Nations Unies A/HRC/31/64

Assemblée générale

Distr. générale
24 novembre 2016
Français
Original : anglais

Conseil des droits de l'homme
Trente et unième session
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, soumis au Conseil des droits de l'homme en application de la résolution 28/16 du Conseil, le Rapporteur spécial sur le droit à la vie privée expose la manière dont il envisage son mandat et présente ses méthodes de travail ainsi qu'un programme de travail triennal. Il donne également une vue d'ensemble de la situation relative à la vie privée au début de l'année 2016.

* Le présent rapport a été soumis après la date limite afin que des renseignements sur les faits les plus récents puissent y figurer.

** Les annexes au présent rapport sont distribuées uniquement dans la langue de l'original.

GE.16-20847 (F) 141216 161216

1620847

Rapport du Rapporteur spécial sur le droit à la vie privée

Table des matières

I. Introduction

1. Dans sa résolution 28/16 sur le droit à la vie privée à l'ère du numérique, le Conseil des droits de l'homme a défini le mandat du Rapporteur spécial sur le droit à la vie privée et souligné que les États devaient s'acquitter pleinement de leurs obligations au regard du droit international des droits de l'homme. Cette tâche est particulièrement difficile pour ce qui est du droit à la vie privée étant donné que le développement rapide des technologies de l'information, s'il ouvre de nouvelles possibilités en termes d'interactions sociales, soulève également des préoccupations quant à la manière de développer encore le droit à la vie privée pour faire face aux nouveaux défis.

2. Conformément à la résolution susmentionnée, le Rapporteur spécial soumettra chaque année un rapport au Conseil des droits de l'homme et à l'Assemblée générale. Dans le présent rapport, il décrit ses méthodes de travail (section II), fait le point de la situation en matière de droit à la vie privée en 2016 (section III), présente les activités menées à ce jour (section IV) et énonce un plan d'action en dix points destiné à mieux appréhender et à développer le concept de droit à la vie privée au vingt et unième siècle (section V). Ses conclusions figurent à la section VI.

3. Le présent rapport est à la fois sommaire et préliminaire, puisqu'il a été établi à peine six mois après la nomination du Rapporteur spécial, le 1er août 2015. Malgré les efforts considérables qu'il a déployés, le Rapporteur spécial n'a donc pas eu le temps de consulter toutes les parties prenantes. Par conséquent, le rapport vise essentiellement à mettre en avant plusieurs questions importantes, sans nécessairement établir un ordre de priorité. Au cours des douze prochains mois (d'ici à janvier 2017), une fois qu'il aura pu prendre connaissance des préoccupations d'un grand nombre d'acteurs supplémentaires issus de toutes les régions du monde, le Rapporteur spécial devrait être bien plus en mesure de déterminer les mesures à prendre en priorité. La manière dont il envisage son mandat et les difficultés auxquelles il s'attend sont énoncées à l'annexe I.

II. Méthodes de travail du Rapporteur spécial

A. Suivi de la situation dans les pays

4. Une base de données des politiques, des lois, des procédures et des pratiques en vigueur est actuellement mise au point et alimentée à partir de divers rapports et textes de loi. Elle permettra au Rapporteur spécial de recenser les sujets de préoccupation et les meilleures pratiques, lesquels pourraient ensuite être communiqués à d'autres acteurs.

B. Études thématiques : analyses et évaluations

5. Il ressort des consultations tenues par le Rapporteur spécial que, à l'heure où un Internet sans frontières apporte des bénéfices considérables, deux principes généraux recueillent l'adhésion : l'offre de garanties sans frontières d'une part, et la fourniture de recours transfrontières d'autre part.

6. L'intérêt attaché à la mise en place de garanties destinées à protéger la vie privée et de recours permettant de faire face aux atteintes à la vie privée sous-tend chacune des études thématiques, présentées ci-après, que le Rapporteur spécial a entreprises dans un certain nombre de secteurs où les risques d'atteinte à la vie privée semble élevés. Chaque étude devrait déboucher sur la publication d'un rapport ad hoc qui rendra compte des consultations en cours ainsi que des différents échanges et observations.

1. Vie privée et personnalité dans les différentes cultures

7. Cette étude a pour objet de mieux comprendre comment la vie privée est ou devrait être envisagée dans les différentes cultures en 2016, en tenant compte des particularités de l'ère du numérique, dans laquelle Internet se joue des frontières. Posant la question du pourquoi de la vie privée et présentant ce droit comme un droit habilitant et non comme une fin en soi, le Rapporteur spécial analyse le concept de la vie privée sous l'angle d'un droit permettant la réalisation d'un droit supérieur et fondamental au développement libre et sans entrave de la personnalité de chacun. L'étude est réalisée en étroite coopération avec plusieurs organisations non gouvernementales et devrait être au cœur d'une grande conférence internationale qui sera organisée en 2016. Elle s'inscrit aussi dans un contexte plus large, dans lequel elle examine les relations entre le droit à la vie privée et d'autres droits fondamentaux. Ainsi, le lien entre le droit à la vie privée et les droits à la liberté d'expression et à la liberté d'accès aux informations publiques devrait y être examiné, notamment avec la collaboration des autres rapporteurs spéciaux de l'Organisation des Nations Unies. Des consultations ont déjà été engagées avec le Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression afin d'étudier les possibilités de mener une action conjointe sur la question en 2016 et en 2017.

2. Business models des entreprises en ligne et utilisation des données personnelles

8. Dans les vingt-cinq premières années de son existence, le Web a stimulé la croissance, en grande partie non réglementée, d'entreprises privées, dont certaines ont essaimé en entités multinationales dont l'activité est transfrontière et qui attirent des clients dans le monde entier. L'une des caractéristique de cette croissance est qu'elle s'est appuyée sur la collecte et l'utilisation de données personnelles : chaque recherche effectuée, chaque article lu, chaque e-mail ou message envoyé, chaque produit ou service acheté génère une myriade de traces électroniques qui peuvent être rassemblées pour établir un profil personnel très fidèle indiquant les choses que la personne aime ou n'aime pas, son état d'esprit, ses capacités financières, ses préférences sexuelles, son état de santé et ses habitudes de consommation ainsi que ses intérêts et opinions intellectuel, politique, religieux et philosophique. La question qui se pose, de manière générale, est de savoir si certains fournisseurs de services en ligne ont le droit de suivre l'activité en ligne d'une personne afin de décider d'une juste rémunération. Avec la collecte d'informations de plus en plus détaillées sur les habitudes de consommation des particuliers, les données personnelles sont devenues des marchandises. L'obtention et l'exploitation de ces données constituent aujourd'hui un des plus gros secteurs d'activité au monde, dont le chiffre d'affaire, de l'ordre de plusieurs centaines de milliards de dollars, provient généralement d'activités publicitaires ciblées. Si les consommateurs ont bien conscience des informations qu'ils publient délibérément sur Internet, il semble qu'ils sont très souvent nettement moins au courant de la quantité, de la qualité et de l'utilisation concrète des métadonnées qu'ils génèrent lorsqu'ils naviguent, discutent, font des achats ou effectuent d'autres actions en ligne. Les données dont on dispose aujourd'hui pour dresser le profil personnel des utilisateurs sont infiniment plus nombreuses qu'il y a vingt-cinq ans, mais l'ampleur des risques pour la vie privée qui sont associés à l'utilisation, parfois abusive, de ces données, n'est pas encore bien comprise. Des éléments montrent que la marchandisation des données personnelles, en particulier dans des secteurs traditionnellement considérés comme sensibles, comme le traitement des données médicales, s'est tellement généralisée que les consommateurs n'ont pas conscience que ces données sont vendues et revendues ou il ne leur est pas demandé de donner leur accord à une telle vente. On ne dispose pas de suffisamment d'informations pour évaluer correctement les risques propres aux données prétendument anonymes, qui peuvent traitées de telle sorte que l'on peut retrouver à quelle personne elles se rapportent. Une telle atteinte à la vie privée pourrait faire courir de multiples risques aux personnes et aux

communautés concernées, en particulier dans les cas où les données seraient confidentielles et seraient obtenues, par exemple, par des acteurs étatiques ayant l'intention de se hisser ou de se maintenir au pouvoir, par des groupes de la criminalité organisée ou par des entreprises commerciales agissant illégalement. Lorsque les premiers ordinateurs sont apparus, une des principales préoccupations était l'utilisation que pouvaient faire les États des données personnelles et leur aptitude à corréler les données provenant de diverses sources de façon à obtenir un tableau détaillé des activités et des ressources d'un individu. En 2016, cependant, il semble que les entreprises privées détiennent beaucoup plus de données sur les particuliers que les États. Face aux énormes revenus tirés de la monétisation des données personnelles, les inquiétudes soulevées concernant le respect de la vie privée ne suffisent pas à inciter les entreprises à changer de business model. De fait, récemment, ce n'est que lorsque les risques pour la vie privée ont mis en péril leurs revenus potentiels que certaines entreprises ont adopté une approche plus rigoureuse, tenant davantage compte du droit à la vie privée. Le moment semble maintenant venu d'engager une discussion globale, en s'appuyant sur des informations pertinentes, afin de déterminer quel type de politique de gestion de l'information permettrait de protéger au mieux la vie privée des individus et de réduire autant que possible les risques d'atteinte à la vie privée, dans le cadre de la collecte de données par les entreprises privées. Cette discussion ferait fond sur les idées et les attentes exprimées par les citoyens. Il est prévu que les sociétés en ligne participent en 2016 aux consultations entamées en 2015 et qu'une consultation publique de grande ampleur se tienne sur la question en 2017.

3. Sécurité, surveillance, proportionnalité et cyberpaix

9. La sécurité est restée une préoccupation majeure au niveau international tout au long de l'année 2015 et en 2016. Les activités de suivi menées dans les pays, évoquées plus haut, ont montré que, dans plusieurs cas, des lois ont été adoptées en toute hâte par les parlements nationaux pour légitimer l'application par les services de sécurité et de renseignement et les services chargés de l'application des lois de certaines mesures portant atteinte au droit à la vie privée. Dans un grand nombre de pays concernés, mais malheureusement pas dans tous, l'adoption de ces lois a entraîné un débat public sur :

a) La question de savoir si les mécanismes de contrôle en place étaient suffisants ;

b) La distinction entre surveillance ciblée et surveillance de masse (ou, pour reprendre l'euphémisme employé dans certains pays, « surveillance à grande échelle ») ;

c) La question de savoir si les mesures prises étaient proportionnées dans une société démocratique ;

d) Le rapport coûts-avantages et l'efficacité générale des mesures visées.

10. Officiellement, ces lois visent essentiellement à combattre le terrorisme, la criminalité organisée et d'autres infractions socialement sensibles, comme les crimes pédophiles. Cela étant, au cours des débats, on a aussi présenté des éléments qui semblaient souvent indiquer que les mesures qui portent atteinte au droit à la vie privée, en particulier les mesures de surveillance de masse, ne renforcent pas la sécurité et que les insuffisances en matière de renseignements doivent être palliées par d'autres moyens. Le Rapporteur spécial a poursuivi son programme de dialogue avec les services de l'application des lois et les services de sécurité et de renseignement partout dans le monde afin de mieux comprendre leurs préoccupations légitimes, de relever les meilleures pratiques, qu'il pourrait être utile de mettre en commun, et de recenser les politiques, les pratiques et les lois appliquées dont l'utilité est contestable ou qui présentent un risque inacceptable d'atteinte à la vie privée, au niveau national comme au niveau international. L'étude en

cours touche à des questions qui sont parfois presque inextricablement liées aux questions de cybersécurité et de cyberespionnage. Un nombre limité mais croissant d'États considèrent le cyberespace comme un théâtre d'opérations supplémentaire pour les nombreux services de sécurité et de renseignement ; ils ne semblent pas encore disposés à discuter entre eux − ni, parfois, avec le Rapporteur spécial − de cette utilisation du cyberespace qui, naturellement, a des répercussions directes sur la vie privée des citoyens, quelle que soit leur nationalité. Bien qu'ils ne soient pas nécessairement la cible principale des mesures de cybersécurité et de cyberespionnage, il arrive souvent que les citoyens lambda soient pris sous les feux croisés et que leurs données personnelles et leurs activités en ligne soient surveillées au nom de la sécurité nationale, au moyen de mesures non nécessaires, disproportionnées et excessives. Parallèlement aux recherches ponctuelles qu'il mène en exécution de son mandat, le Rapporteur spécial a la chance d'avoir à sa disposition la riche base de connaissances fournie par les recherches participatives indépendantes qui sont ou ont été menées dans le domaine de la sécurité, en particulier les recherches financées par l'Union européenne [a]. L'étude présentée ici porte sur quatre domaines principaux, à savoir : a) les moyens de surveillance étatiques dont la portée est proportionnée à l'objectif et qui sont dûment contenus par des garanties législatives, procédurales et techniques, notamment des mécanismes de contrôle solides ; b) la surveillance ciblée, par opposition à la surveillance de masse ; c) l'accès des services chargés de l'application des lois et des services de sécurité et de renseignement aux données personnelles détenues par des entreprises privées et d'autres entités non publiques ; d) l'importance réaffirmée de la cyberpaix. Le Rapporteur spécial est convaincu que la cyberguerre et la cybersurveillance risquent de détruire le cyberespace et soutient que les gouvernements et les autres parties prenantes devraient œuvrer de concert pour garantir la cyberpaix. À cet égard au moins, la protection de la vie privée s'inscrit dans le mouvement en faveur de la cyberpaix. Grâce à la cyberpaix, le cyberespace peut véritablement devenir un espace numérique dans lequel toute personne jouit à la fois de la sécurité et du respect de la vie privée, un espace pacifique qui n'est pas constamment mis en péril par les activités de certains États, en plus des menaces que représentent déjà le terrorisme et la criminalité organisée.

4. Données ouvertes et analyse des données massives : leurs effets sur la vie privée

11. L'une des principales difficultés en matière de politique et de gouvernance de l'information en cette deuxième décennie du vingt et unième siècle est de déterminer le juste équilibre entre, d'une part, l'utilisation de données dans l'intérêt de la société selon les principes des données ouvertes et, d'autre part, les principes établis jusqu'à présent pour protéger des droits fondamentaux tels que le droit à la vie privée, à l'autonomie et au libre développement de la personnalité de chacun. On trouvera un exposé plus détaillé des préoccupations du Rapporteur spécial dans ce domaine à l'annexe II du présent rapport.

5. Génétique et vie privée

12. Le Rapporteur spécial constate qu'environ un quart des États Membres ont mis en place des fichiers nationaux contenant les données ADN des auteurs d'infractions pénales. De telles bases de données peuvent être précieuses pour résoudre certaines affaires, mais elles soulèvent également des préoccupations en matière de droits de l'homme, en ce qui concerne notamment l'utilisation potentiellement abusive de la surveillance exercée par les pouvoirs publics (identification des membres d'une famille ou contestation de la paternité, par exemple) et les risques d'erreur judiciaire. De plus, il semblerait que l'utilisation de données ADN à des fins administratives, pour l'établissement de cartes d'identité ou la gestion de l'immigration par exemple, soit amenée à augmenter de façon exponentielle.

[a] Notamment les projets CONSENT, SMART, RESPECT, SiiP, INGRESS, E-CRIME, EVIDENCE, MAPPING, CITYCoP et CARISMAND.

En outre, il est probable que des mesures soient prises au cours des prochaines années pour établir un fichier contenant les données ADN de l'ensemble des citoyens. D'aucuns pensent que la médecine personnalisée va amener de nombreuses personnes à confier volontairement l'ensemble de leurs informations génétiques à l'industrie de la santé, ce qui n'est pas sans rappeler les inquiétudes suscitées dans les années 1990 par l'utilisation de données génétiques dans le secteur des assurances. Face à ces préoccupations et à d'autres sujets d'inquiétude, et compte tenu de l'augmentation du nombre de bases de données ADN dans toutes les régions du monde, il importe de soumettre davantage ces questions au débat public, et à un débat de fond. Le Rapporteur spécial entend continuer de soutenir des projets qui visent à définir des normes internationales relatives aux droits de l'homme qui soient applicables aux bases de données ADN, en établissant des pratiques optimales et en associant des spécialistes, les décideurs et les citoyens à un débat ouvert sur le sujet. Cette action devrait permettre de formuler des lignes directrices sur les meilleures pratiques, qui tiendront compte des apports et des observations des acteurs de la société civile.

6. Vie privée, dignité et réputation

13. Les préoccupations relatives à la sécurité et à la surveillance ont pu reléguer au second plan les inquiétudes de nombreux citoyens concernant la manière dont leur vie privée, leur dignité et leur réputation sont mises en péril sur Internet. Nous sommes entrés dans l'ère du numérique, ce qui signifie qu'au cours des vingt dernières années, les médias se sont développés et transformés, et notamment qu'Internet a donné à des gens ordinaires, sans formation journalistique, la possibilité de publier à tout moment des documents texte, audio et vidéo de leur choix. Cette évolution a donné du pouvoir aux citoyens, en particulier dans les cas où elle permet de contourner la censure ou d'autres obstacles, ou dans les cas où la technologie favorise la liberté d'expression d'une manière qui renforce la démocratie au sein de la société. Cependant, ce nouveau phénomène des journalistes et blogueurs citoyens, qui s'inscrit dans un monde des médias en pleine mutation et se conjugue à l'usage généralisé des réseaux sociaux, a conduit à craindre une utilisation abusive du droit à la liberté d'expression, qui pourrait avoir des conséquences négatives pour d'autres droits de l'homme fondamentaux, comme le droit à la vie privée et le droit à la dignité. Les travaux de recherche menés au cours des cinq dernières années ont montré que les citoyens sont de plus en plus inquiets face à la facilité avec laquelle leur honneur et leur réputation peuvent être salis sur Internet, et que les internautes se sentent impuissants à faire valoir des garanties ou des recours en cas de diffamation ou d'atteinte à la vie privée. Le Rapporteur spécial souhaiterait collaborer avec le Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, la société civile et des organismes des Nations Unies comme l'Organisation des Nations Unies pour l'éducation, la science et la culture, pour étudier des moyens concrets de protéger la vie privée, la dignité et la réputation de chacun sur Internet, et envisager des recours en cas d'atteinte à ces droits. Tout comme le montrent aussi un certain nombre des études thématiques évoquées plus haut, la relation entre vie privée et gouvernance d'Internet est une des questions fondamentales qu'il convient de prendre en considération en matière de vie privée, de dignité et de réputation.

7. Biométrie et vie privée

14. Un tour d'horizon des études menées actuellement permet de constater que l'intérêt pour l'utilisation de la biométrie à des fins très diverses, allant de l'application des lois à l'accès personnel aux appareils mobiles, connaît une augmentation considérable. La reconnaissance vocale, la lecture rétinienne, la reconnaissance de la démarche ou du visage et la lecture des empreintes digitales ou des empreintes digitales sous-cutanées ne sont que quelques exemples des technologies numériques qui sont élaborées et exploitées à des fins diverses en cette deuxième décennie du vingt et unième siècle. Le Rapporteur

spécial entend poursuivre sa coopération avec les chercheurs du domaine et avec les autorités chargées de l'application des lois, les services de sécurité et de renseignement et la société civile pour mieux définir les garanties et les recours adaptés à l'utilisation d'appareils biométriques.

C. Plaintes individuelles

15. Le Rapporteur spécial a reçu des plaintes émanant de particuliers et d'acteurs de la société civile faisant état d'atteintes aux droits à la vie privée, et continuera probablement d'en recevoir au fur et à mesure que son mandat sera mieux connu. Il donne suite à ces plaintes en correspondant à la fois avec les plaignants et avec les autorités publiques concernées. Cette correspondance est menée conformément à la méthode employée par les titulaires de mandat au titre des procédures spéciales, qui vise à clarifier les allégations formulées, à établir les faits et, si nécessaire, à recommander des mesures correctives. Au besoin, des entretiens peuvent être menés en personne ou en ligne. Si les éléments de preuve reçus requièrent une attention particulière ou urgente et que les formes de communication ordinaires ne s'avèrent pas adaptées, le Rapporteur spécial peut envisager de faire publiquement part de sa préoccupation.

D. Actions conjointes

16. Le Rapporteur spécial reçoit régulièrement des demandes d'action conjointe avec d'autres rapporteurs spéciaux et en lance parfois. Des informations détaillées sur ces actions sont publiées séparément, dans le rapport sur les communications des titulaires de mandat au titre des procédures spéciales.

17. Au 5 mars 2016, faute de temps pour recueillir suffisamment d'éléments de preuve dans les catégories énumérées plus haut, le Rapporteur spécial n'avait pu participer qu'à deux actions conjointes. Cela étant, les renseignements recueillis dans chaque catégorie devraient contribuer à constituer la base de connaissances nécessaire à la poursuite du dialogue avec les rapporteurs spéciaux et de la coopération avec les États concernés, notamment au moyen de communications, de visites dans les pays et d'autres méthodes de collaboration.

E. Collaboration et politique de coopération

18. Dans le cadre de son mandat, le Rapporteur spécial a poursuivi et élargi les activités menées précédemment pour établir des liens avec et entre les parties prenantes. Il a ainsi engagé un dialogue avec des parties prenantes de tout type, et a notamment rencontré des responsables publics et des ministres dans leur capitale ou lors de réunions bilatérales tenues au cours de manifestations internationales, tenu des réunions avec plusieurs Commissaires à la protection des données et de la vie privée, en particulier avec le Président du Groupe de travail « Article 29 » de l'Union européenne et le Président du Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, qui relève du Conseil de l'Europe, eu des discussions avec les représentants d'organismes de normalisation comme l'Union internationale des télécommunications (UIT) et l'Institute of Electrical and Electronic Engineers, eu des discussions approfondies, en tête à tête ou en groupe, avec des acteurs de la société civile, et tenu des réunions avec des spécialistes des droits de l'homme et des représentants des missions permanentes à Genève. Cette liste est purement illustrative et non exhaustive. Le Rapporteur spécial reçoit presque tous les jours des invitations à prononcer des allocutions, à participer à des tables rondes ou à des conférences et à

rencontrer des membres de la société civile. S'il accepte bon nombre de ces invitations, notamment lorsqu'elles ont directement trait aux sept études thématiques citées plus haut, il est obligé d'en décliner d'autres, en particulier lorsque son emploi du temps ou les contraintes budgétaires rendent sa participation impossible. Outre de nombreux autres résultats, cette politique de dialogue s'est traduite par l'élaboration d'une résolution officialisant la coopération avec des autorités de protection des données et de la vie privée[b], qui a été adoptée par la Conférence internationale annuelle des Commissaires à la protection des données et à la vie privée.

III. La question de la vie privée au début de l'année 2016

A. Définition et compréhension

19. Si la notion de vie privée existe dans toutes les sociétés et toutes les cultures, et ce depuis le début de l'histoire de l'humanité, elle ne fait pas l'objet d'une définition contraignante et universellement acceptée[c]. Pour comprendre le droit à la vie privée, il faut l'envisager sous deux angles différents. Premièrement, il faut connaître la portée des éléments positifs au cœur de ce droit. Deuxièmement, il faut s'interroger sur la manière de délimiter ce droit sous la forme d'une définition négative. Ces deux démarches restent à accomplir.

20. Comme l'a réaffirmé le Conseil des droits de l'homme dans sa résolution 28/16, l'article 12 de la Déclaration universelle des droits de l'homme et l'article 17 du Pacte international relatif aux droits civils et politiques constituent le fondement du droit à la vie privée en droit international des droits de l'homme. Ces articles et un certain nombre d'instruments internationaux ou nationaux, notamment des constitutions et des dispositions législatives pertinentes, constituent à l'échelle mondiale un cadre juridique considérable qui peut être utile aux fins de la protection et de la promotion de la vie privée. Toutefois, son utilité est fortement contrariée par l'absence de définition universellement convenue et acceptée de la notion de vie privée. Même si le principe de protection de la vie privée était reconnu par les 193 pays, il n'aurait que très peu de sens sans une description précise de l'objet de cette protection.

21. L'absence de définition universellement reconnue et acceptée de la notion de vie privée n'est pas la seule difficulté à laquelle se heurte le Rapporteur spécial. Même si les rédacteurs de tous les instruments juridiques pertinents avaient inclus dans les textes une telle définition, il faudrait quand même prendre en compte des considérations temporelles, spatiales, économiques et technologiques. Étant donné le passage du temps et les effets des évolutions technologiques, et compte tenu des différents rythmes de développement économique et de déploiement des technologies d'une zone géographique à l'autre, les principes juridiques établis il y a cinquante ans (lorsque le Pacte international relatif aux droits civils et politiques a été adopté), ou trente-cinq ans (par exemple lorsque la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel a été adoptée), sans parler de ceux définis il y a soixante-dix ans (comme la Déclaration universelle des droits de l'homme), mériteraient peut-être d'être revus, approfondis et éventuellement complétés et renforcés, de manière à ce qu'ils correspondent mieux aux réalités actuelles.

[b] Adoptée par la Conférence internationale annuelle des Commissaires à la protection des données et à la vie privée, le 27 octobre 2015 à Amsterdam. Disponible à l'adresse : https://icdppc.org/wp-content/uploads/2015/02/Resolution-on-Cooperation-with-UN-Special-Rapporteur-on-the-Right-to-Privacy.pdf.

[c] Pour un aperçu plus détaillé de l'analyse du Rapporteur spécial de la notion de vie privée et de ses dimensions spatiales et temporelles au cours du millénaire, voir Joseph A. Cannataci, éd., *The Individual and Privacy. Volume I* (Oxford, Ashgate, 2015).

22. Compte tenu de l'absence de définition universellement reconnue et de ces considérations temporelles, spatiales, économiques et technologiques, il apparaît nécessaire de comprendre ce que la vie privée représente pour des personnes différentes, vivant dans des lieux différents et dans des conditions différentes, partout dans le monde. Il est évident qu'une telle mission est non seulement une tâche fondamentale mais aussi une priorité pour le Rapporteur spécial.

23. Dans certaines cultures, le débat sur la vie privée englobe la question de l'avortement. Sans vouloir discuter des mérites d'une telle approche, et pour écarter tout doute, il convient de préciser que, à ce stade préliminaire du mandat, les activités du Rapporteur principal porteront sur la protection des informations personnelles. Il s'agira de déterminer la fonction et le rôle du respect de la vie privée dans la manière dont circulent les informations au sein de la société et les conséquences sur le développement de la personnalité de chacun. D'autres questions, telles que la répartition du pouvoir et des richesses, seront également traitées. Lorsqu'on se penche sur ces questions, toutefois, il apparaît que d'autres droits que le droit à la vie privée ont une incidence sur les flux d'informations, notamment le droit à la liberté d'expression ou le droit d'accéder à des informations de source publique. Chacun de ces droits est important, et la promotion d'un droit ne doit pas faire oublier l'importance d'un autre, ni la nécessité de la protéger. Il est plus productif d'envisager ces droits dans leur complémentarité que de les considérer en opposition les uns par rapport aux autres. Ainsi, concrètement, il vaut mieux parler de « vie privée et sécurité » que d'opposer les deux notions, car elles sont toutes deux nécessaires. Ces deux droits peuvent être considérés comme des droits permettant l'exercice d'autres droits plutôt que comme ayant une fin en soi. Le droit à la sécurité est un droit qui habilite le droit fondamental à la vie, et le droit à la vie privée peut également être considéré comme un droit habilitant dans le contexte de l'enchevêtrement complexe des flux d'informations, qui sont fondamentaux pour l'autonomie des individus et pour leur capacité à connaître les options qui s'offrent à eux et à faire leur choix en connaissance de cause à mesure qu'ils développent leur personnalité tout au long de leur vie.

24. En lançant le débat sur ce qu'est la vie privée et sur ce qu'elle devrait être, le Rapporteur spécial entend se concentrer sur les fondamentaux et éviter que le débat soit perturbé par ce qui pourrait être des particularités locales ou culturelles, supposées ou bien réelles, à la marge de la vie privée, par opposition aux valeurs essentielles en matière de vie privée qui pourraient, à terme, faire l'objet d'un consensus universel. Pour cadrer le débat structuré qu'il entend engager sur les fondamentaux, le Rapporteur spécial se propose, avec un certain degré de provocation, de considérer que la vie privée est un droit habilitant l'exercice d'autres droits et non une fin en soi. Plusieurs pays ont défini un droit fondamental global à la dignité et au développement libre et sans entrave de la personnalité. Des pays aussi différents sur le plan géographique que le Brésil et l'Allemagne ont inscrit ce droit dans leur Constitution et le Rapporteur spécial estime que : a) le droit à la dignité et au développement libre et sans entrave de la personnalité devrait être envisagé comme un droit d'application universelle ; b) des droits déjà reconnus, à savoir le droit à la protection de la vie privée, la liberté d'expression et la liberté d'accès à l'information, constituent une triade de droits habilitants qu'il est préférable d'envisager dans l'optique de leur intérêt pour le développement libre de la personnalité de chaque être humain. Poser en principe la vie privée, et mieux encore la question « pourquoi la vie privée ? », dans le contexte d'un débat plus large sur le droit fondamental à la dignité et au développement libre et sans entrave de la personnalité, correspond aux réalités de la vie à l'ère du numérique. Ce type d'approche devrait aider tous les participants au débat, quelles que soient leur nationalité ou leur culture, à se concentrer sur les fondamentaux du développement de la personnalité et sur le type de vie que le droit à la vie privée devrait concourir à protéger, sans perdre trop de temps à recenser, pour une culture donnée, les traditions liées à la vie privée qu'il leur faudrait privilégier, défendre ou promouvoir.

25. On verra que, dans bon nombre de cas, on ne peut pas vraiment dissocier le débat sur la vie privée de celui sur l'importance de l'autonomie et de l'autodétermination. Le terme « autodétermination » a été largement débattu et, appliqué à la vie privée et aux droits de la personnalité, il a donné naissance en 1983 en Allemagne au droit constitutionnel à l'autodétermination informationnelle. Il convient d'évaluer de façon plus approfondie l'intérêt et la validité de ce concept dans le cadre d'une discussion mondiale sur la manière dont le droit à la vie privée devrait être interprété en 2016, par exemple à l'occasion d'un débat sur la protection du droit fondamental à la dignité et au développement libre et sans entrave de la personnalité.

26. La triade de droits habilitants mentionnée ci-dessus − droit à la vie privée, liberté d'expression et liberté d'accès à l'information − existait avant l'avènement des technologies numériques, tout comme le droit à la dignité et au développement libre et sans entrave de la personnalité. Cela étant, les technologies numériques ont eu des effets considérables sur ces droits, à la fois hors ligne (par exemple les cartes de crédit, l'identification par radiofréquence et d'autres systèmes électroniques) et en ligne, où les internautes génèrent aujourd'hui un volume de données les concernant qui est des dizaines de milliers de fois supérieur à celui d'il y a vingt ans, quand ils ne surfaient pas encore sur Internet. Les appareils mobiles et les technologies convergentes, par exemple les smartphones, qui réunissent téléphonie, photographie et Internet, ont créé un nouveau mode de vie, un nouveau confort et de nouvelles attentes à la fois en matière de commodité et de vie privée.

27. Étant donné l'incidence des nouvelles technologies, la distinction que l'on opère habituellement entre la vie privée individuelle et la vie privée collective va peut-être devoir être revue, tout comme les attentes en termes de protection de la vie privée dans l'espace public comme dans l'espace privé, dans l'optique de la dignité et du développement libre et sans entrave de la personnalité.

B. Observations initiales pour 2015 et 2016

28. Choisir quels ont été les événements les plus importants dans le domaine de la protection de la vie privée depuis l'entrée en fonction du Rapporteur spécial n'a pas été chose facile, d'autant plus que les ressources nécessaires pour mener une enquête approfondie sur ces événements n'étaient pas disponibles. En outre, le Rapporteur spécial ne veut pas empiéter sur les activités des acteurs de la société civile, par exemple celles de Privacy International et de ses organisations affiliées qui organisent, depuis presque vingt ans, les « Big Brother Awards »[d] afin de dénoncer les atteintes à la vie privée. Par ailleurs, il souhaite rendre hommage aux bonnes pratiques, aux textes législatifs, aux décisions de justice et aux idées qui pourraient favoriser ou améliorer la protection de la vie privée. C'est pourquoi, sans prétendre dresser ici une liste exhaustive, et sans établir d'ordre particulier, le Rapporteur spécial souhaiterait appeler l'attention du Conseil des droits de l'homme sur les principaux faits nouveaux présentés ci-après.

1. Une sage décision : les Pays-Bas et les États-Unis d'Amérique disent « non » aux portes dérobées

29. Il faudrait féliciter les Gouvernements des Pays-Bas et des États-Unis d'Amérique pour la réserve dont ils ont fