



Assemblée générale

Distr. générale
19 décembre 2014
Français
Original: anglais

Conseil des droits de l'homme

Vingt-huitième session

Points 2 et 3 de l'ordre du jour

Rapport annuel du Haut-Commissaire des Nations Unies aux droits de l'homme et rapports du Haut-Commissariat et du Secrétaire général

Promotion et protection de tous les droits de l'homme,
civils, politiques, économiques, sociaux et culturels,
y compris le droit au développement

Résumé de la réunion-débat du Conseil des droits de l'homme sur le droit à la vie privée à l'ère du numérique

Rapport du Haut-Commissariat des Nations Unies aux droits de l'homme

Résumé

Le présent rapport est soumis en vertu de la décision 25/117 du Conseil des droits de l'homme. Y figure un résumé de la réunion-débat sur le droit à la vie privée à l'ère du numérique, qui s'est tenue le 12 septembre 2014 à l'occasion de la vingt-septième session du Conseil des droits de l'homme. À la demande de celui-ci, la réunion-débat a porté sur la promotion et la protection du droit à la vie privée dans le contexte de la surveillance et de l'interception des communications numériques et de la collecte des données personnelles sur le territoire national et à l'extérieur, y compris à grande échelle, notamment dans le but de recenser les enjeux et les meilleures pratiques, compte tenu du rapport du Haut-Commissaire des Nations Unies aux droits de l'homme.



Table des matières

	<i>Paragraphes</i>	<i>Page</i>
I. Introduction	1–4	3
II. Déclaration liminaire de la Haut-Commissaire adjointe des Nations Unies aux droits de l’homme	5–16	3
III. Interventions des experts	17–29	6
IV. Résumé des débats	30–57	10
A. Observations générales sur le droit à la vie privée à l’ère du numérique	32–42	11
B. Protection juridique du droit à la vie privée	43–52	13
C. Questions spécifiques relative aux entreprises	53–55	16
D. Marche à suivre	56–57	17
V. Conclusions	58–61	18

I. Introduction

1. Conformément à sa décision 25/117, le Conseil des droits de l'homme a tenu une réunion-débat sur le droit à la vie privée à l'ère du numérique, le 12 septembre 2014. Les débats ont tenu compte des questions soulevées dans le rapport du Haut-Commissaire des Nations Unies aux droits de l'homme, soumis à la vingt-septième session du Conseil des droits de l'homme (A/HRC/27/37).

2. À la demande du Conseil des droits de l'homme, la réunion-débat a porté sur la promotion et la protection du droit à la vie privée dans le contexte de la surveillance et de l'interception des communications numériques et de la collecte des données personnelles sur le territoire national et à l'extérieur, y compris à grande échelle, notamment dans le but de recenser les enjeux et les meilleures pratiques, compte tenu du rapport du Haut-Commissaire des Nations Unies aux droits de l'homme.

3. La réunion-débat était présidée par le Président du Conseil des droits de l'homme, et animée par Marko Milanovic, professeur associé à l'Université de Nottingham. La Haut-Commissaire adjointe des Nations Unies aux droits de l'homme a fait une déclaration liminaire. Les experts suivants ont participé à la réunion-débat: Catalina Botero, Rapporteuse spéciale sur la liberté d'expression auprès de la Commission interaméricaine des droits de l'homme, Sarah Cleveland, professeur titulaire de la chaire «Louis Henkin» de droit constitutionnel et de droits de l'homme de la faculté de droit de l'Université Columbia, Yves Nissim, Administrateur en chef adjoint chargé de la responsabilité sociale d'entreprise chez Orange et ancien Président du groupe d'opérateurs et de constructeurs du secteur des télécommunications Telecommunications Industry Dialogue, et Carly Nyst, Directrice des affaires juridiques de Privacy International.

4. Le présent rapport est soumis en application de la décision 25/117, dans laquelle le Conseil des droits de l'homme a demandé au Haut-Commissariat de lui présenter, à sa vingt-huitième session, un rapport de synthèse sur la réunion-débat.

II. Déclaration liminaire de la Haut-Commissaire adjointe des Nations Unies aux droits de l'homme

5. La Haut-Commissaire adjointe a déclaré que les technologies des communications numériques avaient révolutionné les interactions entre les êtres humains en un très court laps de temps et que l'ère du numérique, synonyme d'émancipation pour des millions de personnes, constituait peut-être le plus grand mouvement de libération que le monde ait jamais connu. Elle a fait observer, à titre d'exemple, que plus d'un million de personnes avaient participé par voie électronique au dialogue et à la consultation à participation non restreinte visant à élaborer un cadre pour les objectifs de développement durable pour l'après-2015, dont les droits de l'homme devaient nécessairement former partie intégrante. Elle a souligné que les défenseurs et militants des droits de l'homme, les partisans de la démocratie, les membres de minorités ainsi que d'autres parties pouvaient à présent communiquer grâce aux réseaux numériques et faire entendre leur voix à l'échelle mondiale d'une manière qui était auparavant inconcevable.

6. La Haut-Commissaire adjointe a également rappelé que les réseaux numériques étaient vulnérables aux systèmes de surveillance, d'interception et de collecte des données. À cet égard, de profondes préoccupations avaient été soulevées au sujet de politiques et de pratiques exploitant cette vulnérabilité, qui étaient apparues partout dans le monde. Elle a ajouté que les pratiques en matière de surveillance pouvaient avoir un effet très concret sur les droits de l'homme individuels, y compris les droits à la vie privée, à la liberté d'expression et d'opinion, à la liberté de réunion, à la vie de famille et à la santé.

Les renseignements recueillis par surveillance numérique avaient, en particulier, servi à repérer des dissidents et, selon des sources crédibles, les technologies du numérique avaient permis de collecter des informations sur la base desquelles des tortures et d'autres formes de mauvais traitements avaient été infligées.

7. La Haut-Commissaire adjointe a rappelé que, dans sa résolution 68/167, l'Assemblée générale avait prié la Haut-Commissaire de lui soumettre un rapport sur «la protection et la promotion du droit à la vie privée dans le contexte de la surveillance et de l'interception des communications numériques et de la collecte des données personnelles sur le territoire national et à l'extérieur, y compris à grande échelle», lequel avait été présenté au Conseil des droits de l'homme à sa vingt-septième session. Ce rapport avait été élaboré sur la base de consultations avec des experts et de recherches approfondies concernant la législation et la jurisprudence existantes aux niveaux national et international, ainsi que d'informations provenant de sources très variées, glanées notamment grâce à un questionnaire envoyé aux parties prenantes.

8. Comme le rapport l'avait démontré, le droit international des droits de l'homme fournissait un solide cadre universel aux fins de la promotion et de la protection du droit à la vie privée, y compris dans le contexte de la surveillance et de l'interception des communications numériques et de la collecte des données personnelles sur le territoire national et à l'extérieur. Toutefois, dans bon nombre d'États, il ressortait des pratiques en vigueur que la législation et l'application des lois au niveau national n'étaient pas adaptées, que les garanties de procédure étaient faibles et les contrôles inefficaces, ce qui contribuait à l'impunité généralisée des atteintes arbitraires et illégales au droit à la vie privée.

9. La Haut-Commissaire adjointe a rappelé que, dans son rapport, la Haut-Commissaire examinait la protection apportée par le droit international des droits de l'homme en matière de vie privée, déterminait ce qui constituait une «immixtion dans la vie privée» dans le contexte des communications numériques, définissait l'expression «arbitraire et illégale» et établissait quelles étaient les personnes dont les droits étaient protégés, et dans quels cas cette protection s'appliquait. Par exemple, pour ce qui était de savoir ce qui constituait une immixtion dans la vie privée, il était clair que les agrégations de données de communication pouvaient donner des indications détaillées sur le comportement, les relations sociales, les préférences personnelles et l'identité d'une personne, allant bien au-delà de la somme d'informations obtenues en lisant son courrier. La collecte et la conservation des données de communication pouvaient donc constituer une immixtion dans la vie privée, que les données soient ou non consultées ou utilisées par la suite. L'existence même d'un programme de surveillance à grande échelle portant sur les communications électroniques et d'autres formes d'expression numérique constituait une immixtion dans la vie privée et il incombait à l'État en cause de démontrer qu'une telle immixtion n'était ni illégale ni arbitraire.

