Nations Unies A/69/397

Assemblée générale

Distr. générale
23 septembre 2014
Français
Original : anglais

Soixante-neuvième session
Point 68 a) de l'ordre du jour
Promotion et protection des droits de l'homme: application des instruments relatifs aux droits de l'homme

Promotion et protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste*

Note du Secrétaire général

Le Secrétaire général a l'honneur de faire tenir à l'Assemblée générale le rapport du Rapporteur spécial sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste, Ben Emmerson, présenté conformément à la résolution 68/178 de l'Assemblée générale et à la résolution 15/15 du Conseil des droits de l'homme.

* Présentation tardive.

14-61490X (F)

Rapport du Rapporteur spécial sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste

Résumé

Il s'agit ici du quatrième rapport annuel présenté à l'Assemblée générale par le Rapporteur spécial sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste, Ben Emmerson.

Les principales activités menées par le Rapporteur spécial entre le 17 décembre 2013 et le 31 juillet 2014 sont énumérées à la section II du rapport. À la section III, le Rapporteur spécial étudie l'utilisation de la surveillance numérique de masse aux fins de la lutte antiterroriste et examine les incidences de cette technologie d'accès global sur le droit au respect de la vie privée consacré par l'article 17 du Pacte international relatif aux droits civils et politiques.

I. Introduction

1. Le présent rapport est soumis à l'Assemblée générale par le Rapporteur spécial sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste, Ben Emmerson, conformément à la résolution 68/178 de l'Assemblée générale et aux résolutions 15/15, 19/19, 22/8 et 25/7 du Conseil des droits de l'homme. Il énumère les activités menées par le Rapporteur spécial entre le 17 décembre 2013 et le 31 juillet 2014. Il étudie ensuite l'utilisation de la surveillance numérique de masse aux fins de la lutte antiterroriste et examine les incidences de cette technologie d'accès global sur le droit au respect de la vie privée consacré par l'article 17 du Pacte international relatif aux droits civils et politiques.

II. Activités relatives au mandat

2. Le 13 février 2014, le Rapporteur spécial a participé en qualité de conférencier à une table ronde intitulée « Débat sur le jugement *Kadi II*: médiateur des Nations Unies v. contrôle judiciaire dans la prise de décisions du Conseil de sécurité concernant des sanctions », à la London School of Economics de Londres.

3. Du 23 au 25 février 2014, le Rapporteur spécial a participé à un séminaire d'experts sur le thème « Le droit à la vie privée à l'ère du numérique », accueilli par les Missions permanentes d'Allemagne, d'Autriche, du Brésil, du Liechtenstein, du Mexique, de la Norvège et de la Suisse à Genève et organisé par l'Académie de droit international humanitaire et de droits humains à Genève.

4. Le 11 mars 2014, le Rapporteur spécial a présenté au Conseil des droits de l'homme, à sa vingt-cinquième session, son rapport sur l'utilisation d'aéronefs télépilotés (ou drones), dans le cadre d'opérations extraterritoriales létales de lutte contre le terrorisme, y compris dans les situations de conflit armé asymétrique, ainsi que sur l'incidence de cette pratique sur les populations civiles (A/HRC/25/59). Il a également eu un dialogue avec le Conseil sur les rapports de ses visites de pays au Burkina Faso (A/HRC/25/59/Add.1) et au Chili (A/HCR/25/59/Add.2).

5. Le 12 mars 2014, le Rapporteur spécial a participé en qualité de membre du groupe d'experts à une manifestation parallèle sur le sujet « Les droits de l'homme et les drones » et il a tenu une conférence de presse à la vingt-cinquième session du Conseil des droits de l'homme.

III. Lutte antiterroriste et surveillance numérique de masse

A. Introduction et aperçu général

6. Au cours de la dernière décennie, la croissance exponentielle des capacités technologiques des États a renforcé les capacités des services de renseignement et des organismes d'application de la loi pour procéder à une surveillance ciblée des personnes et organisations suspectes. L'interception des communications est une source précieuse d'informations permettant aux États de mener des enquêtes, de prévenir et d'engager des poursuites contre des actes de terrorisme et autres graves infractions. La plupart des États ont maintenant la capacité d'intercepter et de contrôler des appels passés sur une ligne téléphonique fixe ou mobile, ce qui permet

de localiser la personne, de suivre ses mouvements par l'analyse du site cellulaire et de lire et enregistrer ses messages. La surveillance ciblée permet également aux services de renseignement et aux organismes d'application de la loi de contrôler l'activité en ligne de personnes spécifiques, d'entrer dans les bases de données et les installations informatiques à distance et de saisir les informations qui y sont stockées. Les États sont de plus en plus nombreux à utiliser des programmes malveillants qui peuvent servir à infiltrer l'ordinateur ou le smartphone d'une personne, à annuler ses paramètres et à contrôler ses activités. Toutes ensemble ces méthodes de surveillance fournissent une mosaïque de données tirées de sources multiples qui peuvent fournir des renseignements utiles sur des personnes ou des organisations particulières.

7. La caractéristique commune de ces techniques de surveillance est qu'elles reposent sur l'existence de soupçons préalables concernant l'individu ou l'organisation visé par des sanctions. Dans ces cas, presque invariablement les États exigent une autorisation préalable (qu'elle soit judiciaire ou exécutive), et dans certains d'entre eux s'y ajoute un examen indépendant à postériori. Par conséquent, dans la plupart des États, il existe au moins une occasion (et parfois plus d'une) d'étudier de manière approfondie les informations qui auraient suscité des soupçons et de procéder à une évaluation de la légalité et de la proportionnalité des mesures de surveillance par rapport aux faits concernant un cas spécifique. Une surveillance ciblée permet d'évaluer objectivement la nécessité et la proportionnalité de la technique envisagée, en pesant le degré d'intrusion proposé par rapport à sa valeur anticipée pour une enquête déterminée.

8. Le rythme dynamique du changement technologique a néanmoins permis à certains États d'obtenir un accès global aux données de communication et à leur contenu sans soupçon préalable. Les autorités compétentes de ces États sont maintenant en mesure d'appliquer des algorithmes « d'exploration de données » automatique pour traquer l'univers potentiellement illimité du trafic des communications. En plaçant des écoutes sur des câbles à fibres optiques par lesquels la plus grande partie des communications numériques est acheminée, les États ont donc été en mesure de réaliser une surveillance de masse du contenu des communications et des métadonnées, donnant aux services de renseignement et aux organismes d'application de la loi la possibilité de contrôler et d'enregistrer non seulement les communications de leurs propres citoyens mais aussi celles de personnes se trouvant dans d'autres États. Cette capacité est généralement renforcée par des lois relatives à la conservation obligatoire des données qui demandent aux fournisseurs de services de télécommunications et d'accès à Internet de garder les données de communications à des fins d'inspection et d'analyse. L'utilisation d'un logiciel de balayage, de critères d'analyse et de termes de recherche déterminés permet aux autorités concernées de filtrer de grandes quantités d'informations stockées afin d'identifier les schémas de communication entre individus et organisations. Des algorithmes d'exploration de données automatique établissent des liens entre les noms, les lieux, les numéros et les adresses de protocole Internet d'identification communs et recherchent les corrélations, les intersections géographiques des données et des schémas de localisation dans des relations sociales et autres en ligne[1].

[1] http://blog.privacystrategy.eu/public/published/Submission_ISC_7.2.2014_-_Caspar Bowden.pdf.

9. Les États ayant des taux de pénétration de l'Internet élevés peuvent ainsi avoir accès au contenu des appels téléphoniques et des courriels d'un nombre effectivement illimité d'utilisateurs et garder un aperçu des activités sur la Toile associées à des sites Web particuliers. Tout ceci est possible sans soupçon préalable concernant une personne ou une organisation spécifique. Les communications de chaque utilisateur d'Internet sont pour ainsi dire potentiellement ouvertes à l'inspection des services de renseignement et des organismes d'application de la loi des États concernés. Ceci équivaut à une immixtion systématique dans le droit au respect du secret des communications et exige une justification obligatoire correspondante.

10. Vu sous l'angle de l'application de la loi, la valeur ajoutée de la technologie de surveillance de masse découle du fait même qu'elle permet de surveiller les communications de personnes et d'organisations n'ayant pas auparavant attiré l'attention des autorités. L'avantage de cette technologie d'accès global pour l'intérêt général semblerait découler précisément du fait qu'elle ne requiert pas de soupçon préalable. Le cercle vicieux de ce raisonnement ne peut être rompu qu'en soumettant la pratique des États dans ce domaine à l'analyse préconisée par l'article 17 du Pacte international relatif aux droits civils et politiques.

11. L'article 17 du Pacte stipule que toute ingérence dans les communications privées doit être prescrite par la loi et constituer un moyen nécessaire et proportionné d'atteindre un objectif légitime des politiques publiques (voir par. 28-31 ci-dessous). La prévention du terrorisme est clairement un objectif légitime à cette fin (voir par. 33 et 34 ci-dessous), mais les activités des services de renseignement et des organismes d'application de la loi dans ce domaine n'en doivent pas moins respecter le Droit international des droits de l'homme[2]. Se borner à affirmer – sans entrer dans les détails – que la technologie de surveillance de masse peut contribuer à l'élimination et à la poursuite des actes de terrorisme ne justifie pas comme il convient son utilisation au regard du Droit des droits de l'homme. Le fait que quelque chose soit techniquement faisable et puisse parfois donner des renseignements utiles ne signifie pas en soi que c'est raisonnable ou légal (en droit international ou en droit interne) (voir A/HRC/27/37, par. 24).

