



Assemblée générale

Distr. générale
25 octobre 2018
Français
Original : anglais

Conseil des droits de l'homme

Trente-septième session

26 février-23 mars 2018

Point 3 de l'ordre du jour

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

Rapport du Rapporteur spécial sur le droit à la vie privée*, **

Note du Secrétariat

Dans son rapport, établi en application de la résolution 28/16 du Conseil des droits de l'homme, le Rapporteur spécial sur le droit à la vie privée rend compte des travaux qu'il a entrepris au cours des trois premières années de son mandat, en particulier ses travaux sur la surveillance et la confidentialité, et examine le rôle et les mandats des titulaires de mandat au titre de procédures spéciales.

* Le présent document est soumis tardivement pour que l'information la plus récente puisse y figurer.
** L'annexe est reproduite telle qu'elle a été reçue, dans la langue de l'original seulement.



Rapport du Rapporteur spécial sur le droit à la vie privée

Table des matières

| | <i>Page</i> |
|--|-------------|
| I. Introduction | 3 |
| II. Mandat du Rapporteur spécial | 4 |
| A. Activités du Rapporteur spécial (2015-2017) | 4 |
| B. Travaux du Rapporteur spécial dans le domaine prioritaire de la sécurité, la surveillance et la vie privée | 19 |
| C. Capacité du Rapporteur spécial de soumettre des communications individuelles | 23 |
| III. Conclusions | 23 |
| IV. Recommandations au Conseil des droits de l'homme | 24 |
| V. Documents complémentaires | 25 |
| Annexes | |
| Paper presented at Expert workshop on the right to privacy in the digital age | 26 |

I. Introduction

1. Le mandat du Rapporteur spécial sur le droit à la vie privée a pris effet le 1^{er} août 2015. Conformément à la résolution 28/16 du Conseil des droits de l'homme, le Rapporteur spécial fait rapport chaque année au Conseil et à l'Assemblée générale¹.
2. Le présent rapport est le troisième rapport du Rapporteur spécial au Conseil et, par conséquent, le dernier de son premier mandat. Il est donc l'occasion de faire le point sur les trois années écoulées, de présenter dans les grandes lignes les activités menées et les résultats obtenus, de tirer des enseignements de l'expérience et d'examiner le mandat actuel et futur du Rapporteur spécial.
3. Dans cette perspective, le présent rapport se compose de quatre parties. Après l'introduction sont présentés, dans la deuxième partie du rapport, les activités que le Rapporteur spécial a menées, ses réalisations et les travaux qu'il envisage d'entreprendre dans chacun des huit domaines de son mandat. Dans la troisième partie du rapport, le Rapporteur spécial expose le fruit de ses travaux sur l'une des questions prioritaires de son mandat, à savoir la protection de la vie privée et la surveillance exercée par les États et d'autres formes de surveillance. Il décrit un projet d'instrument juridique international sur la surveillance, ainsi qu'une série de recommandations à examiner. Dans la quatrième et dernière partie du rapport, il est question des termes du mandat ainsi que des éclaircissements et du renforcement que celui-ci nécessite.
4. Depuis la création du mandat, outre le fait que le droit à la vie privée est consacré et protégé aux niveaux international² et régional³, ainsi que dans d'autres instruments relatifs aux droits de l'homme⁴, l'importance de la vie privée a été réaffirmée par le Conseil, notamment dans sa résolution 34/7. Dans cette résolution, le Conseil reconnaît que le droit à la vie privée peut permettre l'exercice d'autres droits, contribuer au libre développement de la personnalité et de l'identité de chacun et faciliter la participation individuelle à la vie politique, économique, sociale et culturelle, et il note avec préoccupation que les violations du droit à la vie privée et les atteintes à ce droit peuvent avoir des incidences sur la réalisation d'autres droits de l'homme, notamment le droit à la liberté d'expression et le droit de ne pas être inquiété pour ses opinions, ainsi que le droit à la liberté de réunion et d'association pacifiques. Cela va dans le sens de l'approche adoptée par le Rapporteur spécial sur la question de la personnalité dans son rapport de 2016 au Conseil (A/HRC/31/64).

¹ Voir www.ohchr.org/EN/Issues/Privacy/SR/Pages/AnnualReports.aspx.

² Voir Déclaration universelle des droits de l'homme, art. 12 ; Pacte international relatif aux droits civils et politiques, art. 17 ; Convention relative aux droits de l'enfant, art. 16 ; et Convention internationale sur la protection des droits de tous les travailleurs migrants et des membres de leur famille, art. 14. Voir aussi www.ohchr.org/EN/Issues/Privacy/SR/Pages/Internationalstandards.aspx.

³ Voir Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, art. 8 ; et Convention américaine relative aux droits de l'homme, art. 11. Voir aussi www.ohchr.org/EN/Issues/Privacy/SR/Pages/Internationalstandards.aspx.

⁴ Voir, par exemple, Déclaration du Caire sur les droits de l'homme en Islam, art. 18 ; et Charte arabe des droits de l'homme, art. 16 et 21 ; Déclaration de principes sur la liberté d'expression en Afrique de la Commission africaine des droits de l'homme et des peuples ; Charte africaine des droits et du bien-être de l'enfant, art. 10 ; Déclaration des droits de l'homme de l'Association des nations de l'Asie du Sud-Est, art. 21 ; Cadre sur la vie privée de l'Association de coopération économique Asie-Pacifique ; Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du Conseil de l'Europe ; Protocole additionnel à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, concernant les autorités de contrôle et les flux transfrontières de données ; Conseil de l'Europe, Comité des ministres, Recommandation n° R (99) 5 concernant la protection de la vie privée sur l'Internet ; et Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

5. Dans ses travaux, le Rapporteur spécial est guidé non seulement par le cadre juridique international relatif au droit à la vie privée, mais aussi par les résolutions sur le sujet adoptées régulièrement par le Conseil, y compris celle qui est mentionnée ci-dessus.

II. Mandat du Rapporteur spécial

6. Les activités que mène le Rapporteur spécial relèvent en général de plusieurs domaines d'action de son mandat ; il est donc rendu compte de ces activités sous différentes rubriques correspondantes chacune à un domaine du mandat. Le mandat est disponible en ligne (voir partie V, appendice 1).

A. Activités du Rapporteur spécial (2015-2017)

1. Collecte d'informations pertinentes et sujets d'étude

7. Il est dit au premier paragraphe du mandat que le Rapporteur spécial recueillera les informations voulues, étudiera des questions en rapport avec le droit à la vie privée et fera des recommandations afin de garantir la promotion et la protection de ce droit, notamment eu égard aux défis que posent les nouvelles technologies.

8. Pour poursuivre ce premier objectif, le Rapporteur spécial a défini cinq lignes d'action thématiques. Il s'est appuyé, entre autres moyens, pour étudier les questions pertinentes, sur des visites officielles de pays, des consultations, des contacts avec les organisations non gouvernementales (ONG), des débats publics sur le respect de la vie privée, des conférences internationales et des manifestations promotionnelles, comme la semaine annuelle de sensibilisation au respect de la vie privée organisée par les autorités de protection de la vie privée pour la région Asie-Pacifique, et il a examiné les questions portées à son attention, ainsi que des lettres d'allégations.

Lignes d'action thématiques

9. Le Rapporteur spécial a exposé son plan de travail en 2016 dans ses rapports au Conseil et à l'Assemblée générale. Il a invité toutes les parties prenantes à contribuer aux rapports thématiques et à répondre aux appels à consultations consacrés aux cinq lignes d'action thématiques.

10. Les cinq lignes d'action thématiques sont les suivantes : une meilleure compréhension de la notion de vie privée ; la sécurité et la surveillance ; les mégadonnées et les données ouvertes ; les données de santé ; et l'utilisation de données à caractère personnel par les entreprises. Les lignes d'action thématiques traitent des risques d'atteinte à la vie privée à l'ère numérique ; elles sont interdépendantes et ordonnées de façon à ce que chacune des équipes spéciales puisse faire fond sur les travaux des autres équipes. Par exemple, l'Équipe spéciale sur les mégadonnées et les données ouvertes prépare le travail pour les lignes d'action thématiques sur les données de santé et sur l'utilisation de données à caractère personnel par les entreprises. Chaque équipe spéciale est coordonnée par un président qui, sur la base du volontariat, aide le Rapporteur spécial en compilant des recherches et des informations, en recensant les questions et en tenant des consultations aussi larges que possible.

a) Sécurité et surveillance

11. Afin de recenser les meilleures pratiques pour ce qui est des garanties relatives à la surveillance d'Internet, le Rapporteur spécial a créé un Forum international de contrôle des services de renseignement, qui rassemble chaque année des représentants des organismes nationaux et des commissions parlementaires chargés d'assurer le contrôle des services de renseignement nationaux et étrangers dans leur pays respectif. Le Forum sert de plateforme d'échange d'informations et de données d'expérience et de recensement des meilleures pratiques au niveau international.

12. Le Forum a remporté un franc succès. La composition du Comité d'organisation est renouvelée régulièrement. En 2016, le Forum s'est tenu à Bucarest avec l'appui des quatre

commissions de contrôle du Parlement roumain. Plus de 60 personnes représentant 26 institutions de 20 pays différents y ont pris part. En 2017, le Forum a été accueilli par le Parlement belge, avec l'appui des autorités de protection des données de la Belgique, du Luxembourg et des Pays-Bas, et 80 délégués de 30 pays étaient présents. En 2018, il est prévu que le Forum se tienne en automne, au Portugal. Les autorités de contrôle de plusieurs pays sont de plus en plus impliquées dans le processus, qui constitue une préoccupation commune de portée internationale, et s'efforcent de recenser les problèmes ainsi que les solutions possibles dans le domaine du contrôle du renseignement ; elles répondent au besoin émergeant d'adopter des pratiques optimales essentielles à la protection de la vie privée.

13. C'est précisément la mise en balance du respect de la vie privée, de l'intérêt de la sécurité des États et de la surveillance dans le cyberspace qui a conduit à la création du mandat du Rapporteur spécial en 2015, à la suite des révélations faites par Edward Snowden depuis juin 2013. Le Rapporteur spécial partage le sentiment du Président du Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale, qui, en octobre 2017, a souligné, au sujet d'une recommandation visant à sensibiliser au lien existant entre la paix et la sécurité internationales, les droits de l'homme et le développement en ce qui concerne l'environnement des technologies de l'information et des communications (TIC), qu'en mettant en commun les enseignements et les pratiques tirés de la lutte contre l'utilisation des TIC à des fins terroristes et autres fins criminelles, notamment en matière de coopération entre les États et entre les États et le secteur privé, pour prévenir et combattre l'utilisation des TIC à des fins de recrutement et d'incitation à la violence par des groupes terroristes et extrémistes, ainsi que pour financer, planifier et préparer leurs activités, et déterminer où des travaux supplémentaires pourraient être nécessaires, les États devraient examiner leur engagement en faveur des droits de l'homme et des libertés fondamentales et ce qu'ils font pour respecter et protéger ces droits et ces libertés. Le Groupe d'Experts gouvernementaux a formulé plusieurs recommandations visant à appuyer la mise en œuvre de normes facultatives, non contraignantes, de comportement responsable des États, qui ont été présentées dans le rapport de 2015 du Groupe d'experts gouvernementaux (A/70/174), notamment que les États, lorsqu'ils veillent à une utilisation sûre des technologies de l'information et des communications, devraient respecter les résolutions 20/8 et 26/13 du Conseil des droits de l'homme sur la promotion, la protection et l'exercice des droits de l'homme sur l'Internet, ainsi que les résolutions 68/167 et 69/166 de l'Assemblée générale sur le droit à la vie privée à l'ère du numérique, afin de garantir le plein respect des droits de l'homme, y compris le droit à la liberté d'expression. Le Groupe d'Experts gouvernementaux a souligné que les données à caractère personnel utilisées par les technologies de l'information, transmises par leur intermédiaire ou traitées par elles peuvent avoir une profonde incidence sur la vie et la sécurité. Les États devraient prendre des mesures appropriées pour protéger les données à caractère personnel, notamment leur confidentialité, leur intégrité, leur accessibilité et leur authenticité, tout en respectant les instruments internationaux des droits de l'homme pertinents.

14. Relevant que le Groupe d'experts gouvernementaux n'était pas parvenu à un consensus sur un rapport final, le Rapporteur spécial estime qu'il est plus que jamais nécessaire de créer une synergie entre tous les acteurs internationaux dont le mandat a trait à l'utilisation des technologies de l'information et des communications traitant des données personnelles.