10. S'agissant des immixtions «arbitraires» ou «illégales» dans la vie privée, il était noté dans le rapport que la surveillance des données électroniques de communication pouvait être une mesure légitime dans le cadre du maintien de l'ordre, pourvu qu'elle soit conforme à la loi. Toutefois, les États devaient démontrer que la surveillance mise en place était à la fois nécessaire et proportionnée au risque spécifique à traiter. La conservation obligatoire des données de tiers, qui veut que les opérateurs de téléphonie et les fournisseurs d'accès à Internet stockent les métadonnées relatives aux communications de leurs clients pour que les organes de police et les agences de renseignements puissent y accéder ultérieurement, ne semblait ni nécessaire ni proportionnée.

11. La Haut-Commissaire adjointe a rappelé que, comme cela avait été souligné dans le rapport, les États étaient tenus de veiller à ce que la législation protège les personnes contre les immixtions illégales ou arbitraires dans la vie privée. Toute surveillance des communications devait procéder de dispositions juridiques accessibles au public, lesquelles devaient être conformes à la Constitution de l'État concerné et au droit international des droits de l'homme. Les règles secrètes et les interprétations secrètes de la loi, même lorsqu'elles émanaient d'un juge, n'étaient pas compatibles avec le principe de clarté et d'accessibilité de la législation, de même que les lois ou règles qui conféraient un pouvoir discrétionnaire excessif aux autorités chargées de l'application des lois, telles que les services de sécurité et de renseignements.

12. La Haut-Commissaire adjointe a aussi mentionné les préoccupations soulevées dans le rapport au sujet de la surveillance extraterritoriale et de l'interception des communications numériques. Sur la base des travaux menés par le Comité des droits de l'homme et la Cour internationale de Justice sur les notions permettant de reconnaître qu'un État exerce sa compétence, il était noté dans le rapport que tout État était tenu de s'acquitter de ses obligations en matière de droits de l'homme partout où il exerçait un pouvoir ou un contrôle effectif. Toute opération de surveillance supposant l'exercice par un État d'un tel pouvoir ou contrôle effectif sur une infrastructure de communications numériques était donc susceptible de mettre en jeu les obligations de cet État en matière de droits de l'homme. À titre d'exemple, la mise sur écoute directe ou la pénétration d'une infrastructure de communications, de même que l'exercice par un État d'une compétence réglementaire sur une tierce partie ayant le contrôle physique des données relevaient d'un tel cas de figure.

13. Il a été rappelé dans le rapport que le droit international des droits de l'homme était en outre explicite au sujet du principe de non-discrimination et que les États devaient prendre des mesures pour garantir la conformité de toute atteinte au droit à la vie privée avec les principes de légalité, de proportionnalité et de nécessité, quels que soient l'origine ethnique, la nationalité, la situation géographique ou les autres éléments de statut des personnes dont ils surveillaient les communications.

14. Le rapport faisait aussi référence au caractère essentiel des garanties procédurales et d'un contrôle effectif pour préserver le droit à la vie privée dans la législation et en pratique. Le manque de contrôle effectif avait contribué à l'impunité des atteintes arbitraires et illégales au droit à la vie privée dans la sphère numérique. Les protections internes sans contrôle indépendant s'étaient montrées inefficaces contre les méthodes de surveillance illégales ou arbitraires. Une protection appropriée passait par un contrôle civil indépendant et la participation de tous les organes de l'État afin d'assurer la protection effective de la loi. Les États avaient en outre l'obligation légale d'offrir aux victimes d'immixtions dans la vie privée découlant de la surveillance numérique la possibilité de former un recours utile auprès des autorités judiciaires, législatives ou administratives, de les informer des procédures à suivre et de faire en sorte qu'elles aient accès à ces procédures.

15. Enfin, la Haut-Commissaire adjointe a fait référence au rôle du secteur privé, également abordé dans le rapport de la Haut-Commissaire. Les États s'appuyaient de plus en plus sur les entreprises pour assurer et faciliter la surveillance numérique. Dans certains cas, il pouvait être légitime pour une entreprise de communiquer les données d'un utilisateur. Mais quand la demande était contraire au droit des droits de l'homme, ou quand l'utilisation des renseignements ainsi obtenus y contrevenait, l'entreprise en cause risquait de se rendre complice de violations des droits de l'homme. Les Principes directeurs des Nations Unies relatifs aux entreprises et aux droits de l'homme, approuvés par le Conseil des droits de l'homme dans sa résolution 17/4 du 16 juin 2011, avaient valeur de norme mondiale pour les mesures tendant à prévenir les incidences négatives de l'activité des

entreprises sur les droits de l'homme, et à y remédier. Y était précisé qu'une entreprise avait la 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. Un grand nombre de sociétés semblaient trop peu au fait de ces questions.

16. La Haut-Commissaire adjointe a conclu en indiquant que le manque de transparence des gouvernements à l'égard des mesures adoptées pouvait avoir une incidence sur le droit à la vie privée et compliquait souvent à l'extrême les efforts visant à réduire les écarts et à faire appliquer l'obligation de rendre compte. Il était manifestement nécessaire d'examiner plus avant ces questions et de mener une analyse approfondie à mesure que les renseignements concernant ces activités étaient rendus publics.

III. Interventions des experts

17. En réponse aux questions du modérateur, les experts, dans leurs observations initiales, se sont concentrés sur le cadre juridique international relatif aux droits de l'homme dans le contexte du droit à la vie privée, y compris les garanties de procédure, le contrôle effectif et le droit à un recours, ainsi que sur le rôle du secteur privé.

18. La Directrice des affaires juridiques de Privacy International a souligné que la vie privée était importante dans toute société démocratique et insisté sur les liens existants entre la vie privée et la notion de dignité humaine. Elle a noté que le droit à la vie privée était à la fois une condition préalable à d'autres droits et le garant de ces droits car il permettait à ceux qui l'exerçaient de développer leurs pensées et leurs idées en toute indépendance et de les exprimer librement, et d'opter pour la religion et l'affiliation politique de leur choix. M^{me} Nyst a expliqué que la première définition du droit à la vie privée dans le droit international figurait dans la Déclaration universelle des droits de l'homme, dont les rédacteurs avaient clairement conscience de la nécessité de consacrer le droit à la vie privée, ainsi que de l'importance du droit à la confidentialité des communications, comme le montraient les travaux préparatoires de la Déclaration.

19. M^{me} Nyst a fait valoir que bon nombre des activités quotidiennes parmi les plus banales impliquaient une forme de «communication», qu'il s'agisse d'envoyer un message électronique ou un SMS, de se connecter à des services bancaires, de chercher des renseignements sur Internet ou de consulter des sites de services publics. Toute communication numérique reposait sur la circulation de données privées à travers le monde, qui empruntaient les réseaux câblés d'un grand nombre de sociétés privées avant de parvenir à destination. Cette technologie représentait un défi en termes de vie privée; il s'agissait de veiller à ce que les obligations des États en matière de respect, de promotion et de protection du droit à la vie privée, ainsi que les responsabilités du secteur privé, soient à la hauteur des enjeux de l'ère du numérique. M^{me} Nyst a noté qu'il existait déjà un cadre juridique, le droit à la vie privée étant consacré par la plupart des instruments internationaux et régionaux relatifs aux droits de l'homme et par bon nombre de constitutions nationales, et qu'il était nécessaire de réévaluer la façon d'appliquer ces textes.