12. Le Droit international des droits de l'homme exige que les États justifient clairement et sur la base de preuves toute immixtion dans le droit à la vie privée, que ce soit à l'échelle individuelle ou de masse. Un axiome fondamental de la proportionnalité est que plus l'immixtion dans les droits de l'homme protégés est grande, plus sa justification doit être incontournable pour répondre aux prescriptions du Pacte. La vérité est incontestablement que l'utilisation de la technologie de surveillance de masse élimine en fait purement et simplement le droit au secret des communications sur l'Internet. En permettant l'accès global à toutes les communications numériques, cette technologie élimine la possibilité de toute analyse individualisée de la proportionnalité. Elle permet une intrusion dans les communications privées sans autorisation préalable indépendante (ou quelle qu'elle soit) sur la base de soupçons dirigés contre une personne ou une organisation particulière. Un examen approfondi ex ante n'est donc possible qu'au niveau le plus élevé des généralités.

[2] Voir la compilation des bonnes pratiques sur les cadres juridique et institutionnel des services de renseignement et leur surveillance, diffusée par l'ancien Rapporteur spécial (A/HRC/14/46, par. 9-50).

13. Du fait que les mesures de surveillance de masse ne peuvent être justifiées par un objectif précis, il appartient aux États concernés de justifier la pratique générale de la recherche d'un accès global aux communications numériques. L'analyse de la proportionnalité passe donc d'un micro niveau (évaluation de la justification pour s'immiscer dans la vie privée d'une personne ou d'une organisation déterminée) à un macro niveau (évaluation de la justification de l'adoption d'un système impliquant une immixtion totale dans les droits individuels et collectifs à la vie privée de tous les usagers d'Internet). Le simple degré d'immixtion dans les droits à la vie privée demande une justification correspondante du même ordre des politiques publiques.

14. Au strict minimum, l'article 17 exige que les États utilisant des technologies de surveillance de masse rendent publiquement compte des avantages tangibles qu'ils en retirent. Sans une telle justification, il est simplement impossible de déterminer la compatibilité de cette nouvelle pratique des États avec les prescriptions du Pacte. Une évaluation de la proportionnalité dans ce contexte implique l'établissement d'un équilibre entre l'intérêt de la protection de la vie privée en ligne pour la société d'une part et, de l'autre, les impératifs d'une lutte efficace contre le terrorisme et de l'application de la loi. Pour déterminer où cet équilibre doit être établi, un débat public éclairé au sein des États et entre eux est indispensable. La communauté internationale doit sans ambages faire face à cette révolution selon notre conception collective du rapport existant entre l'individu et l'État[3]. La nécessité pour les États utilisant cette technologie de faire preuve de transparence quant à la méthodologie suivie et sa justification est une condition préalable de toute évaluation de la légalité de ces mesures[4]. Autrement, il existe un risque que l'immixtion systématique dans la sécurité des communications numériques continue à proliférer sans que les conséquences d'un abandon total du droit à la vie privée en ligne soient sérieusement prises en considération. Si les États utilisant cette technologie conservent le monopole des informations relatives à son impact, une sorte de censure conceptuelle empêchant un débat éclairé prévaudra.

15. Certains prétendent que les utilisateurs d'Internet ne doivent pas en premier lieu s'attendre à la confidentialité des données et doivent partir du principe que leurs communications peuvent être surveillées par des sociétés tout comme par des organismes publics. L'analogie classique que font ceux qui soutiennent ce point de vue est celle de l'envoi d'un courriel non crypté et d'une carte postale. Quels que soient les mérites de cette comparaison, elle ne répond pas aux questions fondamentales de la légalité, de la nécessité et de la proportionnalité. La prescription du Pacte relative à une législation explicite et publiquement accessible régissant l'immixtion de l'État dans les communications a pour objectif même de permettre à chacun de connaître la portée des droits à la vie privée dont ils jouissent

[3] Comme l'a fait remarquer le Privacy and Civil Liberties Oversight Board (Conseil de surveillance de la vie privée et des libertés civiles) des États-Unis: « Permettre au Gouvernement de recueillir systématiquement les enregistrements des appels de toute la nation déplace fondamentalement l'équilibre du pouvoir entre l'État et ses citoyens »; « Rapport sur le programme des enregistrements téléphoniques effectués au titre de la section 215 de la USA PATRIOT Act et sur les opérations du Tribunal de supervision des renseignements étrangers ».

[4] Dans son rapport sur le droit à la vie privée à l'ère du numérique (A/HRC/27/37, par. 48), la Haute-Commissaire aux Droits de l'homme a fait état de « 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 ».

réellement et de prévoir les circonstances dans lesquelles leurs communications peuvent faire l'objet d'une surveillance (voir par. 35-39 ci-dessous). Pourtant, la valeur de cette technologie comme outil de lutte contre le terrorisme et d'application de la loi réside dans le fait que les utilisateurs de l'Internet partent du principe que leurs communications sont confidentielles (autrement il n'y aurait aucune raison de s'y immiscer). Ceci est mis en évidence dans les affirmations des membres des services de renseignement des États-Unis d'Amérique et du Royaume-Uni de Grande-Bretagne et d'Irlande du Nord suite à la divulgation des programmes de surveillance de masse mis en œuvre par ces deux États, dans lesquels les divulgations auraient porté préjudice à la sécurité nationale en attirant l'attention de terroristes éventuels sur le fait que leurs communications étaient sous surveillance.[5]

16. Toute évaluation de la proportionnalité doit aussi pleinement tenir compte du fait que l'Internet représente maintenant le moyen universel de communication pour des millions de personnes dans le monde entier. La révolution de la technologie numérique a radicalement changé la façon dont nous communiquons les uns avec les autres. Les technologies numériques de communication qui utilisent l'Internet (y compris les appareils portatifs et les smartphones) font partie de notre quotidien (voir A/HRC/27/37, par. 1). Quiconque souhaite participer à l'échange d'informations et d'idées dans le monde moderne des communications mondiales est maintenant obligé d'utiliser la technologie numérique transnationale de communication. Le trafic Internet est fréquemment acheminé par des serveurs situés dans des juridictions étrangères. L'idée que les utilisateurs ont volontairement abandonné leur droit à la vie privée est clairement injustifié (ibidem, par. 18). Selon un principe général du Droit international des droits de l'homme, seules les personnes qui s'en désistent de manière expresse et sans équivoque, volontairement et en connaissance de cause, peuvent être considérées comme ayant abandonné un droit protégé. Dans le monde numérique moderne, la simple utilisation de l'Internet comme moyen de communication privée ne saurait certainement pas constituer un désistement en connaissance de cause du droit à la vie privée au titre de l'article 17 du Pacte.

17. L'Internet n'est pas simplement un espace public. Il est composé de nombreuses couches de domaines privés aussi bien que sociaux et publics.[1] (Voir note 1). Ceux qui utilisent en connaissance de cause les plateformes des médias sociaux sur lesquels sont postés des messages publiquement accessibles ne peuvent évidemment pas raisonnablement s'attendre à ce qu'ils aient un caractère privé. L'analogie de la carte postale est tout à fait appropriée pour la diffusion d'informations sur Twitter et Facebook par exemple, ou pour des affichages sur des sites web publics. Mais la lecture d'une carte postale n'est pas une analogie appropriée pour intercepter des messages privés envoyés par courriel, qu'ils soient cryptés ou non.

18. À supposer par conséquent qu'il subsiste un droit légitime au respect du secret des communications numériques et ceci est incontestable (voir la résolution 68/167 de l'Assemblée générale)), l'adoption de la technologie de surveillance de masse a sans nul doute des effets sur la nature même de ce droit (voir par. 51 et 52 ci-dessous). Elle est potentiellement non conforme au principe fondamental selon

[5] Voir http://abcnews.go.com/Blotter/intel-heads-edward-snowden-profound-damage-us-security/story?id=22285388 et www.itv.com/news/2013-10-09/the-damage-of-edward-snowdens-revelations/.

lequel les États devraient adopter les moyens disponibles les moins intrusifs possible lorsqu'ils empiètent sur des droits de l'homme protégés (voir par. 51 ci-dessous), elle exclut toute évaluation de proportionnalité individualisée (voir par. 52 ci-dessous) et elle est entourée d'exigences de discrétion qui rendent extrêmement difficile toute autre forme d'analyse de la proportionnalité (voir par. 51 et 52 ci-dessous). Jusqu'à présent, les États qui se sont lancés dans la surveillance de masse n'ont pas fourni de justification complète et fondée sur des preuves de sa nécessité et pratiquement aucun d'entre eux n'a adopté une législation interne explicite pour en autoriser l'utilisation (voir par. 37 ci-dessous). Vu sous l'angle de l'article 17 du Pacte, ceci se rapproche d'une dérogation pure et simple du droit au secret des communications numériques. Pour toutes ces raisons, la surveillance de masse du contenu et des données de communications numériques remet sérieusement en cause une norme bien établie du Droit international. De l'avis du Rapporteur spécial, l'existence même de programmes de surveillance de masse constitue une immixtion potentiellement disproportionnée dans le droit à la vie privée[6]. En bref, il est incompatible avec les concepts de vie privée existants que les États recueillent constamment et sans discrimination toutes les données de communication ou métadonnées. Il est dans la nature même du droit au secret des communications que les infractions doivent être exceptionnelles et justifiées au cas par cas (voir par. 51 ci-dessous).

