Nations Unies A/HRC/29/32

Assemblée générale

Distr. générale
22 mai 2015
Français
Original : anglais

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

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

Résumé

Dans le présent rapport, soumis en application de la résolution 25/2 du Conseil des droits de l'homme, le Rapporteur spécial se penche sur le recours au chiffrement et à l'anonymat dans le domaine des échanges numériques. En s'appuyant sur des travaux de recherche relatifs aux normes et la jurisprudence internationales et nationales et sur les apports de certains pays et de la société civile, le rapport aboutit à la conclusion que le chiffrement et l'anonymat permettent aux personnes d'exercer leur droit à la liberté d'opinion et d'expression à l'ère du numérique et qu'ils méritent, à ce titre, une solide protection.

* Soumission tardive.

GE.15-07497 (F) 110815 120815

Table des matières

I. Introduction

1. Les technologies numériques actuelles donnent aux pouvoirs publics, aux entreprises, aux criminels et aux mauvais plaisants une capacité sans précédent d'empiéter sur le droit à la liberté d'opinion et d'expression. La censure en ligne, la surveillance généralisée ou ciblée et la collecte de données, les attaques numériques contre la société civile et la répression consécutive à l'expression en ligne obligent des citoyens, dans le monde entier, à se protéger afin de pouvoir émettre une opinion sans restrictions et rechercher, recevoir et transmettre toutes sortes d'informations et d'idées. Beaucoup cherchent à se protéger en cryptant et en brouillant leurs données pour que seuls leurs destinataires puissent y accéder, qu'il s'agisse de données dynamiques (transitant par exemple via le courrier électronique, les services de messagerie ou la téléphonie sur IP) ou statiques (par exemple le contenu de disques durs ou de services « en nuage »). Certains essayent d'améliorer leur protection en se rendant anonymes au moyen de techniques sophistiquées permettant de masquer leur identité et leur empreinte numérique. Le chiffrement et l'anonymat, qui sont aujourd'hui les principaux instruments de la sécurité en ligne, permettent à chacun de protéger son intimité et de naviguer sur Internet et d'y lire, élaborer et échanger des idées sans risque d'immixtion. Ils permettent également aux journalistes, aux organisations de la société civile, aux membres de groupes ethniques ou religieux, aux personnes persécutées en raison de leur orientation sexuelle ou de leur identité de genre, aux militants, aux universitaires, aux artistes, entre autres, d'exercer leur droit à la liberté d'opinion et d'expression.

2. Cependant, tout comme le téléphone peut aussi bien servir à signaler un crime à la police qu'à en fomenter un, il est possible de détourner Internet pour empiéter sur les droits d'autrui ou compromettre la sécurité nationale ou l'ordre public. Les forces de l'ordre et les services de renseignement se plaignent souvent de ce que l'anonymat ou le chiffrement des communications complique les enquêtes sur les infractions à caractère financier, le trafic de drogues, la pornographie mettant en scène des enfants et le terrorisme. D'aucuns s'inquiètent à raison de ce que les tyrans et les criminels puissent plus facilement se livrer à des actes de harcèlement grâce aux nouvelles technologies. Certains États restreignent ou interdisent le chiffrement et l'anonymat en invoquant notamment ces motifs, tandis que d'autres proposent ou mettent en œuvre des mesures permettant de contourner ces moyens de protection et d'avoir accès aux échanges entre particuliers.

3. À la lumière de ces enjeux, le présent rapport examine deux questions qui sont liées. Premièrement, les droits au respect de la vie privée et à la liberté d'opinion et d'expression s'appliquent-ils à la sécurisation des échanges en ligne, notamment au moyen du chiffrement ou de l'anonymat? Deuxièmement, dans l'affirmative, jusqu'à quel point les autorités peuvent-elles imposer des restrictions au chiffrement et à l'anonymat sans enfreindre le droit relatif aux droits de l'homme? L'objet du présent rapport est de répondre à ces questions, de passer en revue des exemples de la pratique des États et de formuler des recommandations. S'il ne prétend pas traiter toutes les questions techniques ou juridiques soulevées par les technologies numériques, il recense les plus importantes, qui pourront être abordées dans des rapports ultérieurs.

4. Le Rapporteur spécial s'est appuyé sur un questionnaire dans lequel il demandait aux États des informations sur leurs lois, réglementations, politiques et pratiques. Au 1er avril 2015, 16 États lui avaient répondu[1]. Le Rapporteur a également sollicité des parties prenantes non gouvernementales et organisé une réunion d'experts à Genève en

[1] Les pays suivants ont répondu : Allemagne, Autriche, Bulgarie, Cuba, États-Unis d'Amérique, Grèce, Guatemala, Irlande, Kazakhstan, Liban, Norvège, Qatar, République de Moldova, Slovaquie, Suède et Turquie.

mars 2015. Les réponses des États et les communications – plus de 30 au total – d'organisations et de membres de la société civile (que l'on peut consulter sur le site Web du titulaire du mandat), ont grandement contribué à l'élaboration du présent document.

5. Un exposé complet des activités menées par le Rapporteur spécial depuis son entrée en fonctions, en août 2014, est disponible sur le site Web du titulaire du mandat. Le présent rapport, le premier établi par l'actuel titulaire du mandat, a pour objectif de faire progresser les travaux consacrés à la liberté d'expression à l'ère du numérique.

II. Sécurité et confidentialité de la communication à l'ère du numérique

A. Chiffrement et anonymat à l'heure actuelle

6. Les approches actuelles de la sécurité et de la confidentialité de la communication s'inspirent de concepts plusieurs fois millénaires. L'essor du stockage électronique de données, Internet, la collecte et la conservation de grandes quantités d'informations ont fait clairement ressortir la nécessité de disposer de moyens perfectionnés pour assurer la protection des données appartenant aux personnes, aux entreprises et aux administrations. Le courrier électronique, la messagerie instantanée, la téléphonie sur IP, la vidéoconférence et les médias sociaux n'étant plus des services réservés à des groupes restreints d'utilisateurs mais des moyens de communication omniprésents et faciles à contrôler, certains éprouvent désormais le besoin de sécuriser leur activité en ligne pour que leurs recherches et leurs échanges d'informations n'aient pas de répercussions, ne soient ni divulgués ni surveillés et ne donnent lieu à aucune autre utilisation abusive de leurs opinions et prises de position.

7. Le chiffrement – procédé mathématique « consistant à convertir des messages, des informations ou des données dans un format lisible uniquement par le véritable destinataire »[2] – protège la confidentialité et l'intégrité des contenus contre les tentatives d'intrusion ou de manipulation. Le chiffrement renforcé, qui était autrefois l'apanage des militaires et des services de renseignement, permet aujourd'hui au grand public, souvent gratuitement, de sécuriser courrier électronique, communications vocales, images, disques durs et logiciels de navigation sur Internet. Avec le « chiffrement à clef publique », principale méthode de sécurisation des données de bout en bout, l'expéditeur utilise la clef publique du destinataire pour chiffrer le message et ses pièces jointes, et le destinataire sa propre clef privée pour les déchiffrer. Le chiffrement permet également de créer des signatures numériques garantissant l'authenticité d'un document et l'identité de son expéditeur, d'authentifier et de vérifier l'identité d'un serveur et de protéger les communications contre toute falsification ou interception par des tiers (attaques au niveau intermédiaire). Le chiffrement des données en transit ne garantissant pas la protection des attaques menées contre des données non cryptées lorsque celles-ci sont entreposées à l'une ou l'autre des extrémités (pas plus qu'il ne garantit la sécurité d'une clef privée), il est en outre possible de chiffrer les données stockées sur des ordinateurs portables, des disques durs, des serveurs, des tablettes, des téléphones mobiles ou d'autres dispositifs. Il se peut également que les pratiques en ligne commencent à évoluer du système décrit ci-dessus vers la technique de la « confidentialité persistante » qu'utilise par exemple le protocole « *off-the-record* », dans laquelle les clefs ne sont conservées que temporairement, en particulier pour des utilisations telles que la messagerie instantanée.

[2] Voir : SANS Institute, « History of encryption » (2001).

8. Certaines voix s'élèvent pour que les normes de chiffrement soient affaiblies ou compromises, afin que seules les autorités aient accès aux communications chiffrées. Un chiffrement compromis ne résistera pourtant pas aux experts de la détection et de l'exploitation des failles, qu'ils agissent ou non pour le compte des pouvoirs publics et que leurs visées soient légales ou criminelles. Tous les spécialistes semblent considérer qu'il est impossible de ménager un accès privilégié aux seuls services de l'État, même ceux qui, en principe, défendent l'intérêt public. Compte tenu des techniques actuelles, le fait de compromettre intentionnellement le chiffrement, même à des fins légitimes, affaiblit notre sécurité sur Internet.

9. Il est à noter que le chiffrement protège le contenu des communications mais pas les métadonnées qui, telles l'adresse IP, permettent l'identification. Si l'utilisateur n'utilise pas d'outils protégeant son anonymat, des tiers peuvent collecter des informations importantes sur son identité en analysant des métadonnées. C'est l'anonymat qui permet de ne pas être identifié. La volonté de rester anonyme pour protéger son identité du grand public est chose courante. En restant anonyme, l'utilisateur peut se sentir plus libre d'explorer et de diffuser des idées et des opinions que s'il utilisait sa véritable identité. Sur Internet, il est possible d'adopter des pseudonymes (ou, par exemple, de créer une adresse courriel ou d'ouvrir un compte sur un média social sous un nom fantaisiste) afin de dissimuler son identité, son image, sa voix, sa situation géographique, etc., mais de tels artifices n'assurent qu'une discrétion superficielle, facilement déjouée par les autorités ou quiconque dispose des compétences nécessaires. Si l'utilisateur ne se protège pas en combinant méthodes de cryptage et outils garantissant l'anonymat, il laisse derrière lui des traces numériques qui facilitent son identification. Pour se rendre complètement anonyme ou dissimuler son identité (par exemple en masquant sa véritable adresse IP) face aux intrusions de l'État ou de criminels, il est possible d'utiliser certains outils tels que les réseaux virtuels privés (VPN), les services de proxy, les réseaux et logiciels d'anonymisation et les réseaux entre homologues (*peer to peer*)[3]. Le réseau Tor, outil d'anonymisation bien connu, retransmet un grand nombre de fois les données grâce à plus de 6 000 serveurs informatiques disséminés dans le monde entier, de façon à dissimuler les informations relatives aux utilisateurs, auxquels il assure un degré élevé d'anonymat.

