Nations Unies A/HRC/27/37

Assemblée générale

Distr. générale
30 juin 2014
Français
Original: anglais

Conseil des droits de l'homme
Vingt-septième 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

Le droit à la vie privée à l'ère du numérique

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

Résumé

Dans sa résolution 68/167, l'Assemblée générale a prié la Haut-Commissaire des Nations Unies aux droits de l'homme de lui présenter, à sa soixante-neuvième session, ainsi qu'au Conseil des droits de l'homme, à sa vingt-septième session, 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, dans lequel elle proposerait aux États Membres des vues et recommandations. Le présent rapport fait suite à cette demande. Le Haut-Commissariat présentera aussi le rapport à l'Assemblée générale à sa soixante-neuvième session, comme elle le lui a demandé.

GE.14-06872 (F) 090914 100914
1406872

Table des matières

I. Introduction

1. Les technologies des communications numériques, comme Internet, les téléphones portables intelligents et les appareils dotés de la technologie Wi-Fi font désormais partie du quotidien. En améliorant de façon spectaculaire l'accès à l'information et la communication en temps réel, les innovations en matière de technologie des communications ont stimulé la liberté d'expression, favorisé le débat mondial et encouragé la participation démocratique. En faisant mieux entendre la voix des défenseurs des droits de l'homme et en leur fournissant de nouveaux outils pour recueillir des informations sur les violations et les dénoncer, ces technologies puissantes laissent augurer un meilleur exercice des droits de l'homme. Alors même que la vie de nos contemporains se déroule de plus en plus en ligne, le réseau Internet est devenu omniprésent et a progressivement gagné la sphère intime.

2. À l'ère du numérique, les technologies des communications ont aussi renforcé les moyens dont disposent les pouvoirs publics, les entreprises et les particuliers pour surveiller, intercepter et collecter les données. Comme l'a indiqué le Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, grâce aux progrès technologiques, l'efficacité avec laquelle l'État exerce sa surveillance n'a plus de limites, ni d'échelle ni de durée. La baisse des coûts des technologies et du stockage des données a éliminé les obstacles financiers ou pratiques à l'exercice de la surveillance. L'État n'a jamais disposé de moyens aussi importants pour mener des activités de surveillance simultanées, intrusives, ciblées et à grande échelle[1]. Autrement dit, les plates-formes technologiques dont la vie politique, économique et sociale mondiale est de plus en plus tributaire sont non seulement exposées à la surveillance de masse mais peuvent même la faciliter.

3. De vives inquiétudes ont été exprimées lorsque des politiques et des pratiques qui exploitent la vulnérabilité des technologies des communications numériques vis-à-vis de la surveillance et de l'interception électroniques ont été dénoncées dans divers pays à travers le monde. On ne compte plus les exemples de surveillance numérique ouverte ou secrète pratiquée dans des juridictions de par le monde, la surveillance de masse exercée par les États constituant plus souvent désormais une habitude dangereuse qu'une mesure exceptionnelle. Des administrations publiques auraient menacé d'interdire des services de télécommunications et des sociétés de matériel sans fil si ces derniers ne leur accordaient pas un accès direct aux flux des communications, elles auraient mis sur écoute des câbles à fibres optiques à des fins de surveillance et exigé des entreprises qu'elles divulguent systématiquement des informations en vrac sur leurs clients et leurs employés. Qui plus est, certaines auraient recouru à la surveillance des réseaux de télécommunications pour pointer des membres de l'opposition et/ou des dissidents politiques. Des cas ont été signalés où les autorités de certains États enregistrent régulièrement toutes les conversations téléphoniques et les conservent pour les analyser, et selon certaines informations, des gouvernements hôtes auraient surveillé les communications à l'occasion de manifestations d'envergure internationale. Dans un autre cas, l'administration d'un État exigerait que tous les ordinateurs personnels vendus dans le pays soient équipés de logiciels de filtrage susceptibles de présenter d'autres capacités de surveillance. Même des groupes non étatiques seraient en train de mettre en place des capacités de surveillance numérique très poussées. Les technologies de surveillance de masse pénètrent aujourd'hui le marché mondial, d'où un plus grand risque que la surveillance numérique échappe au contrôle des pouvoirs publics.

[1] A/HRC/23/40, par. 33.

4. Les préoccupations se sont accentuées suite à des révélations faites en 2013 et 2014 selon lesquelles la National Security Agency des États-Unis d'Amérique et le General Communications Headquarters du Royaume-Uni de Grande-Bretagne et d'Irlande du Nord avaient collaboré à la mise au point de technologies autorisant l'accès à une grande partie du trafic Internet mondial, à des fichiers de communications aux États-Unis, à des carnets d'adresses électroniques de particuliers et à des volumes considérables d'autres contenus de communications numériques. Ces technologies auraient été déployées par le biais d'un réseau transnational mettant en jeu les relations qu'entretiennent les services de renseignement stratégique des États, des mesures de contrôle réglementaire des sociétés privées et des contrats commerciaux.

5. En réponse aux préoccupations exprimées par les États Membres et d'autres parties prenantes au sujet des incidences néfastes de ces pratiques de surveillance sur les droits de l'homme, en décembre 2013, l'Assemblée générale a adopté, sans la mettre aux voix, la résolution 68/167 sur le droit à la vie privée à l'ère du numérique. Dans cette résolution, coparrainée par 57 États Membres, l'Assemblée a affirmé que les droits dont les personnes jouissaient hors ligne devaient également être protégés en ligne et a invité tous les États à respecter et à protéger le droit à la vie privée dans la communication numérique. Elle a également invité tous 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, en soulignant la nécessité pour les États de veiller à respecter pleinement leurs obligations au regard du droit international des droits de l'homme.

6. Toujours dans la résolution 68/167, l'Assemblée générale a prié la Haut-Commissaire des Nations Unies aux droits de l'homme de lui présenter, à sa soixante-neuvième session, ainsi qu'au Conseil des droits de l'homme, à sa vingt-septième session, 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, dans lequel elle proposerait aux États Membres des vues et recommandations. Le présent rapport fait suite à cette demande. Comme cela le lui a été demandé dans la résolution 68/167, le Haut-Commissariat (HCDH) présentera aussi le rapport à l'Assemblée à sa soixante-neuvième session.

II. Contexte et méthodologie

7. Compte tenu de la résolution 68/167, le HCDH a participé à plusieurs manifestations et a recueilli des informations émanant de sources très diverses. Le 24 février 2014, la Haut-Commissaire a fait un exposé liminaire à un séminaire d'experts sur «Le droit à la vie privée à l'ère du numérique» qui a été coparrainé par l'Allemagne, l'Autriche, le Brésil, le Liechtenstein, le Mexique, la Norvège et la Suisse et organisé par l'Académie de droit international humanitaire et de droits humains à Genève.

8. De novembre 2013 à mars 2014, le HCDH a fait participer l'Université des Nations Unies à un projet de recherche sur l'application du droit international des droits de l'homme aux régimes nationaux de contrôle des activités de surveillance numérique des États. Le HCDH sait gré à l'Université pour la contribution majeure qu'elle a apportée à l'élaboration du présent rapport par le biais du projet de recherche.