19. Il peut y avoir une justification antiterroriste incontournable de la réévaluation fondamentale des droits à la vie privée sur l'Internet qu'exigent ces pratiques. Toutefois, les arguments en faveur d'une abrogation complète du droit à la vie privée sur l'Internet n'ont pas été formulés publiquement par les États concernés ni soumis à un examen minutieux et à un débat. La menace du terrorisme ne peut justifier la surveillance de masse que si les États utilisant cette technologie peuvent démontrer avec précision les avantages antiterroristes tangibles qu'ils en ont tirés. De plus, les mesures justifiées par référence aux obligations qu'ont les États d'assurer une protection contre la menace terroriste ne devraient jamais être utilisées comme un cheval de Troie pour donner des pouvoirs plus étendus de surveillance à des fonctions gouvernementales n'ayant rien à voir avec. Il existe toujours un risque « d'erreur », par lequel des mesures justifiées pour des raisons de lutte antiterroriste sont mises à disposition des autorités publiques à des fins d'intérêt général beaucoup moins importantes (voir par. 55 ci-dessous). Dans ce présent rapport, le Rapporteur spécial s'appuie sur le travail de son prédécesseur (A/HRC/13/37) et de l'ancien Rapporteur spécial sur la promotion et la protection du droit à la liberté d'expression et d'opinion. Il fait valoir que les États utilisant une technologie de surveillance de masse ont la responsabilité d'expliquer rapidement, précisément et publiquement pourquoi cette intrusion totale dans la vie privée collective est justifiée pour prévenir le terrorisme ou tout autre délit grave.

B. Divulgations récentes concernant la nature et la portée des capacités de surveillance numérique des États

20. Le 5 juin 2013, un journal britannique a publié le contenu d'un jugement classifié avec l'autorisation du Tribunal de surveillance des renseignements à

[6] Voir également le point de vue de la Haut-Commissaire aux droits de l'homme, A/HRC/27/37, par. 20 et 25.

l'étranger des États-Unis au titre de la section 215 du Patriot Act. Selon les informations disponibles, le jugement demandait à l'un des plus grands fournisseurs de services de télécommunications des États-Unis de remettre quotidiennement à l'Office national de sécurité toutes les « métadonnées téléphoniques » pendant une période de trois mois et interdisait à la compagnie de divulguer l'existence de cette demande ou du jugement lui-même. Le 6 juin 2013, un journal américain a publié une autre version révélant l'existence d'un programme numérique caché de l'Office national de sécurité appelé PRISM. Ce programme, autorisé selon les informations conformément à la section 702 de la *Foreign Intelligence Surveillance Act* (loi sur les activités de renseignement à l'étranger), aurait permis de recueillir des données de contenu auprès des serveurs centraux des neuf sociétés de technologie principales des États-Unis.

21. Selon les rapports parus dans les deux journaux, le matériel récupéré par le Programme PRISM a été mis à la disposition d'autres services de renseignement, notamment le Siège des communications d'État du Royaume-Uni. Des divulgations ultérieures ont fait état de l'existence d'un autre programme de collecte de données appelé Upstream qui permet, semble-t-il, de capter les communications tant téléphoniques que sur Internet passant par des câbles à fibre optique et des infrastructures appartenant à des fournisseurs de services américains. Une grande partie du trafic mondial d'Internet est acheminé par des serveurs se trouvant physiquement aux États-Unis.

22. Par la suite, les médias ont signalé que la Direction des systèmes de renseignement de l'Office national de sécurité comprend un département des vulnérabilités des applications qui recueille des données à partir de systèmes de communication dans le monde entier. Il paraît que l'Office exploite un mécanisme d'exploitation d'Internet appelé Quantum qui lui permet de réduire l'efficacité des ordinateurs de tiers. D'après les informations disponibles, cette méthodologie consiste à prendre secrètement le contrôle (ou à « s'approprier ») de serveurs situés dans des endroits importants sur le « réseau de base » de l'Internet. En personnifiant des sites web choisis (notamment certains sites courants comme la page de recherche de Google), Quantum est en mesure d'introduire un logiciel de commande à distance non autorisé dans les ordinateurs et les dispositifs Wifi de ceux qui visitent le site clone (qui n'auront bien entendu aucune raison de douter de son authenticité). Les experts considèrent que cette méthodologie peut réduire de façon permanente l'efficacité de l'ordinateur de l'utilisateur, en garantissant qu'il continue à fournir indéfiniment des renseignements à l'Office national de sécurité des États-Unis.

23. Par la suite, les services exécutif et législatif des États-Unis ont pris un certain nombre de mesures en réponse à ces divulgations. Une question qui s'est posée lors de ce processus est la différence de traitement entre les citoyens et les non citoyens américains (même ceux relevant de la compétence territoriale des États-Unis). Les faits essentiels peuvent être résumés comme suit :

a) Le 9 août 2013, le Président Barack Obama a annoncé qu'il avait prié le Privacy and Civil Liberties Oversight Board (Conseil de surveillance de la vie privée et des libertés civiles)[7] d'entreprendre un examen des mesures antiterroristes

[7] Le Conseil est une institution indépendante du Service exécutif habilité à examiner et analyser les opérations antiterroristes et à veiller à ce qu'elles répondent à la nécessité de protéger la vie privée et les libertés civiles; voir www.pclob.gov/.

existantes.[8] Fin août 2013, le Conseil a demandé au Directeur du Service national de renseignement et au Procureur général d'actualiser les procédures de renseignement en matière de collecte, de conservation et de diffusion des informations relatives aux citoyens des États-Unis[9];

b) Le 12 décembre 2013, le Groupe d'étude du Président a publié son rapport intitulé « Liberté et sécurité dans un monde en évolution » dans lequel il a présenté un certain nombre de recommandations de réforme importantes. Le 17 janvier 2014, en réponse à ce rapport, le Président Obama a annoncé une série de projets de changements législatifs et administratifs.[10] Simultanément, l'Administration a publié une nouvelle Directive présidentielle, « PPD-28 » pour renforcer la surveillance des activités d'interception des communications des services de renseignement, tant aux États-Unis qu'en dehors[11];

c) Le 23 janvier 2014, le Privacy and Civil Liberties Oversight Board a publié le premier des deux rapports dans lequel la majorité concluait que le programme de métadonnées téléphoniques était incompatible avec le droit interne du fait que la section 215 de la Patriot Act ne constituait pas une base adéquate pour le justifier[12]. Le 27 mars, le Président Obama a annoncé une série de nouvelles propositions afin de mettre fin au programme existant[13]. Le 22 mai 2014, la Chambre des représentants a adopté la loi des États-Unis sur les libertés, intégrant certaines des propositions du Président;

d) Le 2 juillet 2014, le Privacy and Civil Liberties Oversight Board a publié un second rapport exposant en détail la façon dont fonctionnent dans la pratique les opérations de surveillance au titre de la section 702 de la Foreign Intelligence Surveillance Act (loi sur les activités de renseignement à l'étranger)[14]. Alors que le rapport se préoccupait principalement de la compatibilité de ces programmes avec les prescriptions statutaires et constitutionnelles des États-Unis, le Conseil a reconnu qu'elles posaient également des « questions juridiques et politiques importantes mais difficiles » concernant le traitement des non-citoyens américains[15]. Le Conseil a estimé que l'application du droit à la vie privée à la surveillance de la sécurité nationale effectuée dans un pays et susceptible de toucher les résidents d'un autre pays n'est pas « réglée » entre les États parties au Pacte international relatif aux droits civils et politiques, proposition que semblait prouver le « débat passionnée en cours »[16].

---

[8] Voir www.whitehouse.gov/the-press-office/2013/08/09/remarks-president-press-conference.

[9] Voir www.pclob.gov/newsroom.

[10] Voir www.washingtonpost.com/politics/full-text-of-president-obamas-jan-17-speech-on-nsa reforms/2014/01/17/fa33590a-7f8c-11e3-9556-4a4bf7bcbd84_story.html.

[11] Voir www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence.

[12] « Rapport sur le Programme des enregistrements téléphoniques mené au titre de la section 215 de la USA PATRIOT Act et sur les Opérations du Tribunal de surveillance des activités de renseignement à l'étranger ».

[13] Voir www.whitehouse.gov/the-press-office/2014/03/27/fact-sheet-administration-s-proposal-ending-section-215-bulk-telephony-m.

[14] « Rapport sur le Programme de surveillance effectué conformément à la section 702 de la FISA», voir www.pclob.gov/meetings-and-events/2014meetingsevents/02-july-2014-public-meeting.

