



Assemblée générale

Distr. générale
6 septembre 2017
Français
Original : anglais

Conseil des droits de l'homme

Trente-quatrième session

27 février-24 mars 2017

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 le présent rapport, élaboré en application de la résolution 28/16 du Conseil des droits de l'homme, le Rapporteur spécial sur le droit à la vie privée aborde la question des activités de surveillance étatique sous l'angle national comme sous l'angle international. Il examine de manière approfondie les caractéristiques du cadre juridique international applicable et l'interprétation qui en est faite. Il décrit aussi les faits nouveaux et les tendances récemment observées, les moyens de les analyser et leur incidence sur l'exercice du droit à la vie privée et d'autres droits de l'homme interdépendants. Il esquisse ensuite des approches préliminaires de la surveillance étatique plus respectueuses de la vie privée. Pour conclure, le Rapporteur spécial rend compte des activités qu'il a menées à bien durant la période visée par le présent rapport.

* Le présent document est soumis tardivement pour que l'information la plus récente puisse y figurer.



Rapport du Rapporteur spécial sur le droit à la vie privée

Table des matières

	<i>Page</i>
I. Introduction	3
II. Faits nouveaux et tendances inquiétantes en matière de surveillance étatique.....	6
A. Surveillance étatique et vie privée à l'ère numérique : le statu quo.....	6
B. Défis à relever et tendances inquiétantes	9
III. Premières approches de la surveillance étatique plus respectueuses de la vie privée.....	11
A. Tour d'horizon complet des approches et des questions en jeu	11
B. Examen des questions en jeu	11
IV. Activités du Rapporteur spécial	13
V. Conclusions et recommandations	14

I. Introduction

1. Conformément à la résolution 28/16 du Conseil des droits de l'homme, le Rapporteur spécial sur le droit à la vie privée fait chaque année rapport au Conseil et à l'Assemblée générale. Le présent rapport est le deuxième qu'il soumet au Conseil. Dans son rapport précédent, le Rapporteur spécial avait énoncé un plan d'action en 10 points et une stratégie pour s'attaquer à certains problèmes cruciaux relevant de son mandat en menant des activités appelées « Lignes d'action thématique ». Par ces initiatives, le Rapporteur spécial espère contribuer à élever le niveau de respect, de protection et de réalisation du droit à la vie privée, que l'ère numérique et les changements qu'elle entraîne mettent à rude épreuve.

2. Le Rapporteur spécial a récemment publié une déclaration intitulée « Planned thematic reports and call for consultations » (Rapports thématiques prévus et appel à consultations), dans laquelle il a répertorié les sujets à traiter dans les rapports présents et à venir et a fixé un calendrier pour la soumission de ses rapports¹. Cette déclaration devrait être considérée comme une invitation permanente adressée à toutes les parties prenantes, dans tous les pays du monde, désireuses de s'associer à ses travaux. Quiconque souhaite contribuer ou être associé à l'une quelconque des initiatives mentionnées est invité à contacter, de préférence par courrier électronique (srprivacy@ohchr.org), le Rapporteur spécial ou les membres de son équipe, qui répondront dès que possible.

3. Comme indiqué plus haut, dans le présent document, le Rapporteur spécial s'intéresse essentiellement aux approches préliminaires de la surveillance étatique plus respectueuses de la vie privée. Il a déjà mené à bien plusieurs activités autour de ce thème au cours de son mandat et continuera à travailler dans ce sens. Ayant à cœur de s'acquitter des tâches qui sont les siennes et qu'il avait présentées dans son précédent rapport (A/HRC/31/64), tout particulièrement dans le secteur de la surveillance, il s'est beaucoup investi dans l'organisation du Forum international de surveillance du renseignement, tenu à Bucarest les 11 et 12 octobre 2016. Ce Forum était organisé conjointement par la Commission paritaire de la Chambre des députés et du Sénat pour le contrôle parlementaire du Service de renseignement roumain, la Commission spéciale de la Chambre des députés et du Sénat pour le contrôle parlementaire des activités du Service des renseignements extérieurs et les Commissions de la Chambre des députés et du Sénat pour la défense, l'ordre public et la sécurité nationale, en collaboration avec le Département de la politique de l'information et de la gouvernance de l'Université de Malte et le Groupe de recherche sur la sécurité, la technologie et la vie privée sur Internet de l'Université de Groningen (Pays-Bas). Les objectifs d'une telle manifestation ne pouvaient, on le comprend aisément, qu'être modestes, mais ils ont été largement atteints². Devant un tel succès, le Rapporteur spécial entend coorganiser cet événement chaque année. En 2017, le Forum aura lieu les 20 et 21 novembre à Bruxelles, avec le concours notamment de la Commission pour la protection de la vie privée, autorité belge de protection des données. Le Forum devrait permettre au Rapporteur spécial de remplir sa mission en tirant parti des expériences concrètes et des connaissances opérationnelles acquises par les nombreux organes de surveillance constitués de par le monde. Cela lui permettra de mieux comprendre et analyser les efforts faits pour assurer une surveillance efficace des activités des services de sécurité et de renseignement et des répercussions potentielles sur la vie privée. La première édition du Forum a réuni près de 70 participants, représentant quelque 26 institutions de 20 pays – parmi lesquels des représentants d'autorités indépendantes de surveillance et de

¹ Cette déclaration peut être consultée, en anglais seulement, à l'adresse www.ohchr.org/EN/Issues/Privacy/SR/Pages/ThematicReports.aspx et www.privacyandpersonality.org/2016/12/united-nations-mandate-of-the-special-rapporteur-on-the-right-to-privacy-planned-thematic-reports-and-call-for-consultations/.

² Comme indiqué dans l'invitation officielle adressée aux États, le Forum avait pour objectifs d'engager dans un climat de confiance un débat franc et ouvert sur le caractère adapté ou non des mécanismes de contrôle ; les mesures de surveillance en place et prévues, susceptibles de porter atteinte à la vie privée la distinction entre surveillance ciblée et surveillance de masse ; la question de savoir si les mesures prises étaient proportionnées dans une société démocratique ; le rapport coûts-avantages et l'efficacité générale des mesures visées.

commissions parlementaires, quelques membres de la société civile et même des représentants d'un tribunal de contrôle. Le Rapporteur spécial considère qu'une surveillance mieux pensée et s'appuyant sur davantage de ressources fait partie des nombreux leviers, complémentaires, sur lesquels il est possible de s'appuyer pour améliorer la protection du droit à la vie privée à l'échelle du globe. D'aucuns considèrent même que c'est la voie la plus prometteuse vers des mesures concrètes de protection de la vie privée. Cela reste à démontrer. Il est à souhaiter que les Forums qui se tiendront annuellement contribueront à faire connaître les bonnes pratiques et qu'à terme les mécanismes de surveillance seront considérablement renforcés dans un grand nombre d'États Membres. Il est aussi à souhaiter que les mécanismes de surveillance s'appuieront sur des bases solides, c'est-à-dire sur des législations nationales détaillées et rigoureuses, ne prévoyant que les mesures proportionnées indispensables dans une société démocratique et mettant en place les garde-fous nécessaires. Les législations devraient également prévoir une surveillance efficace aussi bien des services de maintien de l'ordre que des services de sécurité et de renseignement, par des autorités de surveillance indépendantes et dotées de moyens suffisants. À la lumière des débats qui se sont tenus lors des Forums annuels et dans la droite ligne de son mandat, le Rapporteur spécial prévoit de formuler des recommandations visant à garantir la promotion et la protection de la vie privée, notamment au regard des défis posés par les nouvelles technologies.

4. En ce qui concerne la surveillance, le Rapporteur spécial s'est intéressé non seulement aux mécanismes de surveillance mais aussi, dans la mesure du possible, à l'échelle mondiale, aux nouveaux projets de loi applicables et aux rapports consacrés aux bons et mauvais usages de la surveillance. De ce fait, les activités liées à la surveillance comptent parmi ses premières considérations dans ses demandes de visites officielles. Le choix des visites de pays à venir en est une bonne illustration : États-Unis d'Amérique (du 19 au 24 juin 2017), France (visite demandée du 13 au 17 novembre 2017), Royaume-Uni de Grande-Bretagne et d'Irlande du Nord (visite demandée pour fin 2017, éventuellement du 11 au 17 décembre), Allemagne (visite demandée du 29 janvier au 2 février 2018) et République de Corée (visite demandée du 3 au 15 juillet 2018). Ces États sont réputés pour la vigueur de leur démocratie et le Rapporteur spécial attend d'eux qu'ils jouent un rôle de chef de file dans la définition des bonnes pratiques et des garde-fous en ce qui concerne la surveillance et les droits fondamentaux, en particulier le droit à la vie privée. Il s'agit en outre d'États qui ont été particulièrement actifs dans le domaine de la surveillance ces dernières années, sur les plans tant des technologies de surveillance appliquées que de l'adoption de nouveaux textes de loi. Pour chacune de ses visites, le Rapporteur spécial a demandé à rencontrer les services de renseignement et les autorités de surveillance ainsi que les ministres chargés des services de maintien de l'ordre comme des services de sécurité et de renseignement.