15. Le Rapporteur spécial maintient toujours que la cyberpaix dépend de la volonté et de la capacité des États à établir une synergie entre les intérêts en matière de sécurité et le respect de la vie privée dans le cyberspace. Pour éviter la cyberguerre, il faut aussi envisager des mesures visant à restreindre la surveillance et d'autres mesures intrusives portant atteinte à la vie privée dans le cyberspace. Examinant quelles mesures de ce type pourraient être adoptées, en synergie avec le projet MAPPING (Managing Alternatives for Privacy, Property and Internet Governance : « Gestion de solutions alternatives en faveur de la protection de la vie privée, de la propriété intellectuelle et de la gouvernance

d'Internet »), soutenu par l'Union européenne⁵, le Rapporteur spécial a étudié la possibilité d'élaborer un projet d'instrument juridique sur la surveillance et le droit à la vie privée visant à renforcer les normes et créer des mécanismes de protection pour faire face à la violation massive du droit à la vie privée des personnes dans le monde entier.

16. L'examen et l'adoption par les Nations Unies d'un instrument juridique relatif à la surveillance et au droit à la vie privée pourraient permettre d'atteindre simultanément deux objectifs principaux en offrant aux États :

a) Un ensemble de principes et de dispositions types permettant de traduire dans la législation nationale les normes les plus élevées du droit international des droits de l'homme et d'en assurer l'application, notamment le droit au respect de la vie privée, en relation avec la question de la surveillance ;

b) Différentes options, basées sur les meilleures pratiques internationales, permettant de concilier les intérêts en matière de sécurité et impératifs de surveillance et la protection du droit à la vie privée.

17. Il est nécessaire de se doter d'un instrument, qui pourra prendre la forme d'une recommandation non contraignante, ou bien, ce qui semble plus approprié compte tenu de la pratique actuelle des États, d'un traité international multilatéral obligatoire. Les travaux du Rapporteur spécial ont jusqu'à présent donné des résultats très satisfaisants – compte tenu en particulier des défis à relever – mais ils ne sont pas encore suffisamment avancés pour que le Rapporteur spécial puisse garantir au Conseil des droits de l'homme que l'instrument remporte un soutien unanime ou bien même le soutien d'une majorité des États. Malgré le besoin impérieux d'un tel instrument juridique, des questions de calendrier doivent être pris en compte.

b) Mégadonnées et données ouvertes

18. Le rapport du Rapporteur spécial sur les mégadonnées et les données ouvertes a été présenté à l'Assemblée générale en octobre 2017 en tant qu'étude préliminaire visant à recenser les principales questions sur le sujet (A/72/540). Les recommandations préliminaires qu'il contient portent sur les points suivants :

a) La gouvernance, la réglementation, la recherche et la concertation avec les organisations de la société civile ;

b) Les limites à l'utilisation des données à caractère personnel, sur le fondement des normes et principes internationaux, y compris une catégorie d'informations personnelles exemptées ;

c) Des mécanismes d'application solides ;

d) Les ressources nécessaires pour une analyse scientifique publique et rigoureuse des mesures de protection de la confidentialité des données, notamment une évaluation de l'incidence sur le respect de la vie privée ;

e) Le soutien actif des pouvoirs publics et des entreprises à l'élaboration et à l'utilisation des technologies visant à renforcer la protection de la vie privée.

⁵ Pour le Forum international de contrôle des services de renseignement et d'autres manifestations – par exemple, celles relatives à la protection de la vie privée, à la personnalité et à la circulation de l'information – le Rapporteur spécial reçoit un appui logistique de l'Université de Malte et de l'Université de Groningen, ainsi que par l'organisation de manifestations communes avec le projet MAPPING (Managing Alternatives for Privacy, Property and Internet Governance Project : « Gestion de solutions alternatives en faveur de la protection de la vie privée, de la propriété intellectuelle et de la gouvernance d'Internet »), appuyé par l'Union européenne. Depuis 2014, le Rapporteur spécial est le coordonnateur scientifique général du projet Gestion de solutions alternatives, qui porte sur la gouvernance de l'Internet, la protection de la vie privée et la propriété intellectuelle. Dans le cadre de ce projet, qui s'est officiellement achevé en février 2018, le Rapporteur spécial est également personnellement responsable de la question de la gouvernance de l'Internet et du respect de la vie privée, développée par l'Institut pour l'informatique juridique de l'Université Leibniz de Hanovre (Allemagne).

19. Des consultations ont été lancées au moyen d'un appel à soumettre des contributions avant le 28 avril 2018, et une réunion de consultation publique se tiendra en juillet 2018. Les travaux en cours portent sur les éléments suivants :

- a) Les principes et orientations en matière de protection de la vie privée dans le contexte des mégadonnées ;
- b) La consultation sur le rapport et les problèmes de protection de la vie privée que posent les mégadonnées ;
- c) La facilitation des travaux de recherche sur l'anonymisation ;
- d) La réponse à apporter à l'échec de l'anonymisation.

c) Données de santé

20. L'Équipe spéciale du Rapporteur spécial chargée des données de santé s'emploie à examiner un certain nombre de questions, sous la direction de M. Steve Steffensen, professeur associé à l'école de médecine Dell de l'Université du Texas (États-Unis). Une réunion de concertation aura lieu en 2018, très probablement aux États-Unis.

21. Tous les acteurs intéressés, les États et les autres parties prenantes, y compris les organisations non gouvernementales (ONG), sont invités à contribuer à l'élaboration de lignes directrices sur les meilleures pratiques.

d) Utilisation de données à caractère personnel par les entreprises

22. Certaines entreprises, notamment les plus grandes sociétés, s'appuient de façon croissante sur l'exploitation (collecte, traitement, réorientation et vente) de données à caractère personnel, souvent sans veiller à le faire de manière suffisamment transparente et sans le consentement éclairé des personnes concernées⁶. Au cours de sa visite officielle aux États-Unis en juin 2017, le Rapporteur spécial a interrogé les entreprises sur les mesures qu'elles prenaient pour répondre aux demandes des pouvoirs publics concernant les données à caractère personnel qu'elles possédaient. Les préoccupations du Rapporteur spécial concernant ces demandes ont abouti à la présentation d'un mémoire d'*amicus curiae* à la Cour suprême des États-Unis en décembre 2017⁷.

23. Le Rapporteur spécial s'est également entretenu avec un certain nombre d'entreprises américaines tout au long de l'année 2017 au sujet de l'utilisation des données personnelles dans leurs modèles d'activité. Ce dialogue servira de point de départ à l'Équipe spéciale sur l'utilisation des données personnelles par les entreprises pour commencer ses travaux en 2018.

e) Droit à la vie privée et personnalité

24. La reconnaissance par le Conseil des droits de l'homme du droit à la vie privée comme l'un des fondements d'une société démocratique⁸ est l'une des questions sur lesquelles travaille l'Équipe spéciale sur la vie privée et la personnalité, présidée par M^{me} Elizabeth Coombs (Australie), en s'appuyant sur des consultations et sur l'examen des contributions reçues et de la documentation existante. Pour favoriser une meilleure compréhension de la question du respect de la vie privée à l'ère du numérique, le Rapporteur spécial organise des réunions de concertation régionale sur le thème de la vie privée, de la personnalité et de la circulation de l'information. La première (pour les pays occidentaux) s'est tenue à New York en juillet 2016. La deuxième (pour le Moyen-Orient et l'Afrique du Nord) s'est tenue en Tunisie en mai 2017, la troisième (pour l'Asie) a eu lieu en septembre 2017 à Hong Kong. La quatrième (pour l'Amérique latine) se tiendra en mai 2018.

⁶ Voir www.ohchr.org/Documents/Issues/DigitalAge/ConceptNote.pdf.

⁷ *United States of America v. Microsoft Corporation*, affaire n° 17-2, mémoire déposé le 13 décembre 2017. Voir www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2018AnnualReportAppendix6.pdf.

⁸ Résolution 34/7 du Conseil des droits de l'homme.

25. En outre, le Rapporteur spécial mène également les travaux suivants :

a) L'analyse de décisions historiques, comme la décision rendue par la Cour suprême de l'Inde en 2017 dans l'affaire *Justice K.S. Puttaswamy (Retd.) and Another v. Union of India and Others*. Dans cet arrêt, la Cour suprême a déclaré ce qui suit : « La vie privée est l'expression ultime de l'inviolabilité de la personne. C'est une valeur constitutionnelle qui recoupe tout l'éventail des droits fondamentaux de la personne et protège, pour l'individu, un espace de libre choix et d'autodétermination »⁹ ;

b) L'analyse de l'incidence de la privation du droit à la vie privée sur les individus et leur développement personnel ;

c) Un examen de la question de la cyberviolence, mettant l'accent sur une analyse comparative entre les sexes et les groupes vulnérables de la communauté¹⁰ ;

d) L'analyse de l'importance de la vie privée pour l'épanouissement de l'individu et, par extension, pour les sociétés.

Visites officielles de pays

26. Les dates et le calendrier des visites officielles de pays sont négociés avec les États membres concernés. Les pays sont choisis en grande partie en fonction de l'évolution de leur situation du point de vue du respect du droit à la vie privée.

27. Les demandes de visites officielles de pays pour la période 2016-2018 :

| <i>Pays</i> | <i>Date de la demande</i> |
|-----------------------|---------------------------|
| Chine | 31 mars 2016 |
| République de Corée | 31 mars 2016 |
| Afrique du Sud | 31 mars 2016 |
| États-Unis d'Amérique | 20 septembre 2016 |
| Allemagne | 21 octobre 2016 |
| Inde | 21 octobre 2016 |
| Royaume-Uni | 21 octobre 2016 |
| France | 29 novembre 2016 |
| Argentine | 20 décembre 2017 |
| Uruguay | 8 janvier 2018 |

28. Les retards dans la conduite des visites de pays sont généralement le résultat de réponses tardives ou d'une absence de réponse des gouvernements aux demandes de visite, ou encore de circonstances rendant inappropriée la visite du Rapporteur spécial à la date initialement prévue. Les visites font partie intégrante du rôle de suivi de la situation en matière de droit à la vie privée qui incombe au Rapporteur spécial. Les calendriers des réunions concernent :

a) Les autorités, notamment les services de renseignement, de détection et de répression, les autorités de réglementation et de contrôle et leurs ministres de tutelle ;

b) Les représentants de la société civile et d'autres parties prenantes, notamment militants, journalistes et universitaires.

⁹ Voir [http://supremecourtindia.nic.in/pdf/jud/ALL%20WP\(C\)%20No.494%20of%202012%20Right%20to%20Privacy.pdf](http://supremecourtindia.nic.in/pdf/jud/ALL%20WP(C)%20No.494%20of%202012%20Right%20to%20Privacy.pdf).

¹⁰ Hadeel al-Alosi, « Cyber-violence : digital abuse in the context of domestic violence » (« Cyber-violence : maltraitance numérique dans le contexte de la violence familiale »), *University of New South Wales Law Journal*, vol. 40 (4), p. 1573 à 1603.

29. Les points suivants figurent généralement à l'ordre du jour des réunions :

- a) Les cadres constitutionnel, législatif et institutionnel ;
- b) Les mégadonnées, la surveillance, les atteintes à la vie privée, les cinq lignes d'action thématiques du Rapporteur spécial, ainsi que l'évaluation des mécanismes de contrôle des services de renseignement ;
- c) Des préoccupations communes au Rapporteur spécial, aux experts et aux organisations de la société civile.

Visites non officielles de pays

30. Le Rapporteur spécial se rend dans des pays à d'autres fins, notamment pour assister à des conférences internationales, et recueille des informations intéressant ses lignes d'action thématiques. Par exemple, durant les cinq mois précédant la présentation de son rapport à l'Assemblée générale en 2016, il a pris part à de multiples activités dans 11 pays aussi divers et géographiquement éloignés que l'Allemagne, l'Australie, l'Autriche, le Danemark, les États-Unis, la France, l'Italie, la Lettonie, la Nouvelle-Zélande, les Pays-Bas et la Suisse. Ces collaborations ont permis de recenser des questions importantes du point de vue de la promotion du droit à la vie privée, comme celles de la protection de la vie privée des enfants, des dispositions structurelles et organisationnelles relatives à la vie privée et des organismes de réglementation des données, entre autres.

Consultations

31. Le Rapporteur spécial a eu des échanges avec la société civile, les gouvernements, les forces de l'ordre, les services de renseignement, les autorités de protection des données, les autorités de contrôle des services de renseignement, des universitaires, des entreprises et d'autres parties prenantes en Afrique, en Amérique (nord, centre et sud), en Asie, en Australie et en Europe. En 2016 et 2017 seulement, 26 activités ont conduit le Rapporteur spécial dans plus de 30 villes différentes, dont certaines en Asie, en Afrique du Nord et en Amérique centrale, un quart aux États-Unis et plus de la moitié en Europe.

Formulation de recommandations pour la promotion et la protection du droit à la vie privée, notamment eu égard aux difficultés que posent les nouvelles technologies

32. Le Rapporteur spécial s'appuie sur les informations recueillies dans le cadre des activités décrites ci-dessus pour formuler les recommandations figurant dans ses rapports au Conseil des droits de l'homme et à l'Assemblée générale.

