



Assemblée générale

Distr. générale
30 août 2016
Français
Original; anglais

Soixante et onzième session

Point 69 b) de l'ordre du jour provisoire*

Promotion et protection des droits de l'homme :
questions relatives aux droits de l'homme,
y compris les divers moyens de mieux assurer
l'exercice effectif des droits de l'homme
et des libertés fondamentales

Droit à la vie privée**

Note du Secrétaire général

Le Secrétaire général à l'honneur de transmettre à l'Assemblée générale le rapport établi par le Rapporteur spécial sur le droit à la vie privée, Joseph A. Cannataci, en application des résolutions 68/167 de l'Assemblée et 28/16 du Conseil des droits de l'homme.

* A/71/150.

** Le présent rapport a été soumis après la date limite, afin de prendre en compte l'évolution récente de la situation.



Rapport du Rapporteur spécial sur le droit à la vie privée

Résumé

Le présent rapport est le premier soumis à l'Assemblée générale par le Rapporteur spécial sur le droit à la vie. Il a été rédigé un peu plus d'un an après la prise de fonctions du Rapporteur spécial le 1^{er} août 2015 et exactement cinq mois après que celui-ci a présenté son premier rapport au Conseil des droits de l'homme le 9 mars 2016. Jusqu'alors, le Rapporteur spécial s'était attaché à recenser un certain nombre de thèmes qui avaient été mis en avant lors des nombreuses consultations qu'il avait eues avec plusieurs parties prenantes comme étant des axes de travail importants en matière de protection de la vie privée à l'ère du numérique.

Au cours des cinq mois qui ont suivi, le Rapporteur spécial a défini un premier groupe de cinq priorités, comme indiqué dans le présent rapport, sur lesquelles il a commencé à travailler en parallèle. Appelées Lignes d'action thématique (LAT), ces priorités concernent les mégadonnées et les données ouvertes; la sécurité et la surveillance; les données sur la santé; les données à caractère personnel traitées par les entreprises; et doivent permettre de « mieux comprendre la notion de vie privée ». La méthode choisie par le Rapporteur spécial prévoit la mise sur pied d'une équipe spéciale – que certains appelleraient groupe de travail – composée de bénévoles très expérimentés. Un groupe de travail sera créé pour chaque LAT afin d'aider le Rapporteur spécial à préparer et à élaborer une étude thématique qui fera ensuite l'objet d'un rapport au Conseil des droits de l'homme ou à l'Assemblée générale et qui sera présenté au cours de la période 2017-2018.

Le Rapporteur spécial souhaite qu'il soit tenu compte de la répartition géographique, de la diversité culturelle et ethnique, de la représentation des parties prenantes ainsi que d'une représentation équilibrée des sexes au sein de ces équipes spéciales ou groupes de travail. Ainsi, à titre d'exemple, l'Équipe spéciale en charge des mégadonnées et des données ouvertes sera présidée par David Watts, Commissaire chargé de la vie privée et de la protection des données de l'État de Victoria en Australie, tandis que l'Équipe spéciale en charge des données sur la santé sera présidée par Steve Steffensen, Chef du système de santé axé sur le patient à Dell Medical School à Austin au Texas (États-Unis d'Amérique). Au moment de la rédaction du présent rapport, le recrutement des présidents et des membres de certaines équipes spéciales par le Rapporteur spécial était toujours en cours. La composition exacte de chaque Équipe spéciale sera annoncée en temps voulu, probablement d'ici à mars 2017. Chaque Équipe spéciale devrait convoquer des réunions et organiser, le cas échéant, des manifestations publiques, semi-publiques et à huis clos, afin de recueillir des informations mais aussi de définir des stratégies éventuelles susceptibles d'offrir de meilleurs garanties et voies de recours en matière de vie privée dans un secteur d'activité déterminé.

Ainsi, la première activité menée par l'Équipe spéciale chargée de la sécurité et de la surveillance a consisté à mettre sur pied un forum international de surveillance du renseignement (IIOF 2016) qui se tiendra à Bucarest en octobre 2016 et auquel devraient participer plusieurs douzaines d'agences de surveillance et de commissions parlementaires. Ce forum permettra de recenser collectivement les atteintes à la vie privée et à la liberté d'expression dans la collecte de renseignements ainsi que les meilleures pratiques susceptibles d'améliorer les garanties et voies de recours dans

ce domaine. Entre-temps, l'Équipe spéciale chargée d'assurer « une meilleure compréhension de la vie privée » a déjà organisé sa première manifestation à New York les 19 et 20 juillet 2016. Cette Équipe spéciale devrait être la dernière des cinq à soumettre son rapport, certainement pas avant 2018, dans la mesure où plusieurs autres consultations devront probablement être menées dans diverses régions, notamment en Afrique, en Asie, en Australie, en Europe et en Amérique du Sud. Cette équipe a déjà commencé à rassembler des informations sur des concepts tels que la relation entre la vie privée et le droit fondamental général au libre épanouissement de la personnalité. Ses activités devraient constituer un processus continu qui à la fois sous-tendrait et s'inspirerait des constatations de l'ensemble des autres équipes

Alors que les cinq Équipes spéciales fournissent déjà une orientation thématique, le Rapporteur spécial a continué de suivre l'évolution de la situation dans plusieurs douzaines de pays et a entamé un programme de visites de pays informelles qui garantissent un maximum d'interactions avec le plus grand nombre d'acteurs possible à l'occasion de chacune d'entre elles. Au cours des cinq mois allant de mars à août 2016, le Rapporteur spécial a pris part à de nombreuses activités, parfois pendant toute une semaine, dans 11 pays aussi divers et aussi éloignés géographiquement que l'Allemagne, l'Australie, l'Autriche, le Danemark, les États-Unis d'Amérique, la France, l'Italie, la Lettonie, la Nouvelle-Zélande, les Pays-Bas, et la Suisse. Au cours des prochains mois, le Rapporteur spécial devrait effectuer des visites de pays et de terrain aussi bien formelles qu'informelles en Amérique du Sud, en Espagne, aux États-Unis d'Amérique, en France, en Indonésie, en Irlande du Nord (Royaume-Uni de Grande-Bretagne et d'Irlande du Nord), en Israël et au Maroc. Ce programme de travail intense est mené à bien avec l'assistance directe des États, des commissaires en charge de la protection de la vie privée et des données, des instituts des droits de l'homme, des organisations non gouvernementales et des universités.

Table des matières

	<i>Page</i>
I. Introduction	5
A. Présentation	5
B. Observations préliminaires et initiatives de suivi	5
II. Principales activités menées par le Rapporteur spécial	5
A. Ressources nécessaires à l'exécution du mandat du Rapporteur spécial	5
B. Préparation et lancement de multiples activités en rapport avec le mandat	7
C. Participation à de nombreuses manifestations	12
III. Affaires récentes et questions de fond, mars-juillet 2016	13
A. Le droit de garder le silence (<i>nemo tenetur se ipsum accusare</i>) : peut-on produire en justice les données saisies sur un smartphone ou le risque d'atteinte à la vie privée est-il trop grand?	13
B. Conservation des données, surveillance de masse et recours croissant au chiffrement des données	19
C. Meilleure prise en compte du lien entre la vie privée et la personnalité	23
IV. Conclusions	24

I. Introduction

A. Présentation

1. Le présent rapport doit être communiqué à l'Organisation des Nations Unies et faire l'objet d'une traduction vers le 9 août 2016 avant d'être soumis à l'Assemblée générale en octobre 2016, soit approximativement 18 mois après que le Conseil des droits de l'homme a décidé dans sa résolution 28/16 d'établir un mandat sur le droit à la vie privée et un an après que le Haut-Commissaire aux droits de l'homme a pris ses fonctions. À ce stade, le Rapporteur spécial, Joseph A. Cannataci note que les initiatives prises jusque-là ont suscité un grand nombre de réactions, pour la plupart, positives. Le présent rapport mettra en exergue les résultats obtenus grâce aux efforts déployés par le Rapporteur spécial ainsi que l'essentiel des activités à venir.

B. Observations préliminaires et initiatives de suivi

2. Un plan d'action en 10 points a déjà été présenté dans le premier rapport du Conseil des droits de l'homme en mars 2016 (voir A/HRC/31/64, par. 46). Les observations recueillies à cet égard ont été très positives. Par conséquent, le Rapporteur spécial poursuivra ses efforts dans ce sens avec pour objectif de présenter des résultats concrets au cours de son mandat en coopération avec les parties intéressées.

3. L'expérience accumulée au cours des 12 premiers mois du mandat ainsi que le suivi de l'évolution récente dans ce domaine ont montré que certaines questions exigent des réponses plus rapides et déterminées que d'autres. C'est pourquoi un premier ensemble de cinq priorités a été défini. Le Rapporteur spécial prévoit de prendre des mesures appropriées et de présenter, dans différents rapports thématiques, les conclusions des recherches menées dans ces domaines de priorité.

