujours été une entreprise totalement privée.[8]

Cependant, les États détiennent toujours des intérêts dans de nombreuses entreprises de télécommunications dans le monde et, même dans les marchés exclusivement privés, la relation étroite entre les opérateurs télécoms et les gouvernements est fortement empreinte de cet héritage des entreprises publiques et de la prédominance d'un État régulateur. Cette relation s'appuie également sur le cadre régissant l'octroi de licences de télécommunications, qui contraint les opérateurs à respecter les conditions stipulées par le gouvernement pour exercer leurs activités.

Les FAI sont le plus souvent des acteurs privés qui ont émergé avec la naissance d'Internet et fourni ce que l'on nomme la « connectivité du dernier kilomètre », à savoir une connexion entre des usagers individuels et des infrastructures de télécommunication existantes. Bien que les FAI aient rarement été sous la coupe de l'État, dans beaucoup de pays, ils fonctionnent dans les faits comme des monopoles, face à l'absence totale de concurrence. Dans certains cas, y compris dans les communautés rurales ou pauvres, l'absence d'incitations commerciales pour les FAI fait que l'obligation de fournir « une connectivité du dernier kilomètre » revient entièrement à l'État. Récemment, nous avons vu émerger des fournisseurs de services communautaires[9] qui diversifient les opportunités d'accès à l'Internet.

Tous les fournisseurs – qu'ils soient publics, privés ou communautaires – sont tenus de respecter et protéger les droits humains des internautes, en particulier les droits à la liberté d'expression et d'information et le droit au respect de la vie privée. Ces responsabilités, telles qu'énoncées dans le cadre des Principes directeurs, comprennent le devoir positif d'atténuer les impacts négatifs sur les droits de l'homme, de publier des rapports de transparence et de fournir des voies de recours.

Le droit à la liberté d'expression et d'information

Le droit à la liberté d'expression est garanti dans l'Article 19 de la Déclaration universelle des droits de l'homme (DUDH), dans le Pacte international relatif aux droits civils et politiques (PIDCP) et dans les traités régionaux.[10] Il comprend le droit non seulement de diffuser, mais aussi de rechercher et de recevoir des informations et des idées de toutes sortes, sans considération de frontières ; le droit d'accès à l'information est de plus en plus accepté dans le cadre du droit international comme une partie intégrante du droit à la liberté d'expression.[11] Ces dernières années, un grand nombre d'organes et d'instruments internationaux ont confirmé que le droit à la liberté d'expression devait être protégé sur Internet de la même manière qu'il est protégé hors ligne.[12]

Actuellement, le droit d'accès à Internet n'est pas explicitement reconnu comme tel dans le droit international et régional des droits humains. Toutefois, des évolutions dans certaines lois nationales, ainsi que dans le droit international et régional des droits de l'homme, tendent à contraindre tous les États à faciliter l'accès à Internet pour tous.[13] Comme l'a noté le Rapporteur spécial des Nations Unies sur la promotion et la protection du droit à la liberté d'opinion et d'expression dans son rapport 2011, l'accès à Internet a été aussi reconnu comme inextricablement lié à l'exercice de la liberté d'expression :

> [L]'accès à l'information, l'exercice du droit à la liberté d'expression et de participer qu'offre Internet à toutes les couches de la société est indispensable pour bâtir une société véritablement démocratique.[14]

Le droit à la liberté d'expression n'étant pas un droit absolu, il peut être limité dans des conditions très strictes. Les restrictions admissibles de la liberté d'expression sont énoncées dans le dénommé « triple test », qui requiert que toutes les restrictions :

- **Soient fixées par la loi ;**
- **Poursuivent un objectif légitime** – soit l'un des objectifs énoncés de manière exhaustive dans l'Article 19 par. 3 du PIDCP, qui inclut : (a) le respect des droits ou de la réputation d'autrui ; ou (b) la protection de la sécurité nationale ou de l'ordre public, ou de la santé et de la moralité publiques ; et
- Soient **nécessaires et proportionnées** à cet objectif.[15]

Ces restrictions conformes au droit international s'appliquent également à la liberté d'expression en ligne. Il est important de souligner que la question de

la proportionnalité revêt une plus grande importance en ligne dans la mesure où, en raison de la nature même d'Internet, toute restriction des droits humains est potentiellement susceptible d'affecter des centaines de millions d'internautes. Pour évaluer quand une restriction particulière – qui affecte Internet – constitue une violation des normes relatives aux droits humains, il faut avoir une compréhension fine de ses implications techniques et pratiques sur la liberté d'expression et la vie privée, et reconnaître les impacts transjuridictionnels des restrictions à l'accès aux services et aux contenus en ligne.

Dans leur Déclaration conjointe de 2011 sur la liberté d'expression et Internet, les quatre mandataires spéciaux pour la protection de la liberté d'expression[16] ont souligné que, dans le contexte de l'accès à Internet, le respect du test des restrictions licites implique, entre autres, que:

- Les mesures visant à **bloquer** des sites, des services ou des utilisations spécifiques d'Internet, ou à empêcher des **individus d'accéder à Internet**, sont des mesures extrêmes qui doivent se conformer aux exigences strictes du triple test relatif aux restrictions admissibles ;

- Aucune **discrimination** ne doit être permise dans le traitement des données et du trafic sur Internet, qu'elle soit fondée sur le matériel, le contenu, l'auteur, l'origine et/ou la destination du contenu, le service ou l'application ;traffic based on the device, content, author, origin and/or destination of the content, service or application;

- Les intermédiaires d'Internet doivent garantir la **transparence** dans les pratiques de gestion du trafic ou de l'information, et les informations pertinentes sur ces pratiques doivent être rendues disponibles sous une forme accessible à tous ; et

- **La coupure de l'accès** au réseau (coupure d'Internet), ou à des pans d'Internet, à des populations entières ou des fractions de la population ne peut jamais être justifiée, y compris pour préserver l'ordre public ou la sécurité nationale.

En juin 2016, le Conseil des droits de l'homme des Nations Unies (CDH), en réponse à un certain nombre de pays ayant récemment coupé l'accès à Internet ou à des outils de communication numériques, a condamné sans équivoque

> [L]es mesures qui visent 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 invite tous les États à s'abstenir de telles pratiques et à les faire cesser.[17]

La fermeté de la déclaration du CDH traduit la gravité de l'impact des coupures de réseau sur l'exercice du droit à la liberté d'expression. Bien que la résolution ne précise pas les circonstances dans lesquelles la restriction ou la perturbation de l'accès constitue une violation du droit international, le Comité des droits de l'homme des Nations Unies (CDH), qui supervise le respect de ces dispositions du PIDCP par les pays signataires, a précédemment stipulé que les interdictions générales de sites ou d'outils constituaient une violation :

> Toute restriction imposée au fonctionnement des sites web, des blogs et de tout autre système de diffusion de l'information par le biais d'Internet, de moyens électroniques ou autres, y compris les systèmes d'appui connexes à ces moyens de communication, comme les fournisseurs d'accès à Internet ou les moteurs de recherche, n'est licite que dans la mesure où elle est compatible avec le paragraphe 3. Les restrictions licites devraient d'une manière générale viser un contenu spécifique ; les interdictions générales de **fonctionnement frappant certains sites et systèmes ne sont pas compatibles avec le paragraphe 3**. Interdire à un site ou à un système de diffusion de l'information de publier un contenu uniquement au motif qu'il peut être critique à l'égard du gouvernement ou du système politique et social épousé par le gouvernement est tout aussi incompatible avec le paragraphe.[18]

Le droit au respect de la vie privée

Le droit à la liberté d'expression est étroitement lié au droit à la vie privée, en particulier dans le contexte d'Internet. Le respect de la vie privée constitue un bouclier qui permet à des individus de partager des idées et de rechercher des informations en ligne sans faire l'objet d'une surveillance arbitraire ou illicite, d'un contrôle et d'une collecte de données. Il garantit l'exercice de leur droit à parler librement et en toute confidentialité et, s'ils le souhaitent, anonymement. Ainsi, le droit au respect de la vie privée est un moyen de créer les conditions nécessaires à l'exercice libre et total de la liberté d'expression et d'information en ligne.

Le droit au respect de la vie privée, inscrit à l'Article 12 de la DUDH et à l'Article 17 du PIDCP et dans les traités régionaux,[19] interdit toute ingérence illicite dans la vie privée, le domicile, la correspondance et la famille d'un individu. Avec l'évolution d'Internet et des technologies numériques, la notion de vie privée s'est élargie pour inclure dorénavant les données à caractère personnel, dont la protection découle du droit au respect de la vie privée.

Protection des données à caractère personnel

Les Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel de l'OCDE datant de 1980 constituent la première déclaration internationale sur la portée du droit à la protection des données à caractère personnel. Elles ont été depuis complétées par la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (ou « Convention 108 »)[20] , les Principes de l'Assemblée générale des Nations Unies pour la réglementation des fichiers personnels informatisés datant de 1990,[21] et la Directive de l'Union européenne sur la protection des données à caractère personnel, récemment remplacée par le Règlement général sur la protection des données.

À ce jour, on compte plus de 100 lois nationales sur les données à caractère personnel dans le monde, dont près de la moitié a été promulguée hors du continent européen, qui reprennent souvent les normes européennes.[22] La Cour européenne des droits de l'homme et la Cour de justice de l'Union européenne (CJUE) ont été les principaux artisans de l'élaboration des contours du droit à la protection des données à caractère personnel en lien avec le respect de la vie privée.[23] Des instruments régionaux traitant de cette question ont été aussi adoptés par l'Association des nations de l'Asie du Sud-Est (ASEAN) et l'Union africaine.[24]

Le droit à la vie privée n'est pas un droit absolu ; il peut être restreint à condition de répondre aux trois critères du triple test précédemment mentionné en relation avec la liberté d'expression.[25] De ce fait, les activités qui constituent une ingérence dans la vie privée d'une personne – notamment la surveillance ciblée des communications en ligne ou la génération, la collecte, la conservation et l'utilisation de données à caractère personnel – peuvent être justifiées à condition d'être compatibles avec la loi, d'être nécessaires en vue d'atteindre un objectif particulier, et d'être proportionnées à cet objectif.