20. La Rapporteuse spéciale sur la liberté d'expression auprès de la Commission interaméricaine des droits de l'homme a souligné qu'Internet avait créé des possibilités en matière de liberté d'expression, de communication et d'échange d'informations, tout en facilitant l'acquisition, le stockage et l'administration d'énormes volumes de données. Ces données, qu'il s'agisse de contenus ou de métadonnées, pouvaient être très révélatrices des aspects les plus intimes de la vie privée des personnes ou des communautés. Les cadres réglementaires accusaient un retard par rapport au rythme des progrès technologiques à

l'ère du numérique et il était nécessaire de réglementer la collecte comme l'analyse des données, en tenant compte de la liberté d'expression, du droit à la vie privée et d'autres droits fondamentaux pertinents.

21. M^{me} Botero a également fait observer que les politiques de surveillance pouvaient avoir une incidence sur un grand nombre de droits de l'homme. Elle a évoqué l'effet de la surveillance sur le droit à la liberté d'expression, lequel pouvait être soit direct, quand ce droit ne pouvait être exercé anonymement à cause d'une surveillance, soit indirect, quand la simple existence de mécanismes de surveillance pouvait avoir un effet paralysant, inspirer la crainte et inhiber les personnes concernées en les contraignant à la prudence dans leurs dires et leurs agissements. Le droit à la liberté d'expression étant un socle, y porter atteinte pouvait entraîner une violation d'autres droits tels que les libertés d'association, de réunion et de religion et le droit à la santé. Compte tenu de l'effet potentiel des activités de surveillance sur l'ensemble de l'architecture des droits de l'homme, il incombait aux États de revoir leur législation pour fixer les limites des programmes de surveillance en veillant à ce qu'ils soient conformes aux principes de nécessité et de proportionnalité et soient assortis de mécanismes de suivi appropriés. M^{me} Botero a fait valoir que la question de la gouvernance de l'Internet était particulièrement pertinente, compte tenu du caractère spécial et unique de ce moyen de communication qui permettait l'exercice libre, pluriel et démocratique du droit à la liberté d'expression. Elle a déclaré que, pour faire en sorte que toutes les opinions pertinentes soient dûment prises en compte, les États devaient garantir la participation, dans des conditions d'égalité, de tous les acteurs concernés par la gouvernance de l'Internet et promouvoir une coopération renforcée entre les autorités, les universitaires, la société civile, les communautés scientifique et technique et le secteur privé, sur le plan national et à l'échelle internationale.

22. La professeur titulaire de la chaire «Louis Henkin» de droit constitutionnel et de droits de l'homme de la faculté de droit de l'Université Columbia a déclaré que toutes les personnes, quelles que soient leur situation géographique et leur nationalité, étaient protégées par les droits de l'homme, droits universels et inhérents à la dignité humaine. Elle a relevé que les pouvoirs publics, dans leurs pratiques de surveillance, établissaient parfois une distinction entre ressortissants et non-ressortissants. À cet égard M^{me} Cleveland a souligné que, comme l'avait reconnu le Comité des droits de l'homme, le principe de non-discrimination consacré par l'article 2 du Pacte international relatif aux droits civils et politiques s'appliquait aux ressortissants comme aux non-ressortissants¹. En conséquence, la vie privée des non-ressortissants devait être protégée contre toute atteinte illégale ou arbitraire, au même titre que celle des ressortissants. M^{me} Cleveland a aussi noté que les activités de surveillance étaient souvent menées par les États sur leur propre territoire afin de réprimer la liberté d'expression et d'association ou de punir des journalistes, dissidents et autres opposants politiques. En vertu de l'article 17 du Pacte international relatif aux droits civils et politiques, les États étaient tenus de respecter et de garantir le droit à la vie privée de toutes les personnes se trouvant sur leur territoire ou relevant de leur juridiction.

23. M^{me} Cleveland a souligné que la protection consacrée par le Pacte international relatif aux droits civils et politiques s'étendait aux personnes relevant par ailleurs de la juridiction d'un État, comme la Cour internationale de Justice² et le Comité des droits de

¹ Voir l'Observation générale n° 18 (1989) du Comité des droits de l'homme concernant la non-discrimination.

² Voir Cour internationale de Justice, Conséquences juridiques de l'édification d'un mur dans le territoire palestinien occupé, avis consultatif, *Recueil des arrêts, avis consultatifs et ordonnances*, 2004, p. 136 et Activités armées sur le territoire du Congo (*République démocratique du Congo c. Ouganda*), arrêt, *Recueil des arrêts, avis consultatifs et ordonnances*, 2005, p. 168.

l'homme³ l'avaient reconnu. C'était également l'interprétation qui conciliait le mieux le texte du Pacte et son contenu, son propos et son but. Le Comité des droits de l'homme reconnaissait depuis longtemps qu'un État ne pouvait se soustraire à ses obligations internationales relatives aux droits de l'homme en agissant hors de son territoire d'une manière qui lui serait interdite sur le sien propre. M^{me} Cleveland a expliqué que la cyberactivité dépassait le cadre des limites territoriales et que la surveillance numérique pouvait entraîner l'exercice d'un minimum de contrôle physique de l'État sur une personne ou un territoire, ainsi que la conduite, en un lieu donné, d'activités qui pouvaient avoir une incidence sur une personne se trouvant dans un autre lieu. De telles activités pouvaient engager la responsabilité d'un État dans le domaine des droits de l'homme. Enfin, si les droits relatifs à la vie privée s'appliquaient aux non-ressortissants et aux ressortissants d'un État à l'étranger, les activités de surveillance n'en étaient pas pour autant systématiquement illégales. Toute restriction imposée au droit à la vie privée afin de servir certains intérêts légitimes ayant trait à la sécurité nationale ou au maintien de l'ordre devait être adoptée en tenant pleinement compte des prescriptions du droit international des droits de l'homme et, en particulier, n'être ni arbitraire ni illégale.

24. Quant au rôle du secteur privé, le modérateur, M. Milanovic, a noté que les entreprises privées procédaient à l'agrégation de données pour leurs propres besoins mais pouvaient également être mises à contribution dans le cadre de mécanismes relevant des pouvoirs publics. S'agissant des relations entre les gouvernements et les entreprises privées de télécommunications, il s'est interrogé sur la manière dont les entreprises privées devaient répondre aux demandes émanant des pouvoirs publics. L'Administrateur en chef adjoint chargé de la responsabilité sociale d'entreprise chez Orange a indiqué que les problèmes liés aux diverses demandes qui pouvaient être adressées aux opérateurs de télécommunications pour obtenir qu'ils collectent et conservent les données de leurs clients ou rendent leurs réseaux compatibles avec des systèmes d'écoute étaient devenus plus flagrants lors du Printemps arabe. Les entreprises de télécommunications avaient reçu, parfois sous la contrainte, de la part des gouvernements des demandes qui avaient pu avoir des répercussions sur les droits à la liberté d'expression et à la vie privée de leurs clients. En réaction, ces entreprises avaient lancé l'initiative «Telecommunications Industry Dialogue on Freedom of Expression and Privacy» afin d'examiner les questions relatives à la liberté d'expression et à la vie privée à l'échelle du secteur⁴. Dix principes directeurs inspirés des Principes directeurs relatifs aux entreprises et aux droits de l'homme et à la mise en œuvre du cadre de référence «protéger, respecter et réparer» des Nations Unies avaient été publiés le 12 mars 2013 dans le cadre de cette initiative. Ces 10 principes portaient sur la vie privée et la liberté d'expression dans le contexte des activités du secteur des télécommunications et examinaient en particulier l'interaction ainsi que les limites existant entre le devoir des gouvernements de protéger les droits de l'homme et la responsabilité des entreprises de télécommunications de respecter ces mêmes droits.