9. Dans le cadre d'une consultation ouverte, le 27 février 2014, le HCDH a adressé un questionnaire aux États Membres par l'intermédiaire de leurs Missions permanentes à Genève et à New York, à des organisations internationales et régionales, des institutions nationales des droits de l'homme, des organisations non gouvernementales et des entreprises privées. Dans son questionnaire, il a demandé des informations sur les questions

abordées par l'Assemblée générale dans sa résolution 68/167. Il a créé une page spéciale sur son site Web pour que le public puisse consulter le questionnaire et l'ensemble des contributions et que de nouveaux éléments puissent lui être fournis. Des contributions ont été reçues de 29 États Membres de toutes les régions, de 5 organisations internationales et/ou régionales, de 3 institutions nationales des droits de l'homme, de 16 organisations non gouvernementales et de 2 entreprises privées[2].

10. De nombreuses contributions ont décrit de façon détaillée les cadres législatifs nationaux existants et d'autres mesures prises pour assurer le respect et la protection du droit à la vie privée à l'ère du numérique ainsi que des initiatives visant à établir et mettre en œuvre des garanties procédurales et un contrôle effectif. Certaines contributions ont évoqué les difficultés rencontrées dans la mise en œuvre du droit à la vie privée à l'ère du numérique et fait des suggestions d'initiatives à engager au niveau international. Il a notamment été proposé que le Comité des droits de l'homme soit encouragé à mettre à jour ses Observations générales pertinentes, en particulier celles concernant l'article 17 du Pacte international relatif aux droits civils et politiques; que le Conseil des droits de l'homme établisse un mandat au titre des procédures spéciales relatif au droit à la vie privée; et/ou que les titulaires de mandat au titre des procédures spéciales existants dans ce domaine prennent part à des initiatives conjointes ou individuelles visant à traiter les questions liées au droit à la vie privée dans le contexte de la surveillance numérique et à donner des indications de bonnes pratiques.

11. Comme l'a demandé l'Assemblée générale dans sa résolution 68/167, le présent rapport propose des réflexions et des recommandations qui résultent de l'analyse des informations disponibles au moment de son établissement et s'inspirent également des éléments très fournis figurant dans toute la série de contributions reçues.

III. Questions relatives au droit à la vie privée à l'ère du numérique

12. Comme l'a rappelé l'Assemblée générale dans sa résolution 68/167, le droit international des droits de l'homme établit le cadre universel au regard duquel doit être mesurée toute atteinte aux droits individuels à la vie privée. Conformément à l'article 12 de la Déclaration universelle des droits de l'homme, «nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes.». Le Pacte international relatif aux droits civils et politiques, ratifié par 167 États à ce jour, dispose à l'article 17 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». Il dispose aussi que «toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes».

13. D'autres instruments internationaux relatifs aux droits de l'homme contiennent des dispositions analogues. Des textes législatifs adoptés à l'échelle régionale et nationale énoncent aussi le droit de chacun au respect de sa vie privée et familiale, de son domicile et de sa correspondance, ou le droit à la reconnaissance et au respect de sa dignité, de son intégrité personnelle ou de sa réputation. Autrement dit, l'importance fondamentale et la valeur constante du droit à la vie privée et la nécessité d'en assurer la protection sont universellement reconnues, dans la législation comme dans la pratique.

[2] Toutes les contributions sont disponibles à l'adresse www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx.

14. Bien que le présent rapport ait pour principal objet le droit à la vie privée, il convient de souligner que la surveillance de masse, l'interception des communications numériques et la collecte de données personnelles peuvent aussi porter atteinte à d'autres droits. Il s'agit notamment des droits à la liberté d'opinion et d'expression, du droit de rechercher, recevoir et répandre des informations, du droit à la liberté de réunion pacifique et d'association et du droit à la vie familiale − lesquels sont tous étroitement liés au droit à la vie privée et s'exercent de plus en plus par le biais des médias numériques. D'autres droits, comme le droit à la santé, peuvent aussi être affectés par les pratiques de surveillance numérique, par exemple lorsqu'un individu s'abstient de demander ou de communiquer des informations sensibles relatives à la santé de peur de mettre en cause son anonymat. Il existe des éléments crédibles permettant de penser que les technologies numériques ont été utilisées pour recueillir des informations qui ont donné lieu à des actes de torture et autres mauvais traitements. Il ressort aussi de certaines informations que les métadonnées tirées de la surveillance électronique ont été analysées pour localiser les cibles d'attaques létales par drones. Ces attaques continuent de susciter de graves inquiétudes quant au respect du droit international des droits de l'homme et du droit humanitaire et à l'obligation de rendre des comptes en cas de violations de ces droits. Les liens entre la surveillance de masse et ces autres incidences sur les droits de l'homme, bien qu'ils n'entrent pas dans le propos du présent rapport, méritent un examen plus approfondi.

A. Droit à la protection contre les immixtions arbitraires ou illégales dans sa vie privée, sa famille, son domicile ou sa correspondance

15. Plusieurs contributions ont souligné que lorsqu'elle se pratique conformément au droit, notamment au droit international des droits de l'homme, la surveillance des données des communications électroniques peut être une mesure nécessaire et efficace aux fins légitimes de l'application des lois ou du renseignement. Les révélations qui ont été faites concernant la surveillance numérique de masse amènent toutefois à se demander dans quelle mesure ces pratiques sont conformes aux normes juridiques internationales et si de plus fortes garanties doivent être mises en place en matière de surveillance pour protéger les individus contre des violations des droits de l'homme. Plus précisément, les mesures de surveillance ne doivent pas se traduire par des immixtions arbitraires ou illégales dans la vie privée, la famille, le domicile ou la correspondance d'un individu; les États doivent prendre des mesures spécifiques pour faire en sorte que la loi protège les personnes contre ces immixtions.

16. L'examen des diverses contributions reçues a montré que pour traiter ces questions, il faut déterminer ce qui constitue une immixtion dans la vie privée dans le contexte des communications numériques, définir l'expression «arbitraire et illégal» et établir lesquelles des personnes ont leurs droits protégés par le droit international des droits de l'homme, et dans quels cas. Les sections ci-après portent sur les questions mises en relief dans les diverses contributions.

1. Immixtion dans la vie privée

17. Les organes internationaux et régionaux créés en vertu de traités relatifs aux droits de l'homme, les tribunaux, les commissions et les experts indépendants ont tous fourni des orientations pertinentes pour ce qui est du champ et du contenu du droit à la vie privée, notamment du sens à donner à «immixtion» dans la vie privée d'un individu. Dans son Observation générale n° 16, le Comité des droits de l'homme a souligné que le respect de l'article 17 du Pacte international relatif aux droits civils et politiques exigeait que l'intégrité et le caractère confidentiel de la correspondance soient garantis en droit et en fait.