10. L'une des principales caractéristiques de l'ère numérique est que les techniques évoluent constamment pour assouvir la demande des utilisateurs. Bien que le présent rapport se réfère aux techniques qui facilitent aujourd'hui le chiffrement et l'anonymat, les analyses et conclusions qu'il contient s'appliquent plus généralement aux concepts qui sous-tendent la technologie actuelle et devraient rester valables pour celle de demain.

B. Utilisation des techniques

11. Internet est très précieux pour la liberté d'opinion et d'expression, dans la mesure où il joue un rôle d'amplificateur et augmente considérablement la quantité d'informations à la portée de tous ceux qui y ont accès. Il est devenu en peu de temps la principale tribune publique mondiale. C'est pourquoi il faut aujourd'hui considérer l'ouverture et la sécurité d'Internet comme indispensables à l'exercice de la liberté d'expression. Il s'agit pourtant d'un espace constamment menacé où, comme dans le

[3] Les services de proxy envoient des données par l'intermédiaire d'un « serveur cache » qui les transmet au destinataire, au nom de l'utilisateur, en dissimulant efficacement l'adresse IP de ce dernier derrière la sienne. Les réseaux entre homologues scindent les données et les entreposent sur des serveurs interconnectés avant de les chiffrer pour qu'aucun serveur centralisé n'ait accès aux informations pouvant faciliter l'identification. Voir, par exemple, le réseau Freenet.

monde physique, sévissent criminalité, répression ciblée et collecte massive de données. Il est donc essentiel que les citoyens puissent trouver les moyens d'assurer leur sécurité en ligne, que les pouvoirs publics offrent cette sécurité en légiférant et en prenant des mesures et que le secteur privé conçoive, mette au point et commercialise des produits et des services qui soient par défaut sécurisés. Aucun de ces impératifs n'est nouveau. Dès le début de l'ère numérique, les autorités ont reconnu le rôle essentiel du chiffrement dans la sécurité de l'économie mondiale et en ont fait usage ou l'ont recommandé pour sécuriser les numéros d'identité générés par les administrations, les données des cartes de crédit, les informations bancaires, les documents confidentiels des entreprises, voire les enquêtes relatives à la criminalité en ligne[4].

12. Le chiffrement et l'anonymat, qu'ils soient utilisés séparément ou conjointement, instaurent un espace de confidentialité qui sert à protéger les opinions et les convictions. Par exemple, ils rendent possibles les communications privées et sont capables de mettre les opinions à l'abri de la curiosité extérieure, ce qui est particulièrement important dans les environnements politiques, sociaux, religieux ou juridiques hostiles. Lorsque les États imposent une censure illégale en imposant des techniques telles que le filtrage, le chiffrement et l'anonymat peuvent permettre aux citoyens de contourner ces obstacles et d'accéder à l'information et aux idées sans que les autorités ne s'en mêlent. Les journalistes, les chercheurs, les gens de loi et la société civile ont recours au chiffrement et à l'anonymat pour se mettre à l'abri (et protéger leurs sources, clients et partenaires) de la surveillance et du harcèlement. La capacité d'effectuer des recherches sur le Web, d'élaborer des idées et de communiquer en toute sécurité, est peut-être la seule manière, pour beaucoup de gens, d'explorer certains aspects de l'identité aussi fondamentaux que le genre, la religion, l'appartenance ethnique, l'origine nationale ou la sexualité. Les artistes ont recours au chiffrement et à l'anonymat pour garantir et protéger leur droit à la liberté d'expression, en particulier lorsque non seulement l'État y apporte des restrictions, mais la société ne tolère pas les opinions ou les formes d'expression originales.

13. Le chiffrement et l'anonymat ont également un côté « obscur », puisque la délinquance existe en ligne comme dans le monde physique. Les responsables du maintien de l'ordre et de la lutte contre le terrorisme craignent que les terroristes et les criminels de droit commun n'aient recours au chiffrement et à l'anonymat pour dissimuler leurs activités, entravant ainsi les efforts des autorités en matière de prévention et d'enquêtes face au terrorisme, au trafic de drogues, à la criminalité organisée et à la pornographie mettant en scène des enfants. Les technologies visées permettent à ceux qui se livrent à l'intimidation ou au harcèlement, en particulier à l'encontre des membres de groupes vulnérables, de se dissimuler lâchement derrière le masque de l'anonymat. Toutefois, les forces de l'ordre font souvent appel aux mêmes outils pour garantir leur propre sécurité opérationnelle dans le cadre de leurs activités secrètes et les membres des groupes vulnérables ont la possibilité d'utiliser les mêmes méthodes pour se protéger contre le harcèlement. Qui plus est, les autorités ont désormais à leur disposition, pour mieux appliquer les lois et lutter contre le terrorisme, un vaste éventail d'autres outils tels que les écoutes téléphoniques, la géolocalisation, l'exploration de données et la surveillance physique traditionnelle[5].

[4] Voir : OCDE, *Lignes directrices régissant la politique de cryptographie* (1997).

[5] Voir : Center for Democracy and Technology, « Going Dark » versus a « Golden Age for Surveillance » (2011).

III. Le chiffrement, l'anonymat et les droits à la liberté d'opinion et d'expression et au respect de la vie privée

14. Pour répondre à la question de la pertinence du cadre juridique relatif aux droits de l'homme en matière de chiffrement et d'anonymat, il convient dans un premier temps d'évaluer la portée des droits en question et leur applicabilité dans ce domaine, avant de déterminer s'il est licite de restreindre l'utilisation de technologies permettant de promouvoir et protéger les droits au respect de la vie privée et à la liberté d'opinion et d'expression et, dans l'affirmative, jusqu'à quel point.

15. Les droits au respect de la vie privée[6] et à la liberté d'opinion et d'expression[7] ont été codifiés dans des instruments des droits de l'homme universels et régionaux et interprétés par des organes conventionnels et des tribunaux régionaux, et leur respect est évalué par les procédures spéciales du Conseil des droits de l'homme et au titre de l'Examen périodique universel. Les normes universelles relatives au respect de la vie privée et à la liberté d'opinion et d'expression sont énoncées dans le Pacte international relatif aux droits civils et politiques, auquel 168 États sont parties. Même pour les États qui ne sont pas encore liés par cet instrument le Pacte indique à tout le moins un niveau à atteindre et reflète fréquemment une norme juridique coutumière; ceux qui l'ont signé sans l'avoir pour autant ratifié sont tenus de respecter son objet et son but conformément à l'article 18 de la Convention de Vienne sur le droit des traités. Les systèmes juridiques nationaux protègent également le droit au respect de la vie privée et à la liberté d'opinion et d'expression, parfois dans la Constitution ou la Loi fondamentale du pays ou dans l'interprétation qui peut en être donnée. De même, diverses initiatives mondiales de la société civile telles que les Principes internationaux sur l'application des droits de l'homme à la surveillance des communications et les Principes mondiaux relatifs à la sécurité nationale et au droit à l'information montrent de façon décisive le droit qui devrait s'appliquer à l'ère du numérique. Certaines normes spécifiques peuvent varier d'une législation ou d'un instrument à l'autre, mais selon un principe communément observé, les droits au respect de la vie privée et à la liberté d'expression sont essentiels à la dignité humaine et à la gouvernance démocratique. Toute restriction doit être étroitement définie, prévue par la loi et appliquée de manière stricte, uniquement dans des circonstances exceptionnelles. À l'ère numérique, la protection de tels droits exige une vigilance toute particulière.

A. La vie privée en tant qu'espace favorable à la liberté d'opinion et d'expression

16. Le chiffrement et l'anonymat garantissent aux personnes et aux groupes un espace de confidentialité en ligne qui leur permet d'exercer leur liberté d'opinion et d'expression et les protège contre toute immixtion arbitraire ou illégale et contre toute attaque. Le précédent titulaire du mandat a fait observer que les droits au respect de la vie privée et à la liberté d'expression étaient liés et a estimé que le chiffrement et

[6] Le droit au respect de la vie privée est protégé par l'article 12 de la Déclaration universelle des droits de l'homme, l'article 17 du Pacte international relatif aux droits civils et politiques, l'article 16 de la Convention relative aux droits de l'enfant, l'article 22 de la Convention relative aux droits des personnes handicapées, l'article 14 de la Convention internationale sur la protection des droits de tous les travailleurs migrants et des membres de leur famille, l'article 8 de la Convention européenne des droits de l'homme et l'article 11 de la Convention américaine relative aux droits de l'homme.

[7] Le droit à la liberté d'expression est protégé par l'article 19 de la Déclaration universelle des droits de l'homme et l'article 19 du Pacte international relatif aux droits civils et politiques, l'article 9 de la Charte africaine des droits de l'homme et des peuples, l'article 13 de la Convention américaine relative aux droits de l'homme et l'article 10 de la Convention européenne des droits de l'homme.

l'anonymat devaient être protégés en raison du rôle crucial qu'ils peuvent jouer pour garantir ces droits (HRC/23/40 et Corr.1). Faisant écho à l'article 12 de la Déclaration universelle des droits de l'homme, l'article 17 du Pacte international relatif aux droits civils et politiques spécifie que « nul ne sera l'objet d'immixtions arbitraires ou illégales dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes illégales à son honneur et à sa réputation ». L'Assemblée générale, le Haut-Commissaire des Nations Unies aux droits de l'homme et les titulaires de mandat au titre des procédures spéciales considèrent le respect de la vie privée comme un préalable à l'exercice d'autres droits, en particulier les droits à la liberté d'opinion et d'expression (voir la résolution 68/167 de l'Assemblée générale, A/HRC/13/37 et la résolution 20/8 du Conseil des droits de l'homme).