II. Principales activités menées par le Rapporteur spécial

A. Ressources nécessaires à l'exécution du mandat du Rapporteur spécial

4. On ne peut gagner une guerre sans armée. Étant donné qu'il s'agit d'un nouveau mandat, aucune équipe n'était en place quand le Rapporteur spécial a pris ses fonctions, et il a dû consacrer énormément de temps, en dehors de l'ONU, à la recherche des ressources dont il avait besoin. Même si celles fournies par l'ONU avaient été à la hauteur, en quantité et en qualité, ce qui est loin d'avoir été le cas, pour s'acquitter pleinement de ses fonctions, le Rapporteur spécial doit disposer de ressources largement supérieures à celles prévues par l'ONU. Assurer le suivi de l'application de la législation relative à la vie privée et des activités de surveillance dans plus de 190 États, exige de disposer de plusieurs dizaines de personnes. Aller au-devant de la société civile et comprendre ses besoins, ainsi qu'interagir constamment avec les entreprises, les forces de maintien de l'ordre, les services de renseignement et les responsables politiques, nécessite également un investissement important en temps et en énergie de la part du personnel. Organiser des réunions de concertations sur les cinq Lignes d'action thématiques présentées plus haut, requiert

aussi des effectifs non négligeables. Actuellement, la contribution de l'Organisations des Nations Unies à ces effectifs est faible, surtout du fait que les critères exigés incluent de justifier d'une expérience dans ce domaine et d'être spécialisé en droit à la vie privée. Il suffit également de souligner qu'actuellement 90 % des fonds destinés à financer les effectifs contribuant à l'exécution du mandat et environ 80 % de ceux devant couvrir les frais des voyages effectués au cours du mandat, ont dû être trouvés en dehors de l'ONU. En outre, d'importants obstacles administratifs au sein du système font qu'il est difficile de se concentrer sur le fond du mandat.

5. S'agissant des ressources, c'est un euphémisme que de dire que l'assistance fournie au Rapporteur spécial par le Haut-Commissariat des Nations Unies aux droits de l'homme est loin d'être satisfaisante. Si comme le dit la maxime latine contre un fait il n'est point d'arguties, alors laissons parler les faits.

a) Le Rapporteur spécial n'a nul besoin de bureaucrates de la catégorie des services généraux. Ce qu'il recherche, ce sont des personnes ayant des qualifications dans le domaine du droit à la vie privée, c'est-à-dire des compétences qui ne s'acquièrent que par une formation sanctionnée par un diplôme reconnu et une expérience personnelle. Il a donc informé en conséquence les responsables des procédures spéciales du Haut-Commissariat des Nations Unies aux droits de l'homme et un poste de spécialiste des droits de l'homme de la classe (P-3) a effectivement été publié en février 2016, indiquant que la préférence serait accordée aux candidats possédant des qualifications et une expérience dans le domaine du droit à la vie privée. Le Rapporteur spécial a été informé que 349 candidatures avaient ensuite été reçues mais qu'à aucun moment le contenu de ces candidatures n'avait été pris en compte. Le Rapporteur spécial n'a pas pris connaissance de ces candidatures mais des membres d'organisations non gouvernementales lui ont laissé entendre que des titulaires de doctorat en droit à la vie privée avaient postulé;

b) Les haut fonctionnaires du Haut-Commissariat des Nations Unies aux droits de l'homme chargés du mandat du Rapporteur spécial ont totalement ignoré les candidatures reçues et le 4 août 2016, ils l'ont informé qu'ils avaient nommé un spécialiste des droits de l'homme titulaire d'un contrat permanent, choisi parmi une liste interne de candidats présélectionnés. Ce spécialiste des droits de l'homme n'a pas de formation sanctionnée par un diplôme ni de compétences dans le domaine du droit à la vie privée et encore moins d'expérience ou de connaissances approfondies à cet égard, il ne possède que quelques vagues notions de la matière concernée. Le 8 août, le Rapporteur spécial a adressé une note officielle au Président du Conseil des droits de l'homme pour lui demander d'intervenir. Il lui a fait savoir qu'il se dissociait de cette procédure de recrutement et qu'il émettait de vives réserves quant à l'équité de cette procédure et à ses résultats;

c) Jusqu'à la rédaction de cette note, le Rapporteur spécial n'avait été assisté que par un seul spécialiste des droits de l'homme à la fois, l'actuel étant le troisième d'une succession de personnel temporaire. À un moment donné, le poste de spécialiste des droits de l'homme est resté vacant durant un mois entier du fait de complications contractuelles. Aucun de ces spécialistes des droits de l'homme n'avait reçu de formation ni obtenu de diplôme dans le domaine concerné, ni acquis d'expérience en la matière, à l'exception du dernier en date recruté en juillet 2016, lequel pourrait rester plus longtemps, et qui possède une expérience limitée du droit à la vie privée dans le cadre de la procédure spéciale sur la liberté d'expression. Sans remettre en cause leur personnalité amène et leurs compétences dans d'autres

domaines relatifs aux droits de l'homme, il est très difficile d'assurer et de maintenir la continuité et l'efficacité en de telles circonstances;

d) Le 4 août 2016, le Rapporteur spécial a été informé qu'outre le spécialiste permanent des droits de l'homme mentionné à l'alinéa b) ci-dessus, qui travaillera à temps plein pour le Rapporteur spécial à compter du 1^{er} septembre 2016, un poste à mi-temps de classe P-3 et un autre à mi-temps d'agent de la catégorie des services généraux (assistant administratif) seront probablement pourvus après ou durant le mois de septembre. Vu l'efficacité démontrée jusqu'à présent, je ne nourris guère d'espoir;

e) Le niveau d'inefficacité est tel que le remboursement partiel des frais afférents à un voyage autorisé effectué au quatrième trimestre de 2015 est toujours en souffrance; alors que le Rapporteur spécial ne perçoit aucun salaire pour le travail qu'il effectue.

6. Si la maigre assistance fournie par le Haut-Commissariat des Nations Unies aux droits de l'homme a été présentée en détail (mais pas de façon exhaustive) dans le précédent paragraphe, c'est pour garantir que ni l'Assemblée générale des Nations Unies ni le Conseil des droits de l'homme n'aillent s'imaginer que le Rapporteur spécial s'acquitte de ses tâches grâce à un quelconque appui qui serait d'une efficacité incroyable ou à une aide généreuse du HCDH. Je ne souhaite pas revenir sur cette question dans les prochains rapports. Si l'Assemblée générale ou le Conseil des droits de l'homme ne reçoivent pas d'autres observations du Rapporteur spécial à cet égard, ils devraient en conclure que la situation ne s'est pas suffisamment améliorée pour que l'on puisse en faire état. Cela étant, il ne s'agit pas ici de faire la critique des budgets alloués : je laisse cette tâche au futur Secrétaire général de l'ONU qui espérons-le, sera réformateur. Il décidera lui-même si la situation décrite dans les paragraphes précédents est le résultat d'un système désespérément inefficace et qui a grand besoin d'être réformé, ou le fait d'une coterie de fonctionnaires internationaux motivés par leurs intérêts personnels et plus désireux de poursuivre leurs petits arrangements entre amis que de fournir au Rapporteur spécial l'assistance nécessaire à l'accomplissement de son mandat, tant en termes de qualité que de quantité. Si vous représentez un État ou une organisation qui est sincèrement convaincue de l'importance du mandat et qui souhaiterait contribuer, veuillez contacter directement le Rapporteur spécial afin de chercher des moyens d'accroître et d'améliorer l'assistance fournie.

B. Préparation et lancement de multiples activités en rapport avec le mandat

7. Malgré les problèmes administratifs et les problèmes de ressources susmentionnés, le Rapporteur spécial et son équipe sont parvenus à lancer de multiples activités grâce au soutien apporté par de nombreux acteurs de la société civile et d'autres parties prenantes attachées à la cause. Ces activités recouvrent deux grands domaines : le suivi des activités menées dans les différents États Membres et les travaux relatifs aux Lignes d'action thématique définies ci-après.

8. Une part importante des travaux de suivi menés quotidiennement par le Rapporteur spécial consiste à examiner les nouvelles activités de surveillance mises en place dans plusieurs dizaines d'États Membres ainsi que les lois de surveillance et les lois relatives à la protection de la vie privée qui y sont élaborées. Cela

suppose d'examiner chaque nouvelle technologie utilisée et chaque nouvelle loi proposée, ainsi que d'enquêter sur les griefs portés à la connaissance du titulaire de mandat par les personnes concernées ou la société civile. Cette activité de suivi, par les informations qu'elle permet de compiler, est déterminante dans le choix que fait le Rapporteur spécial de se déplacer dans tel ou tel pays, à titre officiel ou non.

9. Outre les activités – très chronophages – visant tel ou tel pays, beaucoup d'attention et d'efforts ont été consacrés aux priorités thématiques. Certains domaines couverts par le plan d'action en dix points qui a été présenté au Conseil des droits de l'homme dans le rapport soumis en mars 2016 requièrent une attention immédiate et des mesures rapides. Ces domaines ont été définis avec soin et constitueront désormais des Lignes d'action thématique¹. Au cours de cette première phase, cinq Lignes d'action thématique ont été établies, dans chacun des domaines prioritaires suivants : mégadonnées et données ouvertes; sécurité et surveillance; données relatives à la santé; données personnelles traitées par les entreprises; « Une meilleure compréhension de la notion de vie privée ». Chaque Ligne d'action devra suivre sa propre dynamique, tout en interagissant avec les autres, afin de permettre au Rapporteur spécial d'établir un rapport thématique une fois que l'examen d'une Ligne d'action particulière aura suffisamment progressé.