[15] Ibid., p. 98.

[16] Ibid., p. 100.

24. Un processus d'examen parallèle a eu lieu au Royaume-Uni. Le 10 juin 2013, en réponse aux allégations que le Siège des communications de l'État avait contourné la loi du Royaume-Uni en utilisant le programme PRISM de l'Office national de sécurité pour avoir accès au contenu des communications qu'il était impossible d'avoir en vertu du droit interne, le Secrétaire d'État aux affaires étrangères a fait une déclaration au Parlement indiquant que toute donnée obtenue des États-Unis impliquant des ressortissants britanniques est « soumise aux contrôles et sauvegardes statutaires appropriés du Royaume-Uni », notamment les dispositions pertinentes de la Loi de 1994 sur les services de renseignements, la Loi de 1998 sur les Droits de l'homme et la loi de 2000 régissant les pouvoirs d'investigation[17].

25. Le 21 juin 2013, les médias ont fait état de l'existence d'un autre programme géré par le Siège des communications d'État (« Tempora »), dans le cadre duquel, selon les informations disponibles, les communications de personnes interceptant des données auraient été placées sur les câbles à fibre optique entre le Royaume-Uni et les États-Unis afin de faciliter l'interception tant de métadonnées que d'informations de contenu. La question de savoir si la législation existante donne au Siège des communications d'État le pouvoir de mener légalement ces opérations et si elles sont conformes au droit à la vie privée tel qu'il est garanti par l'article 8 de la Convention européenne des droits de l'homme a été soulevée au sein du Parlement britannique et en dehors[18]. Des révélations ultérieures ont porté sur le rôle du Joint Threat Intelligence Group du Siège des communications d'État. Cette institution aurait envoyé un virus informatique appelé Réception de l'Ambassadeur à des fins d'action cachée en ligne. Ce virus semblerait pouvoir s'encrypter lui-même et agir comme un « caméléon » imitant les communications d'autres utilisateurs de l'Internet.

26. Suite à des enquêtes préliminaires sur l'accès aux données de communication et de contenu du Siège des communications d'État, le Comité du renseignement et de la sécurité (Comité parlementaire chargé de la surveillance des services de renseignements)[19] a publié une déclaration le 17 juillet 2013. Ayant tenu compte du cadre légal régissant les arrangements relatifs au partage des informations entre le Siège des communications d'État et ses contreparties extérieures, le Comité a conclu qu'aucune loi du Royaume-Uni n'avait été violée et que le Siège des communications d'État s'était conformé à ses obligations statutaires au titre de la Loi de 1994 sur les services de renseignement. Il a néanmoins conclu que d'autres enquêtes s'imposaient pour voir si le cadre statutaire existant régissant l'accès aux communications privées était adapté, étant donné « l'interaction complexe » existant entre la Loi de 1994 sur les services de renseignement, la Loi de 1998 sur les Droits de l'homme et la Loi de 2000 régissant les pouvoirs d'investigation. Le 17 octobre 2013, le Comité du renseignement et de la sécurité a annoncé qu'il allait élargir le champ d'application de son enquête suite aux préoccupations concernant

[17] Voir www.gov.uk/government/speeches/foreign-secretary-statement-to-the-house-of-commons-gchq.

[18] Voir www.theguardian.com/uk-news/2013/oct/14/conservative-peer-spying-gchq-surveillance; and www.publications.parliament.uk/pa/cm201314/cmhansrd/cm131031/halltext/131031h0001.htm.

[19] Voir http://isc.independent.gov.uk/.

les capacités des services de renseignement et l'impact de leurs opérations sur le droit à la vie privée.[20]

27. Le 8 avril 2014, la Cour de justice de l'Union européenne a publié son jugement concernant l'affaire *Digital Rights Ireland* (Droits numériques Irlande), dans lequel elle déclarait que la Directive de l'Union européenne sur la conservation des données était incompatible avec le droit au respect de la vie privée et celui à la protection des données personnelles, les deux étant garantis au titre de la Charte des droits fondamentaux de l'Union européenne.[21] La Directive demandait que les fournisseurs de services de communication conservent les données de trafic de façon à en permettre l'accès aux autorités nationales compétentes dans le but de prévenir, rechercher, détecter et poursuivre des délits graves, notamment le terrorisme. En affirmant que la conservation des données de trafic et leur accès constituaient une « immixtion particulièrement grave » dans ces deux droits, la Cour de Justice de l'Union européenne a estimé que la Directive ne satisfaisait pas au principe de proportionnalité. En réponse à l'arrêt de la Cour, le 10 juillet 2014 le Gouvernement du Royaume-Uni a déposé un projet de Loi sur la conservation des données et les pouvoirs d'investigation. Le Gouvernement a qualifié ce projet (maintenant une loi) de mesure destinée à « préciser » la nature et l'étendue des obligations qui peuvent être imposées aux fournisseurs de services de télécommunication et d'accès à l'Internet basés au Royaume-Uni.[22]

C. Surveillance de masse, lutte contre le terrorisme et droit au respect de la vie privée

1. Droit au respect de la vie privée consacré par l'article 17 du Pacte international relatif aux droits civils et politiques

28. Selon la définition qui en est donnée, le respect de la vie privée présuppose que chacun doit disposer d'une zone de développement personnel autonome, d'interaction et de liberté sans intervention de l'État ni intrusion non sollicitée excessive d'autres personnes qui n'ont pas été sollicitées non plus (voir A/HRC/23/40, par. 22 et A/HRC/13/37, par. 11). L'obligation de respecter la vie privée et la sécurité des communications implique que chacun a le droit de partager des informations et des idées avec les autres sans immixtion de l'État (ou d'un acteur privé), en ayant la certitude que ses communications parviendront à leurs seuls destinataires et ne seront lues que par eux.[23] Le droit au respect de la vie privée englobe aussi le droit de l'individu à savoir qui détient des renseignements à son sujet et l'utilisation qui en est faite.[24]

29. L'article 17 du Pacte international relatif aux droits civils et politiques est la disposition juridiquement contraignante la plus importante à l'échelon international en ce qui concerne le droit au respect de la vie privée. Il stipule 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

[20] Voir http://isc.independent.gov.uk/news-archive/17october2013.

[21] Cour de Justice des Communautés européennes, Jugement dans les affaires jointes C-293/12 et C-594/12, *Digital Rights Ireland and Seitlinger and Others*, Jugement du 8 avril 2014.

[22] Voir www.gov.uk/government/speeches/communications-data-and-interception.

[23] Observation générale n° 16, par. 8 du Comité des droits de l'homme.

[24] Ibidem, par. 10; voir A/HRC/23/40, par. 22.

réputation ». Il précise encore que « Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes». D'autres instruments internationaux des droits de l'homme contiennent des dispositions similaires et, aux niveaux régional et national, les législations tiennent également compte du droit de chacun au respect de sa vie privée et familiale, de son domicile et de sa correspondance.

30. Cependant, le droit à la vie privée n'est pas un droit absolu. À partir du moment où un individu est suspect et fait l'objet d'une enquête formelle de la part des services de renseignement ou des organismes d'application de la loi, il peut faire l'objet d'une surveillance pour des raisons parfaitement légitimes de lutte contre le terrorisme et aux fins d'application des lois (voir A/HRC/13/37, par. 13). Bien que l'article 17 du Pacte ne contienne pas de clause spécifique de limitation décrivant les conditions dans lesquelles une immixtion dans le droit à la vie privée peut être compatible avec le Pacte, il est universellement entendu qu'il autorise la prise de telles mesures à condition a) qu'elles soient autorisées par le droit interne qui doit être accessible, précis et conforme aux prescriptions du Pacte,[25] b) qu'elles poursuivent un but légitime et c) qu'elles répondent à une nécessité et à la notion de proportionnalité.[26]

31. La prise de conscience du fait qu'une grande partie du trafic mondial sur l'Internet est à un moment donné acheminée à travers les États-Unis a poussé un certain nombre d'États à exprimer leurs préoccupations quant à la question de savoir si le programme PRISM violait le droit de leurs citoyens à la vie privée. En décembre 2013, l'Assemblée générale a adopté la résolution 68/167 concernant le droit à la vie privée à l'ère du numérique, coparrainée par 57 États membres et adoptée sans être mise aux voix. Dans cette résolution, l'Assemblée affirme que le droit à la vie privée doit être protégé en ligne et demande à tous les États de 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.

32. Dans la même résolution, l'Assemblée générale chargeait également le Haut-Commissariat des Nations Unies aux droits de l'homme de lui présenter, ainsi qu'au Conseil des droits de l'homme, 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 sur le territoire national et à l'extérieur et de la collecte de données personnelles, y compris à grande échelle. Dans le paragraphe 47 de son rapport publié le 30 juin 2014 (A/HRC/27/37), la Haute-Commissaire a conclu que 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

[25] Observation générale n° 16, par. 3 du Comité des droits de l'homme.