«La correspondance doit être remise au destinataire, sans interception, sans être ouverte, et sans qu'il en soit pris autrement connaissance.»[3]

18. Certains ont suggéré que la communication et l'échange de données personnelles par des moyens électroniques supposent un compromis par lequel des individus, en toute connaissance de cause, livrent volontairement des informations les concernant ainsi que les relations qu'ils entretiennent, en échange de l'accès numérique à des biens, des services et des données. On peut s'inquiéter, toutefois, de la mesure dans laquelle les consommateurs sont bien conscients de ce qu'ils partagent, de quelle façon et avec qui, et de l'usage qui sera fait de ces données. Selon des informations reçues, «de fait, s'agissant des données massives, dès lors que les données sont collectées, il peut être très difficile de garder son anonymat. Bien que des efforts de recherche encourageants soient en cours dans le but de masquer les informations permettant d'identifier une personne dans les grands ensembles de données, des travaux beaucoup plus pointus ont été engagés pour ré-identifier les données apparemment "anonymes". On s'attache beaucoup plus collectivement à trouver les moyens de fusionner les données qu'à investir dans les technologies propres à renforcer le respect de la vie privée.». En outre, les auteurs de ces observations ont noté que «l'accent mis sur le contrôle de la collecte et de la conservation des données, bien qu'important, pourrait ne plus suffire à protéger la vie privée» du fait en partie que les «données massives autorisent de nouveaux modes d'utilisation des données, inventifs et d'une puissance étonnante»[4].

19. Dans le même ordre d'idées, d'aucuns soutiennent que l'interception − ou la collecte − de données sur une communication, et non plus sur le contenu de la communication, ne constitue pas à elle seule une immixtion dans la vie privée. Or du point de vue du droit à la vie privée, cette distinction n'est pas convaincante. Les agrégations d'informations communément appelées «métadonnées» peuvent donner des indications sur la conduite d'un individu, ses relations sociales, ses préférences privées et son identité qui vont bien au-delà de ce que l'on obtient en accédant au contenu d'une communication privée. Comme la Cour européenne de justice l'a récemment observé, les métadonnées de ces communications «prises dans leur ensemble, sont susceptibles de permettre de tirer des conclusions très précises concernant la vie privée des personnes dont les données ont été conservées»[5]. C'est parce que cette évolution a été reconnue qu'ont vu le jour des initiatives de refonte des politiques et pratiques existantes dans le but d'assurer une meilleure protection de la vie privée.

20. Il s'ensuit que tout captage de données sur les communications constitue potentiellement une immixtion dans la vie privée et qu'en outre, la collecte et la conservation de ces données constituent également une telle ingérence, que les données soient ou non consultées ou utilisées par la suite. La possibilité qu'une information relative à des communications soit interceptée constitue même à elle seule une immixtion dans la vie privée[6] et peut être attentatoire à des droits, y compris ceux relatifs à la liberté

[3] *Documents officiels de l'Assemblée générale, quarante-troisième session, Supplément n° 40* (A/43/40), annexe VI, par. 8.

[4] Bureau exécutif du Président des États-Unis, «Big Data: Seizing Opportunities, Preserving Values», mai 2014 (disponible à l'adresse: www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf), p. 54.

[5] Cour européenne de justice, arrêt de la Cour dans les affaires jointes C-293/12 et C-594/12, Digital Rights Ireland et Seitlinger et autres, arrêt du 8 avril 2014, par. 26 et 27, et 37. Voir aussi Bureau exécutif du Président des États-Unis, «Big Data and Privacy: A Technological Perspective» (disponible à l'adresse: www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf), p. 19.

[6] Voir Cour européenne des droits de l'homme, *Weber et Saravia* c. *Allemagne*, par. 78; *Malone* c. *RU*, par. 64.

d'expression et d'association. Ainsi, l'existence même d'un programme de surveillance de masse constitue une immixtion dans la vie privée. Il reviendra à l'État de démontrer que cette immixtion n'est ni arbitraire ni illégale.

2. Qu'entend-on par «arbitraire» ou «illégal»?

21. L'atteinte au droit à la vie privée d'un individu n'est autorisée par le droit international des droits de l'homme que si elle n'est ni arbitraire ni illégale. Dans son Observation générale n° 16, le Comité des droits de l'homme a expliqué que le terme «illégal» signifiait qu'aucune immixtion ne pouvait avoir lieu, «sauf dans les cas envisagés par la loi. Les immixtions autorisées par les États ne peuvent avoir lieu qu'en vertu d'une loi, qui doit elle-même être conforme aux dispositions, aux buts et aux objectifs du Pacte»[7]. Autrement dit, une immixtion qui est autorisée par la législation nationale peut néanmoins être «illégale» si ladite législation n'est pas conforme au Pacte international relatif aux droits civils et politiques. L'expression «immixtions arbitraires» peut également s'étendre aux immixtions prévues par la loi. Le Comité a expliqué que l'introduction de cette notion a pour objet de garantir que même une immixtion prévue par la loi soit conforme aux dispositions, aux buts et aux objectifs du Pacte et soit, dans tous les cas, raisonnable eu égard aux circonstances particulières»[8]. D'après l'interprétation du Comité, pour être raisonnable «l'immixtion dans la vie privée doit être proportionnée à l'objectif recherché et doit être nécessaire dans les circonstances particulières à chaque cas»[9].

22. Contrairement à certaines autres dispositions du Pacte, l'article 17 ne contient pas de clause restrictive expresse. Des indications sur le sens de l'expression limitative «arbitraire ou illégal» peuvent être néanmoins tirées des Principes de Syracuse concernant les dispositions du Pacte international relatif aux droits civils et politiques qui autorisent des restrictions ou des dérogations[10]; de la pratique du Comité des droits de l'homme, ainsi qu'il ressort de ses Observations générales, y compris les Observations générales n[os] 16, 27, 29, 34 et 31, de constatations formulées au sujet de communications individuelles[11] et d'observations finales[12]; de la jurisprudence régionale et nationale[13]; et d'avis d'experts indépendants[14]. Dans son Observation générale n° 31 sur la nature de l'obligation juridique générale imposée aux États parties au Pacte, par exemple, le Comité des droits de l'homme dispose que les États parties doivent s'abstenir de violer les droits reconnus par le Pacte, et que «toute restriction à leur exercice doit être autorisée par les dispositions pertinentes du Pacte. Dans les cas où des restrictions sont formulées, les États doivent en démontrer la nécessité et ne prendre que des mesures proportionnées aux objectifs légitimes poursuivis afin d'assurer une protection véritable et continue des droits énoncés dans le Pacte»[15]. Le Comité a également souligné que «de telles restrictions ne peuvent en aucun cas être appliquées ou invoquées d'une manière qui porterait atteinte à l'essence même d'un droit énoncé dans le Pacte».

---

[7] *Documents officiels de l'Assemblée générale* (voir la note de bas de page 3), par. 3.

[8] Ibid, par. 4.

[9] Communication n[os] 488/1992, *Toonen* c. *Australie*, par. 8.3; voir aussi les communications n° 903/1999, par. 7.3, et 1482/2006, par. 10.1 et 10.2.

[10] Voir le document E/CN.4/1985/4, annexe.

[11] Par exemple, communication n° 903/1999, 2004, *Van Hulst* c. *Pays-Bas*.

[12] CCPR /C/USA/CO/4.

[13] Par exemple, Cour européenne des droits de l'homme, *Uzun* c. *Allemagne*, 2 septembre 2010 et *Weber et Soravia* c. *Allemagne*, par. 4; et Cour interaméricaine des droits de l'homme, *Escher* c. *Brésil*, arrêt du 20 novembre 2009.

[14] Voir les documents A/HRC/13/37 et A/HRC/23/40. Voir aussi les Principes internationaux sur l'application des droits de l'homme à la surveillance des communications, disponible à l'adresse: https://fr.necessaryandproportionate.org/text.

[15] CCPR/C/21/Rev.1/Add. 13, par. 6.