25. En ce qui concernait les défis à relever, M. Nissim a souligné que les entreprises de télécommunications employaient beaucoup de personnel dans divers pays et que leur sécurité constituait une priorité absolue, comme en attestait le cinquième principe directeur⁵. Il a aussi noté que les entreprises participant au Dialogue, toutes désireuses qu'elles soient de faire respecter les droits de l'homme, en particulier la liberté d'expression et le droit à la vie privée, étaient liées par des accords de licence passés avec les

³ Voir l'Observation générale n° 31 (2004) du Comité des droits de l'homme concernant la nature de l'obligation juridique générale imposée aux États parties au Pacte.

⁴ Le groupe Telecommunications Industry Dialogue comprend actuellement sept opérateurs et deux fournisseurs de télécommunications. Voir www.telecomindustrydialogue.org.

⁵ Le principe n° 5 est libellé ainsi: «Toujours chercher à préserver la sécurité et la liberté du personnel de l'entreprise lorsque celui-ci est exposé à des risques.»

gouvernements et soumises aux législations et règlements nationaux. Il leur fallait protéger leurs employés sur place et elles devaient donc être en mesure de dialoguer avec les gouvernements hôtes si nécessaire. M. Nissim a mentionné trois points à aborder de toute urgence. Tout d'abord, les pouvoirs publics ne devaient pas demander ou obtenir l'accès direct aux réseaux de télécommunications. Deuxièmement, le processus par lequel les gouvernements pouvaient présenter des demandes aux entreprises de télécommunications devait être clair et transparent. Enfin, les entreprises de télécommunications étaient disposées à faire preuve de transparence au sujet des demandes qu'elles recevaient, mais il convenait de rappeler que la transparence était en premier lieu la responsabilité des gouvernements.

26. Se penchant sur les conditions présidant à la restriction légale du droit à la vie privée et de la liberté d'expression, M^{me} Botero a fait valoir que toute limitation d'une telle nature devait être au préalable visée par une disposition législative définissant précisément les causes et conditions permettant à l'État d'intercepter des communications personnelles, de collecter des données de communication ou de placer des personnes sous surveillance ou sous contrôle, et de restreindre ainsi leur droit à la vie privée. La législation ne devait pas être vague ou ambiguë, ni conférer à l'exécutif un vaste pouvoir discrétionnaire pour l'interpréter. Elle devait en outre prévoir des garanties concernant la nature, la portée et la durée des mesures de surveillance. Les restrictions au droit à la vie privée devaient aussi être imposées dans la poursuite d'un but légitime. Dans le cas des activités de surveillance, les motifs les plus susceptibles d'être invoqués par les États étaient la sécurité nationale et la lutte contre la criminalité. Toute restriction devait être proportionnée et strictement nécessaire. Partant, il devait être clairement établi qu'une telle restriction procédait d'une nécessité réelle et impérieuse et que l'objectif recherché ne pouvait être atteint par aucun autre moyen moins restrictif. Dans tous les cas, une restriction des droits ne devait être imposée que lorsque la menace pesant sur l'intérêt protégé, dont la définition devait être précise, relevait d'un ordre de priorité supérieur à celui de l'intérêt général du maintien du droit à la vie privée et à la liberté d'expression. M^{me} Botero a aussi déclaré que l'on devait établir avec encore plus de soin la conformité de ces mesures avec les critères cités quand les droits protégés concernaient les aspects les plus intimes de la vie privée des personnes visées. Afin de garantir la protection des principes de légalité, de proportionnalité et de nécessité, toute décision visant à entreprendre des activités de surveillance ayant un effet restrictif pour le droit à la vie privée et d'autres droits devait être visée par une instance judiciaire indépendante.

27. S'agissant du principe de proportionnalité, M^{me} Cleveland a souligné que toute mesure devait être proportionnée à l'importance des intérêts en jeu, à savoir l'intérêt de l'État à ce que la mesure soit prise, et l'intérêt de la personne visée à ce que sa vie privée soit préservée. Elle a ajouté que plus le besoin de confidentialité de la personne visée était élevé, plus il convenait d'adapter finement la mesure. Elle a fait référence à la jurisprudence de la Cour européenne des droits de l'homme, qui fournissait aux États une marge d'appréciation raisonnable, en particulier dans le domaine de la sécurité nationale, pour déterminer, au cas par cas, quelles mesures étaient nécessaires et proportionnées aux fins de la réalisation d'un intérêt particulier de l'État en question. M^{me} Cleveland a aussi insisté sur l'importance des garanties de procédure mises en place par les États afin de veiller à la bonne application des dispositifs de surveillance. Elle a souligné qu'il fallait prévoir des garanties juridiques, un mécanisme de contrôle et la possibilité de former un recours à titre rétroactif, pour prévenir toute utilisation abusive de ces dispositifs de surveillance.

28. M. Milanovic a indiqué que les États établissaient souvent une distinction entre la collecte du contenu des communications et celle des données y relatives (les métadonnées), et que la première était plus strictement encadrée que la dernière. Il a posé la question de la pertinence d'une telle distinction dans le cadre des communications numériques. Selon

M^{me} Nyst, il convenait d'abandonner sans équivoque de telles distinctions car elles correspondaient à une compréhension obsolète de la nature des communications et trahissaient une incapacité à adapter la législation. Elle a indiqué que ce type de distinctions datait d'une époque où il existait une différence entre une enveloppe et son contenu; à l'inverse, dans le cadre des communications numériques, les métadonnées, qui pouvaient s'apparenter à l'enveloppe, contenaient des informations très sensibles, de grande valeur et détaillées. Par exemple, les renseignements déduits des métadonnées pouvaient permettre, après analyse, d'obtenir des informations sur les convictions politiques ou religieuses d'une personne. M^{me} Nyst a fait référence à une étude de l'Université de Stanford, qui avait montré qu'on pouvait déduire des informations à caractère médical, financier et juridique à partir de métadonnées. Elle a souligné qu'il était donc de la première importance de réévaluer cette distinction, comme cela était mentionné dans le rapport de la Haut-Commissaire. Elle s'est félicitée des progrès accomplis dans plusieurs pays, qui avaient reconnu qu'il était nécessaire de renforcer la protection des métadonnées. Elle a en outre noté que la Cour européenne de justice avait récemment invalidé la loi sur la conservation des données⁶. Elle a conclu que la tendance était au renforcement de la protection des métadonnées, tout en soulignant que des orientations supplémentaires s'imposaient quant à la manière d'adapter les législations nationales en conséquence.

29. Du point de vue des opérateurs, M. Nissim a indiqué que des données telles que celles tirées du suivi des appels étaient souvent conservées par les entreprises de télécommunications à des fins techniques, pour garantir la qualité des services et des réseaux. Il a toutefois relevé que les informations collectées, quand les pouvoirs publics demandaient aux entreprises de télécommunications de les conserver pendant de plus longues périodes ou de leur y donner accès, pouvaient être employées à mauvais escient. Il a ajouté que tout accès à ces données par les autorités devrait être encadré par la législation. M. Nissim a enfin fait valoir que les données volumineuses, si elles étaient rendues anonymes, pouvaient être employées à très bon escient, par exemple dans le cadre de la planification du territoire, des transports ou des communications.