Dans le cadre des activités impliquant la génération, la collecte, la conservation et l'utilisation de données à caractère personnel en ligne, la loi sur la protection des données[26] prévoit des restrictions et des garanties en vue de s'assurer que le traitement des données n'enfreint pas le droit à la vie privée des internautes. Bien que la réglementation sur la protection des données diffère d'un pays et d'une région à l'autre, toutes ces lois contiennent des principes communs sur le traitement des données à caractère personnel en ligne :

- **Équité et légalité :** cela comprend l'obligation d'obtenir le consentement

éclairé d'un individu avant de procéder au traitement des données personnelles le concernant ;

- **Limites en matière d'objectifs :** les données doivent être collectées à des fins spécifiques, explicites et légitimes, et ne pas être utilisées à d'autres fins incompatibles ;

- **Réduction des données :** les données doivent être limitées à celles qui sont nécessaires, adéquates et pertinentes ;

- **Exactitude :** les données à caractère personnel doivent être exactes et actualisées ;

- **Limites de stockage :** les données à caractère personnel identifiables ne doivent pas être conservées au-delà des délais nécessaires ;

- **Sécurité et intégrité :** les organisations devraient adopter des mesures organisationnelles ou techniques appropriées pour s'assurer que les données stockées sont sécurisées ;

- **Redevabilité et transparence :** les organisations devraient garantir la transparence sur le traitement des données et rendre des comptes sur le respect des principes relatifs à la protection des données.[27]

Responsabilités du secteur privé

Il existe aujourd'hui de nombreuses lignes directrices, sous forme d'observations générales ou d'observations finales du Comité des droits de l'homme, de rapports des rapporteurs spéciaux des Nations Unies, et de jurisprudence des cours régionales sur les responsabilités des États en matière de protection du droit à la liberté d'expression et d'information sur Internet.[28] Toutefois, il reste comparativement peu de documents définissant les responsabilités des acteurs privés qui entretiennent et fournissent un accès à Internet, et qui facilitent trop souvent une ingérence de l'État dans l'accès à Internet.

Deux rapports du Rapporteur spécial sur la liberté d'opinion et d'expression, dont le rapport 2017 au CDH sur le rôle et les responsabilités du secteur dans la promotion du droit à la liberté d'expression,[29] constituent une exception notable. Ce rapport explicite les frictions survenant quand les obligations légales nationales des FAI entrent en conflit avec le droit international des droits humains, en particulier dans

le contexte des coupures de réseau, des blocages de contenu, du respect des droits d'auteur, de la surveillance des communications et de l'ingérence dans la neutralité du Net. Le Rapporteur spécial sur la liberté d'opinion et d'expression a mis l'accent sur l'obligation des États de respecter la liberté d'expression dans le contexte de deux ingérences particulièrement graves – les coupures d'Internet et la surveillance des communications –, ainsi que le devoir de protéger la liberté d'expression en interdisant des services de priorisation payants et en réglementant les pratiques de « zero-rating » (taux zéro). Il a ensuite exploré les contours de la redevabilité des entreprises dans ce contexte, en détaillant les obligations des acteurs privés de respecter un processus de diligence raisonnable, d'adopter volontairement des mesures de sauvegarde des droits humains, de développer des moyens de pression, d'adopter des stratégies d'atténuation, de publier des rapports de transparence et de garantir que des recours effectifs sont en place.

Le cadre établi dans **les Principes directeurs relatifs aux entreprises et aux droits de l'homme : mettre en œuvre le cadre de référence « Protéger, respecter et réparer » des Nations Unies** (les Principes directeurs) – ainsi que les Dix Principes précédents du Pacte mondial des Nations Unies[31] – fournit un point de départ pour définir le rôle du secteur privé au regard des droits humains et Internet.[32] Les Principes directeurs reconnaissent l'obligation des entreprises commerciales de respecter les droits humains, indépendamment des obligations de l'État ou de la mise en œuvre de ces obligations :

- **En s'engageant par le biais d'une déclaration publique** à respecter les droits humains, approuvée par la direction supérieure ou exécutive ;

- En instituant des **processus de vigilance préalable** et en conduisant **des évaluations de l'impact sur les droits humains** afin d'identifier, d'éviter et d'atténuer les impacts négatifs potentiels des activités des entreprises sur les droits humains ;

- En intégrant **volontairement des protections des droits humains** afin d'atténuer les impacts négatifs, en trouvant des moyens de pression et en agissant collectivement afin de renforcer leur pouvoir vis-à-vis des autorités gouvernementales ;

- En assurant le suivi et en communiquant des informations sur la **performance, les risques et les demandes du gouvernement**; et

- En mettant à disposition **des recours** en cas d'impacts négatifs sur les droits humains.

Des efforts ont été fournis pour appliquer les Principes directeurs aux conditions spécifiques des opérateurs télécoms et des FAI. En particulier, le Telecommunications Industry Dialogue (TID) a élaboré en 2013 ses propres Principes directeurs pour éclairer les pratiques et les processus internes de ses membres.[33] Le Global Network Initiative (GNI), qui se concentre plus sur les entreprises et les intermédiaires d'Internet que sur les entreprises de télécommunications, a également rédigé ses propres Principes,[34] qui sont utilisés par Ranking Digital Rights Corporate Accountability Index – avec les Principes directeurs des Nations Unies – pour classer la performance des entreprises d'Internet et de télécommunications sur une base annuelle.[35]

Alors que les Principes de TID et GNI visent principalement à indiquer des orientations aux entreprises sur la manière de répondre aux demandes du gouvernement, le Ranking Digital Rights (RDR) examine les obligations des FAI en matière de conditions d'utilisation. Le RDR prescrit une série d'indicateurs pour évaluer l'adhésion des entreprises aux principes des droits humains. Ces indicateurs comprennent, *entre autres* :

- La disponibilité de conditions d'utilisation et de politiques de protection de la vie privée ;

- La notification des changements dans les conditions d'utilisation et des restrictions de contenu ou d'accès ;

- Quelle information est divulguée dans les conditions d'utilisation, notamment
    - Si l'entreprise interdit certains types de contenus ou d'activités ;

    - Dans quelles circonstances l'entreprise peut restreindre les services aux internautes ;

    - Quelle procédure utilise l'entreprise pour évaluer et répondre aux demandes des gouvernements de restreindre des contenus ou des services ;

    - Quelles informations sur l'internaute l'entreprise recueille, avec qui elle les partage, et combien de temps elle les conserve ;

- Si l'internaute exerce un contrôle sur les données que l'entreprise recueille et partage ;

- Si l'internaute peut accéder à toutes les informations que l'entreprise détient sur lui ;

- Publication de rapports de transparence sur les demandes du gouvernement et de parties privées de supprimer, filtrer ou restreindre des contenus ou

l'accès à Internet, ou de fournir l'accès à des données stockées ou à des communications en temps réel ;

- Publication de données sur le volume et la nature des actions entreprises pour faire respecter les conditions d'utilisation ;

- Publication de données sur la gestion du réseau ;

- Si l'entreprise informe les internautes quand leurs données sont demandées par des gouvernements ou d'autres tiers ; et

- Si l'entreprise déploie des normes de chiffrement et de sécurité, et permet aux usagers de chiffrer leurs contenus.[36]

Bien qu'ils ne soient ni exhaustifs ni totalement complets, ces indicateurs fournissent des éléments de référence importants pour s'assurer que les conditions d'utilisation tiennent compte des droits à la liberté d'expression et à la protection de la vie privée des usagers d'Internet et ne les remettent pas en cause.

Mesures qui portent atteinte aux droits humains des usagers

Une série de mesures mises en œuvre par les opérateurs télécoms et les FAI menacent gravement les droits à la liberté d'expression et au respect de la vie privée des individus. Certaines sont prises à l'instigation de l'État ou sous contrainte légale : elles incluent des coupures de réseau, la surveillance étatique, la génération et la conservation de certaines données, ou des interdictions frappant des applications ou des services particuliers. D'autres mesures sont prises volontairement, y compris celles qui sont motivées par des intérêts commerciaux : la génération et l'analyse de volumes excessifs de données à caractère personnel, par exemple, ou la mise en œuvre de programmes de priorisation payants. Dans cette section, nous analyserons les pratiques des opérateurs télécoms et des FAI qui ont des incidences sur les droits humains. Des recommandations spécifiques sur la manière dont le secteur privé devrait aligner ces pratiques sur le droit international des droits humains sont proposées dans la section suivante.

Coupure de l'accès

Coupures de réseau

La place centrale d'Internet dans l'exercice de la liberté d'expression à l'ère moderne a favorisé la tendance des États à recourir à des coupures de la totalité du réseau pour supprimer l'accès à, et la diffusion, d'informations et d'idées progressistes et dissidentes. De ce fait, la fréquence des coupures totales et partielles de réseau, en particulier durant des périodes électorales[37] ou des périodes de bouleversement politique, s'est considérablement accrue ces dernières années.[38] Des coupures ont été aussi mises en œuvre durant des périodes d'examen d'entrée à l'université sous prétexte d'empêcher des étudiants de tricher,[39] et durant des manifestations et des protestations,[40] pour empêcher des personnes d'accéder à des communications sur Internet et sur téléphone mobile.

Les coupures de réseau sont mises en œuvre par les fournisseurs, agissant à l'instigation – et souvent en réponse à des demandes directes – des États. Dans certaines circonstances, ces demandes s'appuient sur des cadres législatifs

nationaux, notamment ceux régissant les situations d'urgence et les menaces à la sécurité nationale,[41] tandis que d'autres cas, les États exercent des pressions sur les fournisseurs, ou exigent leur coopération, pour couper l'accès à des réseaux quand il n'existe pas de réglementation applicable. Cependant, indépendamment de l'existence d'une réglementation nationale visant à autoriser des coupures de réseau, des mesures généralisées de ce type ne sont jamais admissibles en vertu du droit international des droits humains. [42]

Lois prévoyant des réponses graduées

Depuis 2009, de nombreux pays ont adopté des lois et des politiques punitives conçues pour pénaliser des auteurs d'infractions répétées au droit d'auteur [43] par la déconnexion de leur accès à Internet. Des dispositifs législatifs de réponses graduées, également connus sous l'appellation de « lois des trois coups » (« three strikes and you're out »), stipulent que les entreprises de télécommunications peuvent couper l'accès à des auteurs d'infractions répétées au droit d'auteur.[43] Dans certains cas, des fournisseurs se soumettent volontairement à ces dispositifs et suppriment l'accès des usagers sans avoir reçu d'injonctions administratives ou judiciaires.[44]

Lorsque l'accès à Internet est devenu une condition aussi essentielle à l'exercice des droits humains, la coupure de l'accès constitue une entrave sévère et grave à l'exercice du droit à la liberté d'expression et d'autres droits humains. En conséquence, cette mesure ne peut être considérée comme proportionnée dans le cadre droit international des droits humains, quels que soient les motifs invoqués.[45]

Restrictions de l'accès

Les fournisseurs peuvent restreindre, entraver et exercer des discriminations sur le trafic du réseau qu'ils gèrent de façons très variées. Un petit nombre de ces restrictions est justifié par la gestion du réseau, qui nécessite de prioriser une partie du trafic pour une gouvernance efficace des flux. Cependant, d'autres mesures permettent aussi de prioriser, limiter ou bloquer des contenus, des applications et des services. Il s'agit, notamment, de :

- **Priorisation payante,** une mesure lucrative par laquelle les fournisseurs acceptent des paiements de plateformes et de fournisseurs de services pour prioriser des contenus sur la base de l'origine, la destination ou le fournisseur de services, délivrant certaines catégories de contenus à des débits plus élevés, tout en ralentissant ou en limitant d'autres catégories.