10. Dans le cadre de la démarche adoptée, le Rapporteur spécial prévoit la mise sur pied d'équipes spéciales – certains parleront de « groupes de travail » – composées de bénévoles très expérimentés. Un groupe de travail sera affecté à chaque Ligne d'action

¹ Pour plus d'informations sur le sujet, on lira le billet que le Rapporteur spécial a publié sur son blog le 3 juin 2016, intitulé : « Parallel streams of action (TAS) for the mandate of the United Nations Special Rapporteur for privacy and the first set of priorities » (<https://www.privacyandpersonality.org/2016/06/privacy-and-personality-blog-3-parallel-streams-of-action-tas-for-the-mandate-of-the-un-special-rapporteur-for-privacy-and-the-first-set-of-priorities/>).

thématique et aura pour tâche d'aider le Rapporteur spécial à préparer et établir une étude thématique qui fera ensuite l'objet d'un rapport au Conseil des droits de l'homme ou à l'Assemblée générale et sera présenté durant la période 2017-2018.

11. Des recherches documentaires et les nombreuses réunions multipartites et les activités d'information organisées durant les déplacements effectués de mars à juillet 2016 en Allemagne, en Australie, en Autriche, au Danemark, aux États-Unis d'Amérique, en France, en Italie, en Lettonie, en Nouvelle Zélande, aux Pays-Bas et en Suisse ont convaincu le Rapporteur spécial d'inclure les mégadonnées et les données ouvertes dans les domaines prioritaires. Une équipe spéciale a été constituée en mai 2016 et David Watts, Commissaire chargé de la vie privée et de la protection des données de l'État de Victoria (Australie), a accepté, à l'invitation du Rapporteur spécial, d'en prendre la tête. L'équipe a entamé ses travaux en juin, élaborant une première ébauche de ses objectifs de travail et recrutant ses premiers membres. Le 20 juillet 2016, lors d'une manifestation organisée à New York par le Rapporteur spécial, celui-ci et M. Watts ont présenté les grandes lignes du programme de travail, tout en invitant les participants à formuler des observations et à rejoindre le groupe de travail. Par la suite, des experts originaires de pays tels que le Brésil, le Canada, les États-Unis, la France et le Sénégal ont fait des offres de collaboration. L'annonce de la composition de l'équipe et la publication d'une première esquisse des objectifs et d'un projet de mandat devraient avoir lieu avant la fin du mois d'octobre 2016. L'équipe sollicite également l'assistance d'organisations indépendantes désireuses de l'aider à tester la résistance des solutions techniques qui, selon leur concepteurs, sont en mesure de rendre anonymes les données personnelles de façon irréversible même dans le cas où l'analyse des mégadonnées permet d'effectuer des recoupements à partir de sources de données ouvertes.

12. La question de la sécurité et de la surveillance a toujours fait partie des principales priorités du Rapporteur spécial. En raison de la complexité de la question, et du fait qu'elle intéresse les services de police et les services de sécurité et de renseignement et touche aux activités de plusieurs grandes entreprises, il a fallu commencer par scinder le sujet en sous-thèmes, l'objectif principal étant toujours de définir et de renforcer les mesures de protection et de recours en matière de vie privée. La première grande initiative lancée à cet égard par le Rapporteur spécial a été de créer le Forum international de contrôle des services de renseignement, qui se tiendra à Bucarest en octobre 2016 et auquel devraient participer les représentants de plusieurs dizaines d'organes de contrôle, de commissions parlementaires et de services de renseignement. Ce forum permettra de recenser ensemble les menaces que fait peser la collecte de renseignements sur la protection de la vie privée et la liberté d'expression ainsi que les meilleures pratiques susceptibles d'aider le Rapporteur spécial et toutes les parties prenantes à définir de meilleures mesures de protection et de recours. Le Rapporteur spécial a mené l'essentiel des travaux préparatoires du forum de mars à juillet 2016. La réaction des principaux États Membres de l'ONU a été très encourageante, plusieurs d'entre eux ayant déjà confirmé leur participation à cette rencontre qui, en cas de succès, pourrait être organisée régulièrement et contribuer ainsi aux rapports, recommandation et autres initiatives du Rapporteur spécial. Le Rapporteur spécial saisit cette occasion pour remercier publiquement les nombreux États Membres de l'Organisation qui ont apporté leur contribution à cette initiative, notamment les quatre commissions de contrôle des services de renseignement du Sénat et du Parlement roumains, qui ont accepté, à son invitation, d'accueillir conjointement

l'événement. Le Rapporteur spécial remercie également l'Agence des droits fondamentaux de l'Union européenne, qui appui l'événement de diverses manières. L'Équipe spéciale chargée des données personnelles traitées par les entreprises (voir ci-après) consacre également une partie de ses travaux à la surveillance. D'autres initiatives et travaux dans ce domaine pourraient être rendus publics ultérieurement.

13. Il ressort des échanges que le Rapporteur spécial mène régulièrement avec les parties prenantes et des recherches approfondies qu'il effectue dans ce domaine que, dans le monde entier, des quantités de données de santé sensibles toujours plus importantes continuent d'être créées, traitées, vendues et revendues. Non seulement ces pratiques font partie intégrante du modèles d'entreprise en vigueur dans un petit nombre de pays novateurs, mais elles sont également favorisées par la tendance de plus en plus forte qu'ont les consommateurs d'utiliser des technologies vestimentaires, des applications de smartphone et d'autres technologies mobiles qui stockent et transfèrent en permanence des données de tout type potentiellement sensibles sur la santé et le style de vie. En outre, les expériences menées dans certains pays consistant à exploiter les dossiers médicaux existants afin d'améliorer le diagnostic par l'utilisation de techniques d'intelligence artificielle peuvent également susciter l'inquiétude. Il est toutefois incontestable que l'utilisation des données de santé présente plusieurs avantages, notamment en matière de recherche médicale. Il ressort également de certaines études de marché indépendantes que les patients sont de plus en plus inquiets à l'idée de voir leurs données personnelles utilisées à de mauvaises fins. Afin que ses travaux sur les données de santé se poursuivent de façon structurée, et après avoir consulté les principales organisations non gouvernementales intervenant dans ce domaine, le Rapporteur spécial a le plaisir d'annoncer que le docteur Steve Steffenson de l'hôpital Dell de l'Université du Texas (États-Unis) a accepté de présider le groupe de travail « MedITAS » chargé de la question. Les autres membres du groupe sont en cours de recrutement. Le projet de mandat qui a déjà été élaboré devrait être complété et adopté dès que le groupe de travail commencera ses travaux au début du quatrième trimestre de l'année 2016.

14. Le Rapporteur spécial met à profit la collaboration qu'il a développée avec de grandes entreprises dans le cadre de projets antérieurs ou en cours, notamment 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 ») financé par l'Union européenne, afin de continuer d'étudier les conséquences qu'a l'utilisation croissante de données personnelles par les entreprises sur la vie privée. Il continue notamment de tirer parti des travaux qu'il mène avec les entreprises dans au moins trois volets du projet MAPPING – droit international, modèles d'entreprise et vie privée –, qui devraient lui permettre d'enrichir ses propres travaux sur le sujet et aboutir à l'élaboration, dans le cadre du projet MAPPING, d'un document d'orientation et d'une feuille de route qui seront soumis à l'Union européenne. Certains de ces travaux intéressent également les activités de surveillance des gouvernements et devraient conduire à une rencontre avec la société civile lors d'une manifestation qui sera organisée conjointement les 15 et 16 février 2017 par le Rapporteur spécial et le projet MAPPING. Le Rapporteur spécial tient à remercier plusieurs grandes entreprises, notamment Microsoft, Google, Facebook, Apple et Yahoo, ainsi que la coalition Global Network Initiative, qui ont bien voulu continuer de prêter leur collaboration aux activités du Rapporteur spécial et du projet MAPPING. Le Rapporteur spécial invite toutes les parties prenantes à

s'associer en temps voulu à ces activités ou à manifester leur intérêt sur cette question ou à l'égard de toute initiative de l'équipe spéciale.

15. Autre initiative de long terme prise dans ce domaine, le Rapporteur spécial a mis sur pied une équipe spéciale chargée d'apporter « une meilleure compréhension de la notion de vie privée ». Il est prévu qu'elle soit la dernière à présenter son rapport, certainement pas avant 2018, dans la mesure où plusieurs autres consultations devront probablement être menées dans diverses régions, notamment en Afrique, en Asie, en Australie, en Europe et en Amérique du Sud. L'équipe a déjà commencé à s'intéresser à plusieurs notions, notamment à l'articulation entre la vie privée et le droit fondamental au libre épanouissement de la personnalité. Ses activités devront se dérouler de façon progressive et venir tout à la fois alimenter les travaux des autres équipes spéciales créées par le Rapporteur spécial et s'en inspirer. Il lui faudra également apporter une grande attention à la relation entre le droit au respect de la vie privée et d'autres droits fondamentaux tels que la liberté d'expression et le libre accès à l'information. Grâce à des contacts pris avec Human Rights Watch dès septembre 2015, l'équipe spéciale a été en mesure d'organiser sa première manifestation sur le sujet, intitulée « Vie privée, personnalité et circulation de l'information », qui s'est tenue à New York les 19 et 20 juillet 2016. Cette rencontre qui pendant deux jours a fait salle comble (90 places), a pu être organisée grâce à la générosité et aux efforts conjugués de Human Rights Watch, du Brennan Center for Justice de la faculté de droit de l'Université de New York, du Global Freedom of Expression de l'Université de Columbia, du projet MAPPING, du Département de la politique de l'information et de la gouvernance de l'Université de Malte et du STeP, le groupe de recherche sur la sécurité, la technologie et la vie privée sur Internet de l'Université de Groningen (Pays-Bas). Le Rapporteur spécial remercie également le Gouvernement allemand qui a mis à sa disposition une partie des sommes ayant permis à plusieurs personnes à travers le monde d'assister à cette manifestation.