23. Ces sources faisant autorité mettent en évidence les grands principes de la légalité, de la nécessité et de la proportionnalité, dont l'importance a aussi été soulignée dans nombre des contributions reçues. Pour commencer, toute restriction des droits à la vie privée énoncés à l'article 17 doit être prescrite par la loi, et la loi en question doit être suffisamment accessible, claire et précise pour qu'un individu puisse s'y référer pour vérifier qui est autorisé à pratiquer la surveillance des données et en quelles circonstances. La restriction doit être nécessaire pour atteindre un objectif légitime, elle doit aussi être proportionnée à cet objectif et constituer l'option la moins intrusive possible[16]. En outre, il doit être démontré que la restriction imposée au droit (une immixtion dans la vie privée, par exemple, aux fins de la protection de la sécurité nationale ou du droit à la vie des autres personnes) a des chances de réaliser l'objectif en question. Il incombe aux autorités souhaitant restreindre le droit de montrer que cette restriction est liée à un objectif légitime. En outre, toute restriction du droit à la vie privée ne doit pas vider le droit de son sens et doit être compatible avec d'autres droits de l'homme, dont l'interdiction de la discrimination. Dans les cas où la restriction ne répondra pas à ces critères, elle sera illégale et/ou l'atteinte au droit à la vie privée sera arbitraire.

24. Les États invoquent souvent des raisons de sécurité nationale, dont les risques présentés par le terrorisme, pour justifier les programmes de surveillance des communications numériques. Plusieurs contributions laissent entendre que dans la mesure où les technologies des communications numériques peuvent être utilisées − et l'ont été − par des individus à des fins criminelles (notamment pour recruter des tiers et obtenir des financements en vue de la commission d'actes de terrorisme), la surveillance ciblée légale des communications numériques peut constituer une mesure nécessaire et efficace pour les services responsables de l'application des lois et les services du renseignement lorsqu'elle s'exerce conformément au droit international et national. La surveillance pour des raisons de sécurité nationale ou de prévention du terrorisme ou d'autres formes de criminalité peut constituer un «objectif légitime» si on l'examine au regard de l'article 17 du Pacte. Le degré d'immixtion doit, toutefois, être évalué selon que la mesure est nécessaire ou non à la réalisation de cet objectif et qu'elle présente un intérêt réel à cette fin.

25. S'agissant d'évaluer la nécessité d'une mesure, le Comité des droits de l'homme, dans son Observation générale n° 27 sur l'article 12 du Pacte international relatif aux droits civils et politiques, a souligné que «les restrictions ne doivent pas porter atteinte à l'essence même du droit […]; le rapport entre le droit et la restriction, entre la règle et l'exception, ne doit pas être inversé»[17]. Le Comité a également expliqué «qu'il ne suffit pas que les restrictions servent les buts autorisés; celles-ci doivent être également nécessaires pour protéger ces buts». En outre, les mesures doivent être proportionnées: «elles doivent constituer le moyen le moins perturbateur parmi ceux qui pourraient permettre d'obtenir le résultat recherché»[18]. Lorsqu'il existe un objectif légitime et que des garanties suffisantes sont en place, un État peut être autorisé à exercer une surveillance très intrusive; toutefois, il incombe à la puissance publique de démontrer que l'immixtion est à la fois nécessaire et proportionnée au risque spécifique à traiter. Les programmes de surveillance de masse ou à grande échelle peuvent donc être jugés arbitraires, même s'ils servent un objectif légitime et ont été adoptés sur la base d'un régime juridique accessible. Autrement dit, il ne suffit pas que les mesures soient ciblées pour trouver certaines aiguilles dans une botte de foin; ce qu'il convient d'examiner, c'est leur impact sur la botte de foin, au regard du risque de préjudice, c'est-à-dire déterminer si la mesure est nécessaire et proportionnée.

[16] CCPR/C/21/Rev.1/Add.9, par. 11 à 16. Voir aussi le document A/HRC/14/46, annexe, pratique n° 20.

[17] CCPR/C/21/Rev.1/Add.9, par. 11 à 16. Voir aussi Cour européenne des droits de l'homme, *Handyside* c. *Royaume-Uni*, par. 48; et *Klass* c. *Allemagne*, par. 42.

[18] CCPR/C/21/Rev.1/Add.9, par. 11 à 16.

26. Dès lors que l'on s'inquiète de savoir si l'accès aux données et leur utilisation correspondent à des objectifs légitimes spécifiques, il faut aussi s'interroger sur le fait que les institutions publiques s'en remettent de plus en plus aux acteurs du secteur privé pour conserver les données «au cas où» elles seraient utiles à l'État. La conservation obligatoire des données de tiers − une caractéristique récurrente des régimes de surveillance dans de nombreux États, qui veut que les pouvoirs publics exigent des compagnies de téléphone et des fournisseurs d'accès à Internet qu'ils stockent des métadonnées de trafic et de localisation de leurs clients pour que les services responsables de l'application des lois et les services du renseignement puissent y accéder ultérieurement − ne semble ni nécessaire ni proportionnée[19].

27. Parmi les facteurs à prendre en compte pour déterminer si les mesures sont proportionnées, on citera l'usage qui est fait des données de masse et le type d'intervenant autorisé à y accéder après leur collecte. De nombreux cadres nationaux ne posent pas de «limites à l'utilisation des données» et, à la place, autorisent la collecte de données pour un objectif légitime ainsi que l'utilisation ultérieure de ces données à d'autres fins. Cette absence de limites effectives s'est accentuée depuis le 11 septembre 2001, la frontière entre la justice pénale et la protection de la sécurité nationale s'étant considérablement brouillée. Le partage de données qui en résulte entre les services responsables de l'application des lois, les services du renseignement et d'autres organes publics risque donc d'enfreindre l'article 17 du Pacte parce que des mesures de surveillance nécessaires et proportionnées pour un objectif légitime peuvent très bien ne pas l'être pour un autre objectif. Une étude des pratiques nationales en matière d'accès public aux données de tiers a permis de constater que «lorsque les services responsables de la sécurité nationale et de l'application des lois bénéficient déjà d'une plus grande facilité d'accès aux données du secteur privé, la liberté de plus en plus grande qu'ont ces organismes de partager ces données et de les utiliser en vue d'objectifs autres que ceux justifiant la collecte entraînent un net affaiblissement des protections dont bénéficiaient jusqu'ici les données»[20]. Dans plusieurs États, les régimes de partage des données ont été abolis suite à un contrôle juridictionnel pour ces motifs. Il a également été suggéré que les limites posées à l'utilisation des données constituent une bonne pratique permettant d'assurer le respect effectif des obligations qui incombent à un État en vertu de l'article 17 du Pacte[21], et ce, en prévoyant les sanctions voulues en cas de violation.

B. Protection de la loi

28. Le paragraphe 2 de l'article 17 du Pacte international relatif aux droits civils et politiques dispose expressément que toute personne a droit à la protection de la loi contre les immixtions arbitraires ou illégales dans sa vie privée. Cela suppose que tout programme de surveillance des communications doit être mené sur la base d'une loi accessible au public, laquelle, à son tour, doit être conforme au régime constitutionnel de l'État en question et du droit international des droits de l'homme[22]. Pour être «accessible», la loi doit

[19] Voir l'avis de l'Avocat général Cruz Villalón de la Cour européenne de justice dans les affaires jointes C-293/12 et C-594/12, qui tend à indiquer que la Directive 2006/24/CE (sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications) enfreint «dans son ensemble» la Charte des droits fondamentaux de l'Union européenne car elle n'impose pas de limitations strictes à la conservation de ces données. Voir aussi le document CCPR/C/USA/CO/4, par. 22.