[26] Voir documents A/HRC/27/37, par. 22-25, et les sources qui y sont citées; A/HRC/23/40, par. 28 et 29; A/HRC/13/37, par. 13-17; les Principes de Syracuse concernant les dispositions du Pacte international relatif aux droits civils et politiques qui autorisent des restrictions ou des dérogations, E/CN.4/1985/4, annexe; les observations générales n° 16, 27, 29, 34 et 31 du Comité des droits de l'homme; la Communication n° 903/2999 de 2004 du Comité des droits de l'homme au sujet de l'affaire *Van Hulst v. Pays-Bas*; la Communication n° 1011/2001 de 2004 sur l'affaire *Madafferi v. Australie*; la Communication n° 488/1992, par. 8.3 sur l'affaire *Toonen v. Australie*; la communication n° 1482/2006 de 2008 sur l'affaire *MG v. Allemagne* et le document CCPR/C/USA/CO/4.

surveillance sur le territoire national et à l'extérieur, de l'interception des communications numériques et de la collecte de données personnelles. Elle a fait remarquer, cependant, que les pratiques suivies par de nombreux États ont fait apparaître l'absence d'une législation nationale et/ou de mesures suffisantes d'application des lois, 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. La Haute-Commissaire a souligné que des informations continuaient à paraître sur la nature et la portée des opérations de surveillance numérique mais elle s'est dite préoccupée par « 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 » (ibidem, par. 48). Elle a invité les États à revoir leurs lois et pratiques nationales afin de les mettre en conformité avec les normes internationales en matière de droits de l'homme et, s'il y a lieu, de les amender. Elle a également demandé à la communauté internationale de poursuivre l'étude approfondie de ces questions (ibidem, par. 49 et 51).

2. La lutte contre le terrorisme: un objectif légitime

33. Contrairement à un certain nombre des droits restreints protégés par le Pacte, l'article 17 ne donne pas une liste exhaustive des objectifs légitimes des politiques publiques susceptibles de constituer la base d'une justification de l'immixtion dans le droit à la vie privée. Néanmoins, la prévention, l'élimination et l'étude des actes de terrorisme équivalent clairement à un but légitime aux fins de l'article 17. Le terrorisme peut déstabiliser les communautés, menacer le développement social et économique, fracturer l'intégrité territoriale des États et compromettre la paix et la sécurité internationales. Au titre de l'article 6 du Pacte, les États sont tenus de protéger les citoyens et autres personnes relevant de leur juridiction contre les actes de terrorisme. Un des aspects de cette obligation est le devoir de mettre en place des mécanismes efficaces pour identifier les menaces terroristes potentielles avant qu'elles se concrétisent. Les États s'acquittent de cette obligation en demandant à leurs services de renseignements et à leurs institutions responsables de l'application de la loi de rassembler et d'analyser les informations pertinentes.

34. Il semble que le renforcement des capacités des États en matière de surveillance de tout le trafic sur Internet soit particulièrement important dans le contexte antiterroriste parce que les communications par Internet ont joué un rôle capital dans le financement et la perpétration d'actes terroristes à l'échelon international, que l'Internet a été utilisé à des fins de recrutement pour des organisations terroristes et que l'identification anticipée de ceux qui participent à la planification d'actes de terrorisme ou en sont les instigateurs pourrait autrement être entravée par les limites du renseignement. Le terrorisme étant une activité mondiale, il est indispensable de rechercher ceux qui sont impliqués au-delà des frontières nationales. La prévention et l'élimination du terrorisme sont donc des impératifs d'intérêt général de la plus haute importance et, en principe, elles peuvent constituer la base d'une justification défendable de la surveillance de masse de l'Internet.

3. Surveillance de masse et prescription relative à la qualité du droit

35. L'article 17 du Pacte dispose explicitement que toute personne a droit à la protection de la loi contre toute immixtion ou atteinte illégale ou arbitraire à sa vie

privée. Ceci suppose une prescription relative à la « qualité du droit » qui impose trois conditions: a) cette mesure doit avoir une base dans le droit interne, b) le droit interne lui-même doit être compatible avec l'état de droit et les prescriptions du Pacte et c) les dispositions pertinentes du droit interne doivent être accessibles, claires et précises. Une immixtion autorisée par le droit interne peut néanmoins être « illégale » et/ou « arbitraire » aux fins de l'article 17 si la législation interne pertinente ne répond pas aux critères essentiels d'accessibilité, de spécificité et de prévisibilité,[27] ou si le droit interne ne parvient pas à satisfaire aux normes de la nécessité et de la proportionnalité.[28] En conséquence, le droit interne doit contenir des dispositions garantissant que les pouvoirs de surveillance intrusive sont adaptés à des buts légitimes spécifiques (voir A/HRC/13/37, par. 60 et A/HRC/27/37, par. 28), et offrent des sauvegardes efficaces contre les abus.[29] Par ailleurs, la discrétion exercée par l'exécutif doit être définie avec suffisamment de clarté dans le droit applicable ou par la publication de directives contraignantes.[30]

36. L'accessibilité requiert non seulement que le droit interne soit publié mais aussi qu'il satisfasse à des normes de clarté et de précision suffisantes pour permettre aux personnes concernées de régler leur conduite en ayant connaissance des circonstances dans lesquelles elles pourraient faire l'objet d'une surveillance intrusive. Au paragraphe 8 de son observation générale n° 16 sur le droit à la vie privée, le Comité des droits de l'homme a souligné que la législation autorisant des immixtions dans les communications privées « doit préciser en détail les conditions précises dans lesquelles de telles immixtions peuvent être permises ». Avant l'introduction des programmes de surveillance de masse décrits dans le présent rapport, cette prescription avait toujours été entendue comme une exigence pour la législation nationale d'énoncer clairement les conditions dans lesquelles toute immixtion pouvait être autorisée et les procédures permettant de le faire, les catégories de personnes dont les communications peuvent être interceptées, les limites imposées à la durée de la surveillance et les procédures d'utilisation et de stockage des données recueillies.[29] (Voir note 29). La Cour européenne des droits de l'homme a également souligné la nécessité de règles claires et détaillées sur cette question.[31]

37. Les programmes de surveillance de masse représentent un défi important par rapport aux prescriptions de l'article 17 du Pacte concernant leur légalité. Lorsque des programmes d'accès à de grandes quantités de données sont opérationnels, il n'y a pas de limites en ce qui concerne les catégories de personnes qui peuvent faire l'objet d'une surveillance ni quant à la durée de cette surveillance. Ces conditions ne peuvent donc pas être précisées dans la législation. Les cadres juridiques et administratifs détaillés relatifs à la surveillance de masse restent souvent secrets, et les utilisations qui sont faites des données recueillies sont encore bien peu connues

---

[27] Observation générale n°16, par. 3 du Comité des droits de l'homme.

[28] Ibidem, par. 8.

[29] CCPR/C/USA/CO/4, par. 22; *Malone v. United Kingdom*, Demande n° 8691/79, Jugement du 2 août 1984, par. 67-68 et *Weber et Saravia v. Allemagne*, Demande n° 54934/00, Jugement du 29 juin 2006.

[30] A/HRC/27/37, par. 29 et Principes de Syracuse concernant les dispositions du Pacte international relatif aux droits civils et politiques qui autorisent des restrictions ou des dérogations (voir E/CN.4/1985/4, annexe), par. 16 et 18.

[31] *Weber et Saravia v. Allemagne*, Demande n° 54934/00, Jugement du 29 juin 2006; *Uzun v. Allemagne* (2012) 54 EHRR 121 par. 35.

du public. Jusqu'à présent, très peu d'États ont promulgué une législation de base autorisant explicitement de tels programmes. Par contre, des règles de droit interne obsolètes, conçues pour des formes plus rudimentaires de surveillance, ont été appliquées aux nouvelles technologies numériques sans être modifiées pour tenir compte des capacités considérablement accrues qu'emploient certains États. En fait, on a même laissé entendre que certains États ont « parfois cherché délibérément à appliquer des régimes de protection plus anciens et plus fragiles à des catégories de données toujours plus sensibles ». (voir A/HRC/13/37, par. 57).

38. Le Rapporteur spécial considère qu'il est urgent que les États révisent leurs lois nationales qui régissent les formes modernes de surveillance afin de garantir la conformité de ces pratiques avec le droit international des droits de l'homme. Les règles de droit interne qui régissent l'interception des communications devraient être actualisées afin de tenir compte des méthodes modernes de surveillance numérique qui ont une portée beaucoup plus large et impliquent une pénétration beaucoup plus profonde de la sphère privée que celles qui avaient été envisagées lors de la promulgation d'une bonne partie de la législation interne existante. L'absence de règles juridiques claires et à jour crée un environnement dans lequel il peut y avoir des immixtions arbitraires dans le droit à la vie privée sans sauvegardes correspondantes. Des lois explicites et détaillées sont indispensables pour garantir la légalité et la proportionnalité dans ce contexte. Elles constituent aussi un moyen indispensable pour permettre à chacun de prévoir si, et dans quelles circonstances, ses communications peuvent faire l'objet d'une surveillance.