IV. Résumé des débats

30. Au cours des débats, les délégations des pays et organismes ci-après ont pris la parole: Allemagne (au nom de l'Allemagne, de l'Autriche, du Brésil, du Liechtenstein, du Mexique, de la Norvège, des Pays-Bas et de la Suisse), Algérie, Australie, Belgique, Canada, Chine, Cuba (au nom du Groupe de pays animés du même esprit), Émirats arabes unis, Équateur, Estonie, États-Unis d'Amérique, Fédération de Russie, France, Inde, Indonésie, Irlande, Italie, Malaisie, Pakistan (au nom de l'Organisation de coopération islamique), Roumanie, Royaume-Uni de Grande-Bretagne et d'Irlande du Nord, République bolivarienne du Venezuela, Sierra Leone, Slovaquie, Union européenne, et Organisation des Nations Unies pour l'éducation, la science et la culture (UNESCO). Les représentants du Chili, du Myanmar et de l'Uruguay n'ont pas pu prononcer leur déclaration, faute de temps. Des copies de ces déclarations ont été affichées sur le site Extranet du Conseil des droits de l'homme.

31. Les représentants des organisations non gouvernementales (ONG) suivantes ont également pris la parole: American Civil Liberties Union (déclaration conjointe avec Human Rights Watch), Article 19, Association pour le progrès des communications et Centre coréen pour la politique des Nations Unies en matière de droits de l'homme.

⁶ Voir l'arrêt du 8 avril 2014 rendu par la Cour européenne de justice au titre des affaires jointes C-293/12 et C-594/12.

A. Observations générales sur le droit à la vie privée à l'ère numérique

32. De nombreuses délégations ont souligné la qualité du rapport de la Haut-Commissaire sur le droit à la vie privée à l'ère numérique et le fait qu'il constituait une étape importante dans le contexte des débats actuels. De nombreuses délégations ont également salué les travaux du Haut-Commissariat des Nations Unies aux droits de l'homme et d'autres organismes visant à garantir le droit à la vie privée en droit et dans la pratique.

33. De nombreuses délégations se sont félicitées de la réunion-débat, car ce débat était nécessaire et son thème d'actualité, en rappelant que les progrès technologiques avaient une longueur d'avance sur la compréhension de leurs incidences sur les droits de l'homme. L'importance des débats sur cette question au Conseil des droits de l'homme, ainsi que dans d'autres instances, telles que le Forum sur la gouvernance de l'Internet, a également été soulignée.

34. Une délégation a fait observer que l'on comptait près de 3 milliards d'internautes dans le monde et que la gratuité et la sécurité de l'Internet étaient devenues une priorité pour toutes les populations. Comme le prévoyaient les objectifs de développement durable pour l'après-2015 et le Programme d'action en faveur des pays les moins avancés pour la décennie 2011-2020 (A/CONF.219/3/Rev.1), chacun devait avoir accès à l'Internet d'ici à 2020.

35. La plupart des intervenants ont fait remarquer, comme la Haut-Commissaire l'avait déjà souligné dans son rapport, que les innovations technologiques avaient eu un effet positif sur la liberté d'expression, avaient facilité le débat au niveau mondial et avaient favorisé la participation démocratique. Certains ont relevé que les communications numériques pouvaient être utilisées pour favoriser l'exercice des droits de l'homme, qu'elles avaient contribué à l'avancement de la civilisation humaine et offert de nouvelles possibilités dans les domaines de la communication, de la connaissance et de l'entreprise. La vie privée faisait partie intégrante d'une société libre, juste et ouverte dans laquelle chacun pouvait exprimer librement ses opinions sans crainte d'être soumis à la répression ou à la détention.

36. La plupart des délégations ont toutefois constaté que ces mêmes plates-formes technologiques avaient aussi renforcé les capacités des acteurs étatiques et non étatiques en matière de surveillance, d'interception et de collecte de données à grande échelle. Certaines délégations ont déclaré que ces plates-formes étaient non seulement vulnérables à la surveillance à grande échelle, mais qu'elles facilitaient cette surveillance. Une ONG a fait observer que lorsque la vie privée en ligne était menacée, la confiance dans l'Internet disparaissait, privant ainsi chacun, y compris les journalistes, les blogueurs et les défenseurs des droits de l'homme, de la liberté de communiquer en toute sécurité, de façon anonyme et confidentielle, ce qui avait un effet dissuasif sur la liberté d'expression. Une autre ONG a souligné que pour tout un chacun, en particulier les personnes vivant sous des régimes répressifs, l'intégrité des communications était essentielle pour préserver les libertés individuelles et la sécurité de la personne, ainsi que les droits politiques.

37. L'attention a été appelée sur la croissance exponentielle des pouvoirs de l'État rendue possible dans certains pays par les infrastructures informatiques. Certaines délégations ont souligné qu'une grande partie des communications électroniques mondiales transitait par un nombre limité de pays et que cela permettait à ces pays d'intercepter les communications privées. Certains pays avaient élaboré des technologies qui donnaient accès à une grande partie du trafic Internet mondial, à des fichiers de communications, à des carnets d'adresses électroniques de particuliers et à des volumes considérables d'autres contenus de communications numériques. Des informations selon lesquelles

certains gouvernements surveillaient les communications lors d'événements mondiaux ont également été évoquées. Plusieurs orateurs ont rappelé que la souveraineté des États devait toujours être respectée en ce qui concernait la surveillance, l'interception et la collecte de données personnelles.

38. D'autres délégations ont fait observer que certains gouvernements avaient tendance à utiliser de plus en plus les cybertechnologies pour contrôler leurs propres ressortissants, en violation de leur droit à la liberté d'expression et du droit d'accès à l'information. Certains ont indiqué que les militants politiques et les membres de minorités religieuses étaient ciblés, détenus et parfois tués. Une ONG a constaté que les effets de la surveillance en ligne se faisaient souvent sentir hors ligne et s'inscrivaient dans une tendance mondiale à la restriction de l'espace civique. Des mouvements de protestation légitimes étaient surveillés par l'État et des acteurs privés dans le but de compromettre des actions pacifiques et les droits s'y rapportant, en particulier les droits à la liberté d'expression et de réunion.

39. La plupart des délégations ont réaffirmé que les droits dont les personnes jouissaient hors ligne devaient également être protégés en ligne, conformément à la résolution 68/167 de l'Assemblée générale et aux résolutions 20/8 et 26/13 du Conseil des droits de l'homme.

40. La plupart des délégations ont estimé que le droit à la vie privée était une condition préalable à la liberté d'expression et un des droits fondateurs de toute société démocratique. De nombreuses délégations ont indiqué que la surveillance avait une incidence sur d'autres droits que le droit à la vie privée, en particulier la liberté d'expression et d'opinion et la liberté de réunion et d'association. Il a été précisé en outre que le droit à la vie privée et la liberté d'expression étaient «intimement liés et interdépendants» (voir A/HRC/23/40, par. 79) et qu'ils rendaient possible et favorisaient le développement d'autres droits fondamentaux et le développement durable. À titre d'exemple, deux ONG ont évoqué le préjudice concret que la surveillance électronique à grande échelle pouvait causer au travail des journalistes et des avocats en portant atteinte à la liberté d'expression et d'association et au droit d'être représenté par un conseil⁷. Une délégation a fait état de tentatives visant à faire taire les médias. Une autre ONG a mentionné le cas de blogueurs devant faire face à des accusations de terrorisme, en partie parce qu'ils avaient codé leurs communications et avaient participé à une formation dans le domaine de la sécurité numérique pour protéger leur vie privée.

41. Une délégation a indiqué que les personnes n'étaient souvent pas conscientes de la mesure dans laquelle les données pouvaient être utilisées ou partagées, même lorsqu'elles étaient recueillies avec leur consentement. Certaines délégations ont évoqué le droit à la protection des données et la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel et son Protocole additionnel, indiquant que cette convention était le premier instrument international contraignant dans le domaine de la protection des données et constituait une contribution importante au droit à la vie privée. Une délégation a mentionné ce que l'on appelait le «droit à l'oubli numérique», dans le cadre duquel le souhait légitime de ne pas être associé à un seul aspect particulier de sa vie ou de son passé pouvait entrer en conflit avec le droit d'être informé et pouvait également conduire à des distorsions dans la mémoire collective.