17. Le chiffrement et l'anonymat sont particulièrement utiles pour l'élaboration et l'échange d'opinions, dont certains outils de communication électronique tels que les courriels et les SMS sont souvent les vecteurs. Le chiffrement permet à chacun « de s'assurer que ses envois ne seront reçus que par leurs destinataires, sans immixtion ou modification, et que les messages qu'il reçoit sont également à l'abri de toute intrusion » (voir A/HRC/23/40 et Corr.1, par. 23). Compte tenu des informations sur « la conduite d'un individu, ses relations sociales, ses préférences privées et son identité » que peut livrer l'analyse des métadonnées (voir A/HRC/27/37, par. 19), l'anonymat a un rôle essentiel à jouer dans la sécurisation de la correspondance électronique. Les mécanismes internationaux et régionaux considèrent en outre que le respect de la vie privée s'étend au-delà du domaine de la correspondance[8].

18. Les citoyens et la société civile sont en butte à l'immixtion et aux atteintes d'acteurs étatiques et non étatiques, dont le chiffrement et l'anonymat peuvent les prémunir. Conformément au paragraphe 2 de l'article 17 du Pacte international relatif aux droits civils et politiques, les États se doivent d'offrir une protection contre les immixtions arbitraires ou illégales dans la vie privée. Soumis à cette obligation expresse, les États devraient veiller à l'existence d'une législation nationale disposant expressément que la vie privée ne doit faire l'objet d'aucune immixtion ou atteinte illégale et arbitraire de la part d'acteurs gouvernementaux ou non gouvernementaux. Une telle protection devrait inclure le droit de disposer d'un recours en cas de violation[9]. Pour que le droit à un recours soit effectif, il faut que les utilisateurs soient informés de toute atteinte à leur vie privée résultant, par exemple, d'un affaiblissement du chiffrement ou de la divulgation forcée des données les concernant.

B. Droit de ne pas être inquiété pour ses opinions

19. L'article premier de la Déclaration universelle des droits de l'homme reconnaît que chacun est « doué de raison et de conscience »; ce principe a été développé par la suite dans le droit des droits de l'homme et s'applique désormais, entre autres, à la protection de l'opinion, de l'expression, de la conviction et de la pensée. Le paragraphe 1 de l'article 19 du Pacte international relatif aux droits civils et politiques, qui fait aussi écho à la Déclaration universelle des droits de l'homme,

[8] Observation générale n° 16 (1988) du Comité des droits de l'homme relative au droit de toute personne à être protégée contre les immixtions arbitraires ou illégales dans sa vie privée, sa famille, son domicile et sa correspondance, ainsi que contre les atteintes illégales à son honneur et à sa réputation. Voir également : Cour européenne des droits de l'homme, fiches thématiques sur la protection des données personnelles (http://www.echr.coe.int/documents/fs_data_fra.pdf) et sur le droit à la protection de l'image (http://www.echr.coe.int/documents/fs_own_image_fra.pdf).

[9] Voir : Comité des droits de l'homme, Observation générale n° 16 et Observation générale n° 31 relative à la nature de l'obligation juridique générale imposée aux États parties au Pacte, ainsi que CCPR/C/106/D/1803/2008.

dispose que « nul ne peut être inquiété pour ses opinions ». L'opinion et l'expression sont étroitement liées puisque les restrictions au droit de recevoir des informations et des idées peuvent nuire à la capacité de se forger une opinion et que toute immixtion dans la formation des opinions restreint forcément leur expression. En droit des droits de l'homme, une distinction d'ordre conceptuel a néanmoins été établie. Lors des négociations relatives à l'élaboration du Pacte, il a été considéré que la liberté de se forger une opinion et de l'enrichir par le raisonnement devait être absolue et, à la différence de la liberté d'expression, ne devait pas être restreinte par la loi ou par toute autre autorité[10]. La possibilité d'être libre de ses opinions a été vue comme une composante essentielle de la dignité humaine et du fonctionnement démocratique, une garantie si cruciale que le Pacte n'autoriserait aucune immixtion, limitation ou restriction. Par conséquent, les restrictions autorisées en vertu du paragraphe 3 de l'article 19 s'appliquent expressément et uniquement au droit à la liberté d'expression énoncé au paragraphe 2 de l'article 19. En revanche, toute atteinte au droit à la liberté d'opinion constitue en soi une violation du paragraphe 1 de l'article 19.

20. Les observateurs et les tribunaux prêtent beaucoup moins attention au droit à la liberté d'opinion qu'au droit à la liberté d'expression. Une plus grande attention serait pourtant justifiée car, à l'ère du numérique, les mécanismes de formation et de l'opinion évoluent et exposent les individus à des risques importants. Chacun fait régulièrement part de ses opinions en ligne, lorsqu'il sauvegarde ses avis, les ressources qu'il a consultées et son historique de navigation sur des disques durs, des serveurs en nuage ou dans les archives de sa boîte aux lettres électronique, autant de données conservées ensuite pour de longues périodes, voire indéfiniment, par des autorités privées ou publiques. Les organisations de la société civile, elles aussi, élaborent et stockent en ligne des notes, des articles et des publications et, ce faisant, forment et expriment des opinions. En d'autres termes, à l'ère du numérique, avoir une opinion n'est pas un concept abstrait qui ne recouvre que ce que l'on pourrait avoir en tête. Malgré cela, aujourd'hui, ceux qui ont des opinions dans l'espace numérique sont exposés à des attaques. Hors ligne, les atteintes au droit à la liberté d'opinion peuvent prendre la forme de harcèlement physique, de placements en détention ou de mesures plus subtiles visant à punir les individus en raison de leur opinion (voir CCPR/C/78/D/878/1999, annexe, par. 2.5, 7.2 et 7.3). L'immixtion peut aussi prendre la forme de la surveillance ciblée, des attaques informatiques ayant pour but de rendre indisponible un service, et de l'intimidation, de l'incrimination ou du harcèlement dans le monde réel ou virtuel. Les intrusions numériques ciblées sont une forme de harcèlement à l'égard de personnes et d'organisations de la société civile au motif d'opinions qu'elles ont consignées sous de multiples formats. Le chiffrement et l'anonymat permettent d'éviter totalement ou partiellement un tel harcèlement.

21. Le droit de ne pas être inquiété pour ses opinions englobe le droit de se forger une opinion. Les systèmes de surveillance, qu'ils soient ciblés ou de masse, peuvent compromettre le droit de se faire une opinion puisque, selon toute probabilité, la crainte de voir ses activités en ligne, comme les recherches effectuées et les pages Web consultées, divulguées contre son gré dissuade d'accéder aux informations, en particulier lorsque la surveillance peut aboutir à une répression. Pour toutes ces raisons, il convient d'évaluer les restrictions au chiffrement et à l'anonymat afin de déterminer si elles constituent une atteinte inadmissible au droit à la liberté d'opinion.

C. Droit à la liberté d'expression

22. Le droit à la liberté d'expression, consacré à l'article 19 (par. 2) du Pacte international relatif aux droits civils et politiques, développe la garantie établie dans la Déclaration universelle des droits de l'homme, déjà de vaste portée, en protégeant « la

[10] Manfred Nowak, *UN Covenant on Civil and Political Rights : CCPR Commentary* (1993), p. 441.

liberté de rechercher, de recevoir et de répandre des informations et des idées de toute espèce, sans considération de frontières, sous une forme orale, écrite, imprimée ou artistique, ou par tout autre moyen de son choix ». Dans de nombreuses sources (jurisprudence, rapports des titulaires de mandat au titre des procédures spéciales, résolutions émanant du système des Nations Unies et de systèmes régionaux des droits de l'homme), il est souligné que la liberté d'expression « est [essentielle] à l'exercice des autres droits de l'homme et des autres libertés, et constitue l'un des fondements essentiels d'une société démocratique et du renforcement de la démocratie » (résolution 25/2 du Conseil des droits de l'homme). Le Conseil des droits de l'homme, l'Assemblée générale et les États affirment régulièrement que les individus jouissent des mêmes droits dans le monde numérique que dans le monde physique[11]. Tous les éléments de ce consensus ne seront pas répétés dans le présent rapport. En ce qui concerne le chiffrement et l'anonymat, trois éléments du paragraphe 2 de l'article 19 du Pacte international relatif aux droits civils et politiques méritent une attention particulière (voir par. 23 à 26 ci-dessous).

23. **Liberté de rechercher, de recevoir et de répandre des informations et des idées** : Lorsque la censure est courante, les personnes peuvent être contraintes d'utiliser le chiffrement et l'anonymat pour contourner les restrictions et pouvoir ainsi exercer leur droit de rechercher, de recevoir et de répandre des informations. Certains États ont restreint l'accès à l'information par différents outils. La censure d'État, par exemple, peut constituer parfois un obstacle insurmontable à l'exercice du droit d'accès à l'information. Certains États imposent des restrictions fondées sur le contenu, souvent discriminatoire, ou criminalisent l'expression en ligne en intimidant les opposants et dissidents politiques et en appliquant des lois relatives à la diffamation et au crime de lèse-majesté pour réduire au silence les journalistes, les défenseurs des droits de l'homme et les militants. L'utilisation d'une connexion VPN, du réseau Tor ou d'un serveur proxy, associée au chiffrement, peut être le seul moyen, dans un tel contexte, d'avoir accès à l'information et de la partager.

24. Il convient de souligner que le droit des droits de l'homme protège aussi le droit de rechercher, de recevoir et de répandre des informations et des idées scientifiques. La Déclaration universelle des droits de l'homme et le Pacte international relatif aux droits économiques, sociaux et culturels protègent le droit à l'éducation et le droit « de participer au progrès scientifique et aux bienfaits qui en résultent ». Les technologies de chiffrement et d'anonymisation permettent aux personnes qui, sans cela, n'en auraient pas la possibilité, d'échanger des informations scientifiques et ces technologies illustrent elles-mêmes le progrès scientifique. Leurs utilisateurs ont ainsi accès aux bienfaits du progrès scientifique, accès qui peut être restreint par le pouvoir exécutif. Selon la Rapporteuse spéciale dans le domaine des droits culturels, « il faut savoir que les droits à la science et à la culture comportent tous deux le droit d'accéder aux technologies de l'information et de la communication et autres technologies, et de les utiliser de manière autonome et valorisante » (voir A/HRC/20/26, par. 19).