16. Même si le point de vue des participants locaux (États-Unis) a été le mieux représenté, des participants originaires d'Australie, du Brésil, du Canada, de la Colombie, de l'Inde, de la République de Corée, du Moyen-Orient, de l'Afrique du Nord et d'Europe², ainsi que des représentants de l'Organisation des Nations Unies pour l'éducation, la science et la culture, ont également pu faire partager leurs vues et leurs connaissances. Lors de la première journée, le principal objectif de la réunion a été de chercher à mieux comprendre ce que signifiait la vie privée en tant que droit de l'homme universel à l'ère du numérique et à déterminer si ce droit devait être interprété de façon plus large de façon à y inclure l'épanouissement personnel. Le deuxième jour, l'objectif a été de faciliter la compréhension et l'élaboration de stratégies de sensibilisation visant à promouvoir plus efficacement le droit au respect de la vie privée à l'échelle mondiale. Fiers du succès de cette réunion pilote, plusieurs autres manifestations sur le même thème seront organisées sur tous les continents, afin de rassembler le plus d'opinions possibles sur la question, l'objectif étant d'établir et d'approfondir une conception plus large de la vie privée et de ses interprétations à l'ère du numérique dans l'intérêt de la

² Plus précisément, la conception allemande de « l'autonomie de décision en matière d'information » et de la protection de la vie privée (« *Datenschutz* ») a été examinée et pourrait servir de base pour concevoir la vie privée comme un droit contribuant au développement de la personnalité. Le Rapporteur spécial remercie Christian Hawellek de l'Institut für Rechtsinformatik de l'Université Leibniz de Hanovre pour sa contribution.

communauté mondiale. Par conséquent, alors que sont en cours les préparatifs de la prochaine manifestation, prévue en Asie, le Rapporteur spécial voudrait inviter toutes les parties désireuses de soutenir ou d'accueillir une rencontre de ce type ou d'y participer dans un avenir proche à le contacter directement.

17. Dans le cadre notamment des travaux entrepris pour mener à bien la mission qui lui a été confiée, le Rapporteur spécial et son équipe ont créé un blog consacré à la question de la vie privée et de la personnalité, que l'on peut consulter à l'adresse suivante : www.privacyandpersonality.org.

C. Participation à de nombreuses manifestations

18. En sus des activités susmentionnées, le Rapporteur spécial a, depuis le 3 mars 2016, participé à de nombreuses manifestations, énumérées ci-après, afin de sensibiliser aux questions de vie privée ainsi qu'il était énoncé dans le plan d'action en 10 points :

- a) Intervention devant l'Institut du droit international de la paix et des conflits armés, Bochum (Allemagne), le 15 mars;
- b) Réunion avec le Président de la Commission nationale de l'informatique et des libertés et le Président du Groupe de travail de l'Union européenne sur l'article 29, Paris, le 18 mars;
- c) Participation à une table ronde lors du Sommet mondial sur la vie privée organisé par l'International Association of Privacy Professionals, Washington, le 5 avril;
- d) Intervention au colloque annuel du *Wisconsin International Law Journal*, Wisconsin (États-Unis), le 8 avril;
- e) Participation à l'atelier préparatoire au congrès annuel de l'Association Data Protection Officer, Milan (Italie), le 18 avril. L'atelier était consacré au Règlement général sur la protection des données et au rôle du délégué à la protection des données de l'Union européenne.
- f) Participation au Forum consacré aux politiques numériques futures tenu à l'Université de Columbia, New York, le 25 avril;
- g) Diverses interventions et participation à plusieurs réunions multipartites lors de la semaine consacrée au respect de la vie privée, Wellington et Auckland (Nouvelle-Zélande), du 9 au 13 mai;
- h) Diverses interventions et participation à plusieurs réunions multipartites lors de la semaine de sensibilisation au respect de la vie privée, Sydney et Canberra (Australie), du 14 au 18 mai;
- i) Participation au colloque de 2016 sur la recherche et l'innovation en matière de sécurité, La Haye, les 1^{er} et 2 juin;
- j) Participation à une table ronde (« La question de la vie privée sous le prochain gouvernement américain ») lors de la conférence de 2016 sur la protection des données organisée par l'Electronic Privacy Information Center, Washington, le 6 juin;

- k) Intervention lors du sixième sommet international sur l'avenir de la confidentialité des données de santé, Washington, le 7 juin;
- l) Rencontre entre les participants au projet MAPPING et le Rapporteur spécial organisée par Alvaro Bedoya au Centre sur la vie privée et les technologies de la faculté de droit de Georgetown, Washington, le 8 juin;
- m) Réunions avec des représentants de Google, de Facebook et du Département d'État des États-Unis, Washington, les 9 et 10 juin;
- n) Lecture publique et intervention devant DataEthics.EU et l'Institut danois pour les droits de l'homme, Copenhague, le 13 juin;
- o) Participation à une table ronde organisée par l'Association pour le progrès des communications, Genève, le 14 juin;
- p) Intervention lors d'un atelier organisé par le Comité international de la Croix-Rouge, Genève, le 14 juin;
- q) Discussion en ligne avec les membres de l'Internet Society (Association Internet), Genève, le 14 juin;
- r) Intervention à la conférence « La Convention n° 108 : d'une réalité européenne vers un traité universel » organisée par le Conseil de l'Europe, Strasbourg (France), le 17 juin;
- s) Participation au Forum des droits fondamentaux organisé par l'Agence des droits fondamentaux de l'Union européenne, Vienne, les 20 et 21 juin;
- t) Participation à un débat du séminaire Alpbach (« Time to share: places for everyone »), organisé en coopération avec *Wiener Zeitung*, Vienne, le 22 juin;
- u) Participation au groupe de travail n° 25 sur le rôle et la responsabilité des entreprises dans le respect de la vie privée dans un contexte de sécurité accrue en Europe, Vienne, le 23 juin;
- v) Participation au deuxième Forum européen sur l'initiation aux médias et à l'information, Riga, du 27 au 29 juin;
- w) « Vie privée, personnalité et circulation de l'information », conférence du Rapporteur spécial, New York, les 19 et 20 juillet.

III. Affaires récentes et questions de fond, mars-juillet 2016

A. Le droit de garder le silence (*nemo tenetur se ipsum accusare*) : peut-on produire en justice les données saisies sur un smartphone ou le risque d'atteinte à la vie privée est-il trop grand?

19. L'année 2016 a vu resurgir le débat sur le chiffrement des données personnelles stockées ou générées par des appareils mobiles. L'affaire la plus emblématique et la plus médiatisée concerne le smartphone utilisé par l'un des auteurs de la terrible attaque terroriste perpétrée à San Bernardino (États-Unis) et la tentative faite par les autorités américaines pour récupérer les données personnelles stockées sur l'appareil de marque Apple. Le 2 décembre 2015, un homme et sa

femme ouvrent le feu dans les locaux de l'administration locale en Californie du Sud, faisant quatorze morts et une vingtaine de blessés graves³. Le Bureau d'enquête fédéral des États-Unis (FBI) veut avoir accès aux informations stockées sur l'appareil et synchronisées avec le service d'informatique en nuage d'Apple (iCloud). Alors que les données stockées en externe jusqu'au 19 octobre 2015 (date à laquelle les sauvegardes ont été arrêtées) peuvent être récupérées, celles stockées sur le smartphone ne sont accessibles ni au FBI ni à Apple. Le FBI tente de contraindre légalement Apple à modifier le logiciel du smartphone afin de le rendre plus vulnérable aux tentatives d'intrusion. Face au refus d'Apple, le FBI porte l'affaire en justice et fait pression sur l'entreprise. Finalement, le FBI trouvera un autre moyen de récupérer les données stockées sur le smartphone et, le 28 mars 2016, abandonnera ses poursuites contre Apple⁴. « Dès le début, nous nous sommes opposés à la demande du FBI qui nous enjoignait de créer une porte dérobée sur l'iPhone, car nous pensions que c'était une mauvaise chose à faire et que cela pouvait créer un précédent dangereux. Suite à l'abandon des poursuites par le Gouvernement, rien de cela n'est arrivé », a déclaré Apple après le classement de l'affaire⁵. Dans son rapport du 9 mars 2016, au paragraphe 30, le Rapporteur spécial a indiqué qu'il n'était pas souhaitable de permettre ou de rendre obligatoire la présence de portes dérobées pour accéder aux données chiffrées, et ce, pour plusieurs raisons, que le Gouvernement des Pays-Bas résume excellemment dans le document d'orientation qu'il a publié le 4 janvier 2016. L'affaire Apple a conforté le Rapporteur spécial dans son opinion. Néanmoins, les smartphones et autres appareils mobiles soulèvent d'autres questions de droits fondamentaux pouvant avoir des conséquences sur la vie privée et il convient sans doute de les examiner avant d'aller plus loin dans notre réflexion sur le chiffrement. Parmi ces droits fondamentaux figure celui de garder le silence.