42. De nombreuses délégations ont rappelé les mesures prises au niveau national pour assurer la protection du droit à la vie privée à l'ère numérique. L'UNESCO a fait référence à ses travaux relatifs à la protection de la vie privée et à la liberté d'expression à l'ère numérique, à une publication sur le droit à la vie privée et la liberté d'expression sur

⁷ Human Rights Watch et American Civil Liberties Union, «With liberty to monitor all: how large-scale US surveillance is harming journalism, law and American democracy» (juillet 2014).

l'Internet, ainsi qu'à une étude détaillée sur les questions liées à l'Internet, mettant notamment l'accent sur la liberté d'expression, la vie privée, l'accès à la connaissance et à l'information, et l'éthique dans une société de l'information.

B. Protection juridique du droit à la vie privée

43. La plupart des délégations ont souligné que le droit international offrait un cadre clair pour la protection du droit à la vie privée, consacré dans l'article 12 de la Déclaration universelle des droits de l'homme et dans l'article 17 du Pacte international relatif aux droits civils et politiques. Nombre d'entre elles ont toutefois constaté que la mise en application du droit à la vie privée faisait défaut et qu'il était nécessaire de prendre des mesures concrètes pour garantir ce droit. Certaines ont fait remarquer que l'accès unilatéral et non autorisé aux données privées et la surveillance intensive devaient faire l'objet d'un examen approfondi, et des appels ont été lancés pour que soient prises des mesures urgentes pour mettre fin aux pratiques actuelles en matière de surveillance et protéger les personnes contre les violations de leur droit à la vie privée.

44. De nombreuses délégations ont rappelé que toute restriction du droit à la vie privée devait être fondée sur des lois accessibles, transparentes, claires, complètes et non discriminatoires, et se limiter aux mesures nécessaires pour protéger l'intérêt public dans une société démocratique. Toute surveillance des personnes par l'État devait être proportionnée et juste, en conformité avec les normes et règles internationales, régie par l'État de droit, et soumise à un contrôle. Il devait exister des garanties appropriées et efficaces contre les abus. Il a été souligné que la définition exacte de la limite à partir de laquelle la surveillance serait considérée comme une immixtion arbitraire ou illégale dans la vie privée constituerait un des défis des prochaines années. Il a également été souligné que la surveillance généralisée pouvait être considérée comme une violation injustifiée du droit. Une délégation a indiqué que l'article 17 du Pacte devait constituer la base des débats relatifs aux principes sur lesquels reposait cette limite (la légalité et le caractère arbitraire) qui étaient mentionnés expressément dans ledit article.

45. Plusieurs délégations ont fait observer que les États avaient des préoccupations légitimes en matière de sécurité, notamment la menace du terrorisme et de la cybercriminalité. Une délégation a indiqué que l'usage de l'Internet pour mener des activités criminelles ou antisociales était en augmentation. Une autre délégation a indiqué que, pour assurer la sécurité, il fallait mener des activités de renseignements, notamment s'agissant des communications numériques, pour combattre le terrorisme, et une autre encore a déclaré que les gouvernements avaient la responsabilité de protéger les personnes, et que la surveillance des données pouvait être une mesure efficace et légitime pour assurer le respect des lois. Toutefois, il a été largement convenu que les préoccupations légitimes liées à la sécurité devaient être abordées dans le cadre du droit international des droits de l'homme, y compris le droit à la vie privée.

46. En réponse à une question relative au partage de données entre les organismes gouvernementaux, M^{me} Nyst a déclaré que les mêmes garanties en matière de contrôle et de procédure devaient s'appliquer aux informations collectées directement et à celles obtenues par le partage de l'information. M^{me} Cleveland a indiqué que le Comité des droits de l'homme s'était dit préoccupé par cette question⁸. Le partage des données entre différents organismes d'État dans un pays donné pouvait être légitime, à condition que le but de la collecte et de l'utilisation de ces données soit le même pour chacun de ces organismes,

⁸ Voir l'Observation générale n° 16 (1988) du Comité des droits de l'homme concernant le droit à la vie privée, par. 10.

de manière à garantir le respect des principes de nécessité et de proportionnalité, et à prévenir toute violation du droit à la vie privée.

47. Certaines délégations ont fait observer que l'Internet n'était pas limité par les frontières géographiques traditionnelles. Plusieurs délégations ont rappelé que, comme l'indiquait la Haut-Commissaire dans son rapport, le droit relatif aux droits de l'homme s'appliquait également lorsqu'un État exerçait un pouvoir en dehors de son territoire, de sorte que celui-ci ne pouvait pas se soustraire à ses obligations internationales en matière de droits de l'homme et ignorer ses propres lois nationales en prenant en dehors de son territoire des mesures qui lui seraient interdites «chez lui». Plusieurs délégations ont rappelé que l'article 17 du Pacte international relatif aux droits civils et politiques devait être lu conjointement avec l'article 2 du Pacte, qui stipulait que les obligations des États s'appliquaient à toutes les personnes se trouvant sur leur territoire et relevant de leur juridiction. Plusieurs délégations ont fait observer que toute immixtion dans la vie privée devait être conforme aux principes de légalité, de proportionnalité et de nécessité, indépendamment de la nationalité des personnes dont les communications étaient directement surveillées et de l'endroit où elles se trouvaient. Alors que de nombreuses délégations ont souligné que la responsabilité incombant à l'État de protéger le droit à la vie privée ne s'arrêtait pas à ses frontières, certaines délégations ont exprimé des préoccupations concernant l'idée d'un élargissement du champ d'application extraterritoriale du Pacte et ont demandé la tenue d'un débat approfondi sur la question de l'extraterritorialité dans le contexte de l'article 17.

48. M^{me} Nyst a rappelé que la majeure partie des activités de surveillance avait lieu à l'intérieur des États. À propos des distinctions fondées sur la nationalité dans le cadre de la surveillance, elle a fait remarquer que non seulement ces distinctions étaient contraires au principe de non-discrimination, mais que cette approche était obsolète et peu pratique, car il était difficile – voire impossible – de connaître la nationalité de l'expéditeur d'une communication numérique. S'agissant de la question de savoir si le contrôle des infrastructures de télécommunications pouvait relever de la juridiction des États aux fins de l'article 2 du Pacte, M^{me} Cleveland a déclaré que, étant donné que les communications numériques dépassaient les frontières géographiques, il fallait adopter une approche de l'application extraterritoriale des droits de l'homme qui garantisse la protection de ces droits en ligne comme hors ligne. Il existait différentes approches de l'extraterritorialité, dont la plupart étaient fondées sur l'idée que la juridiction d'un État en dehors de son territoire supposait une certaine forme de contrôle effectif sur une personne ou un territoire et en vertu desquelles il était possible de considérer l'exercice d'un contrôle sur les infrastructures de l'Internet comme l'exercice, sur un territoire donné, d'un contrôle qui avait des effets sur les droits des personnes, quel que soit l'endroit où elles se trouvaient.

49. Il a été relevé que la responsabilité du respect du droit à la vie privée incombait à un certain nombre d'intervenants différents. Certaines délégations ont souligné que l'absence de contrôle effectif avait contribué à l'absence d'obligation de rendre compte pour ce qui concernait les immixtions illégales dans la vie privée, et que le fait de s'appuyer sur des mesures de protection internes sans disposer de contrôle externe indépendant présentait des inconvénients. La nécessité de protéger les droits des victimes a été soulignée. Une délégation a indiqué qu'il appartenait à chaque État d'élaborer des mécanismes de contrôle indépendants et efficaces au niveau national afin de veiller à l'application effective des règles régissant la surveillance électronique. Une organisation non gouvernementale a déclaré qu'il y avait eu des cas de surveillance à grande échelle ayant pour but d'arrêter des défenseurs des droits de l'homme ou d'identifier les participants à des réunions pacifiques, dans le cadre desquels «l'entérinement automatique» par les tribunaux avait joué un rôle déterminant et où les données personnelles collectées par des opérateurs de télécommunications au moyen de systèmes de vérification du nom réel avaient été fournies à des organes de renseignements ou d'enquête en l'absence de tout examen par le tribunal.