39. Un processus législatif public donne l'occasion aux gouvernements de justifier des mesures de surveillance de masse auprès du public. Un débat public permet d'apprécier l'équilibre qui se créée entre vie privée et sécurité (ibidem, par. 56). Un processus d'activité législative transparent devrait également déterminer les points vulnérabilités inhérentes aux systèmes de communication numériques, permettant ainsi aux utilisateurs de faire des choix en connaissance de cause. Ce n'est pas seulement un élément essentiel de la prescription de l'article 17 du Pacte concernant la certitude juridique; c'est aussi un moyen utile d'assurer effectivement la participation du public à un débat sur une question d'intérêt général national et international (voir A/HRC/27/37, par. 29 et A/HRC/14/46). De l'avis du Rapporteur spécial, lorsque les droits à la vie privée de la communauté numérique dans son ensemble font systématiquement l'objet d'immixtion, seule une autorisation détaillée et explicite dans la législation de base peut répondre au principe de légalité.

40. En revanche, le recours à des mesures législatives subordonnées (instruments promulgués par l'exécutif en vertu d'une délégation de pouvoirs) a déjà permis d'adopter des cadres juridiques secrets pour la surveillance de masse, enlevant ainsi au parlement, au pouvoir judiciaire et au public la possibilité d'examiner à la loupe l'utilisation de ces nouveaux pouvoirs (voir A/HRC/13/37, par. 54). De telles dispositions ne satisfont pas aux exigences de qualité du droit inscrites dans l'article 17 du Pacte parce qu'elles ne sont pas suffisamment accessibles au public (voir CCPR/C/USA/CO/4). Il peut certes y avoir des raisons bien légitimes d'intérêt général pour garder secrètes des spécifications techniques et opérationnelles mais cela ne justifie nullement qu'elles soient cachées des informations génériques publiques relatives à la nature et à la portée de la pénétration de l'Internet par l'État. Sans ces informations, il est impossible d'évaluer la légalité, la nécessité et la proportionnalité de ces mesures. Les États doivent donc faire preuve de transparence

quant à l'utilisation et la portée des mesures de surveillance de masse des communications (voir A/HRC/23/40, par. 91).

4. Programmes de surveillance de masse extraterritoriaux

41. Certains États ont techniquement la capacité de procéder à une surveillance de masse des communications entre des personnes qui ne résident pas dans leur juridiction et ils ont ainsi mis en place des mesures de surveillance ayant des effets au niveau extraterritorial. Certaines de ces activités sont physiquement menées sur le territoire de l'État intéressé et mettent donc en jeu les principes de la compétence territoriale au titre du Pacte. C'est le cas non seulement lorsque les agents de l'État placent des intercepteurs de données sur des câbles à fibre optique qui traversent leur territoire mais aussi lorsqu'un État exerce une autorité règlementaire sur les fournisseurs de services de télécommunication ou d'accès à Internet qui contrôlent physiquement les données (A/HRC/27/37, par. 34). Dans les deux cas, les mesures de protection 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. Il en va de même lorsque la législation relative à la conservation obligatoire des données impose des obligations aux fournisseurs de services situés sur le territoire d'un État ou relevant de sa juridiction. Même lorsque les États s'introduisent dans des infrastructures situées entièrement en dehors de leur compétence territoriale, les autorités concernées n'en restent pas moins liées par les obligations de l'État découlant du Pacte (ibidem, par. 32-35 et les sources qui y sont citées).

42. Les opérations de surveillance à l'extérieur du territoire posent des problèmes particuliers pour l'application des prescriptions de l'article 17 du Pacte concernant la qualité du droit. La législation interne régissant l'interception des communications externes (internationales) offre souvent une protection moindre que les dispositions comparables qui ne protègent que les communications purement internes.[32] Le fait que certains États (notamment les États-Unis d'Amérique) continuent à autoriser des régimes de protection asymétriques des citoyens et des autres est encore plus inquiétant. Cette différence de traitement touche toutes les communications numériques puisque les messages sont souvent acheminés par des serveurs situés dans d'autres juridictions. Elle a néanmoins des ramifications particulièrement importantes en ce qui concerne la pénétration de l'informatique en nuage[33].

43. Toute forme de traitement différentiel est incompatible avec le principe de non-discrimination de l'article 26 du Pacte, principe inhérent aussi à la notion de

---

[32] Dans son rapport sur la vie privée à l'ère du numérique, la Haute-Commissaire a recensé un certain nombre de ces dispositions: aux États-Unis, la Foreign Intelligence Surveillance Act (loi sur les activités de renseignement à l'étranger), sect. 1881a); au Royaume-Uni, la Regulation of Investigatory Powers Act 2000 (loi régissant les pouvoirs d'investigation) de 2000, sect. 8(4); en Nouvelle-Zélande, la Government Security Bureau Act (loi sur le Bureau chargé de la sécurité nationale) de 2003 sect. 15A; en Australie, la Intelligence Services Act (loi sur les services du renseignement)sect. 9; au Canada, la National Defence Act (loi sur la défense nationale), sect. 273.64(1) (voir A/HRC/27/37, par. 35, note 30).

[33] Direction générale du Parlement européen pour les politiques internes et Casper Bowden, « Les programmes de surveillance des États-Unis et leur impact sur les droits fondamentaux des citoyens de l'UE », 2013.

proportionnalité.[34] Par ailleurs, le recours à des programmes de surveillance de masse pour intercepter les communications de personnes relevant d'autres juridictions pose de sérieux problèmes quant à l'accessibilité et la prévisibilité des lois régissant l'ingérence dans les droits à la vie privée et l'impossibilité pour quiconque de savoir qu'il peut faire l'objet d'une surveillance étrangère ou que ses communications peuvent être interceptées dans des juridictions étrangères. Le Rapporteur spécial considère que les États sont juridiquement tenus d'accorder la même protection à leurs ressortissants et aux non-ressortissants et aux personnes se trouvant dans leur juridiction et en dehors.

5. Coopération internationale entre services de renseignement

44. Des préoccupations du même genre se font jour quant aux ententes relatives au partage de renseignements à l'échelle internationale. L'absence de lois règlementant les accords de partage d'informations entre les États a laissé aux services de renseignement la possibilité de conclure des accords bilatéraux et multilatéraux concernant des informations classifiées qui vont au-delà de la supervision exercée par toute autorité indépendante (voir A/HRC/13/37). Des informations concernant les communications de quiconque peuvent être partagées avec des services de renseignements étrangers sans bénéficier de la protection d'un cadre juridique publiquement accessible quelconque et avec peu ou pas de sauvegardes appropriées. Suite à un large processus de consultation, la Haute-Commissaire aux droits de l'homme a récemment trouvé des informations crédibles selon lesquelles 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 (voir A/HRC/27/37, par. 30). De telles pratiques n'assurent pas la prévisibilité du fonctionnement du régime de surveillance aux personnes qui y sont soumises et sont par conséquent incompatibles avec l'article 17 du Pacte.

6. Sauvegardes et supervision

45. L'obligation d'accompagner les systèmes de surveillance de sauvegardes procédurales appropriées pour assurer la protection contre les abus est une des mesures de protection essentielles accordées par l'article 17. (Voir note 29). Ces sauvegardes peuvent revêtir différentes formes mais elles comprennent généralement une autorisation préalable indépendante et/ou un examen ultérieur indépendant. Les meilleures pratiques exigent la participation de l'exécutif, du parlement et du service judiciaire ainsi qu'un contrôle civil indépendant (voir A/HRC/27/37). L'absence de sauvegardes appropriées 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 (Ibidem).

46. Lorsque des programmes de surveillance ciblés sont exécutés, beaucoup d'États prévoient une autorisation judiciaire préalable. La participation d'un service judiciaire répondant aux normes internationales est une garantie importante, bien

[34] Le Comité des droits de l'homme a également 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 », CCPR/C/USA/CO/4, par. 22 a).

qu'il soit prouvé que dans certaines juridictions le niveau et l'efficacité de cet examen approfondi aient été limités par la reconnaissance de la compétence de l'exécutif (ibidem, par. 38). Dans d'autres États comme le Royaume-Uni, des mandats d'interception visant des sujets particuliers sont délivrés par des agents de l'État sans autorité judiciaire préalable. Ceci serait, paraît-il, justifié du fait que ces agents sont démocratiquement responsables devant leurs électeurs. L'emploi de ces pouvoirs par l'Exécutif est alors soumis à l'examen d'un Commissaire indépendant à l'interception des communications, et toute personne peut également déposer plainte auprès d'un organe judiciaire, le Tribunal investi de pouvoirs d'enquête, qui a qualité pour examiner des informations classifiées à huis clos.

47. Dans le contexte de la surveillance ciblée, quel que soit la méthode d'autorisation préalable adoptée (par le judiciaire ou l'exécutif), il existe au moins une possibilité d'examen ex ante de la nécessité et de la proportionnalité d'une mesure de surveillance intrusive par rapport aux circonstances particulières du cas et à la personne ou l'organisation dont les communications doivent être interceptées. Aucune de ces possibilités n'existe dans le contexte des systèmes de surveillance de masse puisqu'ils ne sont pas fondés sur le soupçon individuel. L'examen ex ante se limite ainsi à autoriser l'application du système dans son ensemble plutôt qu'à une personne déterminée. Le Rapporteur spécial estime que les États qui ont recours aux technologies de surveillance de masse doivent mettre en place des organes de contrôle tout à fait indépendants, disposant de ressources suffisantes et chargés de procéder à l'examen préalable de l'emploi de techniques de surveillance intrusive par rapport aux exigences de l'article 17 du Pacte (A/HRC/13/37, par. 62) concernant les critères de légalité, de nécessité et de proportionnalité .