[20] Fred H. Cate, James X. Dempsey et Ira S. Rubinstein, «Systematic government access to private-sector data», *International Data Privacy Law*, vol. 2, n° 4, 2012, p. 198.

[21] Voir le document A/HRC/14/46, annexe, pratique 23.

[22] Voir ibid., annexe.

non seulement être publiée, mais être suffisamment précise pour permettre à la personne concernée de modifier sa conduite, en connaissant à l'avance les conséquences de tel ou tel de ses actes. L'État doit veiller à ce que toute immixtion dans la vie privée, la famille, le domicile ou la correspondance soit autorisée par des textes législatifs qui: a) sont publics et accessibles à tous; b) contiennent des dispositions garantissant que l'accès aux données relatives aux communications, ainsi que leur collecte et leur utilisation soient adaptés à des objectifs légitimes précis; c) sont suffisamment précis, énonçant en détail les circonstances exactes dans lesquelles de telles immixtions peuvent être autorisées, les procédures d'autorisation, les catégories de personnes susceptibles d'être placées sous surveillance, la durée maximale de la surveillance, et les procédures d'utilisation et de conservation des données recueillies; et d) mettent en place des garanties efficaces contre les abus[23].

29. En conséquence, les règles secrètes et les interprétations secrètes − voire même les interprétations jurisprudentielles secrètes − de la loi n'ont pas les qualités nécessaires pour constituer de tels «textes législatifs»[24]. Il en est de même pour les lois et les règles qui confèrent un pouvoir discrétionnaire excessif à des organes exécutifs comme les services de sûreté et les services du renseignement; le champ et les modalités d'exercice du pouvoir discrétionnaire accordé doivent être indiqués (dans la loi proprement dite, ou dans des directives publiées contraignantes) avec une clarté raisonnable. Une loi qui est accessible, mais dont les effets ne sont pas prévisibles, ne conviendra pas. De par leur caractère secret, les pouvoirs de surveillance spécifique présentent un risque plus élevé d'exercice arbitraire du pouvoir discrétionnaire lequel risque exige en retour que la réglementation applicable au pouvoir discrétionnaire soit plus précise, et qu'un contrôle additionnel soit mis en place. Plusieurs États exigent également que le cadre juridique soit établi par une loi examinée au Parlement plutôt que par un simple règlement subsidiaire promulgué par l'exécutif − ce qui permet d'assurer que le cadre juridique n'est pas seulement accessible au public concerné après son adoption mais aussi pendant son élaboration, conformément à l'article 25 du Pacte international relatif aux droits civils et politiques[25].

30. La prescription d'accessibilité est également pertinente lorsqu'on examine la nouvelle pratique qu'ont adoptée les États de déléguer les tâches de surveillance à des tiers. Des informations crédibles portent à croire que certaines administrations publiques font systématiquement effectuer les tâches de collecte et d'analyse des données dans le cadre de juridictions offrant des garanties plus faibles en matière de protection de la vie privée. Certaines de ces autorités auraient administré un réseau transnational de services du renseignement en jonglant avec divers vides juridiques et en coordonnant la pratique de la surveillance pour contourner les protections offertes par les régimes juridiques nationaux. On peut avancer que cette pratique ne remplit pas les conditions voulues pour être légale parce que comme l'ont indiqué certaines des contributions au présent rapport, elle n'assure pas la prévisibilité du fonctionnement du régime de surveillance aux personnes qui y sont soumises. Elle est susceptible de porter atteinte à l'essence du droit protégé par l'article 17 du Pacte international relatif aux droits civils et politiques et donc d'être interdite par l'article 5 du Pacte. Les États n'ont pas pris non plus de mesures effectives pour protéger les individus relevant de leur compétence contre les pratiques de surveillance illégale suivies par d'autres États ou entreprises, en violation de leurs propres obligations en matière de droits de l'homme.

[23] CCPR /C/USA/CO/4, par. 22. Voir aussi Cour européenne des droits de l'homme, *Malone* c. *Royaume-Uni*, n° 8691/79, 2 août 1984, par. 67 et 68; et *Weber et Saravia* c. *Allemagne*, requête n° 54934/00, 29 juin 2006, affaire dans le cadre de laquelle la Cour a énoncé les garanties minimales que la loi doit renfermer.

[24] Voir le document CCPR /C/USA/CO/4, par. 22.

[25] Voir aussi le document A/HRC/14/46.

C. Qui est protégé et dans quels cas?

31. La question de l'application extraterritoriale du Pacte international relatif aux droits civils et politiques à la surveillance numérique a été traitée dans plusieurs des contributions reçues. Même s'il est clair que certains aspects des programmes de surveillance récemment révélés, par exemple, mettront en jeu les obligations territoriales des États qui exercent la surveillance, d'autres préoccupations ont été exprimées au sujet de la surveillance extraterritoriale et de l'interception des communications.

32. L'article 2 du Pacte international relatif aux droits civils et politiques exige de chaque État partie qu'il respecte et garantisse à tous les individus se trouvant sur son territoire et relevant de sa compétence les droits reconnus dans le Pacte, sans distinction aucune, notamment de race, de couleur, de sexe, de langue, de religion, d'opinion politique ou de toute autre opinion, d'origine nationale ou sociale, de fortune, de naissance ou de toute autre situation. Le Comité des droits de l'homme, dans son Observation générale n° 31, a affirmé qu'aux termes du paragraphe 1 de l'article 2, les États parties sont tenus de respecter et garantir à tous les individus se trouvant sur leur territoire et à tous ceux relevant de leur compétence les droits énoncés dans le Pacte. Cela signifie qu'un État partie doit respecter et garantir à quiconque se trouve sous son pouvoir ou son contrôle effectif les droits reconnus dans le Pacte même s'il ne se trouve pas sur son territoire[26]. Cela s'étend aux individus relevant de sa «compétence»[27].

33. Le Comité des droits de l'homme s'est appuyé sur le principe, énoncé même dans sa jurisprudence la plus ancienne, qu'un État ne peut pas se soustraire à ses obligations internationales en matière de droits de l'homme en prenant en dehors de son territoire des mesures qui lui seraient interdites «chez lui»[28]. Cette position est conforme aux vues de la Cour internationale de Justice qui a affirmé que le Pacte international relatif aux droits civils et politiques est applicable aux actes d'un État agissant «dans l'exercice de sa compétence en dehors de son propre territoire»[29], ainsi qu'aux articles 31 et 32 de la Convention de Vienne sur le droit des traités. Les notions de «pouvoir» et de «contrôle effectif» permettent de reconnaître qu'un État exerce une «compétence» ou des pouvoirs publics, dont les mesures de protection des droits de l'homme sont destinées à freiner les abus. Un État ne peut pas se soustraire à ses responsabilités en matière de droits de l'homme simplement en s'abstenant d'inscrire ces pouvoirs dans les limites de la loi. En tirant une autre conclusion, non seulement on affaiblirait l'universalité et l'essence des droits protégés par le droit international des droits de l'homme mais l'on pourrait aussi inciter structurellement les États à se déléguer mutuellement les tâches de surveillance.

34. Il s'ensuit que la surveillance numérique peut donc mettre en cause les obligations d'un État en matière de droits de l'homme si elle fait intervenir l'exercice du pouvoir ou le contrôle effectif dudit État à l'échelle de l'infrastructure des communications numériques, où que cela se produise, par exemple sous la forme d'écoutes directes ou d'une pénétration

[26] CCPR/C/21/Rev.1/Add.13, par. 10.

[27] Voir *Documents officiels de l'Assemblée générale, trente-sixième session, Supplément n° 40* (A/36/40), annexe XIX, par. 12.2; voir aussi l'annexe XX. Voir aussi les documents CCPR/CO/78/ISR, par. 11; CCPR/CO/72/NET, par. 8; CCPR/CO/81/BEL, par. 6; et Commission interaméricaine des droits de l'homme, *Coard* et al. c. *États-Unis*, affaire n° 10.951, rapport n° 109/99, 29 septembre 1999, par. 37, 39, 41 et 43.

[28] Voir *Documents officiels de l'Assemblée générale, trente-sixième session*, (voir la note de bas de page 27), annexe XIX, par. 12.2 et 12.3, et annexe XX, par. 10.3.

[29] Avis consultatif de la Cour internationale de Justice sur les *conséquences juridiques de l'édification d'un mur dans le territoire palestinien occupé*, du 9 juillet 2004 (A/ES-10/273 et Corr.1), par. 107 à 111. Voir aussi Cour internationale de Justice, *Activités armées sur le territoire du Congo* (*République démocratique du Congo* c. *Ouganda*), arrêt, 2005, p. 168.

de l'infrastructure en place. De même, dans les cas où l'État exerce une compétence réglementaire sur une tierce partie qui contrôle physiquement les données, cet État aura aussi des obligations en vertu du Pacte. Si un pays souhaite établir sa compétence sur les données d'entreprises privées au motif que ces entreprises ont été constituées en société sur son territoire, alors les protections des droits de l'homme doivent s'étendre aux personnes victimes d'immixtions dans leur vie privée, que ce soit dans le pays où les sociétés ont été constituées ou ailleurs. Cela reste valable que l'exercice de cette compétence soit légal ou non à l'origine, ou viole de fait la souveraineté d'un autre État.

35. Cette conclusion est tout aussi importante dans le cadre des discussions en cours sur le fait de savoir si les «étrangers» et les «citoyens» devraient avoir le même accès aux mesures de protection de la vie privée sous les régimes de contrôle de la surveillance pour des raisons de sécurité. Plusieurs régimes juridiques établissent une distinction entre les obligations dues aux nationaux ou aux personnes résidant sur le territoire d'un État, et celles dues aux non-nationaux et aux personnes résidant hors du territoire[30], ou, dans d'autres cas, accordent aux communications étrangères ou extérieures des niveaux de protection plus faibles. S'ils ne savent pas à coup sûr si les données sont étrangères ou nationales, les services du renseignement les traitent souvent comme des données étrangères (dans la mesure où les communications numériques passent systématiquement à l'étranger à un stade ou à un autre) et autorisent donc leur collecte et leur conservation. Cela aboutit à une protection de la vie privée beaucoup plus faible − s'il en existe une − pour les étrangers et les non-nationaux que pour les nationaux.

36. Le droit international des droits de l'homme établit clairement le principe de la non-discrimination. L'article 26 du Pacte international relatif aux droits civils et politiques dispose que «toutes les personnes sont égales devant la loi et ont droit sans discrimination à une égale protection de la loi» et aussi que «à cet égard, la loi doit interdire toute discrimination et garantir à toutes les personnes une protection égale et efficace contre toute discrimination, notamment de race, de couleur, de sexe, de langue, de religion, d'opinion politique et de toute autre opinion, d'origine nationale ou sociale, de fortune, de naissance ou de toute autre situation». Ces dispositions doivent être lues en ayant à l'esprit l'article 17, qui dispose que «nul ne sera l'objet d'immixtions arbitraires ou illégales dans sa vie privée» et que «toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes» et le paragraphe 1 de l'article 2. À cet égard, le Comité des droits de l'homme a souligné l'importance des mesures qui garantissent «que toute immixtion dans la vie privée soit faite conformément aux principes de légalité, de proportionnalité et de nécessité, indépendamment de la nationalité des personnes dont les communications sont directement surveillées et de l'endroit où elles se trouvent»[31].

D. Garanties procédurales et contrôle efficace

37. Le paragraphe 2 de l'article 17 du Pacte international relatif aux droits civils et politiques dispose que toute personne a droit à la protection de la loi contre les immixtions ou les atteintes arbitraires ou illégales. La «protection de la loi» doit être conférée par le biais de garanties procédurales effectives, y compris par des arrangements institutionnels efficaces dotés de ressources suffisantes. Il est clair, toutefois, que l'absence de contrôle

[30] Voir, par exemple, aux États-Unis, le Foreign Intelligence Surveillance Act (loi sur les activités de renseignement à l'étranger) S1881 a); au Royaume-Uni, le Regulation of Investigatory Powers Act 2000 (loi régissant les pouvoirs d'investigation), s8 4); en Nouvelle-Zélande, le Government Security Bureau Act 2003 (loi sur le Bureau chargé de la sécurité nationale), s. 15A; en Australie, l'Intelligence Services Act 2001 (loi sur les services du renseignement), S. 9; et au Canada, la loi sur la défense nationale, S. 273.64 1).

[31] CCPR /C/USA/CO/4, par. 22.

effectif a contribué à ce que personne n'ait de comptes à rendre concernant les immixtions arbitraires ou illégales dans la vie privée dans le domaine numérique. Les protections internes sans contrôle indépendant extérieur, en particulier, se sont montrées inefficaces contre les méthodes de surveillance illégales ou arbitraires. Ces protections peuvent prendre diverses formes, mais la participation de tous les services publics au contrôle des programmes de surveillance, et l'existence d'un bureau de contrôle civil indépendant, sont indispensables pour assurer l'efficacité de la protection de la loi.

38. La participation de l'autorité judiciaire, si elle est conforme aux normes internationales relatives à l'indépendance, l'impartialité et la transparence, peut rendre plus probable la conformité du régime légal général aux normes minimales qu'exige le droit international des droits de l'homme. Pour autant, la participation de l'autorité judiciaire au contrôle ne doit pas être considérée comme une panacée; dans plusieurs pays, la garantie judiciaire ou l'examen des activités de surveillance numérique des services du renseignement et/ou des services responsables de l'application des lois se sont limités de fait à tout avaliser. L'attention se tourne donc de plus en plus vers des modèles mixtes de contrôle administratif, judiciaire et parlementaire, un point souligné dans plusieurs contributions utilisées pour le présent rapport. Un intérêt particulier se manifeste en faveur de la création de postes de «défense de l'intérêt public» dans le cadre des procédures d'autorisation de la surveillance. Compte tenu du rôle croissant dévolu à des tierces parties, comme les fournisseurs d'accès à Internet, il faudrait peut-être aussi envisager d'autoriser ces parties à prendre part à la procédure d'autorisation des mesures de surveillance qui touchent leurs intérêts ou à contester les mesures existantes. L'utilité de conseils, d'un suivi et/ou d'un examen indépendants dans la mise en place d'un contrôle strict des mesures imposées sous le régime de surveillance réglementaire a été soulignée catégoriquement dans la jurisprudence pertinente. Les commissions parlementaires peuvent aussi jouer un rôle important; toutefois, elles peuvent aussi être dépourvues de l'indépendance, des ressources ou de la volonté nécessaires pour déceler les violations, et peuvent aussi s'exposer au détournement de la réglementation. La jurisprudence de niveau régional a fait apparaître l'utilité d'un organe de contrôle entièrement indépendant, en particulier pour suivre l'exécution des mesures de surveillance approuvées[32]. En 2009, le Rapporteur spécial sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste a donc indiqué «qu'il ne doit y avoir aucun système secret de surveillance qui ne soit placé sous la supervision d'une instance de contrôle efficace, ni aucune ingérence qui ne soit autorisée par l'intermédiaire d'un organisme indépendant»[33].

E. Droit à un recours utile

39. Le Pacte international relatif aux droits civils et politiques exige des États parties qu'ils fassent en sorte que les victimes de violations du Pacte disposent d'un recours utile. L'alinéa *b* du paragraphe 3 de l'article 2 stipule que les États parties au Pacte s'engagent à «garantir que l'autorité compétente, judiciaire, administrative ou législative, ou toute autre autorité compétente selon la législation de l'État, statuera sur les droits de la personne qui forme le recours et développer les possibilités de recours juridictionnel». Les États doivent aussi veiller à ce que les autorités compétentes fassent appliquer ces garanties lorsqu'ils les accordent. Comme le Comité des droits de l'homme l'a souligné dans son Observation générale n° 31, le fait pour un État partie de ne pas mener d'enquête sur des violations présumées pourrait en soi donner lieu à une violation distincte du Pacte[34]. En outre, la cessation d'une violation continue est un élément essentiel du droit à un recours utile.

[32] Voir par exemple la Cour européenne des droits de l'homme, *Ekimdzhiev* c. *Bulgarie*, requête n° 62540/00, 28 juin 2007.

[33] A/HRC/13/37, par. 62.

[34] CCPR/C/21/Rev.1/Add.13, par. 15.

40. Les recours utiles formés suite à des violations de la vie privée par la surveillance numérique peuvent donc prendre diverses formes judiciaires, législatives ou administratives. Ils ont généralement certaines caractéristiques en commun. Premièrement, toute personne qui peut faire valoir, par des arguments suffisamment étayés, que ses droits ont été atteints doit être informée de ces recours et pouvoir y accéder. Les questions relatives à la notification (de l'existence d'un régime de surveillance générale ou de mesures de surveillance spécifique) et à la qualité (pour contester ces mesures) deviennent donc essentielles au moment de déterminer si un recours utile est accessible. Les États notifient les mesures de diverses façons: certains exigent une notification post facto des objectifs de surveillance, à l'issue des enquêtes, mais de nombreux régimes ne prescrivent pas de notification. Certains peuvent aussi demander officiellement une notification de ce type dans les affaires pénales; toutefois, dans la pratique, cette règle semble couramment éludée. Il existe aussi diverses conceptions de la qualité pour former des recours judiciaires à l'échelle nationale. La Cour européenne des droits de l'homme a jugé que même si l'existence d'un régime de surveillance risquait de constituer une immixtion dans la vie privée, on ne pouvait former de recours judiciaire pour violation des droits que s'il y avait une «probabilité raisonnable» qu'une personne a été effectivement soumise à une surveillance illégale[35].

41. Deuxièmement, les recours utiles donnent généralement lieu à une enquête rapide, approfondie et impartiale des violations présumées. Il peut être prévu à cette fin un «organe de contrôle indépendant […] régi par des garanties de procédure équitable et de contrôle judiciaire suffisants, dans les limites qu'autorise une société démocratique»[36]. Troisièmement, pour que les recours soient utiles, ils doivent être en mesure de mettre fin aux violations en cours, par exemple, en ordonnant l'effacement des données ou une autre forme de réparation[37]. Ces instances de recours doivent disposer d'un «accès illimité et sans obstacle à toutes les informations pertinentes, aux ressources et à l'expertise nécessaires pour conduire leurs enquêtes, et sont habilitées à délivrer des ordonnances contraignantes»[38]. Quatrièmement, dans les cas où les violations des droits de l'homme atteignent le niveau de violations flagrantes, les recours non judiciaires ne sont pas adaptés car il faudra engager des poursuites pénales[39].

IV. Quel rôle peuvent jouer les entreprises?

42. De nombreux faits concourent à indiquer que les autorités publiques s'appuient de plus en plus sur le secteur privé pour l'exercice et la facilitation de la surveillance numérique. Sur tous les continents, elles utilisent à la fois des mécanismes juridiques formels et des méthodes secrètes pour accéder à des contenus et à des métadonnées. Ce processus s'officialise de plus en plus: dès lors que la fourniture de services

[35] Voir *Esbester* c. *Royaume-Uni*, requête n° 18601/91, décision de la Commission du 2 avril 1993; *Redgrave* c. *Royaume-Uni*, requête n° 202711/92, décision de la Commission du 1er septembre 1993; et *Matthews* c. *Royaume-Uni*, requête n° 28576/95, décision de la Commission du 16 octobre 1996.

[36] «Déclaration conjointe sur les programmes de surveillance et leurs incidences sur la liberté d'expression», publiée par le Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression et le Rapporteur spécial pour la liberté d'expression de la Commission interaméricaine des droits de l'homme, juin 2013 (disponible à l'adresse: www.oas.org/en/iachr/expression/showarticle.asp?artID=927&lID=1), par. 9.

[37] Voir par exemple la Cour européenne des droits de l'homme, *Segersted-Wiber et autres* c. *Suède*, requête n° 62332/00, 6 juin 2006. Voir aussi le document CCPR/C/21/Rev.1/Add.13, par. 15 à 17.

[38] A/HRC/14/46.

[39] Principes fondamentaux et directives concernant le droit à un recours et à réparation des victimes de violations flagrantes du droit international des droits de l'homme et de violations graves du droit international humanitaire (résolution 60/147 de l'Assemblée générale, annexe).

de télécommunications passe du secteur public au secteur privé, on observe une «délégation de la force publique et des responsabilités quasi judiciaires aux intermédiaires Internet sous couvert d'"autorégulation" ou de "coopération"»[40]. La promulgation de prescriptions légales faisant obligation aux entreprises d'adapter leurs réseaux en vue d'éventuelles écoutes téléphoniques est un sujet de réelle préoccupation, du fait en particulier qu'elle créée un cadre favorable aux mesures de surveillance à grande échelle.

43. Un État peut avoir des motifs légitimes d'exiger d'une société de technologies de l'information et des communications qu'elle fournisse des données concernant les utilisateurs; toutefois, lorsqu'une société fournit des données ou des informations sur les utilisateurs à un État en réponse à une demande attentatoire au droit à la vie privée en vertu du droit international, lorsqu'elle fournit des technologies ou du matériel de surveillance de masse aux États sans garanties suffisantes en place ou lorsque l'information est utilisée d'une autre façon en violation des droits de l'homme, cette société risque d'être accusée de complicité ou d'une autre implication dans des atteintes aux droits de l'homme. Les Principes directeurs relatifs aux entreprises et aux droits de l'homme, approuvés par le Conseil des droits de l'homme en 2011, ont 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. Une entreprise a 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.

44. D'importants efforts multipartites ont été déployés pour clarifier l'application des Principes directeurs dans le secteur des technologies de l'information et des communications. Les entreprises qui fournissent des contenus ou des services Internet, ou encore des technologies et du matériel facilitant les communications numériques, par exemple, devraient adopter une déclaration de principe dans laquelle elles s'engagent à respecter les droits de l'homme dans le cadre de toutes leurs activités. Elles devraient aussi avoir en place des politiques de diligence raisonnable appropriées pour identifier, évaluer, prévenir et atténuer toute incidence néfaste. Elles devraient établir si et dans quelles circonstances leurs conditions de service et leurs politiques de collecte et de partage de données sur les utilisateurs risquent d'avoir des incidences négatives sur les droits de l'homme de ces derniers.

45. Lorsque les entreprises sont confrontées à des demandes d'accès aux données émanant d'autorités publiques qui ne sont pas conformes aux normes internationales relatives aux droits de l'homme, il est attendu d'elles qu'elles s'efforcent d'honorer les principes des droits de l'homme dans la plus grande mesure possible et soient capables de démontrer les efforts qu'elles ont engagés à cet effet. Il faudra peut-être pour cela interpréter ces demandes aussi étroitement que possible, demander aux autorités publiques de préciser le champ et les fondements juridiques de la demande, exiger une décision de justice avant de répondre aux demandes de données de ces institutions et échanger en toute transparence avec les utilisateurs sur les risques encourus et la suite donnée aux exigences de l'État. Des exemples encourageants existent de mesures prises par des entreprises à cet égard, à titre individuel et par le biais d'initiatives multipartites.

46. Un élément fondamental de la diligence raisonnable en matière de droits de l'homme telle que définie par les Principes directeurs est la tenue de vraies consultations avec les parties prenantes concernées. Dans le cas des sociétés de technologies de l'information et des communications, il faut aussi veiller à ce que les utilisateurs soient informés de façon réellement transparente de la manière dont leurs données sont recueillies,

[40] Voir European Digital Rights, «The Slide from "Self-Regulation" to Corporate Censorship», Bruxelles, janvier 2011, disponible à l'adresse: www.edri.org/files/EDRI_selfreg_final_20110124.pdf.

stockées, utilisées et éventuellement partagées avec d'autres, afin de pouvoir exprimer leur préoccupations et prendre des décisions en connaissance de cause. Les Principes directeurs précisent que lorsque les entreprises déterminent qu'elles ont eu des incidences négatives sur les droits de l'homme, ou y ont contribué, la responsabilité leur incombe de prévoir directement des mesures de réparation ou de collaborer à leur mise en œuvre suivant des procédures légitimes. Pour que ces mesures de réparation puissent être prises aussitôt que possible, les entreprises devraient instituer des mécanismes de réclamation au niveau opérationnel. Ces mécanismes peuvent être particulièrement importants dans les pays d'exploitation où les droits ne sont pas suffisamment protégés ou dans lesquels il n'existe pas de recours judiciaire ou non judiciaire. Outre l'indemnisation et la restitution, entre autres, on devrait aussi, à titre de réparation, prévoir de divulguer des informations sur les types de données partagées avec les pouvoirs publics, et la façon dont ces opérations ont eu lieu.

V. Conclusions et recommandations

47. **Le droit international des droits de l'homme établit un cadre clair et universel pour 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, de l'interception des communications numériques et de la collecte de données personnelles. Les pratiques suivies par de nombreux États ont toutefois fait apparaître l'absence de législation nationale et/ou de mesures d'application des lois suffisantes, la faiblesse des garanties procédurales et l'inefficacité du contrôle, lesquels ont tous contribué à ce qu'il n'y ait pas d'obligation de rendre des comptes pour les atteintes arbitraires ou illégales au droit à la vie privée.**

48. **Deux observations s'imposent lorsque l'on examine les importantes lacunes existantes quant au respect du droit à la vie privée. Premièrement, des informations concernant des politiques et des pratiques de surveillance sur le territoire national et à l'extérieur continuent de sortir. Des enquêtes sont en cours afin de recueillir des informations sur la surveillance électronique et la collecte et le stockage de données personnelles et d'évaluer leurs incidences sur les droits de l'homme. Des tribunaux à l'échelle nationale et régionale ont entamé l'examen de la légalité des politiques et des mesures de surveillance électronique. Toute étude des politiques et pratiques de surveillance au regard du droit international des droits de l'homme doit nécessairement tenir compte de l'évolution constante de la question. La deuxième observation, qui va de pair avec la première, concerne l'inquiétant manque de transparence dont les pouvoirs publics entourent leur politiques, lois et pratiques en matière de surveillance, qui entrave tout effort visant à vérifier la compatibilité de ces dernières avec le droit international des droits de l'homme et à mettre en jeu les responsabilités.**

49. **Pour régler efficacement les problèmes que soulève le droit à la vie privée dans le contexte des technologies des communications modernes, il faut une mobilisation multipartite continue et concertée. Ce processus devrait instaurer un dialogue entre toutes les parties prenantes intéressées, y compris les États Membres, la société civile, les communautés scientifiques et techniques, les entreprises, les universitaires et les spécialistes des droits de l'homme. Au fur et à mesure de l'évolution des technologies des communications, il sera absolument indispensable que des instances supérieures interviennent pour veiller à ce que ces technologies mettent leurs potentialités au service d'un meilleur exercice des droits de l'homme consacrés par le cadre juridique international.**

50. **Compte tenu des observations qui précèdent, il est manifestement nécessaire, de toute urgence, de veiller à la conformité de toute politique ou pratique de surveillance avec le droit international des droits de l'homme, y compris le droit à la vie privée, par la mise en place de garanties effectives contre les atteintes. Dans l'immédiat, les États devraient revoir leurs propres lois, politiques et pratiques nationales pour assurer leur pleine conformité avec le droit international des droits de l'homme. Dans les cas où des lacunes seraient relevées, les États devraient prendre des mesures pour les combler, y compris par l'adoption de cadres législatifs clairs, précis, accessibles, exhaustifs et non discriminatoires. Des mesures devraient être prises pour faire en sorte que des régimes et des pratiques de contrôle effectifs et indépendants soient en place, en prêtant attention au droit des victimes à disposer de recours utiles.**

51. **La promotion et la protection du droit à la vie privée à l'ère du numérique se heurtent à d'importantes difficultés d'ordre pratique. Il est nécessaire, en s'appuyant sur l'étude initiale qui a été faite de ces questions dans le présent rapport, de continuer à examiner en les approfondissant les points relatifs à la protection effective de la loi, aux garanties procédurales, au contrôle effectif et aux voies de recours. Un examen approfondi de ces questions permettrait de dégager de nouvelles orientations pratiques, fondées sur le droit international des droits de l'homme, sur les principes de la nécessité, de la proportionnalité et de la légitimité pour ce qui touche aux pratiques de surveillance; les mesures de contrôle effectif, indépendant et impartial; et les voies de recours. Un examen plus approfondi aiderait aussi les entreprises à assumer leur responsabilité vis-à-vis du respect des droits de l'homme, au moyen notamment de la diligence raisonnable et de garanties en matière de gestion du risque, et à jouer leur rôle en assurant des recours utiles.**