Il a été souligné qu'il était nécessaire de mettre en place des systèmes de contrôle effectif, en se préoccupant du droit des victimes à un recours effectif, notamment du rôle d'un pouvoir judiciaire indépendant et impartial, en tant que mécanisme de protection clef.

50. En réponse aux questions sur les garanties procédurales et les mécanismes de contrôle visant à assurer l'application effective de la loi dans la pratique, M^{me} Nyst a expliqué qu'une condition essentielle à un contrôle renforcé et plus efficace était de mettre fin à l'omniprésence du secret. Les gouvernements devaient exercer une plus grande transparence concernant les activités qu'il leur fallait mener pour assurer la sécurité, et ils ne pouvaient pas compromettre les infrastructures d'une manière qui échappe au contrôle de la population. Elle a également fait observer que toutes les personnes, en particulier les juges et les avocats, devaient avoir une meilleure compréhension du fonctionnement de la technologie Internet, ce qui leur permettrait de mieux comprendre le fonctionnement de la surveillance. Elle a souligné qu'il importait de s'assurer que toute surveillance était autorisée par une autorité judiciaire indépendante et compétente. Elle a ajouté qu'il était essentiel que les personnes soient averties du fait qu'elles avaient été soumises à une surveillance, afin d'être en mesure d'obtenir réparation. Elle a également indiqué qu'il était nécessaire de mettre en place des mécanismes de contrôle indépendants plus stricts, fondés sur une compréhension technique du fonctionnement de la surveillance, pour pouvoir examiner les incidences sur le plan des droits de l'homme de la surveillance effectuée par les services de sécurité. Enfin, elle a fait observer qu'un titulaire de mandat au titre d'une procédure spéciale doté des compétences techniques appropriées pouvait donner un avis sur les bonnes pratiques et sur les améliorations qu'il convenait d'apporter au cadre des droits de l'homme pour garantir la protection du droit à la vie privée. M^{me} Botero a ajouté que les normes nationales régissant la surveillance n'étaient pas uniformes et qu'une bonne pratique au niveau national consistait à disposer d'un organe d'experts consacré spécifiquement aux technologies et aux droits de l'homme dans le contexte de la surveillance. Elle a fait observer que le contrôle pouvait être institutionnel, judiciaire et être exécuté entre différents organes ou par un médiateur, que les garanties procédurales devaient inclure une autorisation judiciaire préalable des mesures de surveillance, et que le fondement juridique et les critères de la décision devaient être publics.

51. Se référant à une question sur l'obligation des États d'accorder une réparation effective contre les violations du droit à la vie privée, M^{me} Cleveland a indiqué que, même si l'article 2 du Pacte international relatif aux droits civils et politiques prévoyait l'obligation pour les États d'accorder une réparation effective, cette question était très complexe en raison du secret entourant les pratiques de surveillance. Les personnes ignoraient souvent qu'elles avaient fait l'objet d'une surveillance et risquaient donc de ne pas réagir car elles ne pouvaient pas démontrer de manière suffisante l'existence d'un préjudice. Elle a estimé que les gouvernements devaient faire montre d'une plus grande transparence concernant les programmes de surveillance qu'ils appliquaient, afin d'en permettre l'examen public. Elle a également souligné qu'il était important que les personnes concernées soient précisément informées du fait qu'elles avaient été soumises à une surveillance une fois qu'il avait été mis fin à celle-ci. Elle a ajouté que les règlements en la matière devaient être assez souples pour permettre une remise en question significative des programmes de surveillance. À cet égard, elle a souligné que la Cour européenne des droits de l'homme exigeait que soit démontrée la probabilité suffisante d'un préjudice réel – et non pas la preuve de celui-ci. Elle a indiqué que les procédures judiciaires classées secrètes posaient des difficultés mais qu'il était néanmoins important d'appliquer une forme ou une autre de vérification judiciaire. Le principal défi était de faire en sorte que ces procédures soient aussi transparentes et efficaces que possible.

52. S'agissant de la question de savoir s'il devait y avoir des tribunaux spécialisés dans l'examen des mesures de surveillance, M^{me} Cleveland a indiqué que les États devaient trouver un moyen de satisfaire aux exigences de transparence et de contrôle démocratique,

tout en permettant un certain degré de confidentialité. Une bonne solution consistait à mettre en place des procédures particulières pour traiter des informations classifiées, mais dans les tribunaux ordinaires. Sur ce point, M^{me} Nyst a ajouté que même si la mise en place de juges spécialisés dotés de connaissances techniques comportait des avantages, il était essentiel que les tribunaux permettent aux parties d'être sur un pied d'égalité en cas de contestation d'une surveillance. Par conséquent, il était essentiel qu'il n'y ait pas de tribunaux secrets ni de procédure permettant une interprétation secrète des lois. Les tribunaux qui ne permettaient pas d'assurer le plus haut niveau de transparence et de contrôle ne permettaient pas de rectifier le déséquilibre de pouvoir entre l'individu et l'État, et risquaient en fait de servir à légitimer des mesures de surveillance illégales.

C. Questions spécifiques relatives aux entreprises

53. Plusieurs délégations ont également relevé le rôle joué par les sociétés du secteur privé. Certaines délégations ont fait état du fait que des sociétés avaient subi des pressions de la part de gouvernements ou avaient été contraintes de remettre des données en leur possession. D'autres ont indiqué que des fournisseurs internationaux de télécommunications et d'accès à Internet avaient élaboré et mis en œuvre leurs propres capacités de surveillance ou aidé des États à surveiller des particuliers. Selon M. Nissim, la technologie exploitée par les sociétés de télécommunications était d'une grande complexité mais les gouvernements étaient néanmoins en mesure d'y accéder. Il a cité l'exemple de «l'inspection des paquets en profondeur», qui consistait à examiner le contenu des communications en cours de transmission et permettait ainsi aux fournisseurs d'accès à Internet de contrôler et analyser les communications Internet d'utilisateurs en temps réel. M. Nissim a affirmé que le recours à ce type d'équipement permettait aux sociétés de télécommunications d'améliorer les services offerts à leur clientèle, mais qu'ils pouvaient aussi être utilisés par certains gouvernements à des fins de surveillance, sans même que la société de télécommunications concernée ne s'en aperçoive, comme ce fut le cas pour Orange dans le cadre de ses opérations⁹.

54. Nombre de délégations ont préconisé que les entreprises et les tiers impliqués exercent leurs activités de façon plus transparente et soient amenés à répondre de leur propre conduite. Certaines délégations ont insisté sur la nécessité de mieux comprendre la façon dont les intermédiaires et autres entreprises pourraient s'acquitter de leurs responsabilités en matière de respect des droits de l'homme, ainsi que d'identifier les pouvoirs réglementaires qui devaient revenir respectivement aux secteurs public et privé. M. Nissim a confirmé l'importance fondamentale de la transparence pour les sociétés de télécommunications, qui subissaient de fortes pressions pour faire en sorte de mener leurs activités avec une plus grande transparence. À ce titre, il a indiqué que le directeur général de sa société avait signé une charte pour la protection des données en vertu de laquelle ladite société s'engageait à garantir la sécurité des données personnelles de ses clients; à offrir à ses clients la faculté de contrôler leurs propres données personnelles et l'usage qui en serait autorisé; à gérer en toute transparence et en toute circonstance les données de ses clients et usagers; et à aider l'ensemble de ses clients et usagers à protéger leur vie privée et à gérer leurs données personnelles. Il a cependant précisé que sa société avait subi deux atteintes à la vie privée depuis la signature de la charte, en insistant sur le fait que la protection des données contre l'ingérence d'autorités gouvernementales était toujours une question problématique. Il a rappelé que, même si un certain nombre de sociétés de télécommunications s'étaient engagées à respecter leurs propres obligations en matière de transparence, il incombait au premier chef à l'État de garantir la transparence. Il a

⁹ Voir Human Rights Watch, «Ils savent tout ce que nous faisons: Surveillance Télécom et Internet en Éthiopie» (mars 2014).