25. **Sans considération de frontières** : Les principaux instruments qui garantissent le droit à la liberté d'expression reconnaissent expressément que ce droit a une dimension transfrontière. Chacun a le droit de recevoir des informations provenant de l'étranger et de transmettre des informations et des idées de toute espèce à l'étranger[12]. Il n'empêche que certains États filtrent ou bloquent les données sur la base de mots

[11] Voir par exemple la résolution 68/167 de l'Assemblée générale, la résolution 26/13 du Conseil des droits de l'homme et la recommandation CM/Rec (2014) 6 du Comité des ministres aux États membres (Conseil de l'Europe) concernant un guide sur les droits de l'homme pour les utilisateurs d'Internet.

[12] La Cour européenne des droits de l'homme a reconnu ce point. Voir *Ahmet Yildirim* c. *Turquie* (2012); *Cox* c. *Turquie* (2010); *Groppera Radio AG et autres* c. *Suisse* (1990).

clefs à l'aide de technologies qui reposent sur l'extraction de données textuelles. Le chiffrement permet d'éviter ce type de filtrage et de faire circuler l'information au-delà des frontières. De plus, les personnes ne contrôlent pas (et, généralement, ignorent même) la manière dont leurs communications franchissent les frontières – si tel est bien le cas. Le chiffrement et l'anonymat peuvent protéger les données qui transitent par des serveurs situés dans des pays tiers filtrant les contenus.

26. **Par tout moyen** : L'article 19 de la Déclaration universelle des droits de l'homme et l'article 19 du Pacte international relatif aux droits civils et politiques ont été élaborés dans l'idée qu'il y aurait de nouvelles avancées technologiques (A/HRC/17/27). Les États parties au Pacte ont choisi de retenir l'expression générale « par tout autre moyen » plutôt que d'énumérer les médias qui existaient à l'époque. C'est en partie pour cela que les mécanismes internationaux affirment régulièrement que les garanties de la liberté d'expression s'appliquent aux activités sur Internet. Les tribunaux régionaux admettent eux aussi que les garanties sont valables en ligne[13]. La Cour européenne des droits de l'homme, lorsqu'elle a examiné la protection analogue de l'expression conférée par la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, a indiqué que les formes et les moyens par lesquels les informations sont transmises et reçues sont eux-mêmes protégés puisque toute restriction imposée sur les moyens empiète nécessairement sur le droit de recevoir et de répandre des informations[14]. Dans ce sens, le chiffrement et l'anonymat sont des moyens particuliers par lesquels les individus exercent leur droit à la liberté d'expression.

D. Rôle des entreprises

27. Les entreprises de différents secteurs favorisent ou entravent le respect de la vie privée et la liberté d'opinion et d'expression, ce qui concerne aussi le chiffrement et l'anonymat. Une bonne partie des communications en ligne (pratiquement toutes les communications dans certains pays) ont lieu sur des réseaux qui appartiennent à des sociétés privées et sont gérés par ces sociétés, tandis que d'autres sociétés privées possèdent et administrent des sites Web hébergeant des contenus essentiellement produits par les utilisateurs. D'autres entreprises se positionnent sur les marchés de la surveillance et de l'espionnage en fournissant aux gouvernements du matériel et des programmes informatiques conçus pour affaiblir la sécurité des internautes. D'autres encore développent et fournissent des services pour le stockage privé et sécurisé de données en ligne. Les organismes de télécommunications, les fournisseurs d'accès Internet, les moteurs de recherche, les services en nuage et de nombreux autres acteurs du secteur privé, souvent qualifiés d'« intermédiaires », favorisent, régulent ou compromettent la confidentialité et l'expression en ligne. Les intermédiaires peuvent stocker d'énormes volumes de données d'utilisateurs, auxquelles les gouvernements demandent souvent l'accès. Le chiffrement et l'anonymat peuvent être facilités ou entravés par chacun de ces acteurs privés.

28. L'exploration approfondie du rôle des entreprises dans la protection de la sécurité de leurs utilisateurs en ligne dépasse l'objet du présent rapport, qui est axé sur les obligations des États. Cela étant, il importe de souligner qu'« une entreprise a la

[13] Commission européenne des droits de l'homme, *Neij et Sunde Kolmisoppi* c. *Suède* (2013); Cour européenne des droits de l'homme, *Perrin* c. *Royaume-Uni* (2005); Cour africaine des droits de l'homme et des peuples, *Avocats du Zimbabwe pour les droits de l'homme [ZLHR] et Institut des droits de l'homme et du développement en Afrique [IHRDA] (au nom de M. Meldrum)* c. *Zimbabwe* (2009); affaire *Herrera Ulloa* c. *Costa Rica*, exceptions préliminaires, fond, réparations et frais et dépens, série C, n° 107, IHRL 1490 (CIDH 2004).

[14] Voir *Autronic A. G.* c. *Suisse* (1990); *De Haes and Gijsels* c. *Belgique* (1997), par. 48; *News Verlags GmbH et Co.KG* c. *Autriche* (2000).

responsabilité de faire respecter les droits de l'homme dans le cadre de toutes ses activités mondiales, où que se trouvent ses utilisateurs, et ce, indépendamment du fait que l'État s'acquitte ou non de ses propres obligations en matière de droits de l'homme » (voir A/HRC/27/37, par. 43). Les entreprises devraient pour le moins appliquer certains principes, comme les Principes directeurs relatifs aux entreprises et aux droits de l'homme, les principes relatifs à la liberté d'expression et au respect de la vie privée énoncés par l'organisation Global Network Initiative, les principes contenus dans le manuel de la Commission européenne *ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights* et les principes directeurs du groupe Telecommunications Industry Dialogue, qui encouragent les entreprises à s'engager à protéger les droits de l'homme, à exercer la diligence voulue pour remédier à toute incidence négative de leurs activités sur les droits de l'homme et à veiller à ce que ces activités n'aient qu'une incidence positive. Dans l'avenir, le Rapporteur spécial se penchera sur le rôle que les entreprises devraient jouer pour préserver la sécurité des personnes dans le cadre de l'exercice de la liberté d'opinion et d'expression.

IV. Évaluation des restrictions relatives au chiffrement et à l'anonymat

A. Cadre juridique

29. Les limitations du droit au respect de la vie privée qui sont autorisées devraient être interprétées strictement, d'autant plus à notre époque où la surveillance en ligne est généralisée – qu'elle soit passive ou active, de masse ou ciblée – et cela que les critères retenus soient ou non « illégaux et arbitraires » au sens de l'article 17 du Pacte international relatif aux droits civils et politiques, « arbitraires » au sens de l'article 12 de la Déclaration universelle des droits de l'homme, « arbitraires ou abusifs » au sens de l'article 11 de la Convention américaine relative aux droits de l'homme ou « nécessaires dans une société démocratique » au sens de l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (voir A/HRC/13/37, par. 14 à 19). Les immixtions dans la vie privée qui limitent l'exercice du droit à la liberté d'opinion et d'expression, comme celles qui sont décrites dans le présent rapport, ne doivent en aucun cas porter atteinte au droit d'avoir des opinions et celles qui limitent la liberté d'expression doivent être prévues par la loi et être nécessaires et proportionnées eu égard à l'objectif visé, sachant que seul un petit nombre d'objectifs sont légitimes.

30. Aucune restriction ne peut être appliquée au droit de ne pas être inquiété pour ses opinions; les limitations prévues au paragraphe 3 de l'article 19 du Pacte ne s'appliquent qu'au droit à la liberté d'expression énoncé au paragraphe 2 de l'article 19. Dans le cas où les opinions d'une personne, même si elles sont exprimées en ligne, donnent lieu à une surveillance ou à du harcèlement, le chiffrement et l'anonymat peuvent apporter la confidentialité nécessaire. Les restrictions à l'utilisation de ces outils de sécurité peuvent nuire à la capacité des individus de former leur opinion.

31. Les restrictions relatives au chiffrement et à l'anonymat en tant qu'outils facilitant l'exercice du droit à la liberté d'expression doivent satisfaire à trois critères bien connus : toute restriction à la liberté d'expression doit être prévue par la loi, ne peut être imposée que pour des motifs légitimes (tels que ceux énoncés au paragraphe 3 de l'article 19 du Pacte) et doit répondre aux critères stricts de nécessité et de proportionnalité.

32. Premièrement, pour qu'une mesure de restriction au chiffrement ou à l'anonymat soit « prévue par la loi », elle doit être précise, publique et transparente, et ne doit pas conférer aux autorités publiques un pouvoir illimité quant à son application (voir Observation générale n° 34 (2011) du Comité des droits de l'homme). Les propositions de restriction au chiffrement ou à l'anonymat devraient être soumises au débat public et uniquement adoptées, le cas échéant, par les voies législatives ordinaires. De solides garanties procédurales et judiciaires devraient aussi être établies pour garantir une procédure régulière à toute personne dont l'utilisation du chiffrement ou de l'anonymat aurait été restreinte. En particulier, la mise en œuvre de la restriction doit être supervisée par une cour, un tribunal ou un autre organe juridictionnel indépendant[15].

33. Deuxièmement, les limitations ne sont justifiées que si elles visent à protéger des intérêts précis : droits ou réputation d'autrui, sécurité nationale, ordre public, santé publique ou morale publique. Même lorsqu'un État interdit par la loi « tout appel à la haine nationale, raciale ou religieuse qui constitue une incitation à la discrimination, à l'hostilité ou à la violence », conformément à l'article 20 du Pacte, toute restriction à l'expression doit être conforme au paragraphe 3 de l'article 19 (A/67/357). Aucun autre motif ne peut justifier une restriction à la liberté d'expression. De plus, comme des objectifs légitimes sont souvent invoqués pour commettre des actes illégitimes, les restrictions elles-mêmes doivent être appliquées de manière restrictive[16].

34. Troisièmement, l'État doit montrer que la restriction au chiffrement ou à l'anonymat est « nécessaire » pour atteindre l'objectif légitime visé[17]. La Cour européenne des droits de l'homme a conclu de façon pertinente que l'adjectif « nécessaire » dans l'article 10 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales signifiait que la restriction devait être plus qu'« utile », « raisonnable » ou « souhaitable »[18]. Une fois l'objectif légitime atteint, la restriction doit être levée. Compte tenu des droits fondamentaux qui sont en jeu, les limitations doivent être soumises à une autorité judiciaire indépendante et impartiale, en vue notamment de garantir le droit à une procédure régulière.