Réalisations

33. Les rapports thématiques présentés à ce jour sont les suivants :

- Premières approches de la surveillance étatique plus respectueuses de la vie privée, Conseil des droits de l'homme, mars 2017 (A/HRC/34/60) ;
- Sécurité et surveillance, Conseil des droits de l'homme, mars 2017 (A/HRC/31/64) ;
- Rapport intérimaire de l'Équipe spéciale sur les mégadonnées et les données ouvertes, Assemblée générale, octobre 2017 (A/72/540) ;
- Quelques options préliminaires dans le cadre de la gouvernance de l'Internet pour un instrument juridique international sur la surveillance étatique, Conseil des droits de l'homme, mars 2018 (voir le présent rapport et son appendice 7 disponible en ligne) ;

Progrès réalisés dans les lignes d'action thématiques

34. Le Rapporteur spécial a élaboré des principes directeurs relatifs aux mégadonnées, qu'il a présentés à l'Assemblée générale en octobre 2017 et qui sont actuellement en cours d'examen, ainsi qu'un projet d'instrument juridique international sur la surveillance et le droit à la vie privée visant à répondre aux problèmes qui ont été recensés.

35. Le Rapporteur spécial a organisé des consultations, notamment la conférence de 2017 sur la vie privée, la personnalité et la circulation de l'information intitulée « Asian

Perspectives for Privacy as a Global Human Right » (« Perspectives asiatiques concernant le respect de la vie privée en tant que droit de l'homme universel »).

36. L'Équipe spéciale chargée des données sur la santé a commencé ses travaux, sous la direction du Rapporteur spécial.

37. Le Rapporteur spécial a obtenu des soutiens pour l'Équipe spéciale sur l'utilisation de données à caractère personnel par les entreprises et a soumis un mémoire en qualité d'*amicus curiae* à la Cour suprême des États-Unis dans l'affaire Microsoft (voir appendice 6).

Visites officielles de pays

38. Le Rapporteur spécial a effectué deux visites officielles, l'une aux États-Unis en juin 2017¹¹ et l'autre en France en novembre 2017¹². Les rapports relatifs à ces visites seront présentés au Conseil des droits de l'homme en mars 2019, afin de ménager le temps nécessaire aux échanges de suivi avec les Gouvernements concernés.

Consultations

39. Diverses manifestations, notamment celles organisées par le Conseil irlandais pour les libertés civiles, l'Union japonaise pour les libertés civiles, la Fédération des barreaux du Japon et la Commission des droits de l'homme d'Irlande du Nord, ainsi que divers ateliers qui ont eu lieu dans le cadre du Forum sur la gouvernance d'Internet et de la RightsCon, ont permis de mieux faire connaître les questions relatives à la vie privée dans différentes juridictions, à différents niveaux et dans différentes parties de la population.

Activités et possibilités futures

40. Si son mandat est renouvelé par le Conseil des droits de l'homme, le Rapporteur spécial entend soumettre les rapports suivants :

- a) Au Conseil des droits de l'homme :
 - i) « Exploiter les enseignements pour améliorer les garanties et les recours dans le cadre du contrôle effectif de la surveillance exercée par les États », en mars 2019 ;
 - ii) « Proportionnalité, nécessité et droit dans le domaine de la surveillance exercée par les États, de l'application des lois et de la circulation transfrontière de données personnelles : efficacité des garanties juridiques et des voies de recours existantes et pistes d'amélioration », en mars 2020 ;
 - iii) « Avancées, reculs et autres aspects du contrôle effectif de la surveillance exercée par les États », en mars 2021 ;
- b) À l'Assemblée générale :
 - i) « Amélioration des garanties et des voies de recours dans le domaine de la protection de la vie privée et des données de santé », en octobre 2018 ;
 - ii) « Profits et vie privée : la monétisation des données personnelles en tant que modèle économique et les responsabilités des entreprises », en octobre 2019 ;
 - iii) « Vie privée, personnalité et circulation de l'information : un premier panorama global du droit universel à la vie privée du point de vue du temps, du lieu et de l'espace », en octobre 2020 ;
 - iv) « La circulation transfrontière des données personnelles entre les entreprises, les forces de l'ordre et les services de surveillance », en octobre 2021.

41. Le Rapporteur spécial pourra aussi, s'il dispose du temps et des ressources nécessaires, établir des rapports sur d'autres questions liées au droit à la vie privée, telles

¹¹ La déclaration faite à l'issue de la mission peut être consultée à l'adresse suivante : www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/VisitUSA_EndStatementJune2017.docx.

¹² Voir les conclusions préliminaires : www.ohchr.org/FR/NewsEvents/Pages/DisplayNews.aspx?NewsID=22410&LangID=F.

que les mégadonnées et les données ouvertes, les données de santé, l'utilisation des données à caractère personnel par les entreprises, la vie privée des enfants et des jeunes, les stratégies pour répondre aux problèmes que posent les activités de surveillance du point de vue du respect de la vie privée, la prise en compte de la question du genre dans l'approche du droit à la vie privée, la gestion des atteintes à la vie privée, par exemple en cas d'échec des procédés d'anonymisation employés dans le traitement des mégadonnées, les plaintes reçues par le Rapporteur spécial, les visites officielles de pays, les questions faisant l'objet de discussions avec les États (lettres accessibles au public) et les questions concernant le droit à la vie privée à l'ère numérique.

42. Les prochaines visites de pays du Rapporteur spécial le conduiront au Royaume-Uni de Grande-Bretagne et d'Irlande du Nord (en juin 2018) et en Allemagne (à l'automne 2018).

43. Le Rapporteur spécial poursuivra ses consultations auprès des institutions étatiques, des particuliers et des organisations sur la question du droit à la vie privée. Parmi les grandes manifestations de 2018, il convient de mentionner la conférence sur le projet MAPPING (Managing Alternatives for Privacy, Property and Internet Governance) qui a eu lieu les 19 et 20 janvier à Rome, la manifestation consacrée à la vie privée, à la personnalité et à la circulation de l'information pour l'Amérique latine prévue en mai ainsi que la consultation de l'Équipe spéciale chargée des données sur la santé et la consultation sur les mégadonnées et les données ouvertes devant se tenir en Australie en juillet.

2. Recherche et réception d'informations, et réponses apportées

Consultations

44. Le Rapporteur spécial a échangé des informations avec les représentants, les ministères et les institutions de divers États (aux niveaux national et infranational), des commissaires à la protection des données et à la vie privée, la présidente du groupe de travail de l'article 29 de l'Union européenne¹³, la présidente du Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatique des données à caractère personnel du Conseil de l'Europe, les organismes de normalisation, tels que l'Union internationale des télécommunications et l'Institute of Electrical and Electronic Engineers, les organisations de la société civile, les missions permanentes auprès de l'Office des Nations Unies et des autres organisations internationales à Genève, d'autres titulaires de mandat au titre des procédures spéciales, des représentants du Haut-Commissariat des Nations Unies aux droits de l'homme (HCDH), des chercheurs, des universitaires et des organismes professionnels. Il a prononcé des allocutions et participé à de nombreuses conférences et manifestations organisées par la société civile.

45. Le Rapporteur spécial a eu des échanges particulièrement productifs avec les commissaires à la protection des données et à la vie privée, qui forment un groupe d'interlocuteurs essentiel dans ce domaine. Il a recueilli leurs observations sur son plan en 10 points au cours de la Conférence internationale des Commissaires à la protection des données et à la vie privée en 2015. À la Conférence de 2016, le Rapporteur spécial a rendu compte des progrès réalisés dans la mise en œuvre de ce plan et à la Conférence de 2017 qui s'est tenue à Hong Kong (Chine), il a pris la parole et a participé à des manifestations parallèles, et a animé la troisième manifestation consacrée à la vie privée, la personnalité et la circulation de l'information, destinée à compléter les travaux de la Conférence.

Correspondance

46. Le Rapporteur spécial reçoit des communications provenant de diverses sources. Cependant, seule la correspondance officiellement enregistrée par le HCDH étant comptabilisée, il est difficile de rendre compte du nombre total de communications reçues. Depuis le début du mandat, le HCDH a toutefois enregistré la correspondance suivante destinée au Rapporteur spécial.

¹³ Groupe de travail sur la protection des données créé par l'article 29 de la directive 95/46/CE.

47. Correspondance enregistrée pour 2015-2017¹⁴ :

| 2015 | 2016 | 2017 | Total |
|-------------------------|------|------|-------|
| Données non disponibles | 3 | 47 | 50 |

48. Ces données n'ont pas été ventilées par pays ou par question, mais, en 2017, l'essentiel de la correspondance provenait des missions permanentes, des ONG et d'organisations internationales¹⁵. Ces chiffres ne tiennent pas compte des centaines, voire des milliers d'autres messages reçus à l'adresse de courriel officielle du Rapporteur spécial (srprivacy@ohchr.org).

Réalisations

49. En octobre 2015, la Conférence internationale des Commissaires à la protection des données et à la vie privée a adopté une résolution concernant la coopération avec le Rapporteur spécial¹⁶.

50. Le Rapporteur spécial a publié, conjointement avec d'autres titulaires de mandat, des communications concernant la situation en Égypte, en Espagne, en Haïti, au Honduras et au Mexique.

51. Le Rapporteur spécial a recensé et traité de nouvelles questions, ainsi que des allégations d'atteintes à la vie privée et d'immixtions dans la vie privée utilisant certaines technologies, comme les logiciels de reconnaissance faciale.

Activités et possibilités futures

52. Le Rapporteur spécial poursuivra ses activités, notamment le dialogue avec toutes les parties prenantes (en particulier sur les questions de sécurité et de surveillance, y compris la cybersécurité), l'élaboration de matériels d'orientation et de recommandations sur les questions émergentes, avec la contribution des organisations de la société civile et d'autres parties prenantes, l'assistance technique sur les risques croissants d'atteinte au droit à la vie privée à l'ère numérique et la coopération avec d'autres titulaires de mandat au titre des procédures spéciales sur la protection des droits de l'homme.

3. Identification des obstacles, promotion des principes et formulation de recommandations

Obstacles au respect de la vie privée

53. L'une des questions les plus importantes auxquelles s'est attaqué le Rapporteur spécial est celle de la sécurité et de la surveillance, une question centrale qui a conduit à la création de son mandat par le Conseil des droits de l'homme. La protection de la vie privée pâtit de l'absence de règles détaillées, de procédures pratiques et de mécanismes de contrôle appropriés visant à garantir un contrôle indépendant, fiable et efficace de la surveillance aux niveaux national et mondial, ou du caractère inadéquat des règles existantes. On trouvera dans l'annexe un aperçu des lacunes qui ont été recensées dans la protection de la vie privée.

54. En ce qui concerne les mégadonnées, il n'est plus nécessaire que les données soient « personnelles » pour qu'elles permettent d'identifier une personne¹⁷. Les capacités technologiques et l'analyse de données peuvent constituer une menace pour la vie privée dès lors que l'on dispose d'informations qui « dirigent » vers une personne et son entourage.

¹⁴ Ces chiffres ne tiennent pas compte des courriels envoyés à l'adresse srprivacy@ohchr.org.

¹⁵ Informations fournies par le HCDH le 19 décembre 2017.

¹⁶ Voir <https://icdppc.org/wp-content/uploads/2015/02/Resolution-on-Cooperation-with-UN-Special-Rapporteur-on-the-Right-to-Privacy.pdf>.

¹⁷ Graham Greenleaf, « Data protection : a necessary part of India's fundamental inalienable right of privacy – submission on the White Paper of the Committee of Experts on a Data Protection Framework for India », University of New South Wales Law Research Paper n° 6, janvier 2018. Consultable à l'adresse https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3102810.

55. Les lignes d'action thématiques ont permis d'identifier les divers obstacles actuels à la protection et à la promotion du droit à la vie privée, tels que les immixtions de la technologie dans le domaine de la santé, l'utilisation du contenu des smartphones comme preuve, la cyberviolence, les différents niveaux de vulnérabilité des communautés, les biais, entre autres de genre, qui persistent dans les algorithmes, l'accès des pouvoirs publics aux données du secteur privé, et la reconnaissance faciale et autres outils technologiques.

Lever les obstacles – promouvoir le respect de la vie privée

56. En ce qui concerne la surveillance, le Rapporteur spécial a entrepris de déployer une stratégie visant à créer un consensus sur les moyens de renforcer le cadre juridique international et de créer, au niveau mondial, des mécanismes appropriés de contrôle de la surveillance.

57. Le Rapporteur spécial a publié des communications officielles sur les questions d'actualité concernant le respect de la vie privée, les visites officielles de pays et les questions appelant une réaction conjointe avec d'autres titulaires de mandat (voir appendice 3).

Promotion des principes et des meilleures pratiques

58. Le Rapporteur spécial a participé à des consultations publiques sur des projets de loi lancées par les Gouvernements indien et britannique et par le Parlement australien¹⁸. Il a aussi fait part de ses préoccupations dans des courriers, dont certains confidentiels¹⁹ et d'autres rendus publics, tels que ceux qui ont été adressés aux Gouvernements japonais et mexicain.

Propositions et recommandations au Conseil des droits de l'homme

59. Les recommandations du Rapporteur spécial concernant les mégadonnées et les données ouvertes figurent à l'appendice 4 du présent rapport.

60. Les recommandations préliminaires formulées par le Rapporteur spécial à l'issue de sa visite officielle aux États-Unis concernent la surveillance à des fins de sécurité nationale (composition du *Privacy and Civil Liberties Oversight Board* et article 702 de la loi de 2008 portant modification de la loi de 1978 sur la surveillance du renseignement étranger), la surveillance urbaine utilisant l'intelligence artificielle et la surveillance à des fins de répression, les situations relevant du décret présidentiel n° 12333, les données personnelles détenues par des entreprises, l'extension à toutes les données de santé de la protection garantie par la loi de 1996 relative à la transférabilité et la responsabilité en matière d'assurance santé, la gestion de l'identité des travailleurs du sexe, la simplification des mesures relatives à la vie privée et la promotion, au niveau de l'État, d'initiatives favorables à la vie privée. En ce qui concerne la surveillance, le Rapporteur spécial a recommandé qu'il soit mis fin à toute discrimination en matière de garanties et de recours concernant la vie privée entre les personnes ayant la nationalité américaine ou résidant aux États-Unis et celles n'ayant ni la nationalité ni le statut de résident, et il a recommandé au Congrès de déposer une proposition de loi disposant que la surveillance de masse est disproportionnée et inutile dans une société démocratique.

61. Le Rapporteur spécial a aussi formulé d'autres recommandations relatives à la sécurité et à la surveillance dans ses rapports annuels au Conseil des droits de l'homme.

Réalisations

62. Le Rapporteur spécial a rendu compte des nouveaux obstacles qui se font jour dans ses rapports annuels à l'Assemblée générale et au Conseil des droits de l'homme (entre

¹⁸ Communication adressée le 24 janvier 2018 à la Commission parlementaire mixte sur le renseignement et la sécurité du Parlement australien dans le cadre de l'examen du projet de loi de 2017 portant modification de la loi sur la sécurité nationale (espionnage et ingérence étrangère).

¹⁹ Confidentiels jusqu'à l'expiration d'un délai de réponse de soixante jours.

2015 et 2017) et dans des communications relatives aux violations du droit à la vie privée commises par les États membres.

63. Le Rapporteur spécial s'est attaqué à ces obstacles en faisant campagne auprès des gouvernements pour qu'ils prennent des mesures face aux initiatives et programmes susceptibles d'entraîner des violations du droit à la vie privée, en créant des équipes spéciales sur les lignes d'action thématiques, en promouvant auprès des entreprises technologiques la notion de protection de la vie privée dès la conception (« *privacy by design* »), en élaborant un projet d'instrument juridique relatif à la surveillance exercée par les États (voir sect. II), en participant à des consultations publiques, en participant à des événements internationaux et en publiant des documents.

64. Le Rapporteur spécial a soumis les propositions et recommandations suivantes, dont certaines ont été présentées ci-dessus : un plan d'action en 10 points, en 2015 ; les priorités du mandat (lignes d'action thématiques), en 2016 ; et des recommandations préliminaires, dans la déclaration faite à l'issue de sa visite officielle aux États-Unis en 2017, ainsi que celles sur la surveillance exercée par les États (A/HRC/34/60) et sur les mégadonnées et les données ouvertes, en 2017 (A/72/540).

Activités et possibilités futures

65. Le Rapporteur spécial rendra en mars 2019 le rapport final concernant sa visite officielle aux États-Unis, qui portera principalement sur les mécanismes de contrôle applicables aux situations relevant du décret n° 12333. Son rapport concernant la visite officielle effectuée en France est également attendu en mars 2019.

66. Le rapport du Rapporteur spécial sur la vie privée et les données de santé sera présenté à l'Assemblée générale en octobre 2018.

67. Les propositions et recommandations finales du Rapporteur spécial relatives aux mégadonnées et aux données ouvertes seront publiées après les concertations internationales prévues à la fin du premier semestre de 2018.

4. Contribution à des manifestations internationales pour promouvoir une approche systématique et cohérente du droit à la vie privée

Activités

68. Le Rapporteur spécial a pris la parole à de nombreuses manifestations, y compris en tant qu'intervenant principal, ce qui lui a permis de s'adresser aux principales parties prenantes et de bénéficier d'une large couverture médiatique.

69. Le titulaire de mandat poursuit sa coopération avec la Conférence internationale des commissaires à la protection des données et à la vie privée, qui est d'une grande importance. Les 19 et 20 février 2018, le Rapporteur spécial a présenté et animé une séance organisée par le HCDH dans le cadre de l'atelier d'experts sur le droit à la vie privée à l'ère numérique. Un rapport sur les travaux de cet atelier sera soumis au Conseil des droits de l'homme à sa trente-neuvième session (conformément à sa résolution 34/7).

70. Le Rapporteur spécial met en œuvre son plan d'action en 10 points, qui a été présenté au Conseil des droits de l'homme en mars 2016 et prévoit (voir A/HRC/31/64, par. 45 à 55) :

a) Des recherches et des consultations sur la protection du droit à la vie privée à l'ère numérique, mettant l'accent sur la nécessité de mieux protéger le droit à la vie privée des enfants et des jeunes, et sur la question de la vie privée envisagée sous l'angle des questions de genre ;

b) Des efforts de sensibilisation, par exemple la semaine de sensibilisation à la protection de la vie privée organisée par les autorités de protection de la vie privée pour la région Asie-Pacifique et d'autres manifestations visant les membres de la communauté, les autorités de régulation et les organisations des secteurs public et privé ;

c) Un dialogue structuré avec les ONG, les commissaires à la protection des données et à la vie privée, les forces de l'ordre et les services de sécurité et de renseignement sur l'articulation entre sécurité, surveillance et respect de la vie privée ;

d) Une approche globale des garanties juridiques, procédurales et opérationnelles et des voies de recours, qui inclut l'élaboration du projet d'instrument juridique et la présentation du mémoire en qualité d'*amicus curiae* mentionnées plus haut ;

e) Des garanties techniques, examinées avec l'Assemblée générale en octobre 2017, et un dialogue constant avec les milieux techniques en vue de promouvoir des garanties techniques efficaces ;

f) Un dialogue avec le secteur privé, comme décrit plus haut ;

g) La promotion des progrès réalisés aux niveaux national et régional dans le domaine des mécanismes de protection de la vie privée, dont le Rapporteur spécial souligne l'utilité au niveau mondial²⁰. Ce travail est facilité par les liens entretenus avec les autorités de protection de la vie privée et des données dans le monde entier ;

h) Une coopération avec la société civile. Pendant les six premiers mois de son mandat, le Rapporteur spécial a rencontré 40 ONG, et le dialogue se poursuit par l'intermédiaire des équipes spéciales thématiques et au moyen de réunions et de manifestations telle que celles qui ont été organisées sur la vie privée, la personnalité et la circulation de l'information ;

i) Le cyberspace, le respect de la vie privée sur Internet, le cyberespionnage, la cyberguerre, et la cyberpaix : ces questions, traitées dans le cadre des travaux de la ligne d'action thématique sur la sécurité et la surveillance, sont régulièrement abordées dans les rapports du Rapporteur spécial. Sont également pertinentes les questions de la cyberviolence contre les personnes les plus vulnérables, et notamment de la violence domestique facilitée par les outils numériques, de la diffusion non consentie d'images intimes et des risques qui pèsent sur la vie privée des jeunes enfants ;

j) La promotion du développement du droit international. En décembre 2017, le Rapporteur spécial a coopéré avec la clinique d'aide juridique sur le droit du cyberspace de la faculté de droit de Harvard en vue de rédiger un mémoire d'*amicus curiae* dans l'affaire Microsoft, citée ci-dessus, en raison de l'incidence que celle-ci pouvait avoir sur le droit international (voir appendice 6). Le 24 août 2017, la Cour suprême de l'Inde a rendu une décision dans une importante affaire de droit constitutionnel, *Justice K.S. Puttaswamy (Retd.) and Another v. Union of India and Others*, jugeant à l'unanimité que le droit à la vie privée était protégé par la Constitution indienne. Cette décision importante pourrait mener à des recours en inconstitutionnalité contre d'autres lois indiennes²¹ concernant des questions de genre, que le Rapporteur spécial suivra de près.

Réalisations

71. Depuis mars 2015, le Rapporteur spécial a prononcé plus d'une centaine de discours pour promouvoir la protection du droit à la vie privée (voir appendice 5), créé un blog sur la vie privée et la personnalité (www.privacyandpersonality.org), soumis un mémoire à titre d'*amicus curiae* à la Cour suprême des États-Unis, formulé des observations en réponse à la consultation organisée par le Royaume-Uni sur la loi de 2016 relative aux pouvoirs d'enquête et concernant la décision de la Cour de justice de l'Union européenne, contribué aux enquêtes du Parlement australien sur l'incidence des avancées dans le domaine des TIC pour les organes chargés de faire respecter la loi et sur le projet de loi de 2017 portant modification de la loi sur la sécurité nationale (espionnage et ingérence étrangère), apporté sa contribution aux travaux du Gouvernement indien sur le Livre blanc relatif à un cadre de protection des données et coopéré avec le centre d'aide juridique sur le droit de l'Internet de la faculté de droit de Harvard.

²⁰ Par exemple, la loi de 2015 relative au partage des données (secteur public) adoptée en Nouvelle-Galles du Sud (Australie), qui exige que le partage des données soit conforme aux dispositions de la loi relative à la protection de la vie privée.

²¹ Voir <https://inforrm.org/2017/09/04/case-law-india-puttaswamy-v-union-of-india-supreme-court-recognises-a-constitutional-right-to-privacy-in-a-landmark-judgment-hugh-tomlinson-qc/>.

Activités et possibilités futures

72. Le Rapporteur spécial continuera à organiser des manifestations internationales telles que les conférences sur la vie privée, la personnalité et la circulation de l'information et à participer à des événements internationaux, et il continuera à examiner les décisions de justice importantes sur les questions de vie privée et de personnalité, notamment sous l'angle des problématiques de genre.

5. Sensibilisation au droit à la vie privée, y compris aux défis qui y sont liés et aux recours utiles

73. Le Rapporteur spécial a poursuivi ses activités de sensibilisation à l'importance de la promotion et de la protection du droit à la vie privée, en mettant l'accent sur les défis de l'ère numérique, et à la nécessité d'assurer un recours utile aux personnes dont le droit à la vie privée a été violé, conformément aux obligations internationales en matière de droits de l'homme.

74. Mi-2016, dans un État membre, des données supposément anonymisées relatives à des remboursements de soins de santé et de médicaments ont été rendues publiques, entraînant un risque d'atteinte à la vie privée pour 1 citoyen sur 10. Il s'est avéré qu'il était possible de réidentifier les praticiens et les patients. Le Rapporteur spécial a écrit à deux reprises à l'État partie concerné. La correspondance demeure confidentielle durant soixante jours. Cette question est étroitement liée à la ligne d'action thématique du mandat portant sur les mégadonnées et les données ouvertes.

75. Le 18 mai 2017, le Rapporteur spécial a fait la démarche inhabituelle de publier sur le site du HCDH une lettre ouverte d'allégation adressée au Gouvernement japonais²², et il attend à présent une invitation dudit Gouvernement à engager des discussions sur les normes du droit international des droits de l'homme.

76. Le 19 juillet 2017, le Rapporteur spécial et d'autres titulaires de mandat ont conjointement appelé le Gouvernement mexicain à mener une enquête transparente, indépendante et impartiale sur les allégations de contrôle et de surveillance illégale de défenseurs des droits de l'homme, de militants de la société civile et de journalistes²³.

77. Le Rapporteur spécial a envoyé un courrier à un État membre au sujet de l'absence de recours disponible pour une personne ayant subi une atteinte grave à sa vie privée. Cette correspondance est publiée dans le rapport sur les communications des titulaires de mandat au titre des procédures spéciales²⁴.

Réalisations

78. Le Rapporteur spécial a continué de porter à l'attention des États les lacunes existant dans la gestion du respect de la vie privée et de veiller à ce que les questions pertinentes relatives à la vie privée aient une place dans le débat public.

Activités et possibilités futures

79. Le Rapporteur spécial s'emploiera à faire en sorte que les personnes qui se disent victimes d'atteintes à la vie privée aient accès à des recours conformes aux obligations internationales et continuera à collaborer avec les États membres et les ONG pour recenser les personnes qui n'ont pas accès aux voies de recours internes et leur permettre d'être entendues.

6. Intégration d'une perspective de genre

Activités

80. Les travaux du Rapporteur spécial sur la vie privée, la personnalité et la circulation de l'information reposent sur la perception de la vie privée comme un droit essentiel

²² Voir www.ohchr.org/Documents/Issues/Privacy/OL_JPN.pdf.

²³ Voir www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=21892&LangID=E.

²⁴ Voir www.ohchr.org/EN/HRBodies/SP/Pages/CommunicationsreportsSP.aspx.

nécessaire à l'exercice du droit fondamental général qu'a chacun au développement libre et sans entrave de sa personnalité. Ils ont débuté en juillet 2016 à New York, avec une manifestation qui a réuni 90 experts et représentants d'autorités de réglementation, d'entreprises et d'organisations de la société civile venus des cinq continents.

81. La deuxième consultation de ce type, tenue pour la région du Moyen-Orient et de l'Afrique du Nord, s'est déroulée les 25 et 26 mai 2017 à Tunis, avec le soutien des autorités nationales de protection des données. Cette manifestation a réuni environ 70 personnes venues d'Algérie, d'Égypte, du Liban, du Maroc, de la République arabe syrienne, de Tunisie et du Qatar. La séance consacrée à la perspective de genre, qui a donné un aperçu de l'expérience particulière des femmes, a été une contribution importante.

82. La troisième consultation a eu lieu les 29 et 30 septembre 2017 à Hong Kong (Chine), pendant la Conférence internationale des commissaires à la protection des données et à la vie privée, en coopération avec le Groupe de recherche sur la sécurité, la technologie et la vie privée sur Internet de la faculté de droit de l'Université de Groningen (Pays-Bas), le Département de la politique de l'information et de la gouvernance de l'Université de Malte et le projet MAPPING. Elle était accueillie par les partenaires locaux, Digital Asia Hub, l'Université de Hong Kong et le Commissaire au droit à la vie privée de Hong Kong. La consultation a porté principalement sur les évolutions et les tendances en Asie, avec des séances séparées consacrées aux traditions asiatiques en matière de vie privée, à la vie privée et à la surveillance en Asie, à la vie privée et ses liens avec les autres droits de l'homme en Asie et au genre et à la vie privée en Asie.

83. La quatrième consultation aura lieu au premier trimestre 2018, et des séances seront consacrées aux questions de genre.

84. Un État membre a soulevé une préoccupation grave, expliquant que son système juridique n'avait pas pu offrir de recours utile à une femme dont les organes génitaux avaient été photographiés au cours d'une intervention gynécologique par un professionnel de santé au moyen d'un téléphone personnel, sans son consentement et sans raison médicale. Cette violation de la vie privée avait eu de graves conséquences psychologiques, financières et familiales.

85. Un autre problème est celui des cas dans lesquels une procédure apparemment licite de communication utilisée dans le cadre d'une procédure judiciaire a des effets inattendus et différenciés sur la vie privée dans les affaires relatives à l'identité de genre. Le Rapporteur spécial examine actuellement les préoccupations que soulèvent ces cas.

86. Pendant la visite officielle du Rapporteur spécial aux États-Unis, un travailleur du sexe a soulevé la question des effets de la criminalisation de la prostitution sur le droit des travailleurs du sexe à la vie privée. Il semble qu'une révision des règles relatives à la surveillance des travailleurs du sexe par les forces de l'ordre puisse être nécessaire²⁵.

87. Plusieurs communications adressées en 2017 à certains États, conjointement avec d'autres titulaires de mandat, portaient sur des questions de genre²⁶ et sur l'objet et le but de la résolution 34/17, dans laquelle le Conseil des droits de l'homme a déclaré que le droit à la vie privée contribuait au libre développement de la personnalité de chacun.

88. Le Rapporteur spécial suivra de près les affaires qui seront jugées après la décision rendue par la Cour suprême de l'Inde dans l'affaire *Justice K.S. Puttaswamy (Retd.) and Another v. Union of India and Others*, selon laquelle l'orientation sexuelle est un élément essentiel de la vie privée.

89. Le Rapporteur spécial souhaite examiner les conséquences d'une atteinte à la vie privée. La proposition en ce sens a été rédigée, mais les ressources doivent encore être trouvées.

²⁵ Voir la déclaration faite à l'issue de la mission : www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/VisitUSA_EndStatementJune2017.docx.

²⁶ Communications adressées conjointement avec d'autres titulaires de mandat aux Gouvernements haïtien (22 septembre 2017), espagnol (12 octobre 2017) et égyptien (31 octobre 2017).

Réalisations

90. Le Rapporteur spécial a tenu des consultations sur la vie privée et le genre dans le cadre des lignes d'action thématiques et animé des séances sur les aspects du droit à la vie privée liés au genre au cours des trois consultations sur la vie privée, la personnalité et la circulation de l'information ; il a encouragé l'échange d'informations entre parties prenantes sur les aspects du droit de la vie privée sur lesquels le genre a une influence et a soulevé certaines questions avec les États membres.

Activités et possibilités futures

91. Au cours de la quatrième consultation sur la vie privée, la personnalité et la circulation de l'information, qui se tiendra au premier trimestre 2018, une séance sera consacrée aux problématiques de genre dans le domaine de la vie privée. Le Rapporteur spécial continuera d'analyser les décisions de justice comme indiqué plus haut et mènera des recherches sur les questions de genre liées au droit à la vie privée.

7. Signalement des violations présumées, notamment des problèmes découlant des nouvelles technologies

92. Le Rapporteur spécial a continué de rendre compte des violations présumées du droit à la vie privée en s'intéressant notamment aux problèmes posés par les nouvelles technologies, et a appelé l'attention du Conseil des droits de l'homme et de la Haute-Commissaire des Nations Unies aux droits de l'homme sur les situations particulièrement préoccupantes.

Activités

93. Il est également utile d'évoquer ici l'atteinte grave à la vie privée survenue en milieu médical dont il est question plus haut, puisqu'elle soulève la question de la nécessité de voies de recours dans de telles affaires²⁷. Les discussions avec l'État concerné se poursuivent.

Réalisations

94. Le Rapporteur spécial a continué d'appeler l'attention des États membres concernés sur les violations présumées du droit à la vie privée. Il a aussi fait mieux connaître au Conseil des droits de l'homme les violations de l'article 12 de la Déclaration universelle des droits de l'homme et de l'article 17 du Pacte international relatif aux droits civils et politiques.

Activités et possibilités futures

95. Le Rapporteur spécial continuera de rendre compte des violations présumées du droit à la vie privée et de chercher à résoudre les problèmes graves avec les États membres.

8. Rapports annuels au Conseil des droits de l'homme et à l'Assemblée générale

96. Conformément à son mandat, le Rapporteur spécial rend compte chaque année au Conseil des droits de l'homme et à l'Assemblée générale.

Rapports annuels au Conseil des droits de l'homme

97. Le présent document est le rapport annuel du Rapporteur spécial au Conseil des droits de l'homme pour 2018. Y sont présentés les activités menées par le Rapporteur depuis 2015 et les travaux qu'il a réalisés sur les questions de la protection du droit à la vie privée et de la surveillance exercée par l'État, ainsi qu'une analyse du mandat confié par le Conseil des droits de l'homme.

²⁷ Au cours de la dernière décennie, les différentes commissions de réforme de la législation de l'État en question ont recommandé à huit reprises la création d'un nouveau recours, la qualification civile d'atteinte grave à la vie privée.

98. Un résumé des deux précédents rapports au Conseil figure ci-dessus.

Rapports annuels à l'Assemblée générale

99. Dans le rapport annuel qu'il a présenté en 2017 à l'Assemblée générale, le Rapporteur spécial a décrit l'état d'avancement des travaux portant sur les lignes d'action thématiques et présenté son rapport d'étape sur les mégadonnées et les données ouvertes. Le Rapporteur spécial a décrit le processus de consultation proposé et exposé un cas dans lequel après que des données de santé anonymisées ont été rendues publiques, il s'est avéré qu'il était possible de faire le lien entre ces données et les personnes auxquelles elles se référaient. Cette affaire est actuellement examinée avec l'État concerné.

100. Un résumé des deux précédents rapports à l'Assemblée générale figure ci-dessus.

Activités et possibilités futures

101. Le Rapporteur spécial continuera de soumettre des rapports annuels retraçant les activités qu'il mène et les nouvelles questions qui se font jour, et de rendre compte, selon le calendrier prévu, des travaux des équipes spéciales portant sur les lignes d'action thématiques.

B. Travaux du Rapporteur spécial dans le domaine prioritaire de la sécurité, la surveillance et la vie privée

102. Depuis quelques années, ainsi que l'a indiqué le HCDH, le droit à la vie privée, et en particulier les politiques et les pratiques en matière de surveillance mises en œuvre par de nombreux États de par le monde, suscitent toujours plus l'attention de l'Assemblée générale et des mécanismes de protection des droits de l'homme. En 2013, l'Assemblée générale a adopté la résolution 68/167, dans laquelle elle s'est déclarée profondément préoccupée par l'incidence néfaste que la surveillance ou l'interception des communications pouvaient avoir sur les droits de l'homme. Elle 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 le contexte de la communication numérique. Les mécanismes de contrôle nationaux, lorsqu'il en existe, sont souvent inefficaces car ils ne réussissent ni à établir la transparence nécessaire ni à obtenir que les États rendent des comptes au sujet de leurs activités de surveillance et d'interception des communications ainsi que de collecte de données privées²⁸.

103. Les attentats terroristes commis en Allemagne, en Belgique, en France et au Royaume-Uni ont entraîné l'adoption de stratégies nationales et parfois internationales privilégiant des mesures de sécurité répressives et de grande ampleur plutôt que des actions prudentes et nuancées tenant compte des intérêts en matière de sécurité et de la nécessité de protéger la vie privée des citoyens. Entre 2016 et 2017, l'Allemagne, la Belgique, la France, les Pays-Bas et le Royaume-Uni, pour ne citer que quelques exemples, ont pris des mesures législatives dont l'efficacité, la proportionnalité et la portée sont très diverses. Aucune législation nationale relative à la surveillance n'est entièrement conforme aux normes internationales relatives au droit à la vie privée ni ne les respecte pleinement.

104. Malgré la mobilisation provoquée par les révélations d'Edward Snowden, la vie privée et la surveillance sont des sujets dont peu de pays souhaitent débattre. La société civile, les scientifiques et les autres parties prenantes, notamment un nombre croissant d'États, ont toutefois exprimé un intérêt sincère dans la tenue d'un débat international constructif et en bonne et due forme sur la vie privée et la surveillance.

105. Dans l'esprit des plans d'action qu'il a proposés au Conseil des droits de l'homme dans son premier rapport annuel et dans ses rapports ultérieurs à l'Assemblée générale, le Rapporteur spécial s'est efforcé de répondre aux préoccupations exprimées par ces différents acteurs et de les rapprocher en organisant différentes rencontres consacrées aux échanges et aux débats. Il a examiné le problème majeur que pose la surveillance du point

²⁸ Voir www.ohchr.org/Documents/Issues/DigitalAge/ConceptNote.pdf.

de vue de la protection de la vie privée en concertation avec les États membres, le projet Managing Alternatives for Privacy, Property and Internet Governance (MAPPING), auquel l'Union européenne apporte son soutien, et des organisations de la société civile afin de ne pas entreprendre d'activités qui feraient double emploi.

1. Vers un instrument juridique international sur la surveillance et la vie privée

106. Il est ressorti des travaux de recherche et des discussions tenues avec les responsables des politiques publiques, les organes chargés d'assurer le respect de la loi et les services de renseignement, ainsi que les organisations de la société civile, qu'un élément fondamental pour éviter l'instauration d'une société fondée sur la surveillance était l'élaboration d'une norme juridique qui soit utilisable tant à l'échelon national qu'au niveau international.

107. Ayant à l'esprit les préoccupations exprimées par le Conseil des droits de l'homme et l'Assemblée générale au sujet du droit à la vie privée, le Rapporteur spécial, en coopération avec le projet MAPPING, a lancé des consultations multipartites, dont les premières ont eu lieu en 2015, à Washington, D.C. En 2016, des ateliers se sont tenus à Malte et à New York. Les éléments de réflexion, prises de position et propositions des participants ont été consignés dans un document qui constitue la première ébauche d'un projet d'instrument juridique et qui peut être utilisé à des fins très diverses, notamment aux fins de l'élaboration de principes directeurs ou comme modèle pour la rédaction d'une loi nationale relative à la surveillance, ou encore comme source de droit contraignant, par exemple pour établir un traité international multilatéral sur la surveillance.

108. Encouragés par l'appui reçu dans le cadre du Forum international de contrôle des services de renseignement, le Rapporteur spécial et les responsables du projet MAPPING ont poursuivi les consultations conjointes sur les nouvelles mesures à prendre en droit international pour améliorer la protection de la vie privée compte tenu de l'accroissement de la surveillance, et pour jeter les bases communes d'un contrôle efficace des pratiques mondiales en matière de surveillance.

2. Élaboration par un groupe d'experts

109. Un projet révisé a été établi en mars 2017, à la suite d'une réunion commune avec le groupe de travail sur la gouvernance d'Internet et la surveillance chargé de l'ensemble de tâches n° 4 (Work Package 4) du projet MAPPING, tenue à Miami (États-Unis) en février 2017.

110. L'idée d'élaborer un instrument juridique ayant reçu un accueil favorable, le Rapporteur spécial et les responsables du projet MAPPING ont mené de nombreuses consultations dans le monde entier en 2017. En mai 2017 à Malte et en septembre 2017 à Paris, un groupe de travail composé d'experts de la société civile, de responsables du projet MAPPING et de grandes entreprises d'Internet a tenu des ateliers, auxquels quelque 50 experts ont participé, sur le projet d'instrument juridique sur la surveillance. L'atelier organisé à Paris a été suivi d'une consultation auprès de professionnels du maintien de l'ordre, qui s'est déroulée le 15 septembre 2017 au siège de l'Organisation internationale de police criminelle (INTERPOL) à Lyon (France).

111. Les résultats des réunions tenues à Paris et à Lyon et le projet d'instrument révisé ont été diffusés à l'occasion du Forum international de contrôle des services de renseignement, tenu les 20 et 21 novembre 2017 à Bruxelles. Cela a permis aux autorités de contrôle du renseignement et aux professionnels du renseignement de commenter le projet d'instrument juridique ainsi que l'idée d'instaurer un collège international de juges et un mandat international d'accès aux données.

112. Ces consultations, et d'autres activités, ont permis de produire un texte suffisamment abouti pour faire l'objet d'une consultation publique plus large, en 2018. Le projet d'instrument juridique a donc été publié en ligne début janvier 2018, en même temps que le premier débat public, tenu du 17 au 19 janvier 2018 à Rome.

113. Le texte actuel du projet d'instrument juridique sur la surveillance exercée par les États et la vie privée énonce des principes généraux et les prescriptions fondamentales

découlant de ces principes, et couvre les questions relatives à son application, à sa portée, aux droits qu'il protège, aux systèmes et aux données, à la collaboration multipartite et aux mécanismes permettant un accès transfrontières aux données à caractère personnel (voir l'appendice 7 au présent rapport).

3. Pistes préliminaires de réflexion pour un instrument juridique international s'inscrivant dans la gouvernance d'Internet

114. Il ne fait aucun doute que la communauté internationale doit prendre d'urgence des mesures pour garantir le respect et la mise en œuvre effectifs de l'article 12 de la Déclaration universelle des droits de l'homme et de l'article 17 du Pacte international relatif aux droits civils et politiques en élaborant un cadre juridique clair et complet sur la vie privée et la surveillance dans le cyberspace, afin de traduire au niveau opérationnel le respect de ce droit, à l'échelon national et au-delà des frontières. Le droit international des droits de l'homme énonce des règles universelles de haut niveau pour protéger le droit à la vie privée, mais ses dispositions ne sont pas suffisamment détaillées pour constituer le cadre juridique complet nécessaire pour assurer une protection adéquate dans de nombreux contextes, notamment celui de la surveillance nationale et extraterritoriale. Dans la plupart des régions du monde, il n'existe pas de mécanismes de mise en œuvre comparables à ceux qui ont été élaborés au cours des quarante dernières années en Europe et en Amérique du Nord. Le cadre juridique international envisagé devrait donc être beaucoup plus détaillé, clair et complet, prévoir des garanties et des voies de recours contre les violations du droit à la vie privée commises quotidiennement dans le cyberspace. Le diable est dans les détails.

115. Le projet d'instrument juridique a été largement salué pour son caractère visionnaire et exhaustif. D'importants acteurs ont exprimé le vœu de voir son élaboration se poursuivre. À l'occasion des récentes consultations organisées conjointement à Rome (les 18 et 19 janvier 2018) par le Rapporteur spécial et les responsables du projet MAPPING, des observations importantes ont été formulées :

a) Les travaux menés à ce jour ont permis de recenser les problèmes et de définir des normes et des voies de recours possibles en matière de surveillance dans le cyberspace. Ces résultats devraient être rendus publics afin qu'ils puissent être utilisés pour enrichir la réflexion et le débat sur le sujet et que les États membres qui envisagent actuellement d'instaurer une législation et de prendre des dispositions institutionnelles en vue de garantir un contrôle efficace des activités de renseignement puissent s'en servir comme projet de modèle ;

b) Sous sa forme actuelle, le projet aborde un grand nombre de questions, et il y aurait des avantages stratégiques et tactiques à le conserver tel quel, mais le diviser pour en faire au moins deux instruments moins longs et de portée plus réduite pourrait en faciliter l'adoption ;

c) Il est nécessaire d'élaborer les stratégies qui seront nécessaires sur le court terme et à plus long terme pour obtenir un large soutien et garantir la viabilité de l'instrument envisagé ;

d) Les enseignements suivants ont été tirés de l'élaboration d'autres instruments juridiques dans le système des Nations Unies :

i) La constitution d'un consensus international autour d'un instrument juridique est un processus long ;

ii) Les États membres à titre individuel, les groupes régionaux et les alliances interrégionales peuvent tous jouer un rôle décisif dans l'adoption d'un instrument juridique ;

iii) Les organisations de la société civile ont un rôle capital à jouer pour promouvoir l'adoption des instruments juridiques internationaux ;

iv) Même les initiatives les plus louables se heurtent initialement à des résistances.

e) Indépendamment des travaux du Rapporteur spécial, le projet MAPPING présentera le texte actuel du projet d'instrument juridique dans la note d'orientation et feuille de route sur la gouvernance d'Internet qui sera soumise d'ici au 30 avril 2018 à la Commission européenne, puis au Parlement européen et au Conseil européen. L'Union européenne pourrait être le groupe régional le mieux à même d'appuyer un instrument juridique sur la surveillance et la vie privée au niveau mondial ;

f) Il ressort des débats préliminaires que l'intérêt suscité par le projet d'instrument juridique est plus fort en Amérique latine et en Afrique, mais cette observation appelle un examen et des recherches plus approfondis ;

g) Les informations en retour reçues des parties prenantes ayant participé aux consultations successives ont montré que :

i) Les organes de répression régionaux et mondiaux, notamment l'Agence de l'Union européenne pour la coopération des services répressifs (Europol) et INTERPOL, ont manifesté un vif intérêt pour un grand nombre des dispositions du projet d'instrument juridique, même s'ils ont aussi indiqué qu'il leur faudrait beaucoup de temps (deux ou trois ans) pour mener des consultations internes plus approfondies ;

ii) Les fédérations de barreaux et les avocats participant à la défense de militants dans des affaires portant sur le droit à la vie privée appuient fermement le projet d'instrument juridique, y compris les mécanismes proposés, tels que le mandat international d'accès aux données ;

iii) Les entreprises ont manifesté pour le projet d'instrument juridique un intérêt d'autant plus fort que celui-ci reprend les principes qui ont été publiquement approuvés par la Reform Government Surveillance coalition²⁹ ;

iv) Les services de renseignement signalent qu'il existe des pays dans lesquels la législation est déjà conforme à 90 % au texte actuel du projet d'instrument juridique. Des travaux supplémentaires sont nécessaires en ce qui concerne la définition de la surveillance ciblée et l'application limitée de la surveillance de masse pour qu'elle soit plus facile à appliquer et mieux adaptée ;

v) Les préoccupations de la société civile ont trait essentiellement au calendrier, au risque que certains États détournent le texte pour affaiblir les protections qu'il instaure, et à la formulation du texte ;

vi) L'Europe attend l'issue de certaines affaires dont sont saisies la Cour de justice de l'Union européenne et la Cour européenne des droits de l'homme (CEDH), qui devraient statuer fin 2018 ou en 2019. Les arrêts prononcés pourraient renforcer l'intérêt des groupes d'États européens pour le projet d'instrument juridique, mais ces affaires freinent pour l'instant toute progression vers un consensus. Cette situation pourrait ne pas évoluer avant 2019 ou 2021.

4. Recommandations portant spécifiquement sur la surveillance

116. Le Conseil des droits de l'homme devrait examiner le contenu de l'appendice 7 afin de définir les questions et les solutions que l'on pourrait envisager d'inclure dans un futur instrument juridique international sur la vie privée et la surveillance.

117. Les États membres intéressés par l'élaboration d'un instrument juridique renforçant les voies de recours et les solutions conformément à ce qui est proposé dans l'appendice 7 devraient prendre contact avec le Rapporteur spécial afin d'étudier plus avant les moyens de renforcer l'application de ces principes aux échelons national, régional et international.

118. Compte tenu des échéances évoquées ci-dessus, le Rapporteur spécial propose de soumettre au Conseil des droits de l'homme en mars 2021 un rapport contenant de nouvelles recommandations, sous réserve que cette date soit jugée adéquate et opportune.

²⁹ Voir www.reformgovernmentsurveillance.com.

C. Capacité du Rapporteur spécial de soumettre des communications individuelles

119. David Weissbrodt a décrit les réactions qu'avait suscitées le premier Rapporteur spécial thématique (sur les exécutions extrajudiciaires, sommaires ou arbitraires) lorsqu'il avait appelé l'attention d'un État sur une affaire. Le gouvernement concerné avait mis en doute la capacité du Rapporteur spécial de lancer des appels³⁰.

120. Dans son rapport à la Commission des droits de l'homme, le Rapporteur spécial sur les exécutions extrajudiciaires, sommaires ou arbitraires a écrit qu'il estimait que cette question méritait un plus ample examen et qu'il saurait gré à la Commission des conseils qu'elle pourrait lui fournir à ce sujet³¹. Dans l'affaire visée, on notera que non seulement la Commission a renouvelé le mandat du Rapporteur spécial concerné à ses sessions annuelles suivantes, mais aussi que, comme l'avait dit le représentant de la Norvège, il est permis de conclure que la Commission a considéré que les cas visés relevaient du mandat du Rapporteur spécial, lequel devrait en rendre compte dans ses prochains rapports (la Norvège était le principal auteur de la résolution sur cette question)³².

121. Le Rapporteur spécial a eu une expérience similaire. En 2017, à deux reprises sa capacité d'appeler l'attention des États sur des affaires a été mise en doute. Adresser des communications à des États membres et à d'autres parties prenantes fait partie des activités essentielles de tous les titulaires de mandat au titre des procédures spéciales. Cette procédure, qui a été abondamment décrite et qui est bien réglementée, permet à tous les titulaires de mandat de s'entretenir directement avec les gouvernements et d'autres parties prenantes d'allégations de violation des droits de l'homme relevant de leur mandat en leur adressant des courriers, pouvant contenir des appels urgents ou faire état d'allégations³³.

122. La décision prise par le Rapporteur spécial d'intervenir dans l'affaire concernant la photographie prise sans autorisation (voir par. 84 ci-dessus) était conforme à la résolution du Conseil des droits de l'homme définissant son mandat, dans laquelle le Conseil a expressément demandé aux États de répondre rapidement aux appels urgents et autres communications du Rapporteur spécial.

III. Conclusions

123. **Le Rapporteur spécial a utilisé pour promouvoir et protéger la vie privée les moyens habituellement employés par d'autres rapporteurs spéciaux, et a notamment adressé aux États des appels urgents et des lettres concernant des allégations, donné suite à des plaintes individuelles, participé à des conférences et mené des visites de pays, officielles et non officielles.**

124. **Le Rapporteur spécial a également innové dans les méthodes employées pour s'acquitter de son mandat, notamment en créant un Forum international de contrôle des services de renseignement, qui se réunit chaque année, en organisant des manifestations régionales bisannuelles sur le droit à la vie privée, la personnalité et la circulation de l'information (dont certaines se sont déjà tenues en Amérique du Nord, au Moyen-Orient et en Afrique du Nord, ainsi qu'en Asie, et la prochaine est prévue en Amérique latine), et en créant des équipes spéciales sur les mégadonnées et les données ouvertes, les données de santé, et le droit à la vie privée et la personnalité, afin d'inscrire l'examen des questions se rapportant à la vie privée dans une vision mondiale plus large.**

125. **Conscient de la gravité de la menace que représente la surveillance pour l'exercice du droit à la vie privée, le Rapporteur spécial codirige les travaux menés au**

³⁰ David Weissbrodt, « The three "Theme" Special Rapporteurs of the UN Commission on Human Rights », *American Journal of International Law*, vol. 80, n° 3 (juillet 1986), p. 685 à 699.