5. Pour éviter de « réinventer la roue » et afin d'optimiser les synergies, le titulaire de mandat suit de très près l'avancée et les résultats des initiatives parallèles, telles que 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 »), qui est subventionné par l'Union européenne et qui vise à globaliser les connaissances et à développer une compréhension commune des multiples aspects économiques, sociaux, juridiques et éthiques des évolutions récentes sur Internet et de leurs conséquences pour les individus et pour la société tout entière. Inauguré en 2014, plus d'une année avant que le Conseil des droits de l'homme n'établisse le mandat du Rapporteur spécial et dix-huit mois avant que ce dernier ne prenne ses fonctions, le projet MAPPING a amorcé des débats variés et relativement bien documentés parmi les parties prenantes, notamment quant à la mise au point d'un instrument juridique international qui régirait la surveillance. Les discussions sur ce sujet devraient se poursuivre jusqu'en février 2018. Le Rapporteur spécial compte se tenir au fait de l'issue de ces discussions puis prendre position sur le bien-fondé et la faisabilité d'un tel instrument entre mars et juillet 2018. Il est possible qu'il expose sa position dans son rapport à l'Assemblée générale, en octobre 2018, et probable qu'il formule de nouveau des recommandations à cet égard afin de promouvoir et de protéger la vie privée, notamment à la lumière des enjeux nés des nouvelles technologies qui relèvent de son mandat.

6. Le Rapporteur spécial travaille également en liaison et en collaboration avec d'autres entités et individus, dont les initiatives visent à introduire un cadre cohérent de coordination internationale de la surveillance du renseignement. Au cours de ces dix-huit derniers mois, un travail acharné lui a permis de nouer ou d'approfondir des relations de travail nombreuses et fructueuses dans le monde entier, et plusieurs autorités se sont montrées désireuses de travailler sur un instrument, encore à définir, qui énoncerait des normes communes en matière de surveillance des transmissions dans le cadre du renseignement extérieur. Ce sont là des évolutions bienvenues. Même si elles risquent de ne pas porter leurs fruits avant longtemps – vraisemblablement pas avant la fin du mandat en cours – ces initiatives sont un premier pas important et le Rapporteur spécial continuera à faire tout son possible pour les promouvoir et les faciliter.

7. Dans le présent document, le Rapporteur spécial se concentre délibérément sur la surveillance étatique. Pour d'autres domaines d'activité, il renvoie aux « Lignes d'action thématiques » qu'il a présentées dans son premier rapport à l'Assemblée générale (A/71/368, par. 7 à 17). Il est à souligner que les questions de sécurité et de surveillance ont volontairement été abordées séparément des questions touchant aux données personnelles détenues par les entreprises et autres – données massives (*big data*), données en libre accès (*open data*), etc. Ces sujets posent des problèmes et des défis au regard du droit à la vie privée qui leur sont propres. Ces thématiques sont traitées séparément et le seront jusqu'à ce qu'elles puissent être intégrées dans une approche commune ; elles continueront à donner lieu à différentes initiatives parallèles, définies par le Rapporteur spécial. C'est pourquoi le présent document porte sur les activités de surveillance menées par un État, en son nom ou à sa demande.

8. Parallèlement, les travaux sur les autres « Lignes d'action thématiques » se poursuivent. Ils seront présentés en temps voulu – en principe selon le calendrier présenté au paragraphe 2 ci-dessus. En particulier, l'Équipe spéciale sur les données massives et les données en libre accès s'emploie à établir son premier rapport, pour examen lors d'une séance de consultation en juillet 2017. Le bilan de ces consultations sera probablement le sujet central du rapport annuel que le Rapporteur spécial soumettra à l'Assemblée générale en 2017. De plus, devant le succès de l'atelier organisé à New York en juillet 2016 sur le thème « Vie privée, personnalité et circulation de l'information », le Rapporteur spécial a commencé à préparer le deuxième atelier, lequel sera axé sur le Moyen-Orient et l'Afrique du Nord. Il se tiendra les 22 et 23 mai 2017 à Tunis et sera coorganisé par le Rapporteur spécial et l'autorité tunisienne de protection des données, en étroite coopération avec des organisations de la société civile. Les travaux préparatoires ont également commencé pour le troisième atelier, qui sera centré sur l'Asie et se déroulera à Hong Kong (Chine) les 29 et 30 septembre 2017. Les gouvernements, les organisations de la société civile, les entreprises, les autorités de protection des données, les établissements universitaires ou les particuliers qui souhaiteraient participer à ces initiatives ou les soutenir sont invités à se mettre en relation avec le Rapporteur spécial le plus rapidement possible³.

9. Le Rapporteur spécial saisit cette occasion pour saluer les Gouvernements de l'Allemagne, des États-Unis, de la France, de la République de Corée et du Royaume-Uni, qui ont immédiatement donné une suite favorable à sa demande de visite officielle, et pour regretter l'absence de réponse d'un certain nombre d'autres pays. Une telle attitude est malheureusement courante pour certains pays, mais il est utile et même indispensable d'appeler l'attention du public sur la réticence de certains gouvernements à accepter les demandes de visites. Si le Rapporteur spécial ne souhaite pas pointer du doigt tel ou tel pays, les réponses ou l'absence de réponses faites à ses demandes sont sans aucun doute un indicateur de la volonté réelle des pays de travailler de bonne foi à améliorer la protection de la vie privée.

10. Avant de passer au thème principal du présent rapport, le Rapporteur spécial juge nécessaire d'appeler l'attention, de manière urgente et immédiate, sur la pratique préoccupante de certains États qui consiste à invoquer les textes relatifs à la vie privée pour

³ Les courriels sont à adresser à srprivacy@ohchr.org ou à l'une quelconque des autres adresses électroniques dont la liste figure sur la page Web du Rapporteur spécial : www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx.

museler le journalisme d'investigation. Ainsi, il a été signalé que dans certaines circonstances les droits à la vie privée et à la protection des données avaient fait l'objet d'interprétations erronées du pouvoir exécutif et de l'institut autonome national qui n'avaient d'autre but que de censurer certaines informations dans des documents historiques, de manière à barrer l'accès à des documents vieux de trente, quarante, voire cent vingt ans, ce qui constitue une violation flagrante de la liberté d'expression. Selon d'autres allégations, certains organismes responsables de la protection du droit à la vie privée resteraient silencieux face à des menaces d'atteintes à ce droit et à des tentatives patentes des autorités de censurer, sous couvert de protection des données, des informations d'intérêt public. Le Rapporteur spécial a noué de bonnes relations avec les autorités concernées et a commencé à examiner ces griefs, sans pour autant pouvoir à ce stade se prononcer de manière définitive sur leur véracité. Il tient à signaler que ce n'est ni la seule ni la première fois que les autorités d'un pays sont accusées de prendre le droit à la vie privée comme prétexte pour refuser de divulguer des informations d'intérêt public. C'est une question qui pourra faire l'objet d'un rapport distinct et que le Rapporteur spécial mentionne ici dans le but précis d'inviter quiconque a connaissance de tels cas, tout particulièrement les organisations de la société civile, à lui en rendre compte, afin que des investigations plus poussées puissent être menées.

11. Le Rapporteur spécial constate avec satisfaction que de nouveaux pays, dont le Brésil, ont décidé d'adopter des lois pour protéger la vie privée et les données et les incite à respecter les normes minima en la matière, notamment celles fixées dans la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel.

II. Faits nouveaux et tendances inquiétantes en matière de surveillance étatique

A. Surveillance étatique et vie privée à l'ère numérique : le statu quo

12. Le débat actuel sur la surveillance étatique a été alimenté par des personnes comme Edward Snowden et celles et ceux qui le soutiennent. Malgré les controverses qu'elles ont suscitées sur le plan national, force est de reconnaître que les informations que M. Snowden a divulguées sur les pratiques de certains services nationaux de sécurité ont provoqué un débat nécessaire sur ce qu'est la vie privée et ce qu'elle devrait être à l'ère numérique. L'opinion que M. Snowden a exprimée lors d'un entretien avec le quotidien *The Guardian*, auquel il a indiqué ne pas vouloir vivre dans un monde où tout ce qu'il fait et dit est enregistré, est à l'origine de nombreuses initiatives et actions⁴.

13. L'Organisation des Nations Unies a contribué au débat sur la surveillance étatique de diverses manières. Dans sa résolution 69/166, l'Assemblée générale a demandé aux États de créer, ou de maintenir en place, des mécanismes nationaux de contrôle judiciaire, administratif ou parlementaire qui soient indépendants, efficaces, impartiaux et dotés de moyens suffisants et qui puissent garantir la transparence, selon qu'il convient, et la responsabilité des États en ce qui concerne la surveillance et l'interception des communications et de collecte de données personnelles. Plusieurs juridictions régionales des droits de l'homme, telles que la Cour européenne des droits de l'homme, ont rendu des décisions établissant des obligations claires et contraignantes que les gouvernements sont tenus de respecter lorsqu'ils déterminent et mettent en place des moyens de surveillance⁵.

14. Le Rapporteur spécial suit l'évolution de la situation mondiale en matière de surveillance étatique de diverses manières, notamment au moyen de contacts réguliers avec différentes organisations nationales et internationales de la société civile. Beaucoup d'entre elles sont très efficaces pour porter différents sujets de préoccupation à l'attention

⁴ Disponible à l'adresse www.theguardian.com/world/2013/jun/09/nsa-whistleblower-edward-snowden-why, consultée le 8 décembre 2016.