35. Le critère de nécessité suppose également une évaluation du caractère proportionné des mesures limitant l'utilisation des outils de sécurité en ligne et l'accès à ces outils[19]. Une telle évaluation devrait garantir que la restriction « constitue le moyen le moins perturbateur parmi ceux qui pourraient permettre d'obtenir le résultat recherché »[20]. La limitation doit être appliquée dans un objectif précis et ne saurait porter atteinte aux autres droits de la personne visée; de plus, tout empiétement sur les droits de tierces parties doit être limité et justifié à la lumière de l'intérêt que cette mesure de limitation vise à défendre. La restriction doit aussi être « proportionnée à l'intérêt à protéger »[21]. Un risque important d'atteinte à un intérêt essentiel et légitime de l'État peut justifier une restriction limitée de la liberté d'expression. Inversement, lorsqu'une mesure de restriction a de nombreuses conséquences pour des individus qui

---

[15] Voir Pacte international relatif aux droits civils et politiques, art. 2 3) b); CCPR/C/79/Add.110, par. 22; Principes de Johannesburg relatifs à la sécurité nationale, à la liberté d'expression et à l'accès à l'information.

[16] Voir Comité des droits de l'homme, Observation générale n° 34 sur la liberté d'opinion et d'expression, par. 30, et Observation générale n° 31.

[17] Voir Comité des droits de l'homme, Observation générale n° 34, par. 2, et communication n° 2156/2012, constatations adoptées le 10 octobre 2014.

[18] Voir *The Sunday Times v. United Kingdom*, arrêt du 26 avril 1979, par. 59.

[19] Voir Cour africaine des droits de l'homme et des peuples, *Lohe Issa Konate* c. *Burkina Faso*, requête n° 004/2013, par. 148 et 149 (2014); Cour européenne des droits de l'homme, *Case of The Sunday Times*, par. 62.

[20] Voir l'Observation générale n° 27 (1999) du Comité des droits de l'homme sur la liberté de circulation, par. 14.

[21] Ibid., par. 14.

ne menacent pas les intérêts légitimes du gouvernement, l'État sera tenu de prouver point par point le bien-fondé de cette mesure[22]. En outre, dans le cadre de l'évaluation de la proportionnalité, il doit être tenu compte du fait que les restrictions du chiffrement et de l'anonymat seront très probablement exploitées par les réseaux criminels et terroristes que les mesures de restriction visent précisément à dissuader d'agir. Dans tous les cas, « une justification publique, complète et fondée sur des preuves » est cruciale pour qu'il puisse y avoir un débat public et transparent sur les restrictions qui concernent la liberté d'expression et risquent de la compromettre (voir A/69/397, par. 12).

B. Pratique des États : exemples et sujets de préoccupation

36. Les tendances en ce qui concerne la sécurité et la confidentialité en ligne sont très préoccupantes. Souvent, les États ne fournissent pas de justification publique à l'appui des mesures de restriction qu'ils adoptent. Les communications chiffrées et anonymes peuvent gêner les agents de la force publique et les responsables de la lutte contre le terrorisme, et elles compliquent aussi la surveillance mais, d'une manière générale, les autorités publiques n'ont pas cité de situations (pas même en termes généraux, pour de possibles raisons de confidentialité) dans lesquelles il a été nécessaire d'imposer une restriction pour atteindre un objectif légitime. Les États minimisent l'importance des outils traditionnels non numériques dans l'application de la loi et dans la lutte contre le terrorisme, y compris la coopération internationale[23]. Par conséquent, les citoyens n'ont pas la possibilité de juger si les restrictions de leur sécurité en ligne seraient justifiées par de réels gains en matière de sécurité nationale et de prévention des infractions. De plus, les mesures de restriction du chiffrement et de l'anonymat sont souvent prises rapidement en réaction à des actes terroristes, même lorsque les auteurs de ces actes n'ont apparemment pas eu recours au chiffrement ou à l'anonymat pour préparer ou mettre à exécution leur attaque. En outre, même lorsqu'il est possible d'affirmer que la restriction vise à défendre un intérêt légitime, de nombreuses lois et mesures ne remplissent pas les critères de nécessité et de proportionnalité et nuisent grandement à la capacité des individus d'exercer librement leurs droits au respect de la vie privée et à la liberté d'opinion et d'expression.

37. Il convient également de noter que l'ONU elle-même n'a pas mis à la disposition de son personnel ni des utilisateurs de ses sites Web des outils solides de sécurisation des communications, ce qui constitue un obstacle pour les personnes menacées qui souhaitent joindre en ligne et en toute sécurité les mécanismes des droits de l'homme de l'Organisation[24].

1. Chiffrement

38. Certains gouvernements cherchent à protéger ou à promouvoir le chiffrement afin de garantir la confidentialité des communications. Par exemple[25], la loi brésilienne établissant un cadre civil pour Internet, adoptée en 2014, garantit le caractère inviolable et secret des communications privées en ligne, tout en prévoyant la possibilité d'exceptions sur ordre de justice exclusivement. Les lois autrichiennes

---

[22] Voir Commission interaméricaine des droits de l'homme, OEA/Serv.L/V/II.149, par. 134.

[23] Voir la publication du Centre for International Governance Innovation and Chatham House, *Toward a Social Compact for Digital Privacy and Security : Statement by the Global Commission on Internet Governance* (2015).

[24] Par exemple, à Genève, le personnel du Haut-Commissariat des Nations Unies aux droits de l'homme (HCDH) n'a pas accès à des outils de chiffrement de courriels de bout en bout et le site Web du HCDH n'est pas chiffré.

[25] Un grand nombre des exemples cités dans le présent paragraphe sont tirés de communications des gouvernements sur la question.

sur le commerce électronique et sur les télécommunications ne prévoient pas de restrictions en matière de chiffrement et le Gouvernement a entrepris des campagnes publiques afin de sensibiliser le public à la question de la sécurité numérique. La législation et la réglementation grecques favorisent l'utilisation efficace du chiffrement et des outils d'anonymat. L'Allemagne, l'Irlande et la Norvège autorisent et encouragent l'emploi des technologies de chiffrement, et s'opposent à tout effort visant à affaiblir les protocoles de chiffrement. De même, les législations suédoise et slovaque ne prévoient pas de restrictions à l'utilisation du chiffrement en ligne. Les États-Unis d'Amérique encouragent l'emploi du chiffrement, et le Congrès américain devrait, en outre, examiner un projet de loi relative à la sécurité des données qui interdirait au Gouvernement d'exiger des entreprises qu'elles affaiblissent la sécurité des produits informatiques ou qu'elles y introduisent des portes dérobées. Plusieurs gouvernements, dont ceux du Canada, des États-Unis, des Pays-Bas, du Royaume-Uni de Grande-Bretagne et d'Irlande du Nord et de la Suède, financent des activités de partage de renseignements et de formation dans le domaine de l'utilisation des technologies de chiffrement et d'anonymat, en vue d'aider les personnes à échapper à la censure et à se protéger en ligne. En outre, la réglementation à l'exportation devrait permettre de faciliter les transferts de technologies de chiffrement, dans la mesure du possible. Bien que le présent rapport ne fournisse pas une évaluation juridique globale des approches nationales en matière de chiffrement, les éléments susmentionnés, à savoir l'absence de mesures restrictives ou la protection exhaustive, l'obligation de fonder toute limitation spécifique sur une décision de justice et l'éducation du public, méritent d'être appliqués plus largement en vue de protéger et de favoriser la liberté d'opinion et d'expression.

39. Néanmoins la réglementation du chiffrement parvient rarement à satisfaire aux normes en matière de liberté d'expression dans deux domaines prééminents. Premièrement, il n'a généralement pas été démontré qu'il était nécessaire d'imposer des restrictions pour répondre à un quelconque intérêt légitime. C'est d'autant plus vrai que les autres outils disponibles, comme les activités traditionnelles de police et de renseignement et la coopération internationale, peuvent déjà suffire, en raison de leur portée et de leur profondeur, à fournir des renseignements conséquents pour les besoins du maintien de l'ordre ou pour atteindre tout autre but légitime. Deuxièmement, la réglementation du chiffrement a des répercussions disproportionnées sur les droits à la liberté d'opinion et d'expression de certaines personnes en particulier ou de la population en général.

Interdictions du chiffrement pour usage personnel

40. L'interdiction totale de l'utilisation de technologies de chiffrement à des fins personnelles entrave de manière disproportionnée la liberté d'expression car elle prive les utilisateurs qui relèvent de la compétence de l'autorité concernée du droit de disposer, en ligne, d'un espace privé où formuler leurs opinions et s'exprimer, sans qu'aucune allégation d'utilisation de ces technologies ne soit à des fins illicites invoquée pour la justifier.

41. La réglementation du chiffrement par un État peut s'apparenter à une interdiction; c'est notamment le cas des règles : a) imposant de disposer d'une licence pour utiliser des technologies de chiffrement; b) établissant des normes techniques faibles pour le chiffrement; et c) visant à surveiller l'importation et l'exportation des outils de chiffrement. En limitant ces outils en vertu des normes qu'ils ont approuvées et en exerçant un contrôle sur l'importation et l'exportation des technologies de chiffrement, les États font en sorte que les logiciels de chiffrement contiennent des failles qui leur assurent un accès au contenu des communications. À titre d'exemple, même si les lois concernées peuvent évoluer, l'Inde interdit aux fournisseurs d'accès de déployer des solutions de « chiffrement par blocs » sur leurs réseaux, empêche les

utilisateurs d'utiliser sans autorisation préalable des clefs de chiffrement d'une longueur supérieure à 40 bits, ce qui les rend aisément déchiffrables, et impose à quiconque utilise des technologies plus sophistiquées de fournir au Gouvernement une copie de ses clefs de chiffrement[26]. Il a été signalé qu'en Chine, les autorités peuvent exiger que les produits de chiffrement soient conformes aux algorithmes qu'elles ont approuvés, dont la sécurité n'a pas fait l'objet d'une évaluation collégiale[27]. L'autorité des télécommunications du Pakistan impose que l'utilisation de réseaux virtuels privés et d'outils de chiffrement soit approuvée au préalable[28]. Cuba exige que les utilisateurs de tels outils obtiennent une autorisation réglementaire[29]. En Éthiopie, le Gouvernement est habilité à établir les normes techniques de chiffrement et a récemment promulgué un règlement incriminant la fabrication, l'assemblage ou l'importation de tout appareil de télécommunication sans permis[30]. De tels règlements entravent de manière inadmissible l'utilisation personnelle des outils de chiffrement des communications.