³¹ E/CN.4/1986/21, p. 100.

³² Résolution 1986/36 du Conseil économique et social.

³³ Procédures spéciales du Conseil des droits de l'homme : voir www.ohchr.org/EN/HRBodies/SP/Pages/Welcomepage.aspx.

niveau international en vue d'établir un cadre juridique international complet pour réglementer la surveillance dans le cyberspace et, ainsi, améliorer les perspectives pour l'instauration de la cyberpaix.

126. Les procédures spéciales constituent un important mécanisme, sur lequel le Conseil des droits de l'homme s'appuie pour assurer la mise en œuvre des règles relatives aux droits de l'homme et élaborer des normes³⁴. En poursuivant l'élaboration de normes internationales relatives à la surveillance exercée par les États, la communauté internationale se donne les moyens d'orienter et d'évaluer l'utilisation des technologies et des pratiques dans ce domaine. Les normes se rapportant aux bonnes et aux meilleures pratiques sont régulièrement examinées dans le cadre du Forum international de contrôle des services de renseignement.

127. Le Rapporteur spécial pense qu'un instrument juridique réglementant la surveillance dans le cyberspace qui compléterait d'autres instruments juridiques en la matière tels que la Convention sur la cybercriminalité du Conseil de l'Europe pourrait permettre la création de garde-fous concrets pour protéger le droit à la vie privée sur Internet (A/HRC/34/60 et A/72/540) et résoudrait aussi des problèmes qui se posent depuis longtemps, notamment celui de la compétence dans le cyberspace. Les travaux réalisés jusqu'à ce jour sont très fructueux et encourageants, mais la forme et le libellé actuels de l'instrument juridique ne suscitent pas encore un soutien suffisamment uniforme pour qu'une recommandation soit adressée au Conseil des droits de l'homme aux fins de l'examen immédiat du projet d'instrument juridique dans son état actuel. Toutefois, moyennant des efforts et du temps supplémentaires, un instrument viable pourrait être soumis au Conseil dans un avenir relativement proche, peut-être même d'ici à 2021.

128. Les titulaires de mandat au titre des procédures spéciales sont des experts indépendants et représentent un important mécanisme de protection des droits de l'homme. Les États membres doivent accepter pleinement les communications qu'ils leur adressent ainsi que les procédures d'enquête, offrir leur coopération et cesser de remettre en question la légitimité des critiques constructives qu'ils formulent.

IV. Recommandations au Conseil des droits de l'homme

129. Le Conseil des droits de l'homme devrait prendre note des résultats obtenus par le Rapporteur spécial dans le cadre de son mandat grâce aux lignes d'action thématiques, de la conformité de ces résultats au plan présenté dans le premier rapport du Rapporteur spécial au Conseil, des étapes à venir – notamment la proposition d'un thème supplémentaire, celui de la vie privée des enfants – et du calendrier des prochains rapports sur les lignes d'action thématiques.

130. Le Conseil devrait prendre note des progrès accomplis dans l'élaboration de normes internationales relatives à la surveillance exercée par les États, de la mesure novatrice et utile qu'a constitué la création du Forum international de contrôle des services de renseignement, et de l'intention d'élaborer à moyen terme un instrument qui pourrait être examiné par les Nations Unies et dont les États membres et d'autres parties prenantes intéressées pourraient le cas échéant parachever l'élaboration.

131. Le Conseil devrait recommander à l'Assemblée générale de donner une vigueur nouvelle à tous les efforts déployés par l'ONU pour étudier, dans le cadre de rapports de synergie avec le Rapporteur spécial sur le droit à la vie privée, les points d'intersection entre la vie privée et la sécurité et le comportement des États dans le cyberspace, afin de s'employer résolument à élaborer un cadre juridique complet sur Internet.

³⁴ Weissbrodt, « The three "Theme" Special Rapporteurs ».

V. Documents complémentaires

132. Faute d'espace, les documents ci-après ont été publiés sur le site Web du Rapporteur spécial :

- Appendice 1 : Mandat du Rapporteur spécial sur le droit à la vie privée
http://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2018AnnualReportAppendix1.docx
- Appendice 2 : Graham Greenleaf, Data Privacy Laws 2017 : 120 National Data Privacy Laws, including Indonesia And Turkey
http://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2018AnnualReportAppendix2.docx
- Appendice 3 : Communications du Rapporteur spécial sur le droit à la vie privée
http://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2018AnnualReportAppendix3.docx
- Appendice 4 : Rapport intérimaire et recommandations préliminaires de l'équipe spéciale sur les lignes d'actions thématiques concernant les mégadonnées et les données ouvertes
http://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2018AnnualReportAppendix4.docx
- Appendice 5 : Contributions à des manifestations internationales de 2015 à 2017
http://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2018AnnualReportAppendix5.docx
- Appendice 6 : Mémoire d'*amicus curiae* à la Cour suprême des États-Unis d'Amérique dans l'affaire *United States v. Microsoft Corporation*.
http://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2018AnnualReportAppendix6.pdf
- Appendice 7 : Projet d'instrument juridique sur la surveillance exercée par les États
http://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2018AnnualReportAppendix7.docx
- Appendice 8 : Remerciements
http://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2018AnnualReportAppendix8.docx

Annexe

[Anglais seulement]

Paper presented at Expert workshop on the right to privacy in the digital age

Office of the High Commissioner for Human Rights

Geneva, 19–20 February 2018

1. Privacy is a fundamental human right recognized as such under international law. It is also a universal right, one which should be enjoyed everywhere by everybody, as such it should be respected everywhere by everybody, by States as well as by non-State actors, irrespective of the ethnicity, nationality, gender, religious, philosophical or political beliefs of any given individual or any other status. The recognition of the universal right to privacy is part of the set of fundamental norms established in the development of human rights law since World War II.

2. Due to its complexity, the right to privacy requires a comprehensive legal framework in order to operationalize it in a number of different contexts. These contexts may be as diverse as medical and health, insurance, statistics, national security, finance, police, social security, education and many others. Each context brings with it the need of a detailed and constantly up-dated understanding of how privacy could be threatened within that particular context and an identification of safeguards that protect it, and remedies available to citizens which may be specific to that context. The devil, literally, is in the detail, and privacy requires very detailed rules which spell out the level and modes of protection that privacy may be accorded in a particular context as well as the remedies that a citizen may resort to if his or her privacy is breached in that context. The importance of this level of detail is even greater in the case of privacy since there exists no universally accepted definition of privacy. In other words, people across the world have agreed that the right to privacy exists and that everybody is entitled to such a right but they have not spelt out precisely what the right is or what it entitles a person to in a wide variety of circumstances. This fact has both advantages and disadvantages: too narrow a definition of privacy would restrict its ability to be protected as circumstances and privacy-threats change and also as we develop our understanding of what constitutes privacy-infringing behaviour in a number of changing or new contexts.

3. The rules and remedies provided for at national law come together with those established under international law to constitute the international legal framework available for the protection of privacy. Those at the national level are most often to be found in an amalgam of principal and subsidiary legislation complemented by the case law of that particular country. The courts of all countries and especially those with constitutional competences interpret the extent — and occasionally the limits — of the right to privacy in accordance with their understanding of that country's constitution, the national law on privacy — if it exists — as well as, often enough, the precepts of international law on the subject. Very importantly, over the past forty years we have witnessed a huge growth in the impact of international law on national law in the sphere of privacy protection. We have seen the concerted development of international law at the regional level, most notably in Europe, which has then guided the development of national law and practices in diverse contexts where privacy may be threatened.

4. Moreover, privacy is not an absolute right. It is a qualified right. There exist a small number of very special occasions when limitations to the right to privacy may be introduced subject to a number of special measures which are normally best spelt out under international law as well as necessarily having a clear legal basis in domestic law. Some of these will be explored below in the context of security. The way that the right to privacy is qualified needs to be spelt out in great detail in a given context. If limitations to the right to privacy are not adequately defined the gaps in privacy protection will increase.

5. An additional but essential overall consideration is that constantly developing technologies pose important challenges for the protection of privacy: these technologies may reveal the most intimate behaviour, wishes, preferences and indeed the very thoughts of individuals in ways that previously were not possible. Smartphones, credit cards and the Internet are three good examples of the types of technology that bring significant new challenges to the protection of privacy.

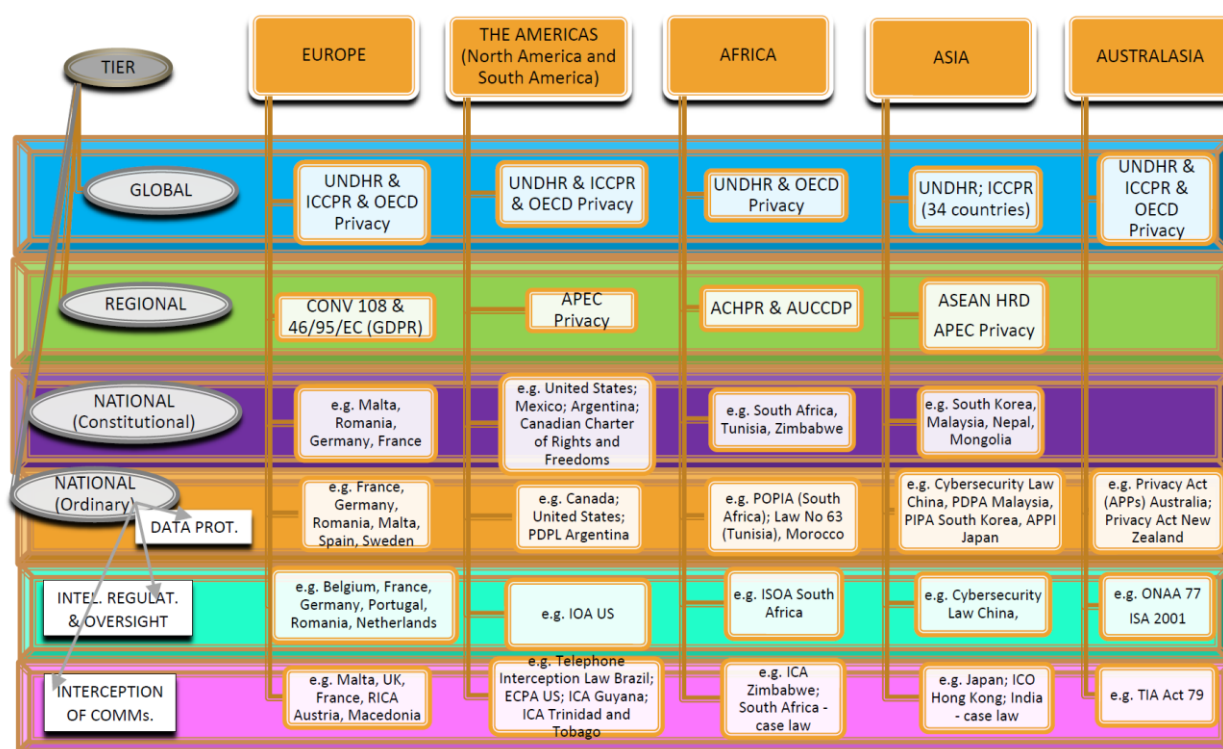
6. When dealing with technologies such as the Internet it is simplistic and naïve to be content with a statement that “whatever is protected off-line is protected on-line”. That is a hopelessly inadequate approach to the protection of privacy in 2018. International law such as Art. 12 UDHR and Art 17 ICPPR only provides an answer to the question “Why?” as in “Why should we protect privacy” i.e. because we have agreed that it is a universal fundamental human right. They however do not provide answers to the questions: When? Which? What? How? Who? When should privacy be protected? How should privacy be protected? Which are the privacy-relevant safeguards to be created in a particular context? Which new contexts pose the greatest risks to privacy? What should be done to protect privacy in given circumstances? Which are the remedies most appropriate and possible in those cases where, despite all the safeguards provided, a breach of privacy still occurs? Who has special duties and obligations in the case of privacy protection, in which circumstances, what measures are the minimum to discharge these obligations and how should such persons be held accountable? The answers to these and other questions can only be found if the international and national legal framework is detailed enough.

7. Over the past fifty years some countries and some inter-governmental organizations have taken the initiative to develop their legal framework with respect to privacy but others have not. As a consequence, in 2018 more than a third of United Nations Member States have no privacy laws at all¹ while most of the other 125 states have laws which cover some of the contexts where privacy may be threatened but not all. Some important threats to privacy especially those arising in the context of national security, intelligence and surveillance are inadequately regulated in most countries of the world. International law, especially in the form of some regional initiatives, helps provide a level of co-ordinated response to some privacy threats for some countries but these remain, at best, a significant minority. The result is a patchwork quilt, in many places crocheted in stitches which are far too open to keep in the warmth and which, in any case, is not large enough to cover all of the bed. This patchwork quilt can in no way be characterized as a comprehensive and sufficiently detailed legal framework through which persons anywhere and everywhere can enjoy the universal right to privacy. It is the duty of the Special Rapporteur on the right to privacy, in conformity with his mandate, to identify the lack of a comprehensive, detailed and universal legal framework as a serious obstacle to the protection of the right to privacy world-wide. The rest of this paper, for reasons of time and space, mostly focuses on the lack of an adequate legal framework in two often-related contexts: national security and the prevention, detection, investigation and prosecution of crime but this is not to say that all other contexts are well served by the international legal framework.

The current international legal framework

8. The diagram below attempts to sketch out the international legal framework for the protection of privacy which exists so far:

¹ Though this does not exclude the possibility that their constitutional courts could be seized of privacy-related matters.



9. The diagram above is intended primarily to illustrate the tiered structure of the international legal framework but limitations of space do not permit one to clearly see that the tiers in Asia and Africa contain many more gaps and vacant spaces than those in Europe and North America. These gaps are however summarized in the overview text below.

Gaps in protection from government-led surveillance.

10. The surveillance of citizen behaviour on the internet can be broadly categorized into two main types: Government-led surveillance, and, surveillance or monitoring of citizens behaviour by private corporations that track citizens browsing, purchasing and other activities on the internet.

11. This overview analysis is focused on Government-led surveillance and the gaps in protection which currently exist in the international legal framework.

12. The surveillance and/or monitoring and/or profiling of citizens by corporations will be the subject of a separate report.

What do we understand by a comprehensive legal framework?

13. A comprehensive legal framework protecting citizens' privacy in cyberspace is one which provides both safeguards and remedies for all facets of the citizens' presence in cyberspace, irrespective of the fact if the threat to privacy comes from inside that citizen's country or from outside it.

14. Tension has continued to build up in cyberspace, with the privacy of many responsible citizens being put at risk by the behaviour of State actors in the form of cyber-surveillance, cyber-espionage and elements of cyber-war.

Problem Statement

15. In cyberspace, the citizen may be surveyed in both a domestic situation by his or her own Government, or else in a transboundary/transnational situation by a Government which is not his/her own. The case studies referenced below outline a fraction of some of the ways in which a citizen in one country finds him/herself subject to infringement of their privacy by their own Government or another State actor.

16. Where a citizen is subject to surveillance by his/her own Government then the safeguards and remedies must normally be sought within domestic law. Where a citizen is subject to surveillance by a State which is not his own, obligations of both the State conducting the surveillance and the State where that person is physically located are relevant; yet a remedy becomes harder to seek, because in practice most states accord the citizens of other States a lower level of protection than that accorded to their own citizens, in breach of the prohibition of discrimination found in articles 4, and 26 of the ICCPR.

17. For individuals not to suffer interferences in their right to privacy, they firstly need to benefit from safeguards which exist within domestic law, in other words, their Government should be subject to a whole set of regulatory procedures provided for by the law of that State, and which would include precautionary measures designed to ensure that surveillance cannot be initiated until or unless, it is proven to an independent and competent authority that this surveillance is legal, necessary and proportionate to objective pursued, “solely for the purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society” (UDHR, Art. 29(2)).

Summary overview of protection gaps

18. In summary: the United Nations has 193 sovereign Member States and two non-member observer States, all of them capable of having their own independent systems/structures such as domestic legislation and data protection authorities.

19. More than 33 percent of United Nations Member States, i.e. over 70 countries, have no privacy law at all.

20. Out of the remaining 125 United Nations Member States which do have one form of privacy law or another, (for an outline of these states please see article by Professor Graham Greenleaf in Appendix Two attached) less than 65 have certain key fundamental characteristics such as a truly independent data protection authority or truly strict enforceable safeguards and remedies. Thus, these laws are not homogeneous and the level of protection of privacy differs quite widely from one country to the next.

21. The types of laws mentioned in Graham Greenleaf’s article are mostly those intended to cover the use of personal data by companies or state departments outside the law enforcement and national security sector. Most of them are therefore not intended to adequately and comprehensively cover the use of surveillance by intelligence agencies.

22. More than 80 percent of the United Nations Member States do not have any law which protects privacy by adequately and comprehensively overseeing and regulating the use of domestic surveillance.

23. 100 percent of existing State legislations concerning the oversight of domestic intelligence within United Nations Member States require amendment and reinforcement.

24. 75 percent of United Nations Member States have no system of detailed safeguards or remedies to which they can readily turn to for cases of surveillance upon their citizens by other states. Even where remedies for citizens exist within the courts of those States, these courts often lack jurisdiction over the surveillance behaviour of other State actors.

25. 25 percent of United Nations Member States — those within the European region encompassed by the Council of Europe, have agreed to a basic principle in the application of privacy law to state security: by agreeing to Article 9 of Convention 108 they have accepted that measures can only limit the right to privacy where these measures are provided for by law and are necessary and proportionate in a democratic society.

26. This however means that it is only the very highest principles that have been agreed to, even in European states with more developed legislation on the right to privacy and this is mostly applied in the case of domestic intelligence. The situation relating to foreign intelligence is much more fluid, elastic. What actually constitutes a necessary and proportionate measure in a democratic society then needs to be translated into very detailed legislation and this is still very much work-in-progress all across Europe. Belgium, the Netherlands and the United Kingdom are some of the European states currently reviewing

their legislation in order to improve compliance with basic principles in a detailed manner. France has done so in 2015 but intends to re-visit its legislative framework in the near future.

27. Even where legislation exists regarding the oversight of intelligence it is often largely silent on what happens when personal data is shared across borders and what further safeguards should be put in place in such cases.

28. In the absence of more detailed regulation, several United Nations Member States have to rely on their existing legislative and judicial frameworks, often at the national constitutional or the regional level in order to develop remedies and safeguards on the hoof. This works slowly but relatively well at the European levels where the European Court of Justice and the European Court of Human Rights often have pan European reach with their judgments about surveillance and privacy.² This however is not a completely satisfactory solution since it is one ex post. Very preferably citizens wish to have their privacy protection provided ex ante and this, especially to protect themselves against or minimize intrusion. In order to resolve problems of jurisdiction in cyberspace, this can be only provided by detailed international law which does not yet exist in the surveillance sector, including in the European region. If the remedies are unclear and imperfect in Europe where the European Court of Human Rights has relatively worked well with over 100,000 cases decided since it was established in 1959, the situation outside Europe is even more concerning. In the Americas, the Inter-American Court of Justice established in 1979 has cross-country reach, as so has in Africa the recently set-up (2006) African Court for Human and People's Rights. Both courts strive but struggle. The United States signed but never ratified the American Convention on Human Rights and, unlike the European human rights system, individual citizens of Member States of the Organization of American States cannot take their cases directly to the Inter-American Court, having to refer first to the Inter-American Commission on Human Rights. Likewise, only seven African states have signed the protocol empowering their regional court to receive petitions from non-governmental organizations and individuals. These limitations substantially weaken the reach of these regional courts. Moreover, in Asia or the Pacific there is no regional court to turn for infringements of privacy whether caused by domestic intelligence or foreign intelligence.

29. The United Nations Human Rights Committee plays a very important role in the protection of human rights, but once again is largely an ex post forum and cannot be expected to provide in-depth regulation and governance structures, which are the required minimum adequate legal response to questions like transborder data flows and cross-border espionage and surveillance.

² *The Snowden revelations – 6 June 2013 – ongoing reverberations across Europe*

The revelations over mass surveillance and other privacy –intrusive programmes carried out by the signals intelligence arms of the United Kingdom and United States intelligence communities have not really receded. They have been followed by legislative changes in both countries, sometimes imposing more constraints and safeguards, on other occasions legitimizing existing practices. The unilateral nature of transborder forays by United States and/or United Kingdom agencies into Belgium, Brazil, France, Germany and other countries led to a great deal of concern which still finds its reverberations in various fora, international and otherwise. Both countries are still struggling to find the right formula to frame their behaviour in cyberspace such that, for example, the legislative measures of the United Kingdom would be found necessary and proportionate by either the European Court of Human Rights or the European Court of Justice. The United Kingdom's intelligence services were found to be in default on several counts by the UK's own Investigatory Powers Tribunal while the United Kingdom law on bulk collection of metadata has been declared disproportionate by the European Court of Justice on the 21st December 2016. An important decision in this respect is also being expected in a case first heard by the European Court of Human Rights on 7th November 2017, *Big Brother Watch and Others v. the United Kingdom* (no. 58170/13), *Bureau of Investigative Journalism and Alice Ross v. the United Kingdom* (no. 62322/14) and *10 Human Rights Organisations and Others v. the United Kingdom* (no. 24960/15).

30. In order to better understand the protection needs in the privacy area, one has to take the Yahoo cases³ cited below and ask “which ex ante safeguards should have been applied by which country in order to protect citizens in, say France, from having their Yahoo e-mail account privacy infringed and what ex post remedies are available to that same French citizen?” The answers to these questions can only be provided by a detailed international law regime which has yet to be worked out. The Human Rights Committee’s interpretative advice of ICCPR’s article 17 should be a last resort; it cannot be the primary mechanism designed to protect the privacy of billions of people who use the Internet on a daily basis.

³ The following two cases are being cited for purposes of illustrating a problem area but are not here being represented as facts proving certain types of behaviour by the United States or Russian authorities. The Special Rapporteur on the right to privacy reserves the right to investigate these cases separately through Letters of Allegation and until doing so remains neutral on the accuracy or otherwise of media and governmental reports on the subject:

Case 1: Privacy of 500 million Yahoo! users infringed – 15 March 2017

Formal indictments were brought in the United States of America by the Justice Department, which announced on 15 March 2017 that the “indictments of two Russian spies and two criminal hackers in connection with the heist of 500 million Yahoo user accounts in 2014, marking the first United States criminal cyber charges ever against Russian government officials. The indictments target two members of the Russian intelligence agency FSB, and two hackers hired by the Russians. The charges include hacking, wire fraud, trade secret theft and economic espionage, according to officials.”

While this case remains sub judice and therefore the evidence available has not yet had time to be exhaustively evaluated by the court in question, the nationality of the accused and the locus of the judicial proceedings are almost immaterial for the purposes of this observation. The point here is that the spread of the damage was global, possibly the largest or one of the largest intrusions in history on the private e-mail accounts of five hundred million Yahoo! users spread across the planet. If it transpires that the men indicted were not responsible after all, we are still left with the problem of the nature and scale of the attack in addition to the instability induced by public accusations made against Russia. If the guilt of the accused is eventually proved beyond reasonable doubt then the problem would be compounded by the involvement of state officials who may or may not have been acting on instructions. Either way the suspicion of their acting as agents of the Russian state is already a destabilising factor in international relations and threatening all forms of peace, above and beyond cyber-peace. The violation of the personal space of hundreds of millions of internet users has not, to date, attracted much attention but it remains a source of major concern to those involved, over and above the charges actually made in the indictment.

Case 2: Privacy of 500 million (?) Yahoo! users breached by United States agency (reported 4th October 2016)

If you’re a Yahoo! e-mail user, if it’s not one government hacking into your e-mail account or scanning your incoming e-mail, then it’s another. Or at least un-contradicted media reports so suggest. For some time during the period 2014–2016, hundreds of millions of Yahoo! e-mail users apparently not only suffered the most massive hack in history as already mentioned above (allegedly by a combination of Russian criminal and state-connected persons) but also had their incoming mail scan-read on the orders of a United States Government agency. There are multiple causes for concern here. Firstly, all those Yahoo! users within the United States may arguably claim that such searches violated their Fourth Amendment rights under the United States constitution, although the scan-reading was carried out in terms of lower-level United States law (FISA). Secondly, it should be clear to all concerned that well more than half of those five hundred million Yahoo users are not United States citizens and would need to seek recourse elsewhere for protection of their fundamental and universal right to privacy...but where to do so is the obvious question. Even if this were ever to be considered a proportional measure – and that is a contentious point in its own right, unless there were to be an international agreement that this would constitute appropriate state behaviour in cyberspace, hundreds of millions of citizens world-wide yet again find themselves without any effective safeguards or remedies when it comes to their fundamental right to privacy.

31. Thus it should be glaringly evident from the above summary that huge gaps exist in the legal protection of privacy at both the national and international levels. Unless and until it will be possible for any citizen, anywhere, irrespective of passport held, to enjoy privacy protection without borders and privacy remedies across borders, then it cannot be said that “a clear and comprehensive legal framework exists”. In order to create such a clear and comprehensive legal framework it is essential that an international legal regime regulating issues of jurisdiction in cyberspace be properly developed, with a commonly agreed set of principles to establish what state behaviour in cyberspace and that especially related to surveillance and cyber-espionage, is acceptable, why and when.