20. À présent que l'affaire *Apple v. FBI* n'est plus entre les mains des juges, il faut souhaiter que les deux parties examinent la question de façon plus claire et moins passionnée. Des centaines de millions de smartphones de marque Apple ayant été vendus sur la planète, il apparaît toutefois que le problème ne concerne plus uniquement les États-Unis mais le monde entier. La même législation utilisée pour contraindre Apple à aider les services de police à accéder aux données dans cette affaire pourrait être appliquée à l'égard d'autres fabricants qui ont vendu des centaines de millions de smartphones de plus qu'Apple à travers le monde et ce, d'autant qu'un nombre croissant de fabricants équipent leurs produits de protections cryptographiques. Les économies d'échelle permettront rapidement à un tiers de la population mondiale de posséder et d'utiliser un smartphone, puis bientôt à la

³ Camilia Domonoske, « San Bernardino shootings: what we know, one day after », *National Public Radio*, le 3 décembre 2015 (www.npr.org/sections/thetwo-way/2015/12/03/458277103/san-bernardino-shootings-what-we-know-one-day-after).

⁴ Voir les articles ci-après publiés dans le *Guardian* : Danny Yadron, Spencer Ackerman and Sam Thielman, « Inside the FBI's encryption battle with Apple », le 18 février 2016 (<https://www.theguardian.com/technology/2016/feb/17/inside-the-fbis-encryption-battle-with-apple>); Danny Yadron, « San Bernardino iPhone: United States ends Apple case after accessing data without assistance », le 29 mars 2016 (<https://www.theguardian.com/technology/2016/mar/28/apple-fbi-case-dropped-san-bernardino-iphone>); Danny Yadron, « FBI confirms it won't tell Apple how it hacked San Bernardino shooter's iPhone », le 28 avril 2016 (<https://www.theguardian.com/technology/2016/apr/27/fbi-apple-iphone-secret-hack-san-bernardino>).

⁵ Hillary Brueck, « This is Apple's response to the FBI hacking into that iPhone », le 29 mars 2016 (<http://fortune.com/2016/03/29/apple-response-fbi>).

moitié. Comme nous le verrons ci-après, le constat est simple : le smartphone est une technologie universelle ayant des incidences considérables sur la vie privée.

21. Dans les observations qui vont suivre, le Rapporteur spécial va tenter de faire évoluer la réflexion sur les smartphones au-delà de la question de la vie privée, l'objectif étant de se recentrer le moment venu sur les enjeux fondamentaux une fois que nous aurons pris connaissance des valeurs sociales touchant à la situation dans son ensemble. De l'avis du Rapporteur spécial, il convient d'étudier d'autres normes et pratiques sociales avant de se prononcer de façon définitive sur certaines questions de vie privée que soulève l'utilisation des smartphones.

22. À l'instar de nombreux droits fondamentaux, le droit à la vie privée est un droit qui évolue. Si pendant des millénaires l'homme a été attaché à sa vie privée, cela ne signifie pas pour autant que l'étendue de ce droit et la protection qui lui a été accordée soient restés identiques, quand bien même on aurait évolué vers davantage de protection. La notion de vie privée a évolué au cours du temps. Bien avant la création du mandat du Rapporteur spécial et la nomination du présent titulaire, de nombreux éléments permettent d'établir que la compréhension de la notion et l'exercice du droit y afférent ont varié au fil du temps et selon les lieux⁶. Contrairement à ce que d'aucuns pensent, ce constat ne remet en cause ni l'existence ni l'universalité de ce droit, mais nous invite au contraire à réfléchir à l'ensemble complexe de valeurs qui le sous-tendent et à la façon dont, en faisant évoluer la conception que l'on en a en fonction des circonstances, l'on peut continuer de protéger ces valeurs, voire – dans la mesure du possible – mieux les protéger. L'apparition de nouvelles technologies et les utilisations qui en sont faites, dont le smartphone offre un exemple emblématique, nous obligent à revoir constamment notre conception de la vie privée. Ainsi que l'a fait observer Samuel Alito, juge à la Cour suprême des États-Unis, dans la célèbre affaire *Riley v. California* :

Nous ne devons pas appliquer systématiquement les règles en vigueur à l'ère pré-numérique à la saisie de données stockées sur téléphone portable. À l'heure actuelle, de nombreux téléphones portables permettent de stocker et d'afficher une grande quantité d'informations, parfois très personnelles, que personne n'aurait cru bon auparavant de transporter sur soi sur papier imprimé⁷.

Le juge Samuel Alito rejoint ainsi l'opinion majoritaire exprimée par John Roberts, Président de la Cour :

Les téléphones portables actuels ne sont pas de simples appareils utilitaires. Au regard de tout ce qu'ils contiennent et peuvent révéler, ils renferment en eux « l'intimité de la vie privée » de nombreux Américains. Le fait que la technologie permette aujourd'hui à tout un chacun de transporter sur soi ces informations ne signifie pas qu'elles ne doivent pas être protégées ainsi que l'ont voulu les Pères fondateurs⁷.

⁶ Pour une présentation plus complète de l'analyse du Rapporteur spécial selon laquelle la notion de vie privée a varié au fil du temps et selon les lieux durant le millénaire, voir Joseph A. Cannataci (dir.), *The Individual and Privacy* (Farnham, Royaume-Uni, Ashgate Publishing, 2015).

⁷ Cour suprême des États-Unis d'Amérique, *Riley v. California*, Décision du 25 juin 2014, n° 12-1332 (https://www.supremecourt.gov/opinions/13pdf/13-132_819c.pdf).

Il va sans dire que les Américains ne sont pas les seuls à abandonner à leur téléphone portable, volontairement ou non, « l'intimité de leur vie privée ». Tout détenteur de smartphone en fait de même partout sur la planète, quels que soient ses croyances, sa couleur, son origine ethnique, son sexe, sa nationalité ou sa situation géographique. C'est pourquoi nombre des observations contenues dans l'arrêt *Riley v. California* revêtent aussi une importance à l'échelle internationale. Le Rapporteur spécial va à présent citer de larges extraits de cet arrêt, dans la mesure où certains des arguments avancés, qui doivent être examinés à la lumière du différend entre Apple et le FBI, peuvent valoir quel que soit l'endroit du monde où le problème se pose.

23. Comme il a été dit dans l'arrêt *Riley v. California*, « les téléphones portables actuels sont tellement intégrés à la vie quotidienne qu'un Martien débarquant sur Terre pourrait croire qu'ils sont un trait essentiel de l'anatomie humaine. » Les juges de la Cour suprême ont fait observer à juste titre ce qui suit :

Les téléphones portables diffèrent des autres objets qu'une personne appréhendée peut transporter sur elle, tant sur le plan qualitatif que quantitatif. Le terme « téléphone portable » lui-même prête à confusion. La plupart de ces appareils sont en fait de petits ordinateurs qui se trouvent pouvoir aussi être utilisés comme téléphones. On pourrait tout aussi bien les appeler appareils photos, lecteurs vidéo, Rolodex, calendriers, magnétophones, livres, agendas, albums, télévisions, cartes ou encore journaux. L'une de leurs caractéristiques les plus remarquables est leur prodigieuse capacité de stockage. Avant leur apparition, la fouille d'une personne était soumise aux contraintes de la réalité physique et ne constituait généralement qu'une intrusion minime dans la vie privée⁷.

Les juges ont fait plus d'une fois observer ce qui suit :

À la différence des documents physiques, les téléphones portables se caractérisent par une certaine omniprésence. Avant l'ère numérique, bien rares étaient ceux qui, tout en vaquant à leurs occupations quotidiennes, avaient pour habitude de porter sur eux un lot de données personnelles sensibles. Aujourd'hui, l'exception est celui qui n'a pas sur lui de téléphone portable, avec tout ce qu'il contient. Selon une enquête, près des trois quarts des utilisateurs de smartphone indiquent se trouver la plupart du temps dans un rayon de deux mètres de leur appareil, 12 % déclarant même s'en servir sous la douche⁷.

Les juges ont souligné de même la manière dont on pouvait à partir d'un smartphone établir un profil très précis et exact de son utilisateur :

Les données enregistrées sur un téléphone portable se distinguent des données physiques d'un point de vue quantitatif et, pour certaines d'entre elles également, d'un point de vue qualitatif. Ainsi, l'on peut extraire d'un téléphone connecté à Internet les résultats d'une recherche sur Internet et l'historique de navigation, qui pourront révéler les centres d'intérêt personnels ou les préoccupations d'un individu – par exemple, la recherche de certains symptômes de maladie, associée à des consultations fréquentes du site WebMD. Les données stockées sur un téléphone portable permettent en outre de connaître les lieux fréquentés par une personne⁷.