- **Dispositifs de « zero-rating »**, par lesquels les fournisseurs offrent un accès gratuit à certains contenus ou services, et restreignent l'accès à d'autres. Bien que ces dispositifs soient supposés donner accès à des communautés mal desservies et susceptibles de ne pas pouvoir accéder à Internet, ils ont pour effet de limiter les contenus auxquels les utilisateurs sont en mesure d'accéder, bloquant ainsi la libre circulation de l'information et isolant des usagers dans des « jardins emmurés ».[46] D'aucuns prétendent que le zéro-rating est « adapté uniquement à des scénarios où la bande passante est extrêmement coûteuse ou que la demande de bande passante excède de loin l'offre, et le zero-rating servirait à encourager un usage plus lent de la bande passante », mais qu'il devrait éviter, même dans ces situations, les dommages découlant de la consommation altérée de contenus, la liberté d'expression et le respect de la vie privée, l'accès aux marchés et autres dommages.[47] Par conséquent, la fourniture d'un accès sans entrave à l'Internet complet est une meilleure solution que d'appliquer un taux zéro à certains contenus.

- **Interdictions de certains services ou applications** : dans de nombreux pays, l'accès à des applications telles que la voix sur IP ou « VoIP »[48] ou des applications de messagerie instantanée[49] et des services tels que les Réseaux privés virtuels (Virtual Private Networks)[50] est bloqué par les fournisseurs, soit volontairement soit à la demande des autorités publiques.

Chacune de ces mesures enfreint un pilier fondamental et fondateur de l'ouverture d'Internet, celui de la neutralité du Net. La neutralité du Net (ou agnosticisme à l'égard des contenus[51]) est un principe selon lequel le trafic sur le web – les « paquets » de données transportant des contenus sur Internet – ne doit faire l'objet d'aucune discrimination fondée sur l'origine, la destination ou le fournisseur de services, ou le type de service ou d'application. La neutralité du Net signifie que les fournisseurs ne peuvent abuser de leur contrôle sur l'infrastructure d'Internet pour bloquer, ralentir ou prioriser l'accès à des contenus venant de certaines origines ou de certains fournisseurs, à des contenus de certains types, ou à des applications ou des services particuliers.

La neutralité du Net est une condition préalable essentielle à l'exercice égal et non discriminatoire des droits à la liberté d'expression et d'information. Sans elle, il n'y a plus d'égalité sur le terrain de jeu en ligne, et la capacité des utilisateurs à déterminer comment ils s'impliquent dans les contenus et les applications en ligne est sévèrement entravée. Les mesures visant à saper la neutralité du Net menacent également le droit à la vie privée et à la protection des données, la mise en œuvre de programmes de priorisation pouvant conduire des fournisseurs à contrôler de manière plus envahissante le trafic du réseau en utilisant, par exemple, une inspection des paquets en profondeur.

La neutralité du Net est également menacée par le déploiement imminent de la 5G, la nouvelle génération de standard de communication mobile, et les capacités considérablement élargies induites par la 5G. Dans la mesure où les réseaux 5G pourront répondre à une diversité incroyable de besoins, il y a un plus grand risque que les fournisseurs choisissent de créer des « routes rapides » pour certains types de contenus, de traiter en priorité certains paquets de données, ou de ralentir la bande passante.[52] En juillet 2016, certains grands opérateurs télécoms ont signé un Manifeste pour la 5G[53] qui remet en question la nécessité des normes de neutralité du Net, suscitant des inquiétudes sur le fait que les droits à la liberté d'expression pourront être soumis à des considérations d'efficacité du réseau.[54]

Parce qu'elles enfreignent les droits à la liberté d'expression et d'information, les mesures qui violent la neutralité du Net ne peuvent être conformes aux standards du droit international des droits humains qu'à condition de satisfaire au test en trois parties pour évaluer l'admissibilité des restrictions. À cet égard, les mesures énoncées ci-dessus soulèvent un certain nombre de préoccupations :

- **Légalité** : Non seulement les programmes de priorisation payante et les dispositifs de « zero-rating » ne sont pas prévus par la loi, mais ils sont souvent interdits par les réglementations nationales. Un certain nombre de pays ont interdit les services à taux zéro,[55] ou ont promulgué des lois nationales contraignant ces services à ne pas restreindre de manière déraisonnable la capacité des usagers à accéder à des contenus gratuitement.[56] En novembre 2015, l'Union européenne a adopté des règles sur la neutralité du Net interdisant le blocage, le ralentissement ou la discrimination des contenus en ligne, des applications et des services, sauf pour certaines exceptions : respect des obligations légales, intégrité du réseau, et gestion des encombrements dans des situations exceptionnelles et temporaires.[57]

  Dans les pays où l'interdiction de certains applications et services est prévue par la législation nationale, ces lois doivent être connues du grand public, et formulées de manière suffisamment claire et précise. Des lois floues ou des références trop larges à diverses justifications (souvent la sécurité nationale) ne peuvent servir à mettre en œuvre des interdictions de certaines applications ou de certains services.

des références trop larges à diverses justifications (souvent la sécurité nationale) ne peuvent servir à mettre en œuvre des interdictions de certaines applications ou de certains services.

- **Nécessaire pour atteindre un objectif légitime et proportionné à cet objectif** : Les restrictions de l'accès à certains contenus, applications et services en ligne ne peuvent pas être considérées comme nécessaires pour protéger les droits et la réputation d'autrui, ou l'ordre public et la moralité publique. Une certaine priorisation des contenus peut se justifier dans des situations exceptionnelles d'urgence, par exemple une menace imminente pour la sécurité nationale ou la santé publique. Dans ces circonstances, toutefois, pour être proportionnées, les restrictions de l'accès doivent demeurer temporaires et limitées à ce qui est strictement nécessaire pendant la durée de la situation d'urgence.

Génération, conservation et divulgation de données

Les fournisseurs se trouvent sur un point unique de la chaîne de valeur des communications, qui leur donne potentiellement accès à des volumes d'informations considérables sur leurs usagers – données d'identification recueillies à l'ouverture de comptes pour facturer des données, informations de géolocalisation enregistrées lors de l'accès à un service, détails des sites consultés et applications utilisées, taille et type de contenu téléchargé par les usagers, contenus des SMS, et dans certains cas, courriers électroniques. Ainsi, les opérateurs télécoms et les FAI gèrent un volume considérable de données à caractère personnel et hautement privé sur leurs usagers.

Bien sûr, les fournisseurs doivent pouvoir accéder à certaines données à caractère personnel, par exemple pour facturer des utilisateurs abonnés, ou les connecter à des sites particuliers. Toutefois, la grande majorité des données gérées par les fournisseurs ne doivent être conservées que momentanément, leur conservation à long terme n'étant pas justifiée par la gestion du trafic.

Néanmoins, avec la commercialisation croissante des données à caractère personnel, les opérateurs télécoms ont découvert les avantages financiers de la génération, la collecte et la conservation de larges volumes de données personnelles non essentielles à la fourniture du service, mais qui, ensemble, permettent aux entreprises de créer des profils d'usagers commercialisables. La vente de données à caractère personnel à des tiers peut conduire à un vaste partage de ces données avec des annonceurs publicitaires et des courtiers de données. Lorsque des opérateurs télécoms proposent des services gratuits, tels que les réseaux wifi publics, ils peuvent collecter encore plus de données, et les

Comme l'a noté la CJUE, les données gérées par les entreprises de télécommunications, prises dans leur ensemble,

> [i]s sont susceptibles de permettre de tirer des conclusions très précises concernant la vie privée des personnes dont les données ont été conservées, telles que les habitudes de la vie quotidienne, les lieux de séjour permanents ou temporaires, les déplacements journaliers ou autres, les activités exercées, les relations sociales de ces personnes et les milieux sociaux fréquentés par celles-ci [...] En particulier, ces données fournissent les moyens d'établir [...] le profil des personnes concernées, information tout aussi sensible, au regard du droit au respect

vente de données à caractère personnel à des tiers peut conduire à un vaste partage de ces données avec des annonceurs publicitaires et des courtiers de données. Lorsque des opérateurs télécoms proposent des services gratuits, tels que les réseaux wifi publics, ils peuvent collecter encore plus de données, et les partager non seulement avec des entreprises, mais aussi avec des États.

Les États sont eux aussi conscients de la valeur des données à caractère personnel pour les autorités policières et les services de renseignement, et ils imposent aux fournisseurs de services de télécommunications des obligations de plus en plus lourdes de générer et conserver des données à caractère personnel sur leurs abonnés, leurs communications et les sites et applications[58] consultés pour faciliter la surveillance du gouvernement. Il existe aujourd'hui dans le monde un certain nombre de lois contraignantes sur la conservation des données, qui obligent les fournisseurs à générer et stocker des enregistrements de communications pendant une durée maximale de deux ans.[59] Les politiques d'enregistrement sous des identités réelles, qui forcent les fournisseurs à enregistrer et vérifier l'identité des utilisateurs, même pour des services prépayés, prolifèrent également dans le monde.

Les données sur l'utilisation d'Internet par un individu – « les métadonnées » – peuvent être tout aussi sensibles que le contenu de leurs communications. De ce fait, les autorités judiciaires reconnaissent de plus en plus que les métadonnées doivent bénéficier des mêmes protections juridiques que celles applicables aux contenus. C'est ce qu'a confirmé la Cour interaméricaine des droits de l'homme dans le contexte des appels téléphoniques :

> [Le droit à la protection de la vie privée] s'applique aux conversations téléphoniques indépendamment de leur contenu, et peut même inclure à la fois les opérations techniques conçues pour enregistrer ce contenu sur bande sonore et l'écouter, ou tout autre élément du processus de communication ; par exemple, la destination ou l'origine des appels effectués, l'identité des interlocuteurs, la fréquence, l'heure et la durée des appels, des éléments vérifiables sans devoir enregistrer le contenu de l'appel sur bande sonore. Bref, la protection de la vie privée se manifeste dans le fait que des personnes autres que celles qui ont participé à la conversation n'ont pas le droit d'obtenir illégalement des informations sur le contenu des conversations téléphoniques ou d'autres aspects inhérents au processus de communication, tels que ceux mentionnés.[60]

> de la vie privée, que le contenu même des communications. L'ingérence que comporte une telle réglementation […] est susceptible de générer dans l'esprit des personnes concernées le sentiment que leur vie privée fait l'objet d'une surveillance constante […] [et] pourrait avoir une incidence […] sur l'exercice […] de leur liberté d'expression."61

Quand des États contraignent des fournisseurs à générer et conserver des données, ces obligations ne sont pas conformes à la législation internationale des droits humains lorsqu'il s'agit de mesures généralisées, lesquelles ne sont « ni nécessaires ni proportionnées ».[62] La CJUE a stipulé que le respect des droits à la vie privée et à la liberté d'expression nécessite que les États établissent un lien entre les données à conserver et l'objectif spécifique poursuivi, et qu'ils limitent la conservation des données à des périodes de temps, des crimes ou des lieux spécifiques.[63]

Outre la conservation de données imposée par l'État, les fournisseurs devraient limiter la quantité de données à caractère personnel demandées à leurs utilisateurs et stockées, y compris à des fins publicitaires. Cela permettrait aux internautes de renforcer leur sentiment de confidentialité et d'exercer leur droit à la liberté d'expression sans craindre de surveillance. De plus, cela garantirait que les fournisseurs sont en mesure de respecter leurs obligations sur la protection des données, qui contraint les entreprises à réduire au minimum la quantité de données collectées, et à supprimer les données à caractère personnel identifiables lorsqu'elles ne sont plus nécessaires. En outre, les entreprises ne sont pas autorisées à utiliser les données recueillies à des fins spécifiques – par exemple pour faciliter l'accès des usagers d'Internet à des applications de messagerie – pour d'autres fins incompatibles, comme la publicité, sans avoir préalablement obtenu le consentement éclairé de l'usager.

Faciliter la surveillance étatique

Bien que les opérateurs de télécommunications aient longtemps agi comme des intermédiaires dans la surveillance étatique, la portée, la diversité et la gravité de la surveillance moderne dépassent de loin les anciens programmes d'interception. Alors que l'interception du courrier postal et les écoutes téléphoniques terrestres ont permis aux opérateurs télécoms de faciliter l'accès de l'État à un faible pourcentage de courriers personnels et d'appels téléphoniques, les fournisseurs sont devenus aujourd'hui le canal par lequel circule la quasi-totalité des communications, du commerce, de l'information et des connaissances du monde. Avec l'augmentation de la puissance de calcul, la diminution des coûts de stockage et l'augmentation des ambitions des gouvernements en matière de surveillance, les fournisseurs sont invités – et dans certains cas forcés – à mettre en œuvre et activer un appareil de surveillance mondial, dans de nombreux cas en violation des standards internationaux en matière de droits humains.

En plus de se conformer aux demandes d'accès à des données et des contenus personnels et à des données de communication (voir ci-dessus), les opérateurs télécoms disposent de nombreux moyens de faciliter la surveillance étatique :

- Modifications et mise à niveau des infrastructures de télécommunications ou élimination des protections sur les infrastructures pour permettre la surveillance par l'État ;

- Installation d'équipements de surveillance étatique directement sur l'infrastructure de télécommunications ; et

- Permettre aux États d'accéder directement – ou de contrôler – les infrastructures de télécommunications à des fins de surveillance.

Bien que la surveillance exercée par les autorités gouvernementales puisse être une restriction justifiée des droits humains, elle doit se conformer au test d'admissibilité des ingérences. Dans le contexte de la surveillance des télécommunications, les considérations suivantes doivent être prises en compte :

- **Légalité** : Alors que les mesures de surveillance doivent s'appuyer sur la législation nationale, et être compatibles avec l'État de droit, dans de nombreux pays, la surveillance n'est pas du tout réglementée, ou elle ne satisfait pas aux exigences relatives à la qualité du droit. Les lois sur la surveillance doivent être suffisamment claires et précises pour permettre aux personnes de savoir précisément dans quelles circonstances leurs communications peuvent être interceptées et surveillées.[64] Elles doivent également préciser la portée du pouvoir discrétionnaire accordé au cadre supérieur ou au juge habilité à ordonner la surveillance, et être accompagnées de garanties spécifiques.[65]

- **Nécessaire pour atteindre un objectif légitime et proportionné à cet objectif** : Parce que les instruments internationaux relatifs aux droits humains ne fournissent pas une liste exclusive d'objectifs légitimes justifiant légalement une surveillance, les droits humains se concentrent plutôt sur les garanties en place pour se prémunir contre les abus des lois sur la surveillance, notamment les lois spécifiant les processus d'autorisation et de surveillance, et les limites de la durée de la surveillance.[66] Les autorisations devraient être ciblées, délivrées par une autorité judiciaire indépendante, et soumises à l'existence d'un soupçon raisonnable contre la personne concernée.[67]

  Le test de proportionnalité nécessite d'examiner si le même objectif peut être atteint par des moyens moins intrusifs. Il doit également tenir compte de l'impact de la mesure sur les droits humains ; dans le contexte des mesures de surveillance, qui affectent potentiellement des centaines de millions d'utilisateurs d'un réseau particulier, le critère de proportionnalité sera rarement satisfait.

Recours contre les violations des droits humains

Bien qu'elles soient considérées comme un pilier essentiel des Principes directeurs, les obligations du secteur privé visant à fournir un accès à des recours effectifs sont souvent négligées dans l'élaboration des politiques. En effet, la fourniture de recours effectifs en cas de violation des droits humains est souvent considérée comme « le pilier oublié » du cadre des Principes directeurs. Par ailleurs, les Principes directeurs se concentrent principalement sur l'obligation de l'État de faciliter la réparation et, par conséquent, la réflexion sur les responsabilités du secteur privé dans ce domaine reste encore peu développée.

Certaines recommandations ont été élaborées par des organisations de la société civile. Par exemple, le Telco Remedy Plan d'Access Now expose les aspects procéduraux et concrets de la réparation dans le contexte des opérateurs télécoms.[68] Ce plan relatif aux recours s'appuie sur des directives plus générales comme celles du Conseil de l'Europe[69] , et sur le Guide du secteur des TIC relatif à la mise en œuvre des Principes directeurs sur les entreprises et les droits de l'homme[70], et décrit spécifiquement les mesures concrètes et procédurales que les opérateurs télécoms et les FAI devraient mettre en place pour permettre la réparation des violations des droits humains des internautes. Le Telco Remedy Plan affirme que les opérateurs télécoms devraient introduire une large gamme de mesures, notamment :

Mesures procédurales

- Intégrer la question des recours dans les processus d'évaluation préalable, avec l'aide de toutes les parties prenantes, avant de pénétrer de nouveaux marchés ou d'offrir de nouveaux services sur des marchés existants ;

- Chercher à mettre en œuvre des mécanismes de traitement des griefs qui soient sécurisés et accessibles aux plaignants ;

- Répondre rapidement et efficacement aux plaintes soumises aux mécanismes de règlement des griefs de l'entreprise ;

Mesures concrètes

- Examiner et trouver des moyens de cesser ou modifier, de manière effective et avec diligence, les activités ayant des effets négatifs sur les droits humains ;

- Interroger les cadres supérieurs et le personnel qui supervisent et mènent les activités incriminées, et réviser les directives internes pertinentes. Clarifier si le personnel a dévié des directives ou si les directives elles-mêmes ont échoué. Pour réduire les risques de reproduction, réviser les politiques internes, reformer le personnel et informer les partenaires commerciaux, le public et le personnel des changements de politiques internes ;

- Conserver les preuves dans la mesure du possible et les publier le cas échéant, en particulier lorsque des obstacles empêchent l'accès à un recours à court terme. Dans le cas où l'État est l'instigateur des activités incriminées des opérateurs télécoms, les éléments de preuve peuvent éclairer la recherche d'un recours effectif par une victime, en particulier lorsque l'État refuse de reconnaître son rôle dans la surveillance illicite, la censure ou l'ingérence dans le réseau ;

- Après consultation des personnes affectées, reconnaître sa part de responsabilité et présenter des excuses, le cas échéant, pour toute contribution à la violation de droits humains. Dans de nombreux cas, des excuses et des garanties qu'il n'y aura pas de répétition des violations peuvent contribuer à réparer les dommages subis par les victimes ;

- Se soumettre à une enquête indépendante ou à une supervision permanente conduite indépendamment de l'opérateur télécoms, et avec un accès complet aux dirigeants et aux dossiers de l'entreprise. Les enquêtes devraient se dérouler de manière transparente, dans un délai connu du public, et en coordination avec de multiples parties prenantes, y compris la société civile, des experts juridiques et des spécialistes de la réglementation et des représentants des gouvernements. Une supervision permanente est nécessaire lorsque la même forme d'infraction s'est reproduite à plusieurs reprises, ou

lorsqu'il apparaît que l'infraction résulte de problèmes systémiques au sein de l'entreprise ;

- Organiser et participer à des entités régionales ou sectorielles, dotées d'une participation multipartite structurée, pour clarifier et atténuer le rôle des opérateurs télécoms dans les violations systémiques des droits humains. Ces organes devraient adopter les meilleures pratiques de transparence et de redevabilité, qui devront être élaborées et mises à jour en collaboration avec d'autres acteurs et selon un calendrier régulier et connu du grand public Les changements de politiques internes et les autres résultats devraient être coordonnés et évalués en fonction de critères de référence bien établis ;

- Indemniser les victimes et les communautés touchées. L'indemnisation des violations des droits humains est devenue compréhensible à la lumière du « Fonds d'affectation spéciale au profit des victimes » de la Cour pénale internationale. Si le secteur des télécommunications créait un tel fonds, il pourrait bénéficier d'un soutien sectoriel, à la fois financier et moral, et s'appuyer sur la vaste expertise des plus grands opérateurs, fondations, gouvernements, investisseurs et acteurs de la société civile dans le monde.

Bien que non exhaustifs, les principes énoncés ci-dessus fournissent une base solide pour entamer des discussions sur les responsabilités des opérateurs télécoms et des FAI en matière de réparations aux victimes de violations des droits humains. Si ces principes étaient appliqués aux mesures incriminées les plus courantes des opérateurs et des FAI, ARTICLE 19 estime que leur respect imposerait aux fournisseurs de suivre différentes étapes en vue de remédier aux violations de la liberté d'expression (voir dernière section).

Recommandations d'ARTICLE 19

Recommandations générales

ARTICLE 19 recommande que les fournisseurs adoptent une approche fondée sur les droits humains dans leurs activités, qui donne corps aux principes et recommandations qui suivent. Nous recommandons également que les fournisseurs participent à – et envisagent de soutenir – des initiatives d'autorégulation afin de surveiller et promouvoir les droits humains conformément à ces recommandations.

Recommandation 1 : Respect des principes internationaux relatif aux droits humains

Les opérateurs télécoms et les FAI devraient garantir que leurs activités sont compatibles avec les standards en matière de droits humains reconnus par la communauté internationale. Lorsque les législations locales et les exigences d'un État entrent en conflit avec ces normes, les fournisseurs devraient chercher à s'aligner autant que possible sur les principes internationaux relatifs aux droits humains.

Les fournisseurs ne devraient pas agir sur une quelconque injonction de l'État qui constitue une infraction manifeste des droits humains, sauf si cette injonction émane d'une autorité judiciaire indépendante, et ils devraient épuiser tous les recours possibles pour les contester. Les fournisseurs peuvent également renforcer leur influence en collaborant avec des entreprises homologues pour contester ces injonctions, et mobiliser le public et la société civile contre de telles injonctions. Il est essentiel que les fournisseurs mettent en œuvre toutes les injonctions de l'État d'une manière qui réduise l'impact sur les utilisateurs finaux individuels.

Dans toute la mesure du possible, les fournisseurs devraient publier des informations sur les demandes ou les injonctions des pouvoirs publics visant à entraver les droits humains. Si des fournisseurs sont astreints au secret, ils devraient envisager d'adopter des approches innovantes telles que les « warrant canaries » pour donner aux individus une indication relative à l'existence de demandes ou d'injonctions. (Les "warrant canaries" ou "canaris de sécurité" (en référence aux canaris en cage utilisés dans les mines pour vérifier que l'air n'était

pas vicié) désignent le fait pour les fournisseurs de confirmer à leurs usagers qu'ils n'ont pas reçu du gouvernement l'ordre de mettre en place des mesures de surveillance.)

Les fournisseurs devraient s'opposer activement à toute demande ou injonction visant à leur arracher le contrôle des infrastructures de télécommunication pour le placer dans les mains du gouvernement. Cela inclut, par exemple, des demandes du gouvernement de fournir un accès direct à leur infrastructure. Les fournisseurs devraient déployer tous les efforts possibles pour empêcher cette éventualité.

Les fournisseurs devraient promouvoir des mesures innovantes pour renforcer les droits individuels, en particulier le droit à la liberté d'expression et le droit à la vie privée, même si de telles mesures devaient empêcher, ou contrecarrer, les demandes ou les injonctions du gouvernement. Cela inclut l'application de technologies avancées de chiffrement aux réseaux de télécommunications, et la réduction des données recueillies et conservées afin de réduire le risque de divulgation forcée.

Recommandation 2 : Garantir la clarté et l'accessibilité

Les conditions d'utilisation des fournisseurs devraient être disponibles et accessibles pour le grand public, et formulées avec suffisamment de précision pour permettre aux individus d'en comprendre les implications et d'adapter leur conduite en conséquence.

Les conditions d'utilisation devraient être formulées clairement et ne pas se dissimuler derrière des références obscures à l'obéissance aux lois locales. Elles devraient énoncer explicitement les législations pertinentes auxquelles les opérateurs télécoms doivent se conformer et indiquer dans quelles circonstances l'entreprise doit se soumettre aux demandes et aux injonctions du gouvernement susceptibles d'enfreindre les droits à la liberté d'expression et au respect de la vie privée d'un individu. Les fournisseurs devraient trouver des moyens innovants d'informer leurs usagers sur l'impact de leurs conditions d'utilisation, y compris en utilisant de l'iconographie, des images et des explications interactives de leur contenu.

Les conditions d'utilisation devraient inclure l'engagement des fournisseurs de s'aligner autant que possible sur les principes internationaux en matière de droits humains et garantir aux utilisateurs que les fournisseurs contesteront les

injonctions des autorités demandant la coupure de l'accès à Internet, la restriction de services et d'applications, l'accès aux données à caractère personnel et la coopération dans la surveillance étatique.

Les conditions d'utilisation devraient assurer aux individus que le fournisseur ne coupera jamais volontairement ou de manière punitive l'accès d'une personne à Internet.

Toute personne devrait avoir un accès facile et gratuit aux conditions d'utilisation des fournisseurs. Ces conditions devraient être accessibles sous une variété de formats qui tiennent compte des disparités d'alphabétisation, d'éducation, d'âge et de capacité des usagers. Les conditions d'utilisation devraient utiliser autant que possible un langage simple.

Recommandation 3 : Participation

Les conditions d'utilisation devraient donner aux individus le droit de participer à la prise de décisions qui affectent leurs droits humains.

Les conditions d'utilisation devraient être fondées sur l'obtention du consentement éclairé et explicite des individus. À cet égard, les conditions de service devraient exiger une manifestation explicite et non ambiguë du consentement de l'utilisateur aux termes de la relation avec l'opérateur télécoms. Le consentement à l'utilisation, la génération, l'analyse et la conservation de données à caractère personnel à certaines fins s'applique uniquement aux fins que le fournisseur aura directement explicitées à l'individu. Quand l'opérateur voudra recueillir un plus grand volume de données à caractère personnel, ou utiliser des données existantes de manière différente et incompatible, il devra obtenir un nouveau consentement éclairé et ne pas se contenter uniquement du précédent.

Les conditions d'utilisation devraient assurer que les individus seront avisés des mesures affectant leurs droits humains. À cet égard, les conditions d'utilisation devraient préciser les circonstances dans lesquelles les utilisateurs pourront ne pas être informés, par exemple dans l'éventualité où des injonctions de confidentialité (« gag orders ») peuvent être délivrées dans le contexte de la surveillance.

Recommandation 4 : responsabilisation des individus

Les individus devraient être suffisamment informés pour être capables de comprendre et utiliser les conditions d'utilisation et de pouvoir les contester dans certaines circonstances.

Les conditions d'utilisation devraient préciser quand et comment les individus ont le droit de contester les termes de la relation contractuelle. Toute personne devrait être informée des mécanismes de règlement des griefs et de réparation disponibles pour pouvoir soumettre des plaintes relatives aux conditions d'utilisation et en demander des modifications.

Les conditions d'utilisation devraient informer les individus de leur droit d'accéder à tout moment à toutes les données à caractère personnel les concernant détenues par les fournisseurs, et d'en demander la modification ou la suppression par l'opérateur et les filiales avec lesquelles elles ont pu être partagées dans le cadre d'un accord. Les utilisateurs devraient pouvoir exporter leurs données personnelles sous un format ouvert et accessible.

Les fournisseurs devraient soutenir les initiatives de littératie numérique destinées à éduquer les internautes sur la meilleure façon de protéger la sécurité et la confidentialité de leurs informations en ligne, et faciliter ainsi l'autonomisation des usagers. Ils devraient également coopérer avec l'ensemble de l'industrie en matière de standards de portabilité des données afin de garantir que le changement de fournisseur devienne une réalité facile à mettre en œuvre pour les internautes.

Recommandation 5 : Non-discrimination et égalité

Les conditions d'utilisation devraient garantir aux personnes un accès sans discrimination au contenu, aux applications et aux services.

La neutralité du Net devrait être garantie dans les conditions d'utilisation. Les fournisseurs devraient garantir aux utilisateurs qu'ils ne mettront pas en place de discrimination contre le contenu des communications sur la base de l'origine, la destination ou le fournisseur de service, et qu'ils ne restreindront en aucune manière que ce soit le contenu, les applications ou les services auxquels un individu peut accéder, sauf exceptions reconnues et lorsque

cela se révèle nécessaire pour la gestion du trafic. Les services gratuits ne doivent pas être conditionnés à une restriction de l'accès au contenu, aux applications ou aux services.

Les conditions d'utilisation devraient préciser aux utilisateurs lorsque le fournisseur est soumis à des injonctions judiciaires visant la restriction de contenu, d'applications ou de services, et que les utilisateurs seront immédiatement informés de la réception de pareilles injonctions. Les conditions d'utilisation devraient alerter les internautes sur l'utilisation potentielle d'injonctions de confidentialité ("gag orders") et des mesures mises en place par l'opérateur télécoms pour les contourner, telles que des « warrant canaries ».

Les mesures de gestion du réseau admissibles devraient être expliquées de manière claire et digeste aux internautes. Les usagers individuels devraient avoir la possibilité de participer à des processus de monitorage indépendants et transparents qui garantissent le respect de la neutralité du Net.

Les fournisseurs devraient publier régulièrement des rapports de transparence, y compris en ce qui concerne le détail des injonctions dont l'opérateur télécoms a fait l'objet, et en vertu desquelles l'accès à certains contenus, applications ou services, a été restreint. Les fournisseurs devraient également publier, au moins une fois par an, des informations sur leurs pratiques de gestion du réseau.

Recommandation 6 : Redevabilité

Dans les conditions d'utilisation, les fournisseurs devraient être clairs et transparents sur les conditions dans lesquelles les droits humains des individus feront l'objet de restrictions. En particulier, les conditions d'utilisation devraient préciser comment et dans quelles conditions les fournisseurs répondront aux injonctions du gouvernement. Les conditions d'utilisation devraient fournir aux individus des voies de recours pour contester ces décisions.

Les conditions d'utilisation devraient expliciter les circonstances susceptibles d'entraîner une violation des droits à la liberté d'expression et au respect de la vie privée des individus. Elles devraient indiquer dans

quelles conditions le fournisseur acceptera ou accédera aux demandes et aux injonctions de l'État. Elles devraient également indiquer comment les utilisateurs peuvent accéder à des informations sur le type et le nombre de demandes et d'injonctions reçues par le fournisseur, et auxquelles il s'est conformé.

Les conditions d'utilisation devraient expliquer en détail comment les individus peuvent accéder aux mécanismes de règlement des griefs et de réparation pour se plaindre de, ou contester, la manière dont l'opérateur télécoms respecte ses conditions d'utilisation.

Recommandations spécifiques

Recommandations sur les coupures de réseau

Face aux injonctions ou demandes visant à faciliter des mesures qui violent manifestement les standards internationaux relatifs aux droits humains, les fournisseurs ont la responsabilité de respecter les principes internationaux en matière de droits humains dans toute la mesure du possible.[71] Cela implique la responsabilité de prendre les mesures suivantes concernant les coupures de réseau :[72]

Préparation et prévision

- Identifier les lois nationales qui pourraient être utilisées pour ordonner des coupures de réseau ;
- Consulter des acteurs locaux de la société civile, des entreprises homologues et d'autres sources d'information pour identifier les situations dans lesquelles l'État est susceptible d'imposer une coupure de réseau ;
- Éduquer le personnel sur la possibilité d'une coupure de réseau et concevoir une stratégie au niveau de la prise de décision, y compris une stratégie de communication publique, à utiliser en cas de coupure ;

Stratégies de résistance

- Demander au gouvernement de clarifier l'intention, la durée et la portée de la coupure ;

- Épuiser les voies de recours internes pour contester l'injonction ordonnant la coupure du réseau, y compris en employant des moyens légaux devant les autorités judiciaires ;

- Coordonner les réponses avec les entreprises homologues afin d'accroître les moyens de pression ;

Atténuation et communication

- Identifier les individus potentiellement affectés et les informer de l'existence de la coupure de réseau, de la durée et de la portée qui ont été prévues pour cette coupure, et leur fournir des moyens d'obtenir de plus amples informations ;

- Maintenir le contrôle de l'infrastructure du fournisseur tout au long du processus ;

- Organiser et limiter la coupure (géographiquement et temporairement) autant que possible ;

- Restaurer l'accès aussitôt que possible.

Les conditions d'utilisation devraient préciser clairement les circonstances dans lesquelles l'accès des individus à Internet sera coupé suite à une décision imposée par l'État. En particulier, dans leurs conditions d'utilisation, les fournisseurs devraient s'engager à :

- Ne pas mettre en œuvre les coupures de réseau tant que toutes les voies de recours internes n'ont pas été épuisées ;

- Informer immédiatement les individus d'une coupure imminente et leur fournir régulièrement des informations actualisées sur la coupure ; et

- Fournir aux individus des mécanismes de règlement des griefs et de réparation pour compenser tout impact négatif de la coupure sur lequel l'opérateur télécoms est en mesure d'agir.

Recommandations sur les lois prévoyant des réponses graduées

Les conditions d'utilisation des fournisseurs devraient indiquer aux utilisateurs quand une loi prévoyant des réponses graduées s'applique au pays où ils opèrent, et énoncer clairement les conditions dans lesquelles l'accès sera coupé en vertu de ces lois.

- Dans leurs conditions d'utilisation, les fournisseurs devraient s'engager à :

- Ne jamais couper l'accès d'un individu à Internet volontairement ou de manière punitive ;

- Couper l'accès d'un individu à Internet uniquement lorsqu'une injonction a été émise par une autorité judiciaire indépendante ;

- Informer immédiatement l'utilisateur si une injonction de déconnexion le concernant est reçue ;

- S'opposer à l'injonction de déconnexion au nom de l'utilisateur jusqu'à épuisement de tous les recours internes.

Recommandations sur la neutralité du Net

Les fournisseurs doivent s'abstenir d'appliquer volontairement des mesures qui enfreignent le principe de la neutralité du Net. Quand ils sont légalement tenus de restreindre l'accès à des services ou des applications spécifiques, ils doivent agir de manière à assurer autant que possible le respect des principes internationaux en matière de droits humains. À cet égard, les conditions d'utilisation des fournisseurs devraient les engager à :

- Ne pas exercer de discrimination contre, ou ne pas prioriser, le contenu sur la base de l'origine, de la destination ou du prestataire de service, ou du type d'application ou de service ;

- Ne restreindre en aucune manière le contenu, les applications ou les services auxquels un utilisateur peut accéder, sauf aux fins de la gestion du réseau, et limiter cette priorisation à ce qui est strictement requis ;

- Ne pas conditionner la fourniture de services gratuits à un accès restreint à des contenus, des applications ou des services ;

- Limiter l'accès au contenu, aux applications ou aux services uniquement lorsqu'une injonction est adoptée par une autorité judiciaire indépendante ;

- Informer immédiatement les usagers lorsqu'une telle injonction est reçue ;

- Contester ces injonctions jusqu'à ce que toutes les voies de recours internes aient été épuisées ;

- Publier régulièrement les détails des injonctions dont l'opérateur télécoms fait l'objet, et en vertu desquelles l'accès à certains contenus, applications ou services est restreint ;

- Publier régulièrement des informations sur les pratiques de gestion du réseau ;

- Se soumettre à un monitorage externe et indépendant des mesures de gestion du trafic, et expliquer aux internautes comment ils peuvent participer à ces processus ;

- S'abstenir d'utiliser des mesures de gestion du trafic qui s'immiscent dans la vie privée (telles que l'inspection approfondie des paquets).

Toutefois, les fournisseurs pourraient envisager des alternatives « positives » au zero-rating, par exemple en offrant un accès gratuit avec des plafonds de données mensuels. Ils pourraient également encourager des fournisseurs tiers à offrir des versions de leurs services avec un usage de données plus efficace à tous les internautes (par exemple en utilisant une meilleure compression, un débit audio et/ou une résolution vidéo plus faibles).

Recommandations sur la protection des données

Les fournisseurs devraient utiliser leurs conditions d'utilisation pour communiquer clairement et explicitement avec les individus à propos des données personnelles qui leur sont demandées, et qui sont générées, collectées et stockées à leur sujet. Ils devraient s'engager à :

- Toujours obtenir un consentement éclairé de l'individu lorsqu'ils utilisent ses données personnelles à des fins nouvelles ou incompatibles ;

- Demander aux individus de divulguer une quantité minimale de données à caractère personnel nécessaires pour la fourniture d'un accès aux télécommunications ;

- Informer les individus sur la manière dont leurs données personnelles sont employées, combien de temps elles sont conservées, et avec qui elles sont partagées ;

- Supprimer les données à caractère personnel identifiables dès qu'elles ne sont plus nécessaires pour fournir un accès à l'utilisateur;

- Permettre aux personnes d'accéder et de réviser, à tout moment, les données à caractère personnel détenues par l'opérateur télécoms et les fins auxquelles elles s'y trouvent ;

- Permettre aux utilisateurs de retirer à tout moment leur consentement au traitement des données personnelles les concernant ;

- S'assurer que les données à caractère personnel sont protégées par des mesures de sécurité techniques et organisationnelles de pointe ;

- Aviser immédiatement les personnes quand des injonctions de conservation des données obligatoire sont reçues ;

- Informer immédiatement les individus quand des demandes d'accès à des données à caractère personnel, ou à des données de communications ou à des contenus des abonnés, sont reçues ;

- Contester ces demandes au nom de l'individu jusqu'à ce que toutes les voies de recours interne aient été épuisées ;

- Informer les individus quand leurs données personnelles sont transmises à une autorité gouvernementale ou à une tierce partie ;

- Publier régulièrement des détails sur toute injonction dont l'opérateur télécoms fait l'objet, et en vertu de laquelle des données sont générées, conservées et divulguées ;

- Publier régulièrement des informations sur les données à caractère personnel et les données de communications ainsi que les contenus divulgués aux autorités gouvernementales ou à d'autres tierces parties ;

- Fournir aux individus un mécanisme de règlement des griefs ou de réparation pour contester la divulgation de données à caractère personnel en infraction aux conditions de service.

Recommandations sur la surveillance

Bien que certaines injonctions ou demandes d'aide à la surveillance étatique puissent être justifiées, les fournisseurs seront d'autant plus capables de garantir qu'ils satisfont à leurs obligations de protéger et promouvoir les droits humains qu'ils résisteront à une demande ou injonction susceptible de leur retirer le contrôle de l'infrastructure des télécommunications pour le mettre aux mains du gouvernement. L'acquiescement à de telles demandes crée un précédent dangereux, qui risque d'induire pour l'Etat une attente que l'opérateur continuera à modifier ses produits et services conformément aux préférences du gouvernement. Tout excès de zèle dans l'obéissance aux injonctions ou demandes émanant des autorités étatiques devrait être évité en toutes circonstances.

Les fournisseurs devraient également promouvoir des mesures innovantes pour renforcer la libre expression et les droits à la vie privée des individus, y compris lorsque ces mesures contrecarrent ou empêchent les objectifs de surveillance de l'État. Cela inclut, principalement, l'application de technologies avancées de chiffrement aux réseaux de télécommunications.

Les fournisseurs devraient préciser à leurs usagers dans leurs conditions d'utilisation comment ils répondront aux requêtes et aux demandes de l'État visant à faciliter la surveillance. Ces informations devraient être complètes et franches, et ne pas se cacher derrière des références génériques au respect des législations locales. Les fournisseurs devraient s'engager à :

- Examiner minutieusement toute requête ou demande des États de mettre à niveau ou de modifier une infrastructure existante, ou d'installer des capacités de surveillance ;

- Épuiser tous les recours disponibles pour contester toute requête ou demande de mise à niveau ou de modification de l'infrastructure ou d'installation de capacités de surveillance ;

- Résister activement, y compris en utilisant des pressions publiques, des actions collectives, et des menaces de retrait du marché, contre toute requête ou demande des États d'accéder directement aux réseaux de télécommunications ;

- Publier des informations, dans la mesure du possible, sur toute mesure prise pour mettre à niveau ou modifier une infrastructure ou installer une surveillance ou fournir un accès direct ;

- Quand cela est faisable, informer les usagers individuels des mesures de surveillance spécifiques dont ils ont fait l'objet ;

- Fournir un mécanisme de règlement des griefs ou de réparation pour permettre à des individus de contester la décision des fournisseurs de se soumettre à des requêtes ou des demandes.

Recommandations sur les réparations

Les opérateurs télécoms et les FAI devraient s'assurer que des mécanismes de règlement des griefs et de réparation sont en place pour traiter les impacts négatifs de leurs actions auxquels ils sont en mesure de remédier.

De solides pratiques de transparence pourraient fournir une forme de réparation[73] en accordant aux usagers affectés le droit d'être entendu sur l'impact de l'ingérence sur leur existence. Par ailleurs, la fourniture d'informations aux usagers affectés sur la nature, la portée et l'origine des

violations des droits humains peut contribuer à les rendre autonomes. Dans le contexte des coupures de réseau, par exemple, la fourniture aux internautes d'informations mises à jour régulièrement et en permanence renforcera leur capacité à atténuer les effets négatifs de la coupure de réseau.

Dans le cas de demandes sérieuses et systématiques de l'État de faciliter les abus des droits humains, les opérateurs télécoms et les FAI devraient examiner si la conformité avec les standards internationaux en matière de droits humains peut être mieux mise en oeuvre à **travers la cessation des activités de l'entreprise** dans un pays ou un contexte particulier.

La cessation d'activité est un recours qui pourrait en soi saper les droits humains des internautes ; elle pourrait priver les internautes de la connectivité de manière temporaire ou permanente, accroître les coûts de la connexion, et faciliter le développement des marchés monopolistiques. Toutefois, quand les opérateurs télécoms sont régulièrement soumis aux pressions du gouvernement en vue de faciliter de graves infractions aux droits humains, en particulier la surveillance et les coupures de réseau, les préjudices causés aux usagers à travers ces infractions dépassent les dommages résultant de la cessation d'activité.

Dans ces circonstances, les opérateurs télécoms devraient entreprendre une évaluation complète, en collaboration avec les parties prenantes, de la nécessité, des effets et des impacts potentiels de la rupture des activités commerciales dans le pays concerné. La cessation d'activité doit être décidée en dernier ressort et uniquement après des consultations avec d'autres entités sectorielles sur la possibilité d'engager une action collective contre le gouvernement concerné.

De plus, les opérateurs télécoms et les FAI devraient envisager les mesures correctives spécifiques suivantes :

Pour les coupures de réseau

- Fournir des informations entières et complètes, par tous moyens efficaces, sur l'existence et l'étendue de la coupure et, le cas échéant, sur l'existence de solutions d'accès alternatif (et les implications de l'utilisation de telles solutions) ;

- Rétablir immédiatement la connexion au réseau dès que la possibilité s'en présente ;

- Solliciter et archiver les rapports des usagers, afin de permettre à ceux dont la connexion a été restreinte d'expliquer et de documenter leur expérience de la coupure ;

- Envisager d'étendre les crédits de compte ou les promotions en tant de compensation universelle ou de modifier les périodes de paiement des factures ;

- Prendre des mesures en vue d'indemniser les individus ayant subi des pertes financières avérées ou des dommages importants en raison de la coupure ; et

- Organiser immédiatement des discussions à l'échelle du secteur pour examiner comment mobiliser une action collective contre de nouvelles coupures imposées par le gouvernement.

Pour les lois prévoyant des réponses graduées

- Rétablir immédiatement la connexion des personnes affectées, soit après avoir réussi à annuler l'injonction de coupure ou après l'expiration de la période de déconnexion ; et

- Prendre des mesures pour indemniser les individus ayant subi des pertes financières avérées ou des dommages importants en raison de la déconnexion.

Pour la neutralité du Net

- Présenter ses excuses aux usagers et fournir des informations entières et complètes sur les mesures prises par l'opérateur pour prioriser, exercer une discrimination contre, ou restreindre, un contenu particulier ;

- Fournir des assurances aux usagers que leur accès futur au réseau ne fera pas l'objet d'une priorisation, d'une discrimination ou d'une restriction ;

- Adopter des mesures de transparence en vue de permettre une supervision indépendante des mesures de gestion du réseau ; et

- Apporter un soutien aux individus pour intenter une action en justice pour réparation ou indemnisation de l'État responsable.

Pour la violation de la protection des données

- Fournir aux usagers affectés des informations entières et complètes sur les données personnelles les concernant qui ont été générées, conservées et divulguées ;

- Fournir des garanties que les données à caractère personnel ont été supprimées et que toute tierce partie ayant reçu ce type de données a été invitée à les supprimer ; et

- Prendre des mesures pour indemniser les individus ayant subi des pertes financières avérées ou des dommages importants suite à la génération, la conservation et la divulgation de données à caractère personnel.

Pour la surveillance

- Informer l'usager affecté, et fournir des informations entières et complètes sur le type et la portée de la surveillance dont il a fait l'objet ;

- Solliciter et archiver les rapports des utilisateurs affectés pour leur permettre d'expliquer et de documenter leur expérience de la surveillance ;

- Prendre des mesures en vue d'indemniser les individus ayant subi des pertes financières avérées ou des dommages importants en raison de la surveillance ; et

- Apporter un soutien aux individus pour intenter une action en justice pour réparation ou indemnisation de l'État responsable, y compris en contestant la légalité de la surveillance, le cas échéant.

À propos d'ARTICLE 19

ARTICLE 19 est une organisation internationale de défense des droits humains créée en 1987, qui défend et promeut la liberté d'expression et le droit à l'information dans le monde entier.

Son mandat s'appuie sur la Déclaration universelle des droits de l'homme, qui garantit le droit à la liberté d'expression et d'information. Les technologies de l'information et de la communication telles que l'Internet sont devenues un moyen de plus en plus important pour s'exprimer, et pour rechercher, recevoir et diffuser des informations. ARTICLE 19 défend les libertés sur l'Internet depuis plus d'une décennie et œuvre à l'élaboration de politiques et de pratiques concernant la liberté d'expression et l'Internet par le biais de notre réseau de partenaires, associés et experts.

ARTICLE 19 encourage chaque organisation et chaque individu à nous adresser ses commentaires sur la manière dont ce document d'orientation est utilisé. Merci de nous envoyer vos commentaires à legal@article19.org.

Cette publication est entièrement ou partiellement financée par le gouvernement de la Suède. Le gouvernement de la Suède ne partage pas nécessairement les opinions exprimées dans ce document. ARTICLE 19 assume seul la responsabilité de son contenu.

Notes

1. L'importance des téléphones mobiles va bien au-delà des communications individuelles; par exemple, dans les pays en développement, la téléphonie mobile a joué un rôle important dans la promotion de la responsabilité démocratique, l'accès à l'information, et la propagation de campagnes nationales efficaces ; voir, par ex. ARTICLE 19, Kenya: Free expression standards should guide fight against "counterfeit" mobile phones, 11 octobre 2011.
2. Voir par ex. Conseil des droits de l'homme, Résolution sur la promotion, la protection et l'exercice des droits de l'homme sur Internet, A/HRC/32/L.20, adoptée le 27 juin 2016.
3. Voir par ex. Persbericht WRR, Policy Brief No. 2: The public core of the internet: an international agenda for internet governance, 10 avril 2015; ou Jacob Kastrenakes, Obama says FCC should reclassify Internet as a utility, The Verge, 10 novembre 2014.
4. Voir ARTICLE 19, Freedom of expression and the private sector in the digital age: Submission to the UN Special Rapporteur, 2016.
5. C.Cath, N. ten Oever & D O'Maley, Media Development in the Digital Age: Five Ways to Engage in Internet Governance, mars 2016.
6. Cela inclut, en particulier les documents d'orientation suivants d'ARTICLE 19:

- Intermédiaires Internet : le dilemme de la responsabilité (août 2013) portant principalement sur les schémas de responsabilité applicables aux acteurs opérant au niveau des contenus (notamment les hébergeurs) et au niveau social (les plateformes en ligne) d'Internet;
- Freedom of Expression Unfiltered: How blocking and filtering affect free speech (décembre 2016) qui examine la compatibilité du blocage et du filtrage de contenus en ligne avec les normes internationales, et fournit des recommandations aux gouvernements et aux entreprises;
- Document d'orientation: le droit à l'oubli (mars 2016) qui propose des recommandations complètes sur la manière d'assurer la protection du droit à la liberté d'expression au regard du dénommé « droit à l'oubli » ;
- The Global Principles on Freedom of Expression and Privacy (mars 2017) qui fournit un cadre analytique systématique permettant d'évaluer comment la liberté d'expression et la vie privée se renforcent mutuellement, et détermine les limites de ces droits en ligne et hors ligne lorsqu'ils entrent en conflit ;
- Policy Brief: ICANN's Corporate Responsibility to Respect Human Rights (octobre 2015) qui définit les raisons pour lesquelles les Principes directeurs des Nations Unies pour les entreprises et les droits de l'homme

sont le cadre le plus approprié pour l'ICANN dans sa mission d'élaboration des politiques et des processus des droits humains, et présente des options sur la manière dont l'ICANN peut commencer à les mettre en œuvre.

7. Par ex., British Telecom, la plus ancienne entreprise de télécommunications du monde, est d'abord passé sous contrôle de l'État sous la Poste avant de devenir une compagnie privée, le précurseur de BT Group Plc; voir par ex. BT, Origins of the BT. Au Brésil, le Code des Télécommunications de 1963 a instauré un monopole accordé par l'État, suivi par la création d'Embratel en 1965 et l'organisation ultérieure du système Telebras en 1972 avec des opérateurs télécoms régionaux, Embratel (responsable des appels nationaux et internationaux) et CPqD (unité de R&D); voir A.Musacchio & S.G.Lazzarin, State-Owned Enterprises in Brazil: History and Lessons, OCDE, 2014.
8. Par exemple aux USA ; voir R. W. Lucky & J. Eisenberg, The Evolution of the U.S. Telecommunications Industry and Effects on Research, NPA, 2016.
9. Voir ARTICLE 19, Brazil: ARTICLE 19 launches guide on community internet providers, 19 janvier 2017.
10. La Convention européenne des droits de l'homme (Article 10), la Charte des droits fondamentaux de l'Union européenne (Article 11), la Convention américaine des droits de l'homme (Article 13), la Charte africaine des droits de l'homme et des peuples (Article 9) et la Déclaration des droits humains de l'ASEAN (Article 23).
11. Voir par ex., le Comité des droits de l'homme, Observation générale n° 34, adoptée en juillet 2011.
12. Déclaration conjointe sur la liberté d'expression et Internet, Rapporteur spécial des Nations Unies sur la promotion et la protection du droit à la liberté d'opinion et d'expression, Représentant sur la liberté des médias de l'Organisation pour la sécurité et la coopération européennes (OSCE), Rapporteur spécial sur la liberté d'expression de l'Organisation des Etats américains (OEA) et Rapporteur spécial pour la liberté d'expression et l'accès à l'information de la Commission africaine des droits de l'homme et des peuples (ACHPR), 1er juin 2011; résolution du CDH sur Internet, *op.cit.*.
13. Voir, par ex., Comité administratif de coordination des Nations Unies, Statement of the Administrative Committee on Coordination on universal access to basic communication and information services, ACC/1997/4, 25 juin

de l'Europe, Comité des ministres, Recommandation n° R(99)14 sur le service universel communautaire relatif aux nouveaux services de communication et d'information, 9 septembre 1999. Au niveau national, un grand nombre de pays européens ont reconnu le droit d'accès à Internet dans leurs dispositifs légaux, soit dans leurs constitutions, leurs législations ou leur jurisprudence ; voir par ex. République d'Estonie, Public Information Act, 15.11.2000, article 33, et la Constitution de la République d'Estonie, 29 juin 1992, article 44; la Constitution de la Grèce, amendée par la résolution parlementaire du 6 avril 2001, article 5A.2, la République de Finlande, Communications Market Act, 393/2003, amendements 363/2011, Section 60c(2); Royaume d'Espagne, Loi sur l'économie durable, 2/2011, 4 mars 2011, Article 52.

14. Rapport 2011 du Rapporteur spécial sur la promotion et la protection du droit à liberté d'opinion et d'expression, *op.cit.*, par. 87.
15. Ce test a été rétabli dans un grand nombre d'instruments internationaux des droits de l'homme, notamment dans *l'Observation générale* n° 34 du Comité des droits de l'homme.
16. Déclaration conjointe 2011, op.cit.
17. Résolution du CDH sur Internet, op.cit.
18. Observation générale n° 34, op.cit. par. 43.
19. Voir la Convention européenne des droits de l'homme (Article 8), la Charte des droits fondamentaux de l'Union européenne (Article 7) et la Convention américaine des droits de l'homme (Article 11).
20. Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du Conseil de l'Europe , 28 janvier 1981.
21. Principes directeurs pour la réglementation des fichiers personnels informatisés, adoptés dans la Résolution 45/95 de l'Assemblée générale le 14 décembre 1990.
22. G. Greenleaf, Asian Data Privacy Laws (Oxford, Oxford University Press: 2014), 55. Pour plus de détails sur chacun des cadres nationaux, voir BakerHostetler, 2015 International Compendium of Data Privacy Laws.
23. Voir par ex.: décisions de la Cour européenne des droits de l'homme dans *Leander c. Suède*, App. No. 9248/81, 26 mars 1987; *S. et Marper c. Royaume-Uni*, App. Nos. 30562/04 et 30566/04, 4 décembre 2008; *Malone c. Royaume-Uni*, No. 8691/79, 2 août 1984; *Copland c. Royaume-Uni,* No. 62617/00, 3 avril 2007; *Klass et autres c. Allemagne*, No. 5029/71, 6 septembre 1978;

CEDH, *Uzun c. Allemagne*, No. 35623/05, 2 septembre 2010; ou les décisions de la Cour de justice de l'Union européenne (CJUE) dans C-293/12 et C-594-12, *Digital Rights Ireland c. Irlande*, 8.4.2014; ou C-362/14, *Schrems c. Data Protection Commissioner*, 6.10.2015.

24. En 2012, l'ASEAN a adopté une Déclaration des droits humains faisant spécifiquement référence à la protection des données à caractère personnel, et en 2014 l'Union africaine a adopté la Convention sur la cyber sécurité et la protection des données à caractère personnel.

25. Dans les observations finales de sa revue 2014 de conformité des États-Unis avec ses obligations en vertu de l'Article 17 du PIDCP, le Comité a observé que les ingérences dans le droit à la protection de la vie privée sont autorisées à condition de satisfaire aux principes de légalité, nécessité et proportionnalité ; CCPR/C/USA/CO/4, par. 22. Ce sentiment faisait écho à celui du Rapporteur spécial sur la protection du droit à la liberté d'opinion et d'expression dans son rapport 2013 sur la protection de la vie privée et la surveillance des communications, affirmant que le cadre de l'Article 17 du PIDCP autorise des restrictions nécessaires, légitimes et proportionnées du droit à la protection de la vie privée au moyen de restrictions admissibles, dont le test devrait s'appuyer sur les mêmes termes que ceux applicables en vertu de l'Article 19, paragraphe 3, bien que l'Article 17 n'utilise pas un langage aussi explicite. Le Haut-Commissariat aux droits de l'homme, dans son rapport 2014, Le droit à la vie privée à l'ère du numérique, a confirmé l'interprétation du Rapporteur spécial et a déclaré que : "Ces sources faisant autorité mettent en évidence les grands principes de la légalité, la nécessité et la proportionnalité..." A/HRC/27/37, par. 23.

26. Mis en évidence dans les Lignes directrices de l'OCDE de 1980 régissant la protection de la vie privée et les flux transfrontières de données à caractère personnel ; la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (connue sous le nom de Convention 108); et les Principes directeurs pour la réglementation des fichiers personnels informatisés des Nations Unies de 1990.

27. Ces Principes sont pris de l'Article 5 du Règlement général sur la protection des données, mais ils reflètent largement les Principes de traitement équitable des informations de la Federal Trade Commission des États-Unis d'Amérique, les Principes inscrits dans les lignes directrices de l'OCDE et des Nations Unies, la Convention 108 et la Directive européenne sur la protection des données, qui ont éclairé les réglementations sur la protection des données dans plus d'une centaine de pays dans le monde.

28. Cela inclut l'Observation générale n° 34, *op.cit.,* la Résolution sur Internet du CDH *op.cit.*; la Déclaration conjointe 2011 *op.cit.*; les rapports du Rapporteur spécial sur la liberté d'expression sur Internet (A/66/290, 2011), la surveillance et le droit à la protection de la vie privée (A/HRC/23/40, 2013), l'accès à l'information (A/68/335, 2014), et la protection des sources et des lanceurs d'alerte (A/70/361, 2015); décisions de la CEDH dans *Delfi AS c. Estonie* [GC], App. No. 64569/09, 16 juin 2015; *Editorial Board of* Pravoye Delo *& Shtekel c. Ukraine*, App. No. 33014/05, 5 mai 2011; *Niskasaari & Otavamedia Oy c. Finlande*, App. No. 32297/10, par. 9 et 54-59, 23 juin 2015; *Mosley c. Royaume-Uni,* App. No. 48009/08, § 129, 10 mai 2011; *Animal Defenders International c. Royaume-Uni* [GC] App. No. 48876/08, § 119, ou *Ahmet Yıldırım c. Turquie*, App. No. 3111/10, § 67, CEDH 2012.

29. Rapport du Rapporteur spécial sur la liberté d'expression relatif aux services de télécommunications et l'accès à Internet, A/HRC/35/22, 30 mars 2017. Le rapport du Rapporteur spécial de mai 2016 à l'Assemblée générale (A/HRC/32/28) est également instructif.

30. *Op.cit.*

31. Le Pacte mondial des Nations Unies est une initiative de l'ONU visant à encourager les entreprises dans le monde entier à adopter des politiques durables et socialement responsables, et à rendre des comptes sur leur mise en œuvre.

32. Les Principes directeurs ont été lancés en 2008 sous la houlette du Représentant spécial des Nations Unies John Ruggie. Ils s'appuient sur le travail du Pacte mondial, créé en 2000 afin d'encourager les entreprises à développer des pratiques commerciales

responsables.

33. Telecommunications Industry Dialogue Guiding Principles, 12 mars 2013.
34. Global Network Initiative, Global Principles on Freedom of Expression and Privacy, principes élaborés par des entreprises, des investisseurs, des organisations de la société civile et des universitaires.
35. Ranking Digital Rights, Corporate Accountability Index.
36. Ranking Digital Rights, 2015 Corporate Accountability Index Indicators.
37. CDT, Iran's Internet Throttling: Unacceptable Now, Unacceptable Then, 3 juillet 2013; Software Freedom Law Centre India, Internet Shutdowns in India, 2016; Access Now, Gambia shuts down Internet on eve of elections, 30 novembre 2016.
38. Voir CDT, Network Shutdowns Timeline, 11 septembre 2014.
39. Par ex. en Inde, Algérie, Éthiopie, Irak et Azerbaïdjan; voir rapport 2017 du Rapporteur spécial sur la liberté d'expression, *op.cit.*
40. D. O'Brien, Venezuela's Internet Crackdown Escalates into Regional Blackout, EFF, 20 février 2014.
41. Voir par ex. les observations préliminaires du rapporteur spécial sur la liberté d'expression à la fin de sa visite au Tadjikistan, 9 mars 2015.
42. Observation générale n° 34, *op.cit.*, par. 43.
43. De telles lois existent en Corée du Sud, Nouvelle-Zélande, France et au Royaume-Uni ; d'autres pays, comme l'Australie, ont envisagé cette approche avant de l'abandonner.
44. La loi HADOPI adoptée en France en 2009 autorisait la suspension de l'accès à Internet jusqu'à ce que les dispositions concernées aient été jugées illégales en 2013. Il y a eu également un programme volontaire "des six coups" aux Etats-Unis d'Amérique (baptisé Copyright Alert System) visant le même effet ; le programme a pris fin en janvier 2017.
45. Rapporteur spécial sur la liberté d'expression, Rapport au CDH, juin 2011 (A/HRC/17/27), par. 78.
46. A. Futter & A. Gillwald, Zero-rated Internet services: What is to be done?, Research ICT Africa.
47. J. Malcolm, C. McSherry & K.Walsh, Zero Rating: What It Is and Why You Should Care, 18 février 2016.
48. Au Maroc, Skype, Viber, Tango, WhatsApp, et Facebook Messenger comptent parmi les applications dont les appels VoIP ont été bloquées par les opérateurs télécoms sur des connexions 3G et 4G en janvier 2016 et des connexions ADSL en février 2016. En Chine, tous les services VoIP

non offerts par les opérateurs étatiques sont interdits.

49. Au Brésil, l'application WhatsApp a été temporairement bloquée en 2016 ; voir ARTICLE 19, Brazil: WhatsApp services blocked nationwide in violation of freedom of expression, 22 juillet 2016.
50. En 2016, le président des Émirats arabes unis a promulgué un certain nombre de lois fédérales liées aux crimes sur Internet, y compris une réglementation interdisant à toute personne des EAU de faire usage des réseaux privés virtuels (VPN).
51. L'agnosticisme du contenu se réfère à l'idée que le trafic du réseau est traité de manière identique quelle que soit la capacité, sauf quelques exceptions concernant la gestion du trafic, par exemple pour retarder des paquets sensibles en fonction de l'en-tête. L'agnosticisme du contenu empêche la discrimination contre des paquets fondée sur la capacité; voir N. ten Oever, Human Rights Protocol Considerations Research Group, Research into Human Rights Protocol Considerations draft-irtf-hrpc-research-11.
52. Voir par ex. ARTICLE 19, Our 5G future: Light at the end of the tunnel or Internet fast-lane for the elite?, 15 septembre 2016.
53. 5G Manifesto for timely deployment of 5G in Europe, 7 juillet 2016.
54. Voir par ex., The Register, EU operators' 5G manifesto misses the point, 13 juillet 2016.
55. Comme le Chili, la Norvège, les Pays-Bas, la Finlande, l'Islande, l'Estonie, la Lettonie, la Lituanie, Malte et le Japon.
56. Voir par ex. FCC, Protecting and Promoting the Open Internet, FCC 15-24, 12 mars 2015.
57. Voir Commission européenne, Our Commitment to Net Neutrality, octobre 2015.
58. En 2016, le Royaume-Uni a promulgué le *Investigatory Powers Act*, qui contraint les fournisseurs de services de télécommunications à générer et conserver des « fichiers des connexions Internet » pendant une durée maximale de 12 mois.
59. L'Australie a adopté une telle loi. En 2014, la Directive européenne sur la conservation des données a été invalidée, revenant sur les lois relatives à la conservation des données à travers l'Europe, bien que des systèmes de conservation des données aient été promulgués ultérieurement. Aux Etats-Unis d'Amérique, la conservation des données est rendue obligatoire par le Freedom Act depuis 2015; précédemment, la Section 215 du Patriot Act imposait des exigences similaires.
60. Cour interaméricaine des droits de l'homme, *Escher et. autres c. Brésil*, 6 juillet 2009, par. 114.
61. Voir, CJUE, *Watson et autres c.*

Royaume-Uni 698/15 (Affaires conjointes C-203/15, C-698/15), 21 décembre 2016, par. 99-101.

62. Haut-Commissaire aux droits de l'homme de l'ONU Navi Pillay, *Le droit à la vie privée à l'ère du numérique,* para 27.
63. CJUE, *Watson et autres c. Royaume-Uni*, *op.cit.*, par. 105-106.
64. CEDH, *Zakharov c. Russie*, App. No. 47143/06, 4 décembre 2015, par. [229].
65. CEDH, *Weber et Saravia c. Allemagne*, App. No. 54934/00, par. [95]
66. Voir par ex., Observations finales du Comité des droits de l'homme concernant le quatrième rapport périodique des États-Unis d'Amérique (CCPR/C/USA/CO/4), 2014, par. 22.
67. CEDH, *Zakharov c. Russie*, *op.cit.* par. [260].
68. Access Now, Forgotten Pillar: The Telco Remedy Plan, mai 2013.
69. Recommandation CM/Rec(2014)6 du Comité des ministres aux États membres sur un Guide des droits de l'homme pour les utilisateurs d'Internet.
70. Guide du secteur des TIC de la Commission européenne sur la mise en œuvre des Principes directeurs des Nations Unies sur les entreprises et les droits de l'homme, 2013.
71. Les Principes directeurs, *op.cit.,* Principe 23 – Questions relatives au contexte
72. Une grande partie de ces orientations proviennent du Guide du secteur des TIC de la Commission européenne sur la mise en œuvre des Principes directeurs des Nations Unies sur les entreprises et les droits de l'homme, p. 53.
73. Cf. le rapport 2017 du Rapporteur spécial sur la liberté d'expression, *op.cit.*

DEFENDING FREEDOM OF EXPRESSION AND INFORMATION

ARTICLE 19 Free Word Centre 60 Farringdon Road London EC1R 3GA
T +44 20 7324 2500 F +44 20 7490 0566
E info@article19.org W www.article19.org Tw @article19org facebook.com/article19org