⁵ Voir, par exemple, Cour européenne des droits de l'homme, *Roman Zakharov c. Russie*, arrêt rendu le 4 décembre 2015, disponible à l'adresse <http://hudoc.echr.coe.int/fre?i=001-160008>.

du Rapporteur spécial, des gouvernements et du grand public. Sans dévaloriser aucunement le travail des autres organisations, le Rapporteur spécial souhaite souligner l'utilité des efforts faits par l'American Civil Liberties Union⁶, Access Now⁷, Amnesty International⁸, l'Association pour le progrès des communications⁹, Article 19¹⁰, Human Rights Watch¹¹, le Réseau international des organisations pour les libertés civiles¹² et Privacy International¹³, avec lesquelles il collabore de différentes manières dans le cadre de son mandat. La publication de rapports pertinents par ces dernières, ainsi que par d'autres organisations de la société civile, est extrêmement bénéfique, car le nombre de mots autorisés par l'ONU pour les rapports officiels ne permet pas au Rapporteur spécial d'y inclure, par exemple, un texte sur les faits nouveaux en matière de surveillance tel que celui figurant dans l'exposé que lui a soumis Privacy International en novembre 2016 avant de le publier sur son site Web¹⁴. Il convient de souligner que le Rapporteur spécial partage les préoccupations de Privacy International au sujet des faits connexes observés en Afrique du Sud, en Colombie, en Estonie, aux États-Unis d'Amérique, en ex-République yougoslave de Macédoine, en Fédération de Russie, en France, au Maroc, au Mexique, en Nouvelle-Zélande, en Ouganda, en Pologne, au Royaume-Uni de Grande-Bretagne et d'Irlande du Nord, au Rwanda, en Suède, au Venezuela (République bolivarienne du) et au Zimbabwe, dont il assure le suivi de manière indépendante. Il invite donc les gouvernements de ces États à prendre note des préoccupations exprimées dans les communications de Privacy International et, de préférence, à répondre publiquement ou à se mettre en contact directement avec lui, selon qu'il convient.

15. Il est profondément inquiétant de constater que malgré l'adoption de la résolution 69/166 et malgré des décisions telles que celles mentionnées au paragraphe 13 ci-dessus, le statut du droit à la vie privée dans le domaine de la surveillance n'a connu aucune amélioration depuis le dernier rapport du Rapporteur spécial. Les États qui sont passés à l'action ont élaboré et adopté de nouvelles lois en la matière qui apportent au mieux des améliorations mineures dans des domaines limités. De manière générale, ces lois ont été élaborées et adoptées en toute hâte pour légitimer des pratiques qui n'auraient jamais dû être mises en œuvre.

16. Le 21 décembre 2016, la Cour de justice de l'Union européenne a rendu un arrêt très important et opportun rappelant aux États membres de l'Union européenne leur devoir de respecter, de promouvoir et de protéger le droit fondamental à la vie privée et d'autres droits à l'ère numérique. En ce qui concerne l'obligation légale qu'ont les fournisseurs de services de télécommunication de conserver des données en vrac, la Cour a déclaré que « [l]'ingérence que comporte une telle réglementation dans les droits fondamentaux [...] s'avère d'une vaste ampleur et doit être considérée comme particulièrement grave. La circonstance que la conservation des données est effectuée sans que les utilisateurs des services de communications électroniques en soient informés est susceptible de générer dans l'esprit des personnes concernées le sentiment que leur vie privée fait l'objet d'une surveillance constante. »¹⁵. Elle a également mentionné l'incidence négative que peut avoir cette obligation sur l'exercice de la liberté d'expression.

⁶ Voir www.aclu.org/issues/national-security/privacy-and-surveillance.

⁷ Voir www.accessnow.org/issue/privacy/.

⁸ Voir www.amnestyusa.org/our-work/issues/security-and-human-rights/mass-surveillance et www.amnesty.org.uk/issues/Mass-surveillance.

⁹ Voir www.apc.org/en/pubs/research.

¹⁰ Voir www.article19.org/cgi-bin/search.cgi?q=privacy.

¹¹ Voir www.hrw.org/sitesearch/surveillance.

¹² Voir www.inclo.net/.

¹³ Voir www.privacyinternational.org/reports.

¹⁴ Privacy International, « Monitoring and oversight of communications surveillance » (Supervision et contrôle de la surveillance des communications), novembre 2016, disponible à l'adresse www.documentcloud.org/documents/3454560-UN-Briefing-Monitoring-and-Oversight-of.html.

¹⁵ Voir Cour de justice de l'Union européenne, *Tele 2 Sverige AB c. Post-och telestyrelsen*, arrêt rendu le 21 décembre 2016.

17. La Cour a également déclaré que « si l'efficacité de la lutte contre la criminalité grave, notamment contre la criminalité organisée et le terrorisme, peut dépendre dans une large mesure de l'utilisation des techniques modernes d'enquête, un tel objectif d'intérêt général, pour fondamental qu'il soit, ne saurait à lui seul justifier qu'une réglementation nationale prévoyant la conservation généralisée et indifférenciée de l'ensemble des données relatives au trafic et des données de localisation soit considérée comme nécessaire aux fins de ladite lutte »¹⁶. Elle a en outre clairement déclaré que la conservation des données relatives au trafic devait être l'exception et non la règle. Lorsqu'il est concrètement indiqué que de telles données doivent être conservées à des fins de lutte contre le terrorisme et la criminalité grave, des critères restrictifs doivent être établis, tels que des limitations géographiques précises. La Cour a de plus rappelé que les personnes concernées devaient disposer de garanties et de voie de recours, et que des mécanismes de contrôle efficaces devaient être mis en place pour effectuer des contrôles croisés¹⁷.

18. Si, comme on pouvait s'y attendre, les défenseurs du droit à la vie privée ont accueilli cette décision avec satisfaction, David Anderson Q.C., inspecteur indépendant chargé d'examiner la législation relative au terrorisme, a résumé les autres aspects de cet arrêt de manière fort utile. Selon lui, l'arrêt de la Cour de justice de l'Union européenne est véritablement radical. L'utilité prouvée des pouvoirs existants en matière de conservation des données et les restrictions désormais imposées à ces pouvoirs ne manqueront pas de susciter de graves préoccupations dans le domaine de l'application de la loi, tant au Royaume-Uni que dans d'autres États Membres. D'autre part, l'avis de la Cour selon lequel ces pouvoirs constituent une ingérence de vaste ampleur dans la vie privée, ou sont susceptibles de donner l'impression aux personnes concernées que leur vie privée fait l'objet d'une surveillance constante (par. 100), ne fait pas l'unanimité. Une analyse plus rigoureuse de la proportionnalité de telles mesures aurait tenté de démontrer les préjudices réels causés par ce pouvoir très utile depuis qu'il est exercé, et ne se serait pas appuyée sur des hypothèses théoriques ou sur des prévisions informelles concernant la perception populaire¹⁸.

19. Le Rapporteur spécial est traditionnellement attaché à l'élaboration de politiques fondées sur la connaissance des faits, raison pour laquelle il souhaite, comme l'inspecteur indépendant, qu'une analyse plus rigoureuse de la proportionnalité soit faite. À ce jour, il n'a pas encore obtenu (au Royaume-Uni du moins) l'accès à certaines données (parfois classées), qui confirmeraient que l'acquisition de données en vrac est à la fois nécessaire et proportionnelle au risque. Ainsi, le Rapporteur spécial accueille avec satisfaction la décision de la Cour, justement parce qu'il ne dispose pas encore d'éléments lui prouvant la proportionnalité ou la nécessité des lois réglementant la surveillance qui autorisent l'acquisition en vrac de toutes sortes de données, y compris de métadonnées et de contenu.

20. Il est important d'appeler l'attention sur la dimension culturelle de ces questions, qui a également été relevée par l'inspecteur indépendant :

« Il convient de souligner qu'à l'échelle de l'Europe, les avis sur ces questions diffèrent, au moins dans une certaine mesure, d'une région à l'autre. Ainsi :

- Les commentaires de la Cour de justice de l'Union européenne au sujet de la gravité de l'ingérence dans la vie privée ne trouvent pas d'écho réel dans les trois rapports parlementaires et d'experts qui ont conduit à la soumission du projet de loi relatif aux pouvoirs d'enquête, ni dans les rapports réguliers du Commissaire à l'interception des communications, ancien doyen des juges, qui assure le contrôle rigoureux de cette activité au Royaume-Uni ;
- Dans la partie orientale de l'Europe et en Allemagne il existe cependant une plus grande circonspection qui s'explique par l'histoire de ces régions et par le fait que, jusqu'à récemment, elles étaient relativement peu exposées au terrorisme. Même avant l'affaire *Digital Rights Ireland*, des règles nationales relatives à la conservation des données avaient donné lieu à controverse et avaient été annulées en Bulgarie, en Roumanie, en Allemagne, à Chypre et en République tchèque.

¹⁶ Ibid.

¹⁷ Ibid.

¹⁸ Voir www.terrorismlegislationreviewer.independent.gov.uk/cjeu-judgment-in-watson/.

Ces faits illustrent peut-être ce que j'ai déjà décrit comme des "divergences d'opinions marquées et constantes entre les tribunaux européens et les juges britanniques (...) dues au moins en partie à des perceptions différentes de la police et des forces de sécurité et aux conclusions différentes (mais toutes aussi légitimes) qui ont été tirées de l'histoire du XX^e siècle dans les différentes parties de l'Europe" (*A Question of Trust*, 2.24). »¹⁹.

B. Défis à relever et tendances inquiétantes

21. Il ressort de différentes activités de recherche ayant trait au mandat du Rapporteur spécial et d'autres projets de recherche connexes qu'il est de plus en plus difficile de distinguer les activités de surveillance menées par les services de maintien de l'ordre de celles menées par les services de sécurité et de renseignement. Alors que les activités des premiers concernent généralement la surveillance à l'intérieur des frontières nationales et les activités des seconds, la surveillance des territoires étrangers, la nature des flux transfrontières de données et les moyens techniques nécessaires pour les intercepter entraînent souvent l'utilisation du même équipement, ou d'équipements similaires, à l'ère numérique.

22. Il est de plus en plus fréquent que les données personnelles se retrouvent mélangées à des données qui peuvent être utilisées et réutilisées à diverses fins, connues ou inconnues, ce qui soulève de graves questions, notamment pour ce qui est des critères appliqués pour collecter, stocker, analyser et, enfin, supprimer des données. À titre d'exemple, une étude récemment menée par le Center on Privacy and Technology (Centre sur la vie privée et la technologie) de la faculté de droit de Georgetown, à Washington, a montré qu'un adulte américain sur deux figurait dans un réseau de reconnaissance faciale des forces de l'ordre. Les auteurs de l'étude indiquent qu'il n'existe que très peu d'informations sur ces systèmes : on ignore leur incidence sur la vie privée et sur les libertés civiles, tout comme la manière dont les problèmes d'exactitude sont réglés. On ignore également les incidences de ces systèmes, que ce soit au niveau local, au niveau des États ou au niveau fédéral, sur les minorités raciales et ethniques²⁰.

23. Ces conclusions, et d'autres du même ordre, amènent à tirer certaines considérations. Premièrement, au vu de la nature des flux transfrontières de données et des technologies de l'information moderne, une approche holistique de la protection et de la promotion des droits de l'homme, et en particulier du droit à la vie privée, est nécessaire. Si les flux d'informations restent mondiaux, avec tous les avantages substantiels que cela a eu et continue d'avoir pour l'humanité, ils doivent circuler dans un environnement stable et fiable. Dans un tel environnement, il ne peut pas y avoir de discrimination entre les personnes de différentes nationalités, origines, races, sexes, âges, capacités, confessions, etc. Il faut établir un ensemble de droits et de valeurs que la communauté internationale doit respecter, protéger et promouvoir de manière constante.

24. Deuxièmement, au vu de l'importance croissante que revêt l'échange d'informations dans l'espace virtuel, des méthodes privées, fiables et sûres sont nécessaires. Des technologies telles que le chiffrement ont déjà été largement discutées par le Rapporteur spécial, en particulier dans son premier rapport à l'Assemblée générale (voir A/71/368, par. 19 à 40). En outre, d'autres titulaires de mandat comme le Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression ont déjà réalisé des travaux importants et bienvenus dans ce domaine (voir A/HRC/29/32).

25. Si les forces de l'ordre et les services de sécurité et de renseignement s'inquiètent de leur incapacité à intercepter ou à lire tous les messages envoyés et reçus par tous les individus qui utilisent les technologies de l'information modernes, ils devraient garder à l'esprit le fait que nous vivons à une époque où l'échange d'informations a lieu sur des milliers de canaux. Les individus se sont mis à échanger de telles quantités d'informations par des moyens numériques que, même si certains d'entre eux ne sont pas accessibles pour

¹⁹ Ibid.

²⁰ Clare Garvie, Alvaro Bedoya et Jonathan Frankle, « The perpetual line-up: unregulated police face recognition in America » (Identification permanente : le recours non réglementé de la police à la reconnaissance faciale aux États-Unis), octobre 2016, disponible à l'adresse www.perpetuallineup.org/.

l'État, cela ne signifie pas qu'il n'existe pas d'autres moyens de suivre les personnes mal intentionnées. En particulier, la grande quantité de métadonnées créées par les smartphones et les appareils connectés, qui contiennent souvent autant d'informations que le contenu réel des communications, fournissent de nombreuses occasions d'analyser le comportement des individus²¹. En outre, si l'État était potentiellement capable de s'immiscer dans chaque flux d'informations, même de manière rétroactive, grâce à la conservation de données en vrac et à des technologies comme le « gel rapide », le droit à la vie privée ne connaîtra tout simplement pas de transition intégrale vers l'ère numérique.

26. Il convient de saluer le fait que certains pays et organisations ont commencé à redoubler d'efforts pour relever ces défis. Le Conseil de l'Europe, en particulier, a apporté sa contribution dans ce domaine en proposant une initiative relative à l'application de la loi dans les environnements informatiques en nuage. Cette dernière est liée à la Convention sur la cybercriminalité et a pour but de mettre au point un nouvel outil juridique²².

27. Il est cependant préoccupant que les lois modernes relatives à la surveillance permettent de plus en plus la création et l'analyse de données personnelles, ainsi que l'accès à ces dernières, sans autorisation et supervision adéquates. Une autorisation et supervision adéquates devraient être requises « lorsqu'on ordonne la surveillance, pendant qu'on la mène ou après qu'elle a cessé »²³. Si les méthodes « traditionnelles », comme l'interception d'appels téléphoniques et de communications en général, sont souvent soumises à une autorisation judiciaire préalable, d'autres techniques, comme la collecte et l'analyse de métadonnées liées au protocole qui établit l'historique de navigation Internet ou des données provenant de l'utilisation de smartphones (localisation, appels téléphoniques, utilisation d'applications, etc.), font l'objet de garanties beaucoup plus faibles. Ce phénomène n'est pas justifié puisque cette dernière catégorie de données fournit au moins autant d'informations sur l'activité individuelle d'une personne que le contenu réel d'une conversation. Ainsi, des garanties adéquates doivent également être mises en place pour ces mesures.

28. Bien que l'autorisation judiciaire de mesures intrusives entraîne généralement une amélioration du degré de protection de la vie privée, il faut également garantir l'indépendance et l'impartialité des juges lorsqu'ils rendent des décisions dans le cadre d'affaires individuelles. Ces derniers doivent en outre posséder les connaissances et les informations nécessaires pour examiner en détail les demandes de telles mesures et comprendre les conséquences potentielles de leurs décisions, en particulier pour ce qui est du choix de la technologie à utiliser et de l'incidence de son utilisation. Ainsi, les États devraient garantir que les juges reçoivent une formation et disposent des ressources nécessaires pour pouvoir s'acquitter de cette tâche difficile.

29. En principe, il devrait en aller de même pour le contrôle des activités de surveillance par des organes spécialisés des assemblées parlementaires. Ces organes ont besoin non seulement d'avoir les informations nécessaires pour comprendre les activités des forces de l'ordre et des services de sécurité et de renseignements, mais aussi de disposer de ressources adéquates leur permettant de les comprendre et de les assimiler.

30. Dans la plupart des États, cet objectif sera difficile à atteindre au vu du volume important de données en jeu. Les autorités menant des activités de surveillance devraient prendre des mesures pour garantir que les pratiques en matière de contrôle soient révisées et contrôlées de manière permanente et en détail. Les contrôles, en particuliers lorsqu'ils sont effectués dans le domaine politique, devraient pouvoir cibler des problèmes structurels et répondre à l'orientation générale des opérations.

²¹ Voir par exemple le rapport du Berkman Center for Internet and Society à l'Université de Harvard, « Don't panic. Making progress on the "going dark" debate », 2016, disponible à l'adresse https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf.

²² Voir <https://www.coe.int/fr/web/portal/-/cybercrime-towards-a-new-legal-tool-on-electronic-evidence#>.

²³ Cour européenne des droits de l'homme, *Zakharov c. Russie*.

31. La nature internationale des activités de contrôle est une autre question qui suscite beaucoup d'attention. C'est un phénomène qui comprend deux dimensions particulières auxquelles il convient de s'intéresser en particulier. Il est en premier lieu essentiel que les États respectent le droit à la vie privée reposant sur la dignité humaine au niveau mondial. Les activités de surveillance, qu'elles ciblent des nationaux ou des étrangers, doivent se dérouler dans le respect des droits de l'homme fondamentaux, comme le droit à la vie privée. Toutes les lois nationales et tous les accords internationaux ne respectant pas ce principe doivent être considérés comme obsolètes et incompatibles avec l'universalité de la vie privée et les droits fondamentaux à l'ère numérique.

III. Premières approches de la surveillance étatique plus respectueuses de la vie privée

A. Tour d'horizon complet des approches et des questions en jeu

32. Les recherches et les échanges menés avec des représentants des pouvoirs publics, de la société civile et d'entreprises de différentes régions du monde, notamment à l'occasion du Forum international de surveillance du renseignement en 2016, ont permis de dégager plusieurs thèmes dans le domaine de la surveillance étatique, dont les suivants :

- a) La nécessité d'internationaliser et d'harmoniser les termes et le langage utilisés ;
- b) La nécessité d'instaurer un dialogue ouvert et confidentiel pour mieux comprendre les systèmes nationaux, leurs similarités et leurs différences ;
- c) La promotion et la protection des droits de l'homme fondamentaux s'agissant des méthodes utilisées ;
- d) Les mesures de sauvegarde et les voies de recours, de préférence au niveau international ;
- e) Le respect du principe de responsabilité et la transparence ;
- f) Le recensement et l'analyse des bonnes et des mauvaises pratiques ;
- g) La progression des discussions sur la manière de structurer le contrôle de la surveillance étatique ;
- h) Les réponses aux questions concernant la participation du public ;
- i) La nécessité de moins cultiver le secret et d'être plus proactif afin d'expliquer les activités de surveillance des services secrets et des forces de l'ordre ;
- j) La nécessité de disposer de davantage d'instances où échanger des idées pour progresser sur le sujet.

B. Examen des questions en jeu

33. L'internationalisation et l'harmonisation des termes et du langage utilisés ont pour but de définir des termes tels que « surveillance », « surveillance de masse », « collecte massive de données », « interception massive de données », « piratage massif », « intrusion dans des appareils », etc. Les autorités britanniques ont publié un document utile, bien que controversé, intitulé *Operational case for bulk powers* (Guide pratique sur les pouvoirs en matière de surveillance), dans lequel figurent des définitions ambitieuses de certains de ces termes²⁴. Il est important que les autorités publiques qui mènent des activités de surveillance, la société civile et d'autres parties prenantes aient une idée précise de ce qu'elles entendent lorsqu'elles utilisent des termes relatifs à la surveillance, dont certains, tels que « surveillance de masse », sont très connotés et controversés. Il est nécessaire que ces termes soient utilisés de manière plus systématique et harmonisée et

²⁴ Disponible à l'adresse : www.gov.uk/government/uploads/system/uploads/attachment_data/file/504187/Operational_Case_for_Bulk_Powers.pdf.

qu'ils soient compris lors des échanges entre les autorités publiques qui mènent des activités de surveillance. Toutefois, les organes de contrôle du pouvoir judiciaire et du pouvoir politique, la société civile, les chercheurs dans le domaine de la sécurité et les entreprises devraient également pouvoir comprendre et utiliser ces termes de manière appropriée.

34. La surveillance revêt une dimension internationale, c'est pourquoi il est nécessaire d'aborder ce sujet au sein d'une instance internationale confidentielle et digne de confiance. Il est important de renforcer le dialogue entre les autorités nationales qui mènent des activités de surveillance. En outre, les experts de la société civile doivent pouvoir apporter leur contribution et partager leurs préoccupations au cours de ces échanges.

35. Toute évaluation des mesures de surveillance étatique, quelles qu'en soient la forme et la nature, doit absolument être axée sur le respect des droits de l'homme fondamentaux, en particulier le droit à la vie privée, le droit à la liberté d'expression et le droit à l'information. Même si la protection des droits à la vie et à l'intégrité physique est une condition indispensable à l'existence humaine, il convient de garder à l'esprit qu'il n'existe pas de hiérarchie stricte entre les droits de l'homme. Ces droits se renforcent mutuellement. En d'autres termes, il faut promouvoir largement les droits de l'homme dans leur ensemble, et pas seulement un ou deux d'entre eux.

36. Un droit ne vaut que s'il est correctement délimité et si des mécanismes d'application sont en place. Cet aspect est essentiel dans le cadre de la surveillance étatique, étant donné qu'il est nécessaire d'offrir des garanties sans frontières et de fournir des recours transfrontières. L'entraide judiciaire, comme cela est mentionné plus haut, doit être appliquée et améliorée. S'il n'est pas possible de parvenir à une approche commune à l'échelle mondiale, ce qui n'est pas exclu, il est alors nécessaire de recourir à des initiatives régionales et interrégionales.

37. Au sein des organisations gouvernementales qui mènent des activités de surveillance, le respect des principes de responsabilité et de transparence doit s'inscrire dans un cadre clairement établi. Il est également nécessaire de préciser pourquoi un certain ensemble de données est collecté, quels sont les objectifs de l'analyse et quels objectifs ne sont pas légaux. De tels mécanismes doivent être mis en place en tout premier lieu au sein des autorités qui mènent des activités de surveillance. Il est en outre nécessaire de déterminer précisément à qui incombe la responsabilité de veiller au respect des prescriptions légales qui auront été établies en la matière.

38. À cet égard, il est utile de recenser des exemples de bonnes et de mauvaises pratiques. Par exemple, certains organismes de surveillance du renseignement ont créé des organes de consultation composés d'experts externes dignes de confiance qui leur dispensent des conseils sur des questions particulières. En outre, il est essentiel de réaliser une évaluation des activités et de réfléchir au rôle de ces organismes en ce qui concerne la promotion et la protection des droits de l'homme fondamentaux. Enfin, les agents des autorités qui mènent des activités de surveillance doivent être formés afin qu'ils ne se reposent pas uniquement sur la technologie et qu'ils comprennent que, en définitive, la technologie doit les assister, et non les guider, dans leur prise de décisions.

39. Il est nécessaire de disposer d'autres mécanismes correcteurs dans l'éventualité où les mécanismes internes de respect des principes de responsabilité et de transparence ne rempliraient pas leur rôle. Les États doivent avoir les moyens de détecter et d'évaluer les problèmes structurels dans les organismes chargés des activités de surveillance. Dans certains États, ces fonctions sont assumées par des commissions parlementaires. Cependant, les autorités de contrôle manquent souvent de connaissances dans ce domaine, de ressources ou d'accès aux informations. Il en va de même pour les mécanismes de contrôle judiciaire lorsqu'ils existent.

40. Par ailleurs, les révélations faites par Edward Snowden et les répercussions qu'elles ont eues ont clairement montré qu'il était impératif que les autorités publiques expliquent leurs activités. Pour ce faire, il serait possible par exemple d'informer a posteriori, lorsqu'il n'existe plus de risque, les personnes qui ont fait l'objet d'une surveillance et de leur expliquer les conséquences de cette opération. Ces personnes devraient avoir le droit de faire modifier ou supprimer les informations personnelles non pertinentes les

concernant, pour autant que ces informations ne soient plus nécessaires à l'enquête, en cours ou à venir, pour laquelle leur collecte et leur utilisation ont été dûment autorisées.

41. En outre, le public doit avoir à nouveau confiance dans les activités des organismes de surveillance. Il est évident que la sécurité est une préoccupation légitime pour tous, c'est pourquoi, même si le public n'a pas besoin de connaître les tenants et les aboutissants de chaque opération, il doit avoir accès à l'information afin de comprendre les aspects généraux des activités menées pour le protéger. Un passager n'a pas besoin de savoir piloter un avion pour réserver un vol, mais il n'achètera pas de billet s'il n'a pas confiance en la gestion et la sécurité du trafic aérien et en l'efficacité des systèmes de sécurité.

IV. Activités du Rapporteur spécial

42. Le Rapporteur spécial sur le droit à la vie privée rend compte des principales activités publiques ou semi-publiques menées dans le cadre de son mandat de juillet 2016 au début de février 2017. Il s'agit notamment des activités suivantes :

- a) Atelier européen sur l'innovation dans le domaine de la protection de la vie privée, Huawei German Research Center, à Munich (Allemagne), le 3 août 2016 ;
- b) Intervenant principal à la Conférence du Conseil de l'Europe sur le thème « La liberté d'Internet : un facteur constant de la sécurité démocratique en Europe », à Strasbourg (France), le 9 septembre 2016 ;
- c) Présidence d'un groupe d'experts sur la biométrie et la vie privée, Conférence sur les projets de recherche de l'European Association for Biometrics, à Darmstadt (Allemagne), les 19 et 20 septembre 2016 ;
- d) Réunion du groupe consultatif sur la protection et la sécurité pour le programme Horizon 2020, Commission européenne, Direction générale de la migration et des affaires intérieures, à Bruxelles, le 27 septembre 2016 ;
- e) Rapporteur spécial pour le Forum international de surveillance du renseignement, à Bucarest, les 11 et 12 octobre 2016 ;
- f) Intervenant principal et président d'un groupe d'experts, Conférence « Intelligence in the Knowledge Society », à Bucarest, les 13 et 14 octobre 2016 ;
- g) Intervenant principal, 38^e Conférence internationale annuelle des Commissaires à la protection des données et à la vie privée, à Marrakech (Maroc), du 18 au 22 octobre 2016 ;
- h) Deuxième assemblée générale annuelle du projet MAPPING, à Prague, du 31 octobre au 2 novembre 2016 ;
- i) Intervenant principal, Cyberspace Conference 2016, à Brno (Tchéquie), les 25 et 26 novembre 2016 ;
- j) Intervenant principal, Forum des autorités de protection de la vie privée pour la région Asie-Pacifique, à Manzanillo (Mexique), du 30 novembre au 2 décembre 2016 ;
- k) Intervenant principal et membre d'un groupe d'experts, Symposium sur la surveillance, Conseil irlandais pour les libertés civiles, à Dublin, le 7 décembre 2016 ;
- l) Intervenant principal, déclaration annuelle, Commission nord-irlandaise des droits de l'homme, à Belfast (Royaume-Uni), le 8 décembre 2016 ;
- m) Réunions préparatoires pour le deuxième atelier sur la protection de la vie privée et de la personnalité et la libre circulation de l'information, en Tunisie, du 12 au 14 décembre 2016 ;
- n) Membre d'un groupe d'experts sur l'intelligence artificielle et la vie privée, dixième Conférence internationale de Computers, Privacy and Data Protection, à Bruxelles, du 25 au 27 janvier 2017 ;

o) Intervenant principal sur la vie privée et la sécurité au neuvième Forum ISMS sur la vie privée, à Madrid, les 1^{er} et 2 février 2017.

V. Conclusions et recommandations

43. À ce stade, le Rapporteur spécial souhaite formuler cinq recommandations distinctes qui découlent de ses conclusions provisoires. Elles portent sur les questions suivantes :

- a) Pourquoi le populisme et la protection de la vie privée sont difficiles à concilier avec la sécurité ;
- b) Comment les États peuvent contribuer à renforcer la protection de la vie privée en améliorant la surveillance du renseignement ;
- c) Qui mérite de jouir du droit à la vie privée (tout le monde, partout) ; l'universalité du droit à la vie privée a un sens particulier dans ce contexte ;
- d) Comment adapter le droit national et le droit international pour mieux protéger le droit à la vie privée ;
- e) À quel moment les dispositions de droit international, en particulier celles concernant un instrument juridique réglementant la surveillance, sont à un stade d'élaboration suffisamment avancé pour faire l'objet d'un examen à plus grande échelle.

Pourquoi le populisme et la protection de la vie privée sont difficiles à concilier avec la sécurité

44. Dans un souci de précision, cette section devrait peut-être s'intituler « Sécurité, populisme et vie privée ». Entre 2015 et 2017, on a observé, en Europe en particulier mais pas uniquement, une tendance croissante à verser dans la démagogie. En d'autres termes, au cours de ces dix-huit derniers mois, des responsables politiques soucieux de donner l'impression qu'ils prenaient les choses en main dans le domaine de la sécurité ont inscrit dans la loi certains pouvoirs ou ont légalisé des pratiques existantes qui portent atteinte au droit à la vie privée, sans démontrer d'aucune manière que ces mesures étaient proportionnées ou constituaient un moyen efficace de lutter contre le terrorisme.

45. Les nouvelles lois ainsi adoptées reposent sur la psychologie de la peur, c'est-à-dire la peur disproportionnée, bien que compréhensible, que peuvent ressentir les électeurs face à la menace terroriste. Un tel sentiment empêche les électeurs d'analyser objectivement l'efficacité des mesures proposées.

46. Il n'existe pas ou peu d'éléments qui puissent convaincre le Rapporteur spécial de l'efficacité ou de la proportionnalité de certaines mesures extrêmement intrusives qui ont été instaurées par des nouvelles lois sur la surveillance en Allemagne, aux États-Unis, en France et au Royaume-Uni. Comme le juge qui a récemment statué sur une affaire en lien avec le décret anti-immigration aux États-Unis, le Rapporteur spécial doit examiner les éléments attestant la proportionnalité des mesures prévues par les lois²⁵. De la même manière que le juge s'est interrogé précisément sur le nombre d'actes de terrorisme commis par des ressortissants des pays visés par cette mesure depuis 2001, le Rapporteur spécial doit se demander si le fait d'accorder davantage de fonds aux ressources humaines nécessaires aux activités de surveillance et d'infiltration ciblées et de déployer moins d'efforts dans le domaine de la surveillance électronique ne constituerait pas une mesure plus proportionnée, mais aussi plus rentable et moins intrusive, étant donné que la grande majorité des attentats terroristes ont été perpétrés par des personnes connues des autorités.

²⁵ Voir www.npr.org/2017/02/04/513446463/who-is-judge-james-l-robart-and-why-did-he-block-trumps-immigration-order.

47. Il est de plus en plus évident que les informations détenues par les gouvernements, y compris les données collectées au moyen de l'acquisition massive ou de la surveillance de masse, sont toujours plus vulnérables aux actes de piratage commis par des gouvernements hostiles ou des groupes liés à la criminalité organisée. Il n'a en aucun cas été démontré que la diminution de la menace terroriste grâce à l'acquisition massive de données était proportionnée aux risques engendrés par la collecte de données.

48. En outre, l'utilisation abusive des informations obtenues par l'acquisition massive de données reste la principale source de préoccupations. Sans pour autant discréditer le nouveau Gouvernement des États-Unis, il convient de relever les préoccupations exprimées à ce sujet par une éminente chercheuse de Human Rights Watch : « Aux États-Unis, la National Security Agency continue de surveiller des millions de personnes chaque jour, malgré les timides réformes entreprises en 2015. À présent, le système de surveillance le plus sophistiqué au monde se trouve entre les mains [...] d'un candidat [qui] a menacé d'emprisonner son opposant politique, de ficher les musulmans et de les interdire d'entrée sur le territoire, d'expulser des millions d'immigrés et de s'attaquer à la liberté de la presse. »²⁶. Toutefois, l'équilibre des pouvoirs existant aux États-Unis ou les principes éthiques du Gouvernement lui-même peuvent, il faut l'espérer, empêcher ces risques de se concrétiser ; ce que le Rapporteur spécial souhaite souligner ici est que, dans n'importe quel pays, lorsqu'un ensemble de données a été collecté au moyen de la surveillance de masse ou de l'acquisition massive et qu'une administration peu scrupuleuse arrive au pouvoir, le risque d'une utilisation abusive de ces données est tel qu'il remet fondamentalement en question leur collecte.

49. Le Rapporteur spécial recommande donc aux États de cesser de tirer parti de la peur et de renforcer la sécurité en mettant en œuvre des mesures proportionnées et efficaces plutôt qu'en adoptant des lois portant atteinte à la vie privée et extrêmement disproportionnées. Il rappelle à cet égard les propos du cardinal Vincent Nichols, archevêque de Westminster, qui a déclaré : « Je ne pense pas que la peur soit la meilleure manière d'exercer le pouvoir. La véritable autorité ne repose pas sur la peur. »²⁷.

Comment les États peuvent contribuer à renforcer la protection de la vie privée en améliorant la surveillance du renseignement

50. Le Forum international de surveillance du renseignement de 2016 a montré que les discussions portant sur la manière de contrôler les services de renseignement de façon à renforcer la protection de la vie privée sont complexes et requièrent beaucoup de temps et de ressources, des changements culturels éventuels, une volonté politique et l'instauration d'un certain niveau de confiance. Il n'existe pas de moyen simplifié d'identifier et d'améliorer les bonnes pratiques.

51. La recommandation du Rapporteur spécial est simple, mais non moins importante : tous les États Membres de l'Organisation des Nations Unies devraient prendre part aux discussions laborieuses sur le contrôle des services de renseignement lancées par le Rapporteur spécial à l'occasion du Forum international de surveillance du renseignement de 2016, qui reprendront lors du prochain Forum en 2017. Les gouvernements devraient encourager les organismes de contrôle et les services de renseignement à prendre part aux forums et faciliter leur participation.

²⁶ Cynthia M. Wong, « Surveillance in the age of populism », Human Rights Watch, février 2017, disponible à l'adresse : www.hrw.org/news/2017/02/07/surveillance-age-populism.

²⁷ Cardinal Vincent Nichols s'exprimant au cours d'un programme sur la BBC Radio 4, « the Westminster Hour 175 », le 5 février 2017.

Qui mérite de jouir du droit à la vie privée

52. Le Rapporteur spécial recommande aux États de faire en sorte que, aux niveaux national et international, la vie privée soit considérée comme un droit véritablement universel et, en particulier concernant les activités de surveillance menées sur Internet, que le respect de ce droit ne dépende pas de la nationalité.

53. Il y a beaucoup à dire concernant cette recommandation, mais les exemples se limiteront ici à la jurisprudence et aux changements apportés à la législation des États-Unis. Il convient de préciser d'emblée que toutes les recommandations faites aux États-Unis sont également valables dans des situations analogues pour tous les autres États Membres de l'Organisation des Nations Unies.

54. Le 6 février 2017, la Chambre des représentants des États-Unis a pris une décision fort louable que le Rapporteur spécial attendait depuis longtemps. Elle a adopté à l'unanimité la loi sur la confidentialité des courriers électroniques qui a permis de combler un vide juridique ; cette loi dispose qu'un mandat judiciaire est nécessaire pour accéder aux courriers électroniques datant de plus de six mois hébergés dans le nuage ou ailleurs. Le Rapporteur spécial se réjouit de cette avancée, qui, il l'espère, satisfera le Sénat, qui avait refusé d'adopter cette loi en avril 2016. Le Rapporteur spécial invite le Sénat à franchir une nouvelle étape en saisissant l'occasion historique qui lui est donnée de démontrer l'attachement des États-Unis aux droits de l'homme dans le monde entier, tout en mettant fin à une idée fausse et xénophobe, que certains gouvernements promeuvent volontairement ou involontairement, qui veut que seuls les « étrangers mal intentionnés » cherchent à « nous nuire » et que, par conséquent, ils ne méritent pas que leurs droits fondamentaux soient protégés par la loi.

55. Cette lacune n'est pas unique à la législation des États-Unis. Par exemple, récemment, le Gouvernement allemand a lui aussi adopté une loi établissant une distinction entre, d'une part, les ressortissants allemands et de l'Union européenne et, d'autre part, les ressortissants des autres pays (voir A/71/368, par. 35 et 36). Ces lois sont bien évidemment contestables d'un point de vue logique : la grande majorité des attentats terroristes perpétrés en Europe, n'ont pas été commis par des étrangers, mais, dans la plupart des cas, par des ressortissants de l'Union européenne titulaires de cartes d'identité et de passeports européens. La situation semble être similaire pour les récents attentats commis aux États-Unis. Alors pourquoi souscrire à l'idée erronée selon laquelle il est logique et sensé d'appliquer des mesures discriminatoires à l'égard de certaines personnes au motif qu'elles ne sont pas ressortissantes du même pays que les législateurs ? Si les gouvernements souhaitent réellement combattre et faire diminuer le terrorisme, il est plus logique qu'ils s'attaquent aux causes profondes du problème, telles que la radicalisation. Il serait beaucoup plus efficace d'investir davantage dans des mesures visant à lutter contre ce phénomène et d'allouer plus de ressources à la surveillance ciblée à long terme et à l'infiltration des cellules terroristes plutôt que de verser dans le populisme. De toute évidence, essayer de faire preuve de fermeté sur la question de la sécurité en légitimant des mesures essentiellement inutiles, extrêmement coûteuses et absolument disproportionnées qui portent atteinte au droit à la vie privée et aux autres droits de tant de personnes n'est pas la voie à suivre pour les gouvernements.

56. Avec le plus grand respect, le Rapporteur spécial suggère qu'il serait nettement plus utile et logique que la législation des États-Unis s'accorde avec le principe reconnu récemment par la Cour européenne des droits de l'homme et la Cour de justice européenne dans les affaires *Zakharov c. Russie* et *Tele 2 Sverige AB c. Autorité suédoise de surveillance des postes et télécommunications*, respectivement, à savoir que la condition fondamentale à l'exercice d'une surveillance ciblée est l'existence d'un motif raisonnable et non la citoyenneté, ajoutant que cela servirait d'exemple au reste du monde. Si les services de sécurité et de renseignement ou les services de maintien de l'ordre peuvent prouver l'existence d'un motif raisonnable, alors ils devraient pouvoir obtenir d'un juge l'autorisation d'accéder aux données voulues quelle que soit la nationalité du suspect. Le risque et la gestion du risque sont et devraient rester les principaux éléments à prendre en considération. S'il est prouvé qu'une personne

représente un risque, cette personne devrait être soumise à une surveillance où qu'elle se trouve et où qu'elle aille, indépendamment de sa nationalité. Les garanties mises en place contre les perquisitions et saisies injustifiées – en l'occurrence l'obligation d'obtenir un mandat judiciaire – s'appliquent de la même manière concernant la surveillance ciblée, quelle que soit la nationalité de la personne visée. Dans la Déclaration universelle des droits de l'homme, il n'est pas dit, à fort juste titre, que seuls les citoyens américains ont le droit à la vie privée, mais que toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes (voir art. 12), ce qui, de l'avis du Rapporteur spécial, vaut également pour la loi américaine. Ainsi, les États-Unis ont aujourd'hui l'occasion de montrer l'exemple au reste du monde, de se conformer à l'esprit et aux principes de la Déclaration universelle et de prendre des mesures concrètes, dont celles énoncées ci-dessous, pour mettre la législation américaine en pleine conformité avec la nature universelle du droit à la vie privée en modifiant comme il se doit la loi sur la confidentialité des courriers électroniques.

57. Si, tout comme le droit de ne pas être soumis à la torture et bien d'autres droits, le droit à la vie privée est un droit fondamental, c'est aussi un droit universel, ce qui signifie que toute personne jouit de ce droit, partout dans le monde, quels que soient l'endroit où elle se trouve, sa nationalité, sa couleur de peau, ses croyances, son origine ethnique, ses opinions politiques ou son orientation sexuelle. C'est cette vérité que le Rapporteur spécial engage aussi le Sénat des États-Unis à reconnaître. Au fil des ans, le Gouvernement des États-Unis s'est maintes fois efforcé de sanctionner les responsables de violations des droits de l'homme dans d'autres pays et a souvent ouvert la voie à des initiatives visant à fixer les limites à ne pas dépasser et à prévoir des sanctions pour les faire respecter. En étendant à tout un chacun les garanties de la vie privée accordées aux citoyens américains, supprimant ainsi la distinction entre les citoyens américains et les autres, le Sénat ferait un grand pas en avant dans la mise en œuvre universelle du droit fondamental à la vie privée et porterait un coup décisif au tour xénophobe que prennent les textes législatifs. Il mettrait également la législation des États-Unis en concordance avec les textes législatifs de l'Union européenne et du Conseil de l'Europe relatifs à la vie privée et à la protection des données, qui reconnaissent le même droit à la vie privée aux citoyens européens et aux autres.

Comment adapter le droit national et le droit international pour mieux protéger le droit à la vie privée

58. Alors que la recommandation précédente traite en grande partie des moyens de protéger la nature universelle du droit à la vie privée dans le droit national, les paragraphes qui suivent portent sur les moyens de compléter les mesures prises au niveau national par des mesures internationales.

59. Une des préoccupations majeures soulevées par le libellé actuel de la loi américaine sur la confidentialité des courriers électroniques est la question de savoir si les garanties renforcées par la loi s'appliquent aussi aux données indépendamment de l'endroit où elles sont stockées, que ce soit aux États-Unis ou en dehors. L'affaire concernant la contestation par Microsoft de la validité des mandats de perquisition américains relatifs à des données stockées en dehors des États-Unis²⁸ illustre bien cette question. On peut très facilement comprendre le refus de Microsoft de transmettre aux autorités américaines des données stockées en dehors des États-Unis. En répondant favorablement à cette demande, l'entreprise risque de perdre en compétitivité au niveau international. En outre, elle se heurte à la question particulièrement épineuse de savoir comment répondre aux diverses demandes de données émanant de toutes sortes de gouvernements partout dans le monde, et elle n'est pas la seule. La plupart des autres géants de la technologie, qui sont en majorité américains, comme Google, Facebook, Apple et Twitter (pour ne citer qu'eux), reçoivent chaque année des gouvernements du monde entier des milliers de demandes d'accès à des données.

²⁸ Voir blogs.microsoft.com/on-the-issues/2016/07/14/search-warrant-case-important-decision-people-everywhere/#sm.0019d8sjw1492dnrz7k1yawh09b46 (en anglais).

60. Si le Congrès des États-Unis veut progresser de manière sensée dans le règlement de cette question, voire la résoudre, dans le respect des droits de l'homme et sans désavantager les entreprises américaines sur le plan commercial, il doit être conscient que la solution ne peut venir uniquement du droit interne. Il doit également se rendre compte que, dans ce domaine juridique particulier, des mécanismes tels que l'entraide judiciaire, qui ont été mis au point il y a plusieurs dizaines d'années, ne sont pas d'une grande utilité. Il doit reconnaître en outre que, malgré les progrès accomplis grâce à la Convention sur la cybercriminalité, le transfert de données personnelles entre pays et la communication des données requises à des fins d'enquête ne sont pas aussi rapides et simples que certains l'auraient voulu. Cet échec relatif s'explique notamment par le fait que la Convention reste trop axée sur le concept de l'État-nation souverain du XIX^e siècle et ne tient pas suffisamment compte de la réalité de l'Internet sans frontière du XXI^e siècle. Elle est un bon exemple des progrès que l'on peut accomplir en avançant à petits pas et il ne fait aucun doute qu'elle a permis quelques avancées, notamment l'identification et la codification des infractions liées à l'informatique et à Internet, mais elle n'a pas été à la hauteur des attentes pour ce qui est du transfert ponctuel de données personnelles entre pays, qui peut faciliter la détection et la prévention de la criminalité et la réalisation d'enquêtes à l'ère d'Internet. Cette lacune est peut-être due principalement au fait que la Convention n'a pas été jusqu'à créer un mécanisme, comme un organe international, chargé de délivrer les autorisations d'accès aux données au niveau international et investi des pouvoirs requis en la matière.

61. De même que d'autres instruments internationaux portent création d'organismes chargés d'établir la confiance et de mettre en place des garanties appropriées dans des domaines aussi variés que le droit maritime, le droit de l'espace, les armes atomiques et les armes chimiques, entre autres, la Convention sur la cybercriminalité peut être étoffée de manière à créer, en conjonction avec d'autres accords multilatéraux, dont certains conclus expressément à cet effet, une autorité internationale habilitée à délivrer l'équivalent d'un mandat international de surveillance ou d'accès aux données qui ait force de loi dans le cyberspace. Les pays qui adhèrent à un nouvel accord ou à un protocole additionnel portant création d'une telle autorité pourraient désigner des juges indépendants spécialisés pour constituer une liste de réserve, laquelle servirait à former des groupes faisant office de guichet unique pour la délivrance de mandats judiciaires ayant force probante au niveau international, dans les pays parties à l'accord susmentionné. De cette façon, pour en revenir à l'exemple de l'affaire Microsoft et de la décision de juillet 2016 y relative, Microsoft, Google, Facebook, Amazon, Apple et les autres géants de la technologie qui gèrent des centres de données à l'échelle internationale n'auraient pas à craindre qu'un État abuse de ses prérogatives puisqu'ils auraient devant eux une autorisation internationale d'accès aux données, délivrée sur la base d'un motif raisonnable en vertu d'un instrument international précis. De même, les citoyens du monde entier seraient assurés que leur droit à la vie privée est protégé par des garanties suffisantes, de manière impartiale et universelle, au même titre que leurs autres droits comme le droit à la liberté d'expression et d'association. Il ne fait aucun doute que des mécanismes internationaux et universels qui appliquent les mêmes normes et les mêmes garanties partout dans le monde doivent être mis en place si l'on veut garantir la mise en œuvre universelle du droit à la vie privée.

62. Ce n'est pas une utopie, c'est la réalité brute et crue. C'est ce qui distinguera les vraies démocraties des États qui entendent utiliser Internet avant tout pour exercer un contrôle social et conserver le pouvoir au sein de leurs propres juridictions. C'est aussi une initiative qui pourrait être rattachée aux autres mesures visant à protéger le cyberspace, comme l'a récemment préconisé le Président et Directeur juridique de Microsoft²⁹.

²⁹ Voir www.itpro.co.uk/security/28134/how-can-nation-states-win-the-unfolding-cyberwar?_mout=1&utm_campaign=newsletter&utm_medium=email&utm_source=newsletter&tpid=109380765640 (en anglais).

63. À l'heure actuelle, les informations dont dispose le Rapporteur spécial semblent indiquer que plusieurs États, dont de grandes démocraties, utilisent malheureusement Internet de manière opportuniste, considérant que leurs services de maintien de l'ordre et, en particulier, leurs services de sécurité et de renseignement peuvent y opérer quasiment sans restriction, intercepter des données et pirater des millions de dispositifs (tant des smartphones, tablettes et ordinateurs portables que des serveurs) partout dans le monde. Ainsi, entre 15 et 25 États assimilent Internet à leur terrain de jeux, se chamaillant pour en récolter les avantages et cherchant constamment à avoir le dessus, que ce soit en termes de cyberguerre, d'espionnage et de contre-espionnage ou d'espionnage industriel. La liste de leurs motivations est longue. Les quelque 175 États restants, pour leur part, semblent impuissants et ne peuvent qu'espérer que la cyberpaix s'imposera d'une façon ou d'une autre.

64. Pour le dire franchement, une petite minorité d'États a tenté activement et officieusement de dissuader le Rapporteur spécial de chercher des solutions dans ce domaine. Il est cependant de son devoir d'indiquer que ces États semblent être les seuls à ne pas souhaiter la mise en place de garanties et de voies de recours ayant force probante au niveau international concernant Internet. Le Rapporteur spécial n'a pas encore rencontré une seule organisation de la société civile ou entreprise ni un seul service de maintien de l'ordre ou de sécurité et de renseignement raisonnable qui ne souhaite pas que l'on gagne en clarté et que l'on instaure des garanties et des voies de recours universels ; ces entités pourraient toutefois être découragées par le fait que l'on ignore si les résultats recherchés pourront être obtenus prochainement.

65. Le renforcement de la clarté et la mise en place de garanties et de voies de recours disponibles de manière plus ponctuelle, plus équitable et plus rapide passe inévitablement par la conclusion d'accords multilatéraux consacrés par le droit international. Le monde n'a pas besoin des manigances qui s'exercent sur Internet avec l'appui des États mais d'un accord rationnel et civilisé concernant la manière dont les États doivent se comporter sur Internet, ce qui nous ramène à la question de la surveillance.

66. Certains des mécanismes internationaux renforcés évoqués plus avant seraient très utiles pour faire appliquer les lois dans le cyberspace. Ce domaine relève actuellement de la Convention sur la cybercriminalité, à laquelle environ 25 % des États Membres de l'Organisation des Nations Unies ont déjà souscrit. Toutefois, comme son nom l'indique, la Convention traite uniquement des aspects liés à la justice pénale, et non de la sécurité nationale et de la surveillance exercée au nom de la sécurité nationale. Autrement dit, les activités dénoncées par Edward Snowden n'entrent pas dans le champ d'application de la Convention. Pour qu'elles soient réglementées de manière satisfaisante, il faudrait étendre considérablement la portée de la Convention ou conclure un accord distinct mais complémentaire qui traite de la surveillance dans le cyberspace de manière appropriée. Cela serait nettement préférable à la situation actuelle où plusieurs démocraties, notamment l'Allemagne, la France, les États-Unis et le Royaume-Uni, luttent pour mettre en place de nouvelles lois sur la surveillance et où la mentalité semble imprégnée, à tort, du concept de l'État-nation souverain du XIX^e siècle.

67. Si le nationalisme et le jingoïsme, de même que le populisme, affichent ce qui pourrait s'avérer être une hausse cyclique, leur succès lors des élections ne doit pas être interprété comme un signe de l'efficacité à garantir véritablement la sécurité, tant au niveau national qu'international. Il doit être reconnu – y compris par les politiciens qui s'expriment au niveau national – que la grande majorité des États Membres n'ont aucun intérêt à promouvoir la criminalité organisée ou le terrorisme, où que ce soit et par qui que ce soit. Concrètement, si un enquêteur belge s'adressait à un groupe international composé de juges provenant de l'Allemagne, du Brésil, des États-Unis, de la France, du Ghana, de l'Inde et du Royaume-Uni, au hasard, il y a peu de risques que ce groupe, ou un groupe ayant une composition similaire, refuse de délivrer un mandat d'accès à des données personnelles si l'existence d'un motif raisonnable a été établie. La mise en place d'un système d'autorisations internationales d'accéder aux données simplifiera considérablement les choses pour les gouvernements et les entreprises qui relèvent de la juridiction d'États ayant approuvé un tel système au titre d'un accord international.

68. Un instrument juridique relatif à la surveillance du cyberspace ne doit pas être confondu avec un accord global sur la gouvernance d'Internet ou une « Convention de Genève relative à Internet », pour reprendre les mots de certains. De nombreux aspects de la gouvernance d'Internet resteront en dehors du champ d'application d'un tel instrument, notamment, et ce n'est pas le moindre, l'autre droit évoqué à l'article 12 de la Déclaration universelle des droits de l'homme et à l'article 17 du Pacte international relatif aux droits civils et politiques, à savoir le droit à la protection de la réputation, primordial et pourtant souvent négligé, qui est à la fois semblable au droit à la vie privée et différent.

À quel moment les dispositions de droit international, en particulier celles concernant un instrument juridique réglementant la surveillance, sont à un stade d'élaboration suffisamment avancé pour faire l'objet d'un examen à plus grande échelle

69. En résumé, un instrument juridique relatif à la surveillance dans le cyberspace viendrait compléter la législation existante, notamment la Convention sur la cybercriminalité, et pourrait faciliter considérablement l'établissement de garanties de la vie privée sur Internet. Par chance pour le Rapporteur spécial, un projet relatif à la gestion de solutions alternatives en faveur de la protection de la vie privée, de la propriété intellectuelle et de la gouvernance d'Internet (projet MAPPING) subventionné par l'Union européenne a déjà été lancé, et les moyens d'élaborer un instrument juridique régissant la surveillance dans le cyberspace sont actuellement étudiés dans le cadre de cette initiative. Un projet de texte a été rédigé ; il est actuellement examiné par des experts issus de la société civile et de certaines des plus grandes entreprises internationales et devrait être rendu public dans le courant de 2017 ou, au plus tard, avant le printemps 2018. Il serait prématuré pour quiconque, y compris le Rapporteur spécial, de prendre une position sur ce texte, ou un autre texte similaire, alors que l'on commence seulement à étudier les différentes options. Ce projet de texte pourrait bien s'avérer un précieux tremplin pour la tenue de dialogues intergouvernementaux sous les auspices des organisations intergouvernementales, notamment, pour ne pas dire en particulier, l'Organisation des Nations Unies.

70. À l'heure où le Rapporteur spécial se prépare à examiner la question, ce qu'il fera plus particulièrement entre mars et juillet 2018, il serait bon que le pouvoir exécutif de nombreux pays soit chargé par le parlement – et, dans les cas où des élections sont prévues en 2017 et 2018, le corps électoral – d'étudier activement les moyens de réglementer convenablement les activités de surveillance et de mettre en place des garanties et des voies de recours respectueuses de la vie privée dans le cyberspace. Non seulement cela aurait une grande valeur intrinsèque pour les citoyens du monde entier, mais cela adresserait un message sans équivoque aux États, aux démocraties, aux pseudo-démocraties et aux autres acteurs qui pensent à tort que la meilleure manière d'évoluer dans le cyberspace est d'affirmer leur souveraineté sur des parties d'Internet et sur les activités en ligne de leurs ressortissants. Les droits de l'homme sont universels, et la législation relative au cyberspace devrait être conçue de façon à protéger l'ensemble des droits de l'homme, et pas seulement le droit à la vie privée.

71. Une telle tâche est, certes, difficile, mais pas impossible. Il est à la fois plausible et logique qu'un grand nombre d'États finissent par s'accorder sur un instrument juridique qui régisse la surveillance et protège la vie privée dans le cyberspace. Un tel instrument serait bénéfique pour les citoyens, pour les gouvernements, pour le respect de la vie privée et pour les entreprises. Le nombre d'États adhérant aux nouveaux principes et mécanismes pourrait croître progressivement pour atteindre une masse critique. C'est ce qu'on a observé concernant l'évolution du droit international au cours des siècles passés, et il n'y a pas de raison qu'il en aille différemment pour la législation relative à la vie privée, à la surveillance et au cyberspace. Le processus n'aboutira peut-être pas avant la fin du mandat du Rapporteur spécial, mais cette manière de procéder est probablement la plus prometteuse. Tout ce que le Rapporteur spécial a observé depuis le début de son mandat l'a persuadé que c'était la voie la plus judicieuse à emprunter le moment venu, et ce moment pourrait bien arriver plus tôt qu'on ne le pense.