24. Fait sans doute plus important encore, les juges ont pris conscience que les informations contenues dans un téléphone portable, par leur nombre et leur caractère intime, permettaient de s'ingérer dans la vie privée d'une personne bien plus qu'une perquisition de domicile conventionnelle effectuée dans les conditions du Quatrième Amendement à la Constitution des États-Unis d'Amérique :

Saisir les données d'un téléphone permet en général aux autorités d'en apprendre bien plus qu'une perquisition de domicile, aussi complète soit-elle : un téléphone contient non seulement sous forme numérique de nombreuses informations sensibles qu'une perquisition peut mettre à jour, mais également un grand nombre d'informations privées que l'on ne peut pas recueillir au domicile d'une personne, sous quelque forme que ce soit – sauf si on trouve un téléphone⁷.

Dans cette affaire, les juges de la Cour suprême ont montré en quoi les nouvelles technologies – dont les smartphones sont le symbole – bouleversaient l'approche de la question et qu'à ce moment déterminé du « temps » (à savoir : 2014), le « lieu » (à savoir : les États-Unis et le téléphone situé sur ce territoire) où les données personnelles étaient censées être recueillies s'était transformé en un lieu où les données personnelles, par leur portabilité, leur quantité et leur caractère, parvenaient à totalement altérer et renforcer la dimension privée de l'« espace » personnel.

25. Dans l'affaire *Riley v. Californie*, les juges entendaient principalement bannir les saisies illégales de données de smartphones en invoquant le respect de la vie privée ancré dans le Quatrième Amendement à la Constitution des États-Unis. Il convient néanmoins de souligner que les questions relatives à la sécurité et au chiffrement des téléphones portables peuvent s'avérer bien plus complexes et ne pas renvoyer uniquement à des considérations de vie privée et de sécurité. Les juges de la Cour suprême ne vont sans doute pas tarder à faire face au même dilemme que connaîtront les nombreux pays à travers le monde ayant consacré, comme principe de bonnes mœurs publiques auquel doit souscrire toute société démocratique, le droit de garder le silence ou le droit de ne pas témoigner contre soi-même. Ce sont en effet justement les mêmes caractéristiques qui font du téléphone portable un réceptacle si particulier de données personnelles, comme indiqué dans l'affaire *Riley v. Californie*, qui en font également l'instrument le plus apte à complètement vider de son contenu le droit de garder silence – un droit qui, à partir du seizième siècle, a été progressivement reconnu dans divers pays et qui, aux États-Unis, est consacré dans le Cinquième Amendement. Pour dire les choses simplement, dans de nombreux pays de par le monde (mais pas tous), toute personne faisant l'objet de poursuites pénales a le droit de ne pas témoigner contre elle-même en gardant le silence. Très rares sont les exceptions ou les restrictions apportées à ce droit dans des pays aussi différents que l'Allemagne, l'Australie, le Bangladesh, les États-Unis, l'Inde et la Nouvelle-Zélande, pour ne citer que ceux-là. Toutefois, un mandat judiciaire permettant d'accéder aux données d'un téléphone pourrait dans les faits le remettre en cause. Car si la personne poursuivie, n'ayant pas le statut de témoin contraignable, est en droit de garder le silence, son téléphone en revanche est une source d'information très riche sur ses pensées, ses centres d'intérêt ou ses actions les plus intimes. De même, dans de nombreuses juridictions, le conjoint ou les membres de la famille proche peuvent ne pas être obligés de témoigner en justice. Nombreux toutefois sont ceux qui font valoir que leur smartphone en sait bien plus sur eux que leur conjoint. Dès lors, va-t-on continuer de considérer que les données

saisies sur un smartphone peuvent être produites en justice, même après qu'un mandat de saisie a été délivré? Que nous commandent la logique et le souci de cohérence?

26. Pour l'heure, le Rapporteur spécial considère que la réflexion sur les smartphones et les appareils de même type (dont les technologies vestimentaires et les implants) doit se poursuivre, éventuellement dans le cadre de travaux d'autres rapporteurs spéciaux ou en collaboration avec eux. Il ne formule aucun avis ou recommandation à ce stade préliminaire. Il se borne à cerner les limites d'une question dont l'examen doit être approfondi du fait de ses répercussions considérables sur la vie privée, et qui ne concerne pas uniquement le droit au respect de la vie privée mais aussi d'autres droits fondamentaux – notamment le droit à une procédure pénale régulière. D'aucuns pourraient soutenir que la conclusion logique à tirer de l'affaire *Riley v. Californie*, pour ce qui est du droit de garder le silence, un droit distinct du droit au respect de la vie privée, est que, dans la plupart des cas, les informations issues du smartphone d'une personne faisant l'objet de poursuites pénales ne devraient pas être produites devant un tribunal. Une telle position aurait toutefois une incidence considérable sur le droit au respect de la vie privée, dans la mesure notamment où elle sanctionnerait le caractère potentiellement particulièrement privé et intime des données enregistrées sur un smartphone.

27. Le Royaume-Uni de Grande-Bretagne et d'Irlande du Nord, qui – situation ironique – a donné naissance au droit au silence il y a plus de quatre cents ans, considère que la sécurité nationale et la répression du crime prévalent sur ce droit au silence ou sur la protection de la vie privée lorsqu'il s'agit d'appareils électroniques. Aux termes des articles 49 et 53 de la loi de 2000 régissant les pouvoirs d'enquête, constitue un délit le fait de ne pas divulguer la clef d'accès aux données chiffrées quand demande en est faite (délict sanctionné d'une peine de deux ans de prison ou de cinq ans dans les affaires d'atteintes sexuelles sur mineurs). Ainsi, au Royaume-Uni, non seulement les données issues d'un smartphone peuvent être produites devant un tribunal, mais toute personne refusant de fournir la clef d'accès à l'appareil peut être condamnée à une peine de prison. L'affaire *Apple v. FBI* était quelque peu différente, les accusés étant morts et leur culpabilité hors de doute. Les enquêteurs voulaient déverrouiller le téléphone pour avoir une vue d'ensemble des faits, en savoir davantage sur la préparation de l'acte terroriste, identifier les complices et découvrir les liens de ce qui pouvait être un réseau terroriste national ou international. L'intérêt qu'a suscité l'affaire est toutefois pleinement justifié car elle s'inscrit au cœur des débats relatifs au respect de la vie privée, à la sécurité et au droit de garder le silence. Peut-être la prochaine étape sera-t-elle de préparer une étude portant sur des thématiques relevant tout à la fois du droit au respect de la vie privée et du droit de garder le silence. Le Rapporteur spécial consultera l'Association internationale du barreau, les associations européennes du barreau et d'autres parties prenantes avant de décider s'il est opportun de lancer une enquête approfondie sur la question et si des recommandations doivent être formulées aux fins de l'élaboration de politiques concrètes dans ce domaine.

B. Conservation des données, surveillance de masse et recours croissant au chiffrement des données

28. En dépit des nombreuses décisions de cours constitutionnelles nationales et de mécanismes régionaux de droits de l'homme, le Rapporteur spécial constate la propension croissante des gouvernements à élaborer des lois de surveillance de plus en plus envahissantes, qui mettent en place une surveillance de masse permanente et à peine dissimulée des citoyens.

29. On en trouve une illustration dans l'examen en troisième lecture du projet de loi sur les pouvoirs d'enquête à la Chambre des communes du Royaume-Uni, le projet devant être également examiné en commission à la Chambre des lords en septembre 2016. Le Rapport spécial présume que les lecteurs sont au fait des critiques qu'il a formulées dans son rapport du 9 mars 2016 à l'égard de ce texte, dont les dispositions consacrées à la surveillance de masse et au piratage de masse continuent d'être étudiées de près par la communauté internationale. La Cour de justice de l'Union européenne va prochainement statuer sur la question suite à l'avis rendu le 19 juillet 2016 par l'Avocat général de la Cour, qui estime que le traitement de masse des données n'est justifiable que dans le cadre de la lutte contre les infractions graves – une condition qui restreint fortement le champ d'application du projet de loi. En matière de vie privée, le texte est plein de chausse-trappe et, pour les analyser en profondeur, il conviendrait de rédiger un rapport dix fois plus long que les 10 300 mots auxquels nous sommes astreints; les parlementaires, l'association Liberty, la Law Society, l'Open Rights Group et Privacy International s'attèlent toutefois volontiers à cette tâche. Il reste à souhaiter que le Gouvernement britannique prenne le temps de la réflexion, reste attentif aux avis rendus en matière de surveillance par les juges de la Cour européenne des droits de l'homme et de la Cour de justice européenne et laisse le bon sens l'emporter. Il aurait également tout intérêt à écouter certains membres de la Chambre des lords. Lord Paddick, un ancien policier de haut rang, a fustigé les dispositions du projet relatives à la conservation des données de connexion à Internet, déclarant à ce propos : « La conservation des données de connexion à Internet – le seul territoire vierge du projet de loi – va conduire à des ingérences dans la vie privée de personnes innocentes. » Il a fait valoir par la suite que le caractère disparate de ces données était disproportionné sachant que le projet de loi autorise la police à accéder sans mandat aux données personnelles de tous les internautes au Royaume-Uni⁸.

30. Peu importe que le projet de loi sur les pouvoirs d'enquête n'aurait jamais dû être proposé dans sa forme actuelle, ni même déposé initialement devant la Chambre des communes pour adoption. Les débats engagés à ce jour à la Chambre des lords n'ont rien d'encourageant. Earl Howe, Ministre de la défense et Chef parlementaire suppléant à la Chambre, déclarait ainsi le 13 juillet 2016 :

Il peut être tout à fait légitime que le gouvernement collabore avec des [opérateurs de communication] afin d'établir s'il est souhaitable de prendre des mesures visant à acquérir et conserver des capacités techniques permettant de désactiver le chiffrement qui protège des communications ou des données.

⁸ Chambre des lords du Royaume-Uni de Grande-Bretagne et d'Irlande du Nord, débat relatif au projet de loi sur les pouvoirs d'enquête du 27 juin 2016, vol. 773 (<https://hansard.parliament.uk/lords/2016-06-27/debates/1606278000466/InvestigatoryPowersBill>).

Les services de police et les services de renseignement doivent continuer de pouvoir contraindre les opérateurs de télécommunications à désactiver le chiffrement dans certaines situations⁹.

31. L'on peut faire quatre hypothèses face à des déclarations de ce genre : a) le Ministre est mal informé; b) le Ministre est informé par des collaborateurs qui ne comprennent pas en quoi consiste le chiffrement; c) le Ministre n'a pas compris les explications qui lui ont été fournies; d) le Ministre donne sciemment une image fausse de la situation à la Chambre des lords. Le Rapporteur spécial ne veut pas croire à cette dernière hypothèse et invite donc l'honorable Lord et tous ses collègues de la Chambre à appréhender quelques faits simples. S'ils parviennent ainsi à comprendre les arguments avancés par le Gouvernement des Pays-Bas le 4 janvier 2016, ils se rendront compte que les tentatives de légiférer contre le chiffrement sont une mauvaise idée et, dans la pratique, une idée ridicule, que les propositions de cet ordre, loin d'être « tout à fait légitime[s] », sont totalement absurdes, et que des déclarations comme celles-ci : « les services de police et les services de renseignement doivent continuer de pouvoir contraindre les opérateurs de télécommunication à désactiver le chiffrement dans certaines situations », sont illusoires et ne correspondent pas à la réalité. Les services de police et de renseignement ne sont absolument pas en mesure de contraindre les opérateurs à désactiver le chiffrement – sauf à vouloir s'épuiser à leur demander – pour la simple raison que, la plupart du temps, ces opérateurs eux-mêmes n'en ont pas la capacité. Si le Parlement britannique se fourvoie au point d'adopter un texte aussi absurde, il ne sera difficile pour personne de télécharger des algorithmes de chiffrement ou des programmes de communication chiffrés conçus en dehors du Royaume-Uni ou des États-Unis, mais d'un accès libre sur Internet, et de les utiliser pour communiquer avec des complices dans le but de perpétrer des actes nuisibles sur le territoire britannique. Un opérateur de télécommunication est totalement impuissant dans cette situation et un service spécialisé dans l'interception des communications ne pourrait rien faire d'autre que de tenter de déchiffrer le code.

32. Certains membres de la Chambre des Lords sont tout à fait conscients de ce problème. Lord Strasburger en a fait une analyse très succincte :

Le chiffrement de bout en bout se caractérise, entre autres, par l'impossibilité, pour le fournisseur de le décrypter sans la clef, les données chiffrées restant alors privées lors de leur envoi d'un utilisateur à l'autre. [Earl Howe] semble insinuer que les fournisseurs ne peuvent utiliser que des chiffrements qu'il est possible de forcer, excluant ainsi le chiffrement de bout en bout, ce qui rendrait donc théoriquement illégale la prochaine version de l'iPhone d'Apple. Nous sommes donc loin d'avoir fait le tour du problème⁹.

Le Rapporteur spécial partage ce point de vue et estime que l'essentiel des efforts déployés doivent tendre à démontrer au Gouvernement du Royaume-Uni qu'il ne peut raisonnablement prétendre proscrire le chiffrement de bout en bout ou rendre cette technologie inaccessible aux habitants du Royaume-Uni. Cette proposition est aussi illogique que de vouloir interdire complètement les couteaux sous prétexte qu'ils pourraient occasionnellement être utilisés pour causer des dommages ou les voitures car elles peuvent faciliter la fuite de malfaiteurs. Affaiblir délibérément le

⁹ Ibid., débat relatif au projet de loi sur les pouvoirs d'enquête du 13 juillet 2016, vol. 774 (<https://hansard.parliament.uk/lords/2016-07-13/debates/16071337000437/InvestigatoryPowersBill>).

chiffrement présente par ailleurs des risques de sécurité disproportionnés par rapport aux avantages que cela pourrait représenter. Lord Strasburger a résumé ainsi la situation :

Il faut souligner, et personne dans le domaine de la cryptographie ne me contredira, qu'il est impossible de jouer sur les deux tableaux. Soit le chiffrement est sûr, soit il ne l'est pas; il ne peut être décryptable pour un petit groupe d'individus et hermétique pour le reste du monde⁹.

Lord Paddick a proposé une stratégie davantage conforme à la jurisprudence de la Cour européenne des droits de l'homme, telle qu'appliquée récemment dans l'affaire *Zakharov c. Russie* : « Il conviendrait de remplacer la capacité de contraindre une entreprise à retirer le chiffrement protégeant l'ensemble d'un service ou d'une technologie par d'autres méthodes plus ciblées⁹ ». Le Rapporteur spécial ne peut que se demander quand le bon sens prévaudra enfin dans les débats de l'État sur le sujet, sans parler du respect indispensable des droits fondamentaux tels que le droit à la vie privée.

33. Voilà plusieurs décennies que l'Allemagne montre l'exemple en ayant été la première à introduire la protection de la vie privée dans certains domaines. Au mois d'avril 2016, la Cour constitutionnelle allemande est restée fidèle à cette tradition en jugeant inconstitutionnelles certaines dispositions d'une loi (« BKA-Gesetz ») autorisant la police fédérale à mener des activités de surveillance, au motif qu'elles ne prévoyaient pas suffisamment de garde-fous pour préserver l'équilibre entre le droit individuel à la vie privée et la nécessité pour l'État de mener d'éventuelles enquêtes criminelles. Elle a ainsi estimé que certaines prérogatives, comme mener des opérations de surveillance en enregistrant des conversations ou en prenant des photographies, réaliser des écoutes téléphoniques ou fouiller des ordinateurs à distance, exigeaient davantage de mesures de protection, telles que le contrôle judiciaire, afin de garantir le bien-fondé et l'adéquation des intrusions dans la vie privée des citoyens allemands¹⁰.

34. Le contrôle démocratique des activités des services de renseignement en Allemagne demeure une source de préoccupations. Le Rapporteur spécial partage l'inquiétude de M. Nils Muižnieks, Commissaire aux droits de l'homme du Conseil de l'Europe, et note que les conclusions qu'il a formulées en octobre 2015 n'ont pas été contestées, notamment celles-ci :

Le manque de ressources et de compétences, les limites de la surveillance des télécommunications, les problèmes de coordination, ainsi que l'absence de voies de recours efficaces pour les personnes dont les télécommunications sont surveillées sont autant de problèmes qui empêchent actuellement un contrôle en bonne et due forme des activités des services allemands de renseignement et de sécurité.

L'insuffisance des ressources et des compétences techniques dont souffrent les organes de contrôle et leur secrétariat est particulièrement préoccupante. Le rapport entre le nombre de contrôleurs et le nombre de personnes surveillées est éloquent : deux organes comptant 13 membres, et soutenus par un petit secrétariat, sont

¹⁰ Wenzel Michalski, « Dispatches: rare victory for privacy in Germany's "war against terror" », Human Rights Watch, 27 avril 2016. Consultable à l'adresse suivante : <https://www.hrw.org/news/2016/04/27/dispatches-rare-victory-privacy-germanys-war-against-terror>.

chargés de contrôler des activités impliquant, dans le cas de la plus grande entité (le Service fédéral du renseignement), environ 6 000 employés¹¹.

Le Rapporteur spécial abordera ces questions à l'occasion de divers forums, y compris l'IIOF2016, ainsi que directement avec le Gouvernement allemand lui-même lorsque l'occasion se présentera.

35. Le 28 juin 2016, le Gouvernement allemand a approuvé un projet de loi sur le Service fédéral du renseignement (Bundesnachrichtendienst), qui modifiait plusieurs lois en vigueur contenant des dispositions relatives à la surveillance de ressortissants étrangers hors de l'Allemagne. Le 8 juillet 2016, le projet a été adopté en première lecture au Parlement. Les deux lectures restantes, y compris le vote final, pourraient avoir lieu dès le quatrième trimestre de 2016.

36. À ce sujet, il convient tout d'abord de s'intéresser à la question de la nationalité, puisque le projet de loi continue de faire une distinction entre Allemands et non-Allemands. La mesure dans laquelle cette distinction reflète la réalité est loin d'être évidente. La plupart des attaques terroristes qui ont eu lieu en Europe ces deux dernières années ont été menées par des citoyens de l'Union européenne, et le plus souvent par des citoyens de l'État visé par l'attentat. Sachant que la menace vient essentiellement des propres citoyens de l'État touché, quel est l'intérêt de lois discriminatoires sur la nationalité ? L'article 17 du Pacte international relatif aux droits civils et politiques disposant que toute personne a droit à la protection de sa vie privée, indépendamment de sa nationalité ou de sa citoyenneté, il est parfaitement légitime de se demander si de telles dispositions sont utiles, appropriées ou même légales. M. Muižnieks a également relevé cette anomalie, notant que « selon les autorités, la protection conférée par l'article 10 de la loi fondamentale ne s'étend pas au-delà du territoire allemand mais se limite aux citoyens allemands ou aux activités menées en Allemagne ». Cette interprétation est aussi inacceptable que toute disposition des lois d'autres États prétendant limiter la protection des droits de l'homme à leurs propres citoyens ou résidents. M. Muižnieks a d'ailleurs signalé également que :

L'interprétation en question est toutefois contestée depuis 1999, lorsque la Cour constitutionnelle fédérale a considéré que la protection prévue par la loi fondamentale s'étend au-delà des frontières du territoire allemand et que les droits fondamentaux doivent être respectés, du moins lorsque les renseignements obtenus à l'étranger sont traités en Allemagne¹¹.

Le nouveau projet de loi allemand passe à côté d'une occasion unique de réaffirmer que le droit à la vie privée et les garanties correspondantes concernent tous les individus indépendamment de leur nationalité, de leur citoyenneté ou de leur lieu d'habitation et que la surveillance soit réalisée en Allemagne ou hors du pays.

37. Le projet de loi allemand suscite par ailleurs une multitude de nouvelles préoccupations :

a) Définition de l'objectif : les conditions de la collecte et du traitement des données sont vagues et trop générales;

¹¹ Conseil de l'Europe, Rapport établi par Nils Muižnieks, Commissaire aux droits de l'homme du Conseil de l'Europe, à l'issue de ses visites en Allemagne le 24 avril et du 4 au 8 mai 2015, 1^{er} octobre 2015. Consultable à l'adresse suivante : https://www.ecoi.net/file_upload/1226_1447235185_commdh-2015-20-en.pdf.

b) Surveillance de masse : la surveillance de masse et la surveillance ciblée des communications extraterritoriales entre non-Allemands seraient autorisées à condition que les communications soient interceptées en Allemagne. Si la surveillance ciblée, selon les critères définis dans le cadre de l'affaire *Zakharov c. Russie*, est moins problématique, la surveillance de masse demeure très inquiétante et semble, de prime abord, contraire aux normes du droit européen;

c) Contrôle indépendant : la nouvelle loi ne prévoit pas de contrôle judiciaire indépendant adapté;

d) Les ressources prévues dans le projet de loi pour les activités de surveillance de masse proposées sont manifestement encore insuffisantes et inadaptées. La nouvelle loi prévoit un comité composé de trois membres qui ne sera tenu de se réunir que quatre fois par an et ne disposera probablement ni du personnel ni des ressources nécessaires pour superviser les opérations de surveillance de masse, vastes par définition. Le Rapporteur spécial partage donc les préoccupations de M. Muižnieks. Par ailleurs, le fait que le pouvoir exécutif soit chargé de nommer les membres du comité ne contribue pas à renforcer la notion de surveillance indépendante.

38. Compte tenu de ce qui précède, le nouveau projet de loi allemand semble de prime abord indiquer que les autorités allemandes n'ont tiré aucun enseignement du rapport établi au mois d'octobre 2015 par M. Muižnieks. Au lieu de présenter au Rapporteur spécial une loi type pouvant servir de modèle de bonne pratique dans le monde entier, le Gouvernement allemand a proposé un texte qui est plus que décevant. Malgré ses nombreux défauts, le projet de loi du Royaume-Uni sur les pouvoirs d'investigation s'efforçait au moins de remédier en partie à la faiblesse du régime de contrôle, que le Rapporteur spécial, entre autres, avait déjà critiqué. Bien que loin d'être parfait, le nouveau régime de contrôle proposé au Royaume-Uni semble toutefois représenter une amélioration par rapport à la situation précédente. L'Allemagne, pour sa part, à moins de renoncer à son projet et de changer radicalement de direction, semble déterminée à prendre la place du Royaume-Uni en tant que pays ayant le régime de contrôle le plus faible du monde occidental par rapport à la taille de ses services de renseignement.

39. Si le Rapporteur spécial peut comprendre l'anxiété provoquée par la récente vague d'attaques en Allemagne, il continue d'attendre de ce pays qu'il montre la voie en matière de protection de la vie privée ainsi que des données et il lui propose, comme il l'a fait avec le Royaume-Uni, de collaborer avec lui pour établir une nouvelle loi et un régime de contrôle doté des ressources voulues pouvant servir d'exemple de meilleure pratique dans le monde entier.

C. Meilleure prise en compte du lien entre la vie privée et la personnalité

40. Le 13 juillet 2016, l'Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) du Mexique a rendu un jugement très intéressant (Expediente PPD.0050/16), qui se lit notamment comme suit : « il convient de noter que, si le droit à la protection des données personnelles relève, conformément aux règles constitutionnelles du pays, d'un droit autonome à la protection de la vie privée, il est nécessaire de proposer une interprétation plus large de ces deux concepts, selon laquelle le droit à la protection de la vie privée

visé à assurer à l'individu un domaine où il peut développer librement sa personnalité ». Ainsi, en règle générale, la protection de la vie privée implique d'autres droits et garanties spécifiques relatifs au stockage de l'information, à l'accès aux données personnelles ainsi qu'aux règles concernant la protection des communications privées, des noms et de l'intégrité physique et morale.

IV. Conclusions

41. Au cours de l'année qui a suivi son entrée en fonctions, le Rapporteur spécial s'est rendu dans 14 pays à l'occasion de 20 voyages entrepris dans le cadre de son mandat. Il a notamment visité des pays géographiquement éloignés comme l'Australie, le Brésil, les États-Unis et la Nouvelle-Zélande, ainsi que 10 États européens. Même si, techniquement, il s'agissait de visites de pays « informelles », le Rapporteur spécial a souvent été amené à remplir l'ensemble des engagements normalement réservés aux visites officielles traditionnelles, notamment des réunions avec des ministres, des fonctionnaires des ministères, des membres des services de renseignement et des organismes de contrôle, des responsables de la protection des données, des membres des services de maintien de l'ordre ainsi que des représentants de la société civile et de grandes entreprises. Dans la grande majorité des cas, le Rapporteur spécial a été très favorablement accueilli. Au moins deux visites de pays officielles, peut-être même trois, seront en principe programmées au cours des 12 prochains mois, chacune sur un continent différent (Afrique, Asie et Amérique latine).

42. Le Rapporteur spécial a lancé un système de consultations structurées partout dans le monde. Des représentants de la société civile, des particuliers, des gouvernements, des entreprises et d'autres parties prenantes ont manifesté leur intérêt pour divers sujets ayant trait au respect de la vie privée en écrivant au Rapporteur spécial ou en soumettant des demandes de réunions, dont la plupart ont été acceptées. Ces rencontres ont permis au Rapporteur spécial de dresser des listes de parties prenantes par secteurs afin de convier les acteurs intéressés à des réunions dans le monde entier. Les consultations structurées ont souvent lieu à huis clos (à la demande des parties prenantes) mais peuvent être ouvertes à des invités et des personnes ayant expressément demandé à y participer.

43. Le Rapporteur spécial s'est en outre employé à favoriser les recherches et les consultations en créant cinq équipes spéciales, se consacrant chacune à une des lignes d'action thématique identifiées dans le premier groupe de cinq priorités : mégadonnées et données ouvertes; sécurité et surveillance; données relatives à la santé; données à caractère personnel traitées par les entreprises; et meilleure compréhension de la notion de vie privée ». Ces priorités serviront de point de départ à l'établissement de rapports thématiques, qui devraient être présentés en 2017-2018. Cette démarche a permis au Rapporteur spécial de surmonter partiellement les contraintes en matière de ressources en puisant dans un vivier mondial d'experts disposés à partager bénévolement leurs compétences spécialisées. Le Rapporteur spécial continuera cependant à rechercher des financements externes et est ouvert à toute forme d'aide lui permettant de s'acquitter convenablement de son mandat.

44. En raison du nombre maximum de mots fixé arbitrairement pour le présent rapport, certaines observations portant sur au moins une douzaine de domaines dans lesquels le Rapporteur spécial a travaillé ont dû être omises. Ces domaines devraient pouvoir être abordés plus en détails dans les futurs rapports thématiques et généraux.

45. Si, dans l'ensemble, le Rapporteur spécial se dit satisfait des liens de collaboration établis jusqu'ici, il invite toutefois davantage de gouvernements à contribuer à l'exécution de son mandat et, comme certains l'ont fait au cours de la première année d'activité, à le consulter sur les projets de loi relatifs à la protection de la vie privée et aux domaines connexes, comme la surveillance, dès les premiers stades de leur élaboration. En outre, le Rapporteur spécial encourage et apprécie vivement la participation aux activités dont il a pris l'initiative, comme l'HOF2016, les visites de pays informelles ou les divers ateliers-conférences, ainsi que les mesures à même de les faciliter.