Affaiblissement intentionnel des moyens de chiffrement

42. Certains États ont introduit, ou ont proposé de le faire, des «portes dérobées» dans des produits commercialisés, en obligeant les développeurs à installer des failles qui donnent aux autorités accès aux communications chiffrées. Certains gouvernements ont mis au point des outils permettant d'accéder à de telles données à des fins de surveillance domestique ou en ont fait l'acquisition[31]. Il semble que de hauts fonctionnaires du Royaume-Uni et des États-Unis plaident en faveur de l'installation obligatoire de portes dérobées[32]. Les États qui défendent de telles mesures font souvent valoir qu'il est nécessaire de disposer d'un cadre juridique pour intercepter le contenu des communications chiffrées au moyen de portes dérobées. Les gouvernements qui se font les avocats d'un accès aux données chiffrées par porte dérobée n'ont toutefois pas démontré que l'emploi du chiffrement à des fins criminelles ou terroristes constituait un obstacle insurmontable pour les objectifs de maintien de l'ordre. De plus, compte tenu des technologies existantes, les failles intentionnelles nuisent systématiquement à la sécurité de tous les utilisateurs des moyens de communication électroniques puisqu'une porte dérobée, même si elle est conçue uniquement à l'usage d'un gouvernement, peut être exploitée par des entités non autorisées, y compris d'autres États ou des agents non étatiques. Compte tenu de la vaste portée et de la nature indiscriminée des effets de ce type de failles, l'ensemble des utilisateurs de services en ligne pâtiraient, de manière disproportionnée, de leur création.

43. Les débats sur cette question font ressortir une préoccupation essentielle : le fait d'exiger un accès aux données chiffrées par porte dérobée, même pour des motifs légitimes, menace la confidentialité indispensable à l'exercice sans entrave du droit à

---

[26] Gouvernement indien, Ministère de la communication et de l'informatique, Licence Agreement for Provision of Internet Services, (2007). À consulter à l'adresse : http://dot.gov.in/sites/default/files/internet-licence-dated%2016-10-2007_0.pdf. Voir, en particulier, la section 2.2 vii).

[27] Voir, par exemple, l'art. 15 de la loi sur le contre-terrorisme, (projet initial daté du 8 novembre 2014). À consulter à l'adresse : http://chinalawtranslate.com/en/ctldraft/.

[28] Voir www.ispak.pk/Downloads/PTA_VPN_Policy.pdf.

[29] Communication de Cuba.

[30] Voir la proclamation de l'Éthiopie n° 761/2012 concernant les fraudes dans le domaine des télécommunications (Ethiopia Telecom Fraud Offences Proclamation), sect. 3 à 10.

[31] Voir Morgan Maquis-Boire *et al.*, *For Your Eyes Only* (2013, Citizen Lab).

[32] Voir le discours prononcé le 12 janvier 2015 par le Premier Ministre David Cameron à la conférence du Parti conservateur pour les annonces de contribution à l'élection générale de 2015 ainsi que le discours prononcé le 16 octobre 2014 par James Comey, Directeur du Bureau d'enquête fédéral (FBI) sous le titre « Going dark : are technology, privacy and public safety on a collision course? », à la Brookings Institution (Washington, États-Unis).

la liberté d'expression. Ce type de dispositif a des limites pratiques; l'exploitation de failles intentionnelles peut rendre les contenus chiffrés vulnérables aux attaques, même si les failles en question sont censées servir uniquement au gouvernement ou aux autorités judiciaires. Les gouvernements se trouvent certainement face à un dilemme lorsque leur devoir de protéger la liberté d'expression entre en conflit avec leur obligation de prévenir les atteintes au droit à la vie ou à l'intégrité physique des personnes, lesquelles sont mises en danger par le terrorisme et d'autres comportements criminels. Mais les États ont à leur disposition d'autres moyens pour demander la divulgation de données chiffrées, notamment la décision de justice. En pareilles situations, ils doivent démontrer que les restrictions imposées à la sécurité qu'apporte le chiffrement seraient nécessaires et proportionnées. Ils doivent montrer, publiquement et en toute transparence, que d'autres moyens moins intrusifs n'existent pas ou ont échoué et que l'objectif légitime recherché ne pourrait être atteint qu'à l'aide de mesures globalement intrusives telles que l'emploi de portes dérobées. Quoiqu'il en soit, il est presque certain que des mesures imposant des restrictions générales au plus grand nombre, si elles sont dépourvues d'une évaluation au cas par cas, ne répondraient pas au critère de proportionnalité.

Dépôt de clefs

44. Un système de dépôt de clefs permet aux utilisateurs privés d'utiliser le chiffrement à condition qu'ils confient leurs clefs à l'administration ou à une « tierce partie approuvée ». De tels systèmes comportent toutefois de sérieuses failles. Ils sont, par exemple, tributaires de l'intégrité de la personne, du service ou du système chargé de conserver les clefs personnelles; en outre, la base de données où sont stockées les clefs pourrait subir une attaque, ce qui nuirait à la sécurité et à la confidentialité des communications de tous les utilisateurs. Des systèmes de dépôt de clefs, dont le principe avait été rejeté (de même que celui des portes dérobées) à la suite de nombreux débats menés aux États-Unis dans les années 1990 lors des Crypto Wars (guerres de la cryptographie), sont actuellement en place dans plusieurs pays et ont fait l'objet de propositions dans d'autres. En 2011, la Turquie a approuvé un règlement imposant aux fournisseurs d'outils de chiffrement de transmettre aux autorités de réglementation des copies des clefs de chiffrement avant de remettre aux utilisateurs les produits concernés[33]. Les failles qui caractérisent les systèmes de dépôt de clefs constituent une grave menace pour la sécurité qui est nécessaire à l'exercice de la liberté d'expression.

Divulgation de clefs obligatoire contre ordres de mise au clair ciblés

45. Lorsqu'une demande d'accès aux communications peut être justifiée par des arguments ayant trait au maintien de la loi ou à la sécurité nationale, les autorités peuvent opter pour deux possibilités : soit ordonner la mise au clair de communications spécifiques, soit, lorsqu'il n'est pas certain que la partie concernée se conformera à un tel ordre, exiger la divulgation de la clef nécessaire au déchiffrement. On peut considérer que les ordres de déchiffrement spécifiques ont une portée plus limitée et sont moins susceptibles de poser problème en ce qui concerne le critère de proportionnalité que les ordres de divulgation de clefs, en cela qu'il s'agit de cibler des communications particulières plutôt que l'ensemble des communications qu'une personne a chiffrées à l'aide d'une clef. À l'inverse, la divulgation d'une clef peut compromettre des données privées dans une mesure dépassant largement les exigences

[33] Loi n° 5651 relative à la réglementation des communications électroniques et à la lutte contre la cybercriminalité.

de la situation[34]. En outre, en ordonnant la divulgation de clefs ou le déchiffrement de données, les Gouvernements forcent souvent les entreprises à coopérer avec eux, ce qui engendre des situations très difficiles dont les utilisateurs de moyens de communication électroniques font les frais. La divulgation de clefs est autorisée par la loi dans un certain nombre de pays européens[35]. Dans les deux cas, il faut toutefois que de tels ordres reposent sur des lois qui peuvent être consultées publiquement, dont la portée est clairement limitée et ciblée, qui sont appliquées par une autorité judiciaire indépendante et impartiale, notamment pour préserver les droits des personnes visées à une procédure équitable, et qui sont adoptées uniquement en cas de nécessité, faute d'autres moyens d'enquête moins intrusifs. De telles mesures ne pourront se justifier que lorsqu'elles visent un utilisateur ou un groupe d'utilisateurs spécifiques et qu'elles font l'objet d'un contrôle juridictionnel.

Présomptions juridiques

46. Pour certains États, la simple utilisation de technologies de chiffrement s'apparente à un comportement illicite. Par exemple, les chefs d'accusation retenus contre le collectif de blogueurs Zone 9 en Éthiopie laissaient entendre que le simple fait de se former à la sécurité des communications relevait d'un comportement criminel[36]. De telles présomptions ne sont pas conformes aux normes relatives aux restrictions autorisées. De même, les États qui incriminent le développement et la diffusion d'outils visant à faciliter l'accès des activistes aux moyens de communication électronique empiètent sur les droits à la vie privée et à la liberté d'expression.

2. Anonymat

47. Il est reconnu que l'anonymat joue un rôle important dans la préservation et la promotion de la vie privée, de la liberté d'expression, de la responsabilité politique, de la participation à la vie publique et du débat public[37]. La question de l'anonymat n'est pas traitée dans la Déclaration universelle des droits de l'homme ni dans le Pacte international relatif aux droits civils et politiques. Pendant les négociations qui ont précédé l'adoption du Pacte, il a été proposé d'ajouter, au paragraphe 1 de l'article 19, les mots « l'anonymat n'est pas autorisé ». Cette proposition a toutefois été rejetée au motif, notamment, que l'anonymat pouvait être nécessaire pour protéger les auteurs et qu'une telle clause risquait d'être un obstacle à l'utilisation de noms de plume[38]. Selon le Rapporteur spécial sur la liberté d'expression de la Commission interaméricaine des droits de l'homme, le droit à la liberté de pensée et d'expression ainsi que le droit à la vie privée sont un rempart contre les restrictions imposées par les gouvernements à l'expression anonyme[39]. L'anonymat est célébré de longue date dans la culture

---

[34] Le coordonnateur de l'UE pour la lutte contre le terrorisme a exhorté les parties intéressées à examiner la question de la divulgation obligatoire des clefs de chiffrement. Voir Conseil de l'Union européenne, Secrétariat général, document de réunion D1035/15 (2015).

[35] Voir, par exemple : Royaume-Uni, loi sur la réglementation des pouvoirs d'enquête (divulgation obligatoire des clefs de chiffrement); France, loi n° 2001-1062 (divulgation des clefs de chiffrement sur autorisation juridictionnelle); Espagne, loi n° 25/2007 sur les télécommunications (divulgation des clefs de chiffrement).

[36] Voir : http://trialtrackerblog.org/2014/07/19/contextual-translation-of-the-charges-of-the-zone9-bloggers/.

[37] Voir, par exemple, Commission interaméricaine des droits de l'homme, OEA /Serv.L/V/II.149, par. 134; États-Unis, *McIntyre v. Ohio Elections Commission* (1995); et le discours prononcé par Lord Neuberger à la « RB Conference on the Internet » sous le titre « What's a name? Privacy and Anonymous Speech on the Internet » (2014).

[38] Marc J. Bossuyt, *Guide to the « Travaux Préparatoires » of the International Covenant on Civil and Political Rights* (1987), p. 379 et 380.

[39] Voir Organisation des États américains, communiqué de presse n° 17/15.

politique de plusieurs États, mais très peu de pays ont consacré dans leur droit la protection de l'expression anonyme. Certains États exercent une forte pression à l'encontre de l'anonymat, que ce soit hors ligne ou en ligne. Or l'anonymat favorise grandement les libertés d'opinion et d'expression en ligne; c'est pourquoi les États devraient le protéger et, d'une manière générale, s'abstenir de limiter les technologies qui le rendent possible. Les organes judiciaires de plusieurs États se sont faits les défenseurs de l'anonymat, du moins dans certains cas. Par exemple, la Cour suprême du Canada a récemment invalidé l'acquisition non autorisée d'identités d'utilisateurs anonymes en ligne[40]. Le Tribunal constitutionnel de la République de Corée a déclaré inconstitutionnelles des lois anti-anonymat, qu'il a donc invalidées[41]. La Cour suprême des États-Unis protège constamment le droit à l'expression anonyme[42]. La Cour européenne des droits de l'homme a reconnu que l'anonymat était important pour la liberté d'expression mais permet qu'il soit restreint lorsque cela s'avère nécessaire à l'atteinte d'objectifs légitimes.

48. De nombreux États jugent licite de préserver l'anonymat des sources journalistiques. La Cour suprême et le Code de procédure pénale du Mexique reconnaissent le droit des journalistes de préserver l'anonymat de leurs sources, même si, dans les faits, les journalistes subissent de fortes pressions[43]. La protection des sources des journalistes est expressément consacrée par les constitutions de l'Argentine, du Brésil, de l'Équateur et du Paraguay; le Chili, El Salvador, le Panama, le Pérou, l'Uruguay et le Venezuela (République bolivarienne du) protègent les sources journalistiques dans leur droit[44]. La Constitution du Mozambique assure la protection des sources, tandis que l'Angola est censé en faire autant par sa législation[45]. L'Australie, le Canada, le Japon et la Nouvelle-Zélande ont mis au point des méthodes visant à évaluer l'équilibre judiciaire en fonction des cas d'espèce, afin d'analyser la protection des sources, bien que les pressions exercées sur les journalistes puissent entraver de telles protections dans le temps[46]. Les États enfreignent souvent l'anonymat des sources dans la pratique, même lorsqu'il est prévu par la loi.

Interdiction de l'anonymat

49. L'interdiction de l'anonymat en ligne est en conflit avec le droit à la liberté d'expression. De nombreux États la pratiquent sans qu'un quelconque intérêt public ne soit pour cela invoqué. La Constitution du Brésil (art. 5) interdit les déclarations anonymes. Dans sa Constitution (art. 57), la République bolivarienne du Venezuela interdit également l'anonymat. En 2013, le Viet Nam a proscrit l'utilisation de pseudonymes, ce qui a contraint les auteurs de blogues privés à publier leurs noms et adresses véritables[47]. En 2012, la République islamique d'Iran a ordonné que toutes

---

[40] *R.* c. *Spencer* (2014).

[41] Décision 2010 Hun-Ma 47, 252 (version consolidée) promulguée le 28 août 2012.

[42] *McIntyre v. Ohio Elections Commission* (1995), p. 342 et 343.

[43] Voir le nouveau Code fédéral de procédure pénale, art. 244.

[44] Voir Argentine, Constitution, art. 43; Brésil, Constitution, titre II, chap. I, art. 5, XIV; Équateur, Constitution, art. 20; Paraguay, Constitution, art. 29 1. Voir aussi Chili, loi n° 19733; El Salvador, Code de procédure pénale; Panama, loi n° 67, art. 21; Pérou, Code de procédure pénale; Uruguay, loi n° 16.099; République bolivarienne du Venezuela, loi n° 4.819 relative au journalisme, art. 8.

[45] Voir Mozambique, Constitution, art. 48 3); Angola, loi n° 7/06 relative à la presse, art. 20 1).

[46] Australie, loi de 2007 portant modification de la loi relative à l'administration de la preuve (secret professionnel des journalistes) 2007; Canada, Tribunal de Queen's Bench (Alberta), *Wasylyshen* c. *Canadian Broadcasting Corporation* (2005); Japon, Affaire 2006 (Kyo) n° 19 (2006); Nouvelle-Zélande, loi relative à l'administration de la preuve, sect. 68 (2006).

[47] Human Rights Watch, « Vietnam : new decree punishes presspress », 23 février 2011; Freedom House, « Vietnam : freedom of the press », 2012; art. 19, observation relative au décret n° 02 promulgué en 2011 par le Premier Ministre de la République socialiste du Viet Nam en ce qui

les adresses IP utilisées sur son territoire soient enregistrées et que les utilisateurs des cybercafés renseignent leur nom véritable avant de pouvoir utiliser un ordinateur[48]. Le droit équatorien dispose que les personnes publiant des commentaires sur les sites Web et les propriétaires de téléphones portables doivent s'enregistrer sous leur nom véritable[49].

50. Certains États ont approuvé des lois qui imposent de s'enregistrer à l'aide de son patronyme véritable pour avoir accès à Internet, ce qui constitue une forme d'interdiction de l'anonymat. En Fédération de Russie, les blogueurs dont les sites sont consultés quotidiennement par 3 000 personnes ou plus doivent s'enregistrer auprès de l'autorité de réglementation des médias et s'identifier publiquement, et il a été signalé que les utilisateurs des cybercafés étaient tenus de s'identifier pour pouvoir se connecter aux réseaux publics sans fil[50]. La Chine aurait annoncé des règlements imposant aux utilisateurs d'Internet de s'enregistrer sous leur nom véritable sur certains sites Web et de s'abstenir de diffuser des contenus contraires aux intérêts de la nation[51]. L'Afrique du Sud impose aussi aux utilisateurs d'Internet et de téléphones portables de s'enregistrer sous leur nom véritable[52].

51. De même, les gouvernements exigent souvent l'enregistrement des utilisateurs de cartes SIM; par exemple, près de 50 pays d'Afrique imposent (ou sont en passe de le faire) de renseigner des données personnelles identifiables lors de l'activation d'une carte SIM[53]. La Colombie s'est dotée en 2011 d'une politique d'enregistrement obligatoire pour les téléphones portables et le Pérou associe, depuis 2010, toutes les cartes SIM à un numéro national d'identification[54]. D'autres pays envisagent d'adopter de telles mesures. Or ce type de politique nuit directement à l'anonymat, en particulier pour ceux qui se connectent à Internet uniquement à l'aide de technologies mobiles. L'obligation d'enregistrement pour les utilisateurs de cartes SIM peut donner aux gouvernements la capacité de surveiller les personnes et les journalistes bien au-delà de tout intérêt légitime qu'ils pourraient faire valoir.

52. Certains États ont aussi tenté de combattre des outils d'anonymat comme le réseau Tor, les proxy et les réseaux virtuels privés (VPN), en y interdisant l'accès. La Chine a longtemps bloqué l'accès au réseau Tor[55] et des fonctionnaires russes auraient offert plus de 100 000 dollars des États-Unis en échange de techniques permettant d'identifier les utilisateurs anonymes de ce réseau[56]. En outre, selon certaines sources, l'Éthiopie[57], l'Iran (République islamique de)[58] et le Kazakhstan[59] ont cherché à

---

concerne la responsabilité administrative dans le cadre des activités de presse et de publication (juin 2011).

[48] République islamique d'Iran, projet de loi n° 106, autorité de réglementation des communications.

[49] Voir http://www.derechoambiental.org/derecho/legislacion/ley_organica_comunicacion_ecuador_2013.htmlÉquateur, loi organique relative aux communications (2013).

[50] Projet de loi n° 428884-6 portant modification de la loi fédérale relative à l'information, aux technologies de l'information et à la protection de l'information d'un certain nombre d'actes législatifs de la Fédération de Russie en ce qui concerne la rationalisation de l'échange d'informations avec l'utilisation de l'information et des réseaux de télécommunications; Reuters, « Russia Demands Internet Users Show ID to Access Public Wifi », 8 août 2014.

[51] China Copyright and Media, Internet User Account Name Management Regulations, art. 5 (2015).

[52] Afrique du Sud, loi n° 70 (2003) portant réglementation de l'interception des communications et de la mise à disposition d'informations ayant trait aux communications; voir aussi loi de 2002 relative aux communications et transactions électroniques (exigeant des prestataires de services qu'ils enregistrent le nom véritable).

[53] Kevin P. Donovan et Aaron K. Martin, « The Rise of African SIM Registration », 3 février 2014.

[54] Voir Colombie, décret 1630 de 2011; Perú 21, *Los celulares de prepago en la mira*, 27 mai 2010.

[55] MIT Technology Review, *How China Blocks the Tor Anonymity Network*, 4 avril 2012.

[56] Le texte original de l'offre peut être consulté à l'adresse : http://zakupki.gov.ru/epz/order/notice/zkk44/view/common-info.html?regNumber=0373100088714000008.

[57] Runa Sandvik, Ethiopia Introduces Deep Packet Inspection, The Tor Blog (31 mai 2012); voir aussi art. 19, 12 janvier 2015.

bloquer le trafic sur ce même réseau. Il convient de protéger et de promouvoir l'accès à ces outils car ceux-ci sont parfois les seuls mécanismes permettant à certaines personnes d'exercer leur liberté d'opinion et d'expression en toute sécurité.