également rappelé que les sociétés de télécommunications étaient soumises aux lois locales et que le cadre législatif auquel devaient se conformer leurs opérations variait d'un pays à l'autre. Il a fait état de la tendance actuelle des sociétés à recenser les cadres juridiques en vigueur dans tous les pays où elles exerçaient leurs activités. Il a indiqué que dans certains pays, la législation permettait le respect de la transparence a posteriori, soit en autorisant les sociétés à fournir des informations sur les requêtes qui leur étaient adressées par les gouvernements, ou sur les données transmises à ces derniers, soit en autorisant l'État à le faire. Dans d'autres pays, ni les sociétés ni l'État ne pouvaient faire preuve de transparence à propos des mesures imposées aux sociétés. M. Nissim a fait observer que les sociétés de télécommunications s'efforçaient de protéger le droit international des droits de l'homme en recourant aux moyens dont elles disposaient. Il a évoqué à titre d'exemple le cas d'un gouvernement qui, pendant les révolutions du Printemps arabe, avait enjoint à sa société d'envoyer des messages texte à tous ses clients. Suite au refus initial de l'entreprise, ce gouvernement avait formulé une nouvelle fois ses exigences par l'intermédiaire de représentants des forces armées. Sa société avait alors accepté d'envoyer le message prescrit, mais avec la signature d'un des militaires présents. Il s'agissait d'un élément d'information minime, mais non négligeable, qui permettait à la société civile de se faire une idée de la situation.

55. M. Nissim a souligné l'importance de la participation des différentes parties prenantes. Il a cité à titre d'exemple un autre cas auquel sa société avait dû faire face, où le gouvernement en question avait renoncé aux requêtes qu'il avait adressées aux sociétés de télécommunications, pour plusieurs raisons, dont le fait que la société civile avait rendu ces requêtes publiques. Il a indiqué qu'il apporterait son appui à l'élaboration d'un instrument juridique international qui porterait sur les obligations des entreprises du secteur privé concernant la protection du droit à la vie privée face aux mesures de surveillance, en précisant que l'élaboration de lois types et de meilleures pratiques constituerait également une aide précieuse pour les gouvernements.

D. Marche à suivre

56. De nombreuses délégations ont souligné qu'il était nécessaire de s'assurer de la participation continue des diverses parties prenantes. Elles ont indiqué que la participation des États n'était pas suffisante, mais que les entités privées, la société civile, les communautés scientifiques et techniques, les entreprises, les universitaires et les spécialistes des droits de l'homme devaient prendre part aux débats. La nécessité d'une participation accrue du Conseil des droits de l'homme a également été soulignée.

57. Plusieurs délégations ont invité les États à revoir leurs procédures, leurs pratiques et leur législation relatives à la surveillance et à l'interception des communications, et à la collecte de données personnelles, afin de les adapter aux besoins du XXI^e siècle et de s'assurer qu'ils étaient pleinement conformes au droit international des droits de l'homme. D'autres ont préconisé la mise en place d'un système international transparent doté d'un cadre international approprié en matière de gouvernance de l'Internet, notamment de garanties suffisantes concernant la protection des données à caractère personnel. Une délégation a demandé que soit élaboré un code de conduite sur ces questions. Plusieurs délégations et organisations non gouvernementales ont invité le Conseil à établir le mandat d'un rapporteur spécial sur le droit à la vie privée, car il était essentiel d'appeler l'attention de manière ciblée et durable sur ces questions.

V. Conclusions

58. Les intervenants ont conclu que l'évolution technologique pouvait entraîner de nouveaux défis pour la législation en vigueur. Dans ce cas, les cadres juridiques établis, notamment le droit international des droits de l'homme, continueraient de s'appliquer, même si la mise en application de la loi devait être adaptée pour faire face à cette nouvelle réalité. S'agissant de la promotion et la protection du droit à la vie privée, y compris dans le contexte de la surveillance sur le territoire national et à l'extérieur, le cadre international relatif aux droits de l'homme était clair. Il était toutefois nécessaire d'assurer une meilleure application au niveau national des normes internationales relatives au droit à la vie privée, au moyen d'une législation nationale appropriée et de mesures de protection et de contrôle plus fortes.

59. Les intervenants ont fait observer qu'il était essentiel de mettre en place des protections juridiques contre les violations et un contrôle effectif associant toutes les parties prenantes. Des tribunaux indépendants, impartiaux et compétents devaient participer davantage, et avec plus de moyens, à l'examen de ces questions complexes. En outre, ils ont souligné la nécessité d'une transparence accrue concernant les politiques, la législation et les interprétations juridiques en matière de surveillance, ainsi que les décisions de justice, lorsque de telles décisions étaient prises. Les lois et les règlements, ainsi que la façon dont ils étaient interprétés et appliqués, devaient être accessibles à tous. Le pouvoir dont disposaient les gouvernements d'accéder aux données sur les communications devait s'appuyer sur un cadre juridique clair et transparent, qui tienne compte des progrès technologiques et soit conforme à l'État de droit et aux normes internationales relatives aux droits de l'homme.

60. Appuyant le point de vue exprimé par les États, les organisations régionales et les organisations non gouvernementales, les intervenants ont souligné que la protection, la promotion et le respect du droit à la vie privée nécessitaient la participation continue de toutes les parties prenantes, y compris les gouvernements, l'industrie, la société civile et les organisations internationales. Ils ont mis l'accent sur la capacité unique qu'avait l'Organisation des Nations Unies de réunir toutes les parties prenantes et de rechercher les moyens les plus efficaces de protéger le droit à la vie privée, et ont souligné que le Conseil des droits de l'homme devait continuer à examiner cette question, notamment dans le cadre de l'Examen périodique universel, avec la participation accrue de la société civile. Le Haut-Commissariat aux droits de l'homme et le Haut-Commissaire devaient également continuer à travailler sur cette question, et les titulaires de mandat au titre des procédures spéciales devaient coopérer dans le cadre de leurs propres mandats, selon les besoins. Il fallait également envisager d'établir un nouveau mandat au titre des procédures spéciales sur le droit à la vie privée et d'examiner les problèmes actuels et les moyens de conceptualiser plus largement ce droit.

61. Enfin, les intervenants ont mis en avant le rôle essentiel joué par l'Organisation des Nations Unies et d'autres organisations internationales dans la promotion des normes juridiques internationales qui orientent l'action des entreprises privées lorsqu'elles s'attachaient à assurer le respect des droits de l'homme de leurs clients et d'autres utilisateurs. Les entreprises s'efforçaient d'obtenir l'appui de l'ONU pour promouvoir l'adoption de ces normes dans le droit interne des États Membres. En développant le cadre international s'y rapportant, les organisations internationales aidaient également les entreprises à s'acquitter de leur responsabilité en matière de respect et de protection de la vie privée des utilisateurs, à mesure de l'évolution des progrès technologiques. La question de savoir si une loi type ou un code de conduite pouvait être rédigé devait être examinée.