48. L'examen a posteriori des mesures de surveillance intrusive est l'autre aspect procédural de l'article 17. Certains États prévoient un examinateur indépendant chargé de surveiller le fonctionnement de la législation en matière de surveillance en analysant la manière et la portée de son utilisation et, partant, sa justification. Ces examens devraient toujours comprendre une analyse de la compatibilité de la pratique de l'État avec les prescriptions du Pacte.

49. Outre ce type d'examen général, les États ont l'obligation spécifique de prescrire un recours aux personnes dont les droits découlant du Pacte ont dans une certaine mesure été violés. Le paragraphe 3 b) de l'article 2 du Pacte exige que les États parties garantissent 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. Afin que ce droit soit effectivement respecté, le droit interne doit prévoir un mécanisme indépendant capable de réaliser un examen approfondi et impartial, ayant accès à toute la documentation pertinente et donnant des garanties d'application régulière de la loi, qui soit habilité à prendre une décision exécutoire (y compris, s'il y a lieu, d'ordonner la cessation de la surveillance ou la destruction du produit) (voir A/HRC/14/46 et A/HRC/27/37, par. 39).

50. Pour invoquer le droit à un recours effectif, il faut généralement que la personne établisse qu'elle a été victime d'une violation. Dans le contexte de mesures de surveillance secrète, il peut être difficile, voire impossible, de satisfaire à cette exigence. Très peu d'États ont adopté des dispositions exigeant la notification a posteriori de la surveillance au suspect. La Cour européenne des droits de l'homme a, en conséquence, assoupli l'exigence pour les personnes concernées

de prouver qu'elles ont été secrètement surveillées. Une distinction a été faite entre les plaintes portant sur l'existence d'un régime qui ne répondrait plus aux exigences de la Convention européenne des droits de l'homme et celles concernant des cas spécifiques d'activité illégale de l'État. Dans le premier cas, la Cour a été préparée à examiner les dispositions mises en cause de prime abord,[35] tandis que dans le deuxième, elle a généralement demandé aux plaignants de donner une « preuve raisonnable » qu'ils ont fait l'objet d'une surveillance illicite.[36] Dans le cadre des régimes de surveillance de masse, le Rapporteur spécial considère que tout utilisateur d'Internet devrait avoir le droit de contester la légalité, la nécessité et la proportionnalité des mesures en cause.

7. Nécessité et proportionnalité des programmes de surveillance de masse

51. Il appartient aux États de démontrer que toute immixtion dans le droit à la vie privée au titre de l'article 17 du Pacte est un moyen nécessaire pour atteindre un but légitime. Pour ce faire, il faut qu'il existe un lien rationnel entre les moyens employés et le but poursuivi. Il faut aussi que la mesure choisie « constitue le moyen le moins perturbateur parmi ceux qui pourraient permettre d'obtenir le résultat recherché » (voir CCPR/C/21/Rev.1/Add.9 et A/HRC/13/37, par. 60). Le principe connexe de proportionnalité implique l'établissement d'un équilibre entre la portée de l'intrusion dans les droits à la vie privée sur l'Internet et l'avantage spécifique pour les enquêtes entreprises par les pouvoirs publics dans l'intérêt général. Il y a cependant des limites à la mesure dans laquelle une ingérence est permise dans un droit couvert par le Pacte. Comme l'a souligné le Comité des droits de l'homme, « 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 ».[37] Dans le contexte de la surveillance cachée, le Comité a donc souligné que toute décision visant à autoriser une immixtion dans les communications doit être prise par l'autorité désignée par la loi « au cas par cas ».[38] La proportionnalité de toute immixtion dans le droit à la vie privée devrait donc être jugée en fonction des conditions particulières de chaque cas.[39]

52. Aucun de ces principes ne s'associe aisément à l'utilisation des technologies de surveillance de masse par les États. La capacité technique de réaliser de vastes programmes de collecte et d'analyse de données offre indéniablement un moyen de plus pour lutter contre le terrorisme et mener des enquêtes sur l'application de la loi. Mais une évaluation de la proportionnalité de ces programmes doit également prendre en considération les dommages collatéraux causés aux droits collectifs à la vie privée. Les programmes de collecte de grandes quantités de données semblent porter atteinte à la prescription selon laquelle les services de renseignement doivent choisir la mesure la moins intrusive possible pour les droits de l'homme (à moins que les États concernés ne soient à même de démontrer que rien d'autre qu'un accès global à toutes les communications sur Internet ne peut suffire pour assurer une protection contre les menaces terroristes et autres délits graves). Puisqu'il n'est pas

---

[35] *Klass v. Allemagne* (1979-80) 2 EHRR 214.

[36] *Halford v. Royaume-Uni* (1997) 24 EHRR 523.

[37] Observations générales n° 27 et 31 du Comité des droits de l'homme.

[38] Observation générale n° 16, par. 8 du Comité des droits de l'homme.

[39] Observation générale n° 16, par. 4 du Comité des droits de l'homme, *Van Hulst v. Pays-Bas*, Communication n° 903/1999, 2004, par. 7.3; *Toonen v. Australie*, Communication n° 488/1992, par. 8.3.

possible d'entreprendre une évaluation personnalisée de la proportionnalité avant de recourir à de telles mesures, ces programmes semblent aussi mettre en cause l'essence même du droit à la vie privée. Ils excluent purement et simplement l'analyse « au cas par cas » jugée essentielle par le Comité des droits de l'homme et ils peuvent donc être jugés arbitraires, même s'ils servent un objectif légitime et ont été adoptés sur la base d'un régime juridique accessible (voir A/HRC/27/37, par. 25). En conséquence, le Rapporteur spécial arrive à la conclusion que de tels programmes ne peuvent être compatibles avec l'article 17 du Pacte que si les États concernés sont en mesure de justifier la proportionnalité de l'immixtion systématique dans les droits à la vie privée sur l'Internet d'un nombre potentiellement illimité de personnes innocentes n'importe où dans le monde.[40]

8. Législation relative à la conservation obligatoire et à l'exploitation automatique des données de communications détenues par les fournisseurs de services de télécommunication et les fournisseurs d'accès à l'Internet

53. Les programmes de surveillance de masse ne se limitent pas à l'interception du contenu des communications. Les communications numériques produisent de grandes quantités de données transactionnelles. Ces données de communications (ou métadonnées) comprennent des informations personnelles sur des personnes, l'endroit où elles se trouvent et leurs activités en ligne. Beaucoup d'États ont adopté une législation obligeant les fournisseurs de services de télécommunications et d'accès à l'Internet à recueillir et conserver les données de communications afin de les mettre à disposition en vue de leur analyse ultérieure. Ces lois requièrent généralement que les prestataires de services fournissent aux autorités publiques des allocations de protocole Internet, permettant d'identifier l'utilisateur d'une adresse de protocole Internet déterminée à tout moment. La saisie des données de communications est devenue une technique de surveillance de plus en plus utile pour les États. Les données de communications sont facilement stockées et recherchées et elles peuvent être utilisées pour la compilation de profils de personnes tout aussi sensibles au respect de la vie privée que le contenu des communications (voir A/HRC/27/37, par. 19). En combinant et en regroupant des informations tirées de données de communications, il est possible d'identifier l'endroit où se trouve une personne, ses associations et ses activités (voir A/HRC/23/40, par. 15). En l'absence de sauvegardes spéciales, il n'y a pratiquement aucun des aspects secrets de la vie privée d'une personne qui puisse résister à une analyse approfondie de métadonnées.[1] (Voir note 1). L'exploitation automatique des données a donc un effet particulièrement destructeur sur la vie privée.

54. Dans beaucoup de pays, un large éventail d'organismes publics ont accès aux données de communications, à des fins diverses, souvent sans autorisation judiciaire ni contrôle indépendant valable. Au Royaume-Uni par exemple plus de 200 institutions sont autorisées à rechercher des données de communications au titre de la loi régissant les pouvoirs d'investigation (Regulation of Investigatory Powers

[40] Voir A/HRC/27/37, par. 25, où la Haute- Commissaire aux droits de l'homme faisait remarquer: « 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 ».

Act) de 2000[41] et, rien qu'en 2013, les pouvoirs publics ont présenté 514 608 demandes de données de communications.[42] Les tribunaux reconnaissent depuis un certain temps que la diffusion de métadonnées à une instance publique constitue une immixtion dans le droit à la vie privée et la Cour de justice de l'Union européenne a récemment statué que la conservation de métadonnées relatives à la vie privée et aux communications d'une personnes constitue, en soi, une immixtion dans ce droit,[43] (l'octroi de l'accès à des métadonnées conservées à des fins d'analyse constituant une autre immixtion distincte).[44] En parvenant à cette conclusion, la Cour de justice de l'Union européenne a souligné que 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 ».[45]

55. Si on applique l'approche adoptée par la Cour de justice de l'Union européenne, il s'ensuit que la collecte et la conservation de données de communications constitue une immixtion dans le droit à la vie privée, qu'un organisme public s'en serve ou les analyse ultérieurement ou non. Ni la saisie de données de communications en vertu d'une législation concernant leur conservation obligatoire ni leur divulgation ultérieure aux autorités gouvernementales (et leur analyse par elles) n'exige qu'il y ait préalablement des soupçons à l'égard d'une personne ou d'une organisation quelconque. Le Rapporteur spécial fait donc siennes les réserves émises par la Haute-Commissaire quant à la nécessité et la proportionnalité de lois relatives à la conservation obligatoire des données (voir A/HRC/27/37, par. 26).

9. Spécification de l'objectif

56. Beaucoup d'États n'ont pas de dispositions de « spécification de l'objectif » empêchant l'utilisation des informations recueillies dans un but déterminé à d'autres fins gouvernementales n'ayant rien à voir avec. Il en résulte que des données officiellement collectées à des fins de sécurité nationale peuvent être partagées entre les services de renseignement, les organismes d'application de la loi et autres organismes publics, notamment les autorités fiscales, les conseils locaux et les autorités responsables de la délivrance de permis.[46] Les institutions nationales responsables de la sécurité et de l'application de la loi sont généralement exclues des dispositions de la législation relative à la protection des données qui limite le partage de données personnelles. De ce fait, il peut s'avérer difficile pour des personnes de prévoir quand et par quelle institution publique elles pourraient être soumises à une surveillance. Cette « erreur d'objectif » risque d'être en contradiction avec l'article 17 du Pacte, non seulement parce que les lois pertinentes

---

[41] La liste des institutions autorisées à rechercher des données de communications comprend les autorités fiscales et les institutions des pouvoirs locaux et elle peut être étendue par législation déléguée (décret-loi).

[42] Voir www.intelligencecommissioners.com/.

[43] Cour de justice de l'Union européenne, Jugement prononcé dans les affaires jointes C-293/12 et C-594/12, *Digital Rights Ireland and Seitlinger and Others* (*Les droits numérique, Irlande et Seitlinger et autres)*, Jugement du 8 avril 2014, par. 34.

[44] Ibidem, par. 35.

[45] Ibidem, par. 26, 27 et 37.

[46] Pour une analyse de la manière dont une telle erreur d'objectif s'est glissée au Royaume-Uni, voir www.whatdotheyknow.com/request/127491/response/315758/attach/html/2/Summay%20of%20Counsels%20advice.pdf.html.

ne sont pas prévisibles mais aussi parce que des mesures de surveillance nécessaires et proportionnées pour un objectif légitime peuvent très bien ne pas l'être pour un autre objectif (ibidem, par. 27). Le Rapporteur spécial appuie donc la recommandation de son prédécesseur que les États doivent avoir l'obligation d'indiquer le fondement juridique autorisant la réutilisation d'informations personnelles, conformément aux principes des droits de l'homme (voir A/HRC/13/37, par. 50 et 66). Ceci revêt une importance particulière lorsque les informations sont partagées d'un pays à l'autre ou entre États.

10. Le secteur privé

57. Les États s'appuient de plus en plus sur le secteur privé pour simplifier la surveillance numérique. Ceci ne se limite pas à la promulgation de lois relatives à la conservation obligatoire de données. Des sociétés ont également été directement complices de l'exploitation de la technologie d'accès global en concevant des infrastructures de communications qui facilitent la surveillance de masse. Les fournisseurs de services de télécommunications et d'accès à Internet ont été invités à intégrer les vulnérabilités dans leurs technologies afin de garantir que ces dispositifs d'écoute sont prêts à être utilisés. La Haute-Commissaire aux droits de l'homme a caractérisé ces pratiques de « délégation de la force publique et des responsabilités quasi judiciaires aux intermédiaires Internet sous couvert d'autorégulation ou de coopération » (voir A/HRC/27/37, par. 42). Le Rapporteur spécial souscrit à cette évaluation. Afin de garantir qu'ils ne se rendent pas complices de violations des droits de l'homme, les fournisseurs de services devraient veiller à ce que leurs opérations soient conformes aux Principes directeurs relatifs aux entreprises et aux droits de l'homme, adoptés par le Conseil des droits de l'homme en 2011 (ibidem, par. 43-46).

IV. Conclusions et recommandations

58. **Les obligations qu'ont les États au titre de l'article 17 du Pacte international relatif aux droits civils et politiques sont notamment celles du respect de la vie privée et de la sécurité des communications numériques. Ceci signifie en principe que chacun a le droit de partager des informations et des idées avec d'autres sans immixtion de l'État, en ayant la garantie que ses communications parviendront à leurs seuls destinataires et ne seront lues que par eux. Toutes mesures portant atteinte à ce droit doivent être autorisées par la législation interne, accessibles, précises et conformes aux prescriptions du Pacte. Elles doivent également poursuivre un objectif légitime et satisfaire aux critères de nécessité et de proportionnalité.**

59. La **prévention et l'élimination du terrorisme sont des impératifs d'intérêt général de la plus haute importance et peuvent en principe constituer la base d'une justification défendable de la surveillance de masse de l'Internet. Cependant, la portée technique des programmes actuellement mis en œuvre est si étendue qu'ils ne peuvent être compatibles avec l'article 17 du Pacte que si les États concernés sont en mesure de justifier la proportionnalité de leur immixtion systématique dans les droits à la vie privée sur Internet d'un nombre pratiquement illimité de personnes innocentes se trouvant n'importe où dans le monde. La technologie d'accès global porte systématiquement atteinte à la vie privée en ligne et à l'essence même du droit garanti par l'article 17. En**

l'absence d'une dérogation formelle aux obligations des États au titre du Pacte, ces programmes mettent directement et constamment en cause une norme bien établie du droit international.

60. L**e Rapporteur spécial partage l'avis de la Haute-Commissaire aux droits de l'homme quant à la nécessité pour les États qui utilisent cette technologie de procéder d'urgence à la révision et à l'actualisation de leur législation nationale afin de la mettre en conformité avec le droit international des droits de l'homme. Ceci est non seulement une prescription de l'article 17 mais encore une occasion importante de tenir un débat éclairé susceptible de sensibiliser l'opinion publique et de permettre à chacun de faire ses choix en connaissance de cause. Lorsque les droits à la vie privée de toute la communauté numérique sont en jeu, seule une législation de base détaillée et explicite serait appropriée. Des limites appropriées devraient être imposées à l'utilisation qui peut être faite des données saisies, en demandant aux pouvoirs publics compétents de justifier juridiquement la réutilisation des informations de caractère personnel.**

61. **Les États devraient mettre en place des organismes de contrôle forts et indépendants, disposant de ressources suffisantes et habilités à effectuer des examens ex ante, pour étudier les demandes d'autorisation non seulement par rapport aux prescriptions du droit interne mais aussi en fonction des critères de nécessité et de proportionnalité du Pacte. De plus, chacun devrait avoir le droit de rechercher une réparation effective pour toute violation en ligne alléguée de ses droits à la vie privée. Il faut pour ce faire un moyen permettant aux personnes touchées de déposer plainte auprès d'une instance indépendante capable de procéder à un examen approfondi et impartial, ayant accès à toute la documentation pertinente et donnant des garanties de procédure régulière. Les mécanismes redditionnels peuvent prendre différentes formes mais ils doivent être habilités à rendre un jugement contraignant. Les États ne sauraient imposer des prescriptions permanentes réduisant à néant le droit à une réparation effective.**

62. **Comme la Haute-Commissaire aux droits de l'homme, le Rapporteur spécial estime que lorsque les États s'introduisent dans des infrastructures situées en dehors de leur juridiction territoriale, ils restent liés par leurs obligations découlant du Pacte. Par ailleurs, l'article 26 du Pacte interdit toute discrimination fondée, notamment, sur la nationalité et la citoyenneté. Le Rapporteur spécial considère donc que les États sont juridiquement tenus d'accorder la même protection de leur vie privée à leurs ressortissants et aux non ressortissants ainsi qu'à ceux relevant ou non de leur juridiction. Les régimes asymétriques de protection de la vie privée sont clairement en contradiction avec les prescriptions du Pacte.**

63. **Le Rapporteur spécial demande instamment à tous les États qui exploitent actuellement des technologies numériques de surveillance de masse de fournir des justificatifs publics détaillés et fondés sur des preuves de l'immixtion systématique dans les droits à la vie privée de la communauté numérique par rapport aux prescriptions de l'article 17 du Pacte. Les États doivent faire preuve de transparence quant à la nature et la portée de leurs mesures de pénétration de l'Internet, la méthodologie appliquée et sa justification; ils doivent aussi rendre compte publiquement et de manière détaillée des avantages tangibles qu'ils en tirent.**

64. **Le Rapporteur spécial partage l'avis de son prédécesseur (voir A/HRC/13/37, par. 19) et celui de l'ancien Rapporteur spécial sur la promotion et la protection du droit à la liberté d'expression et d'opinion (voir A/HRC/23/40, par. 98) que le Comité des droits de l'homme devrait élaborer et adopter une nouvelle observation générale sur le droit à la vie privée en ligne, reflétant l'évolution de la situation en matière de surveillance des communications numériques intervenue depuis l'adoption de l'observation générale n° 16 en 1988.**