Restrictions imposées lors de troubles publics

53. L'expression anonyme est une nécessité pour les activistes et les protestataires, mais les États s'emploient fréquemment à museler ou à intercepter les communications anonymes dans les situations de contestation. De telles tentatives d'interférence avec la liberté d'expression reviennent à poursuivre illégalement un objectif illégitime, celui de saper le droit de manifester pacifiquement, consacré par la Déclaration universelle et le Pacte international relatif aux droits civils et politiques.

Responsabilité des intermédiaires

54. Certains tribunaux nationaux et régionaux tendent à imputer aux fournisseurs d'accès à Internet et aux médias la responsabilité de réglementer la publication de commentaires en ligne par des utilisateurs anonymes. Par exemple, l'Équateur exige des agents intermédiaires, au titre de sa loi organique sur les communications, qu'ils prévoient des mécanismes permettant d'enregistrer les données personnelles et ainsi d'identifier les auteurs de commentaires. Dans l'affaire *Delfi AS* c. *Estonie* (requête n° 64569/09), la Cour européenne des droits de l'homme a confirmé une loi estonienne imputant la responsabilité des déclarations diffamatoires anonymes publiées sur un site Web à l'administrateur du site en question. L'attribution d'une telle responsabilité aux intermédiaires risque d'aboutir soit à la mise en place de politiques d'enregistrement des utilisateurs sous leur nom véritable, ce qui nuirait à l'anonymat, soit à l'élimination pure et simple des commentaires sur les sites Web qui n'ont pas les moyens d'appliquer des procédures de modération, au détriment des petits médias indépendants. Les Principes de Manille concernant la responsabilité des intermédiaires, récemment établis par une coalition d'organisations de la société civile, offrent aux États et aux mécanismes internationaux et régionaux une série de directives efficaces pour protéger l'expression en ligne.

Conservation des données

55. Les politiques imposant la conservation obligatoire et généralisée des données limitent la capacité des personnes à rester anonymes. Le fait pour un État d'être à même d'exiger des fournisseurs d'accès à Internet et des opérateurs de télécommunications qu'ils collectent et stockent des données relatives aux activités en ligne de tous leurs utilisateurs implique forcément que l'État en question est en possession de l'empreinte numérique de chaque individu. Le pouvoir qu'a un État de collecter et de conserver des données personnelles augmente sa capacité de surveillance et accroît les risques de vol et de divulgation d'informations personnelles.

V. Conclusions et recommandations

56. **Le chiffrement et l'anonymat, ainsi que les notions de sécurité qui les sous-tendent, offrent la confidentialité et la sécurité nécessaires à l'exercice du droit à la liberté d'opinion et d'expression à l'ère du numérique. Une telle sécurité peut s'avérer indispensable pour l'exercice d'autres droits, notamment les droits économiques, les droits à la vie privée, à une procédure équitable, à la liberté de**

[58] « Phobos », « Iran partially blocks encrypted network traffic », The Tor Blog (10 février 2012).
[59] « Phobos », « Kazakhstan upgrades censorship to deep packet inspection », The Tor Blog (16 février 2012).

réunion et d'association pacifiques et le droit à la vie et à l'intégrité physique. Compte tenu de leur importance au regard des droits à la liberté d'opinion et d'expression, les restrictions imposées au chiffrement et à l'anonymat doivent être limitées de manière stricte conformément aux principes de légalité, de nécessité, de proportionnalité et de légitimité de l'objectif poursuivi. Le Rapporteur spécial présente donc les recommandations suivantes.

A. États

57. **Les États devraient réviser ou établir, selon les cas, des lois et règlements nationaux en vue de promouvoir et de protéger les droits à la vie privée et à la liberté d'opinion et d'expression. En ce qui concerne le chiffrement et l'anonymat, les États devraient adopter des politiques de non-restriction ou de protection globale, adopter des restrictions uniquement au cas par cas et conformément aux critères de légalité, de nécessité, de proportionnalité et de légitimité de l'objectif poursuivi, subordonner toute limitation spécifique à une décision de justice et promouvoir la sécurité et la vie privée en ligne par l'éducation publique.**

58. **Trop souvent, les débats relatifs au chiffrement et à l'anonymat sont focalisés sur une utilisation potentielle à des fins criminelles dans le cadre d'agissements terroristes. Mais les situations d'urgence n'exonèrent pas les États de leur obligation de garantir que le droit international des droits de l'homme soit respecté. Les propositions législatives qui tendent à réviser ou à adopter des restrictions à la sécurité des personnes en ligne devraient faire l'objet d'un débat public et être adoptées dans le cadre d'une procédure législative régulière, publique, éclairée et transparente. Les États doivent favoriser la participation effective d'un large éventail d'acteurs de la société civile et de groupes minoritaires à de tels débats et procédures, et s'abstenir d'adopter ce type de législation par le truchement de procédures accélérées. Le débat général devrait être axé sur la protection apportée par le chiffrement et l'anonymat, en particulier aux groupes les plus vulnérables aux immixtions illégales. Il faudrait également tenir compte, dans ce débat, du fait que les restrictions font l'objet d'une évaluation stricte : si elles interfèrent avec le droit à la liberté d'opinion, elles doivent être rejetées. Toute restriction imposée à la vie privée qui limite la liberté d'expression – aux fins du présent rapport, toute restriction au chiffrement et à l'anonymat – doit être légale, proportionnée et nécessaire à la réalisation d'un but compris dans un petit groupe d'objectifs légitimes.**

59. **Les États devraient tendre à renforcer le chiffrement et l'anonymat. Les lois nationales devraient reconnaître la liberté de protéger la confidentialité de ses communications électroniques à l'aide de technologies et d'outils de chiffrement permettant d'être anonyme en ligne. La législation et les règlements qui régissent la protection des défenseurs des droits de l'homme et des journalistes devraient aussi contenir des dispositions autorisant et facilitant l'accès aux technologies permettant d'assurer la sécurité des communications.**

60. **Les États ne devraient pas imposer de restrictions au chiffrement et à l'anonymat, qui facilitent et, souvent, rendent possible l'exercice des droits à la liberté d'opinion et d'expression. Les interdictions généralisées ne sont ni nécessaires ni proportionnées. Les États devraient s'abstenir de toute mesure qui affaiblit la sécurité des personnes en ligne comme l'introduction de portes dérobées, l'affaiblissement des normes de chiffrement et la mise en place de systèmes de dépôt de clefs. En outre, les États devraient éviter de subordonner l'accès aux communications numériques et aux services en ligne à l'identification**

des utilisateurs et d'exiger des utilisateurs de téléphones portables qu'ils enregistrent leur carte SIM. De même, les acteurs privés devraient examiner dans quelle mesure leurs propres pratiques constituent un frein au chiffrement et à l'anonymat (y compris par l'utilisation de pseudonymes). La mise au clair sur ordre de justice, qui doit être conforme au droit national et international, ne peut être acceptable que si elle découle de lois transparentes qui peuvent être publiquement consultées et qui sont appliquées uniquement à des personnes (non à des groupes) de manière ciblée, au cas par cas, à la suite d'une décision de justice et dans le respect du principe de protection du droit à une procédure équitable.

B. Organisations internationales, secteur privé et société civile

61. **Les États, les organisations internationales, les entreprises et la société civile devraient promouvoir la sécurité en ligne. Compte tenu de la pertinence des nouvelles technologies de communication pour la promotion des droits de l'homme et du développement, toutes les parties prenantes devraient systématiquement promouvoir l'accès sans discrimination au chiffrement et à l'anonymat. Le Rapporteur spécial demande instamment à tous les organismes du système des Nations Unies, en particulier ceux qui sont actifs dans le domaine de la protection des droits de l'homme et de la protection humanitaire, d'appuyer l'utilisation d'outils renforçant la sécurité des communications afin de garantir que les personnes qui interagissent avec elles puissent le faire en toute sécurité. Les organismes des Nations Unies doivent revoir leurs pratiques et leurs outils dans le domaine des communications et allouer des ressources au renforcement de la sécurité et de la confidentialité des nombreuses parties prenantes qui échangent avec eux par voie électronique. Les mécanismes de protection des droits de l'homme doivent être particulièrement attentifs lorsqu'ils demandent et traitent des informations émanant de la société civile et de témoins et victimes de violations des droits de l'homme.**

62. **Si le présent rapport ne tire aucune conclusion quant à la responsabilité des entreprises dans le domaine de la sécurité des communications, il est toutefois clair que, compte tenu des menaces qui pèsent sur la liberté d'expression en ligne, les acteurs privés devraient réexaminer le bien-fondé de leurs pratiques à la lumière des normes relatives aux droits de l'homme. Au minimum, les entreprises devraient adhérer à des principes tels que ceux qui sont énoncés dans les Principes directeurs relatifs aux entreprises et aux droits de l'homme, les Principes de la Global Network Initiative relatifs à la liberté d'expression et à la vie privée, le Guide pratique de la Commission européenne sur le secteur informatique concernant la mise en œuvre des Principes directeurs des Nations Unies relatifs aux entreprises et aux droits de l'homme et les Principes directeurs du Telecommunications Industry Dialogue. Les entreprises, tout comme les États, devraient s'abstenir de bloquer ou de limiter la transmission de communications chiffrées et autoriser les communications anonymes. Il faudrait favoriser les efforts visant à étendre la disponibilité des liaisons vers les centres de données chiffrées, promouvoir les technologies permettant de sécuriser une page Web et mettre au point un système de chiffrement par défaut généralisé de bout en bout. Les acteurs du monde des entreprises qui fournissent des technologies ayant pour but d'affaiblir le chiffrement et l'anonymat devraient se montrer particulièrement transparents quant à leurs produits et leur clientèle.**

63. **Il convient d'encourager l'utilisation d'outils de chiffrement et d'anonymisation et de favoriser une meilleure connaissance des technologies numériques. Le Rapporteur spécial, reconnaissant que les outils de chiffrement et**

d'anonymisation, pour être valables, doivent être adoptés largement, encourage les États, les organisations de la société civile et les entreprises à s'engager dans une campagne visant à fournir aux utilisateurs du monde entier des technologies de chiffrement par choix ou par défaut et, si nécessaire, à garantir que les utilisateurs les plus vulnérables soient dotés des outils nécessaires pour exercer leur droit à la liberté d'opinion et d'expression en toute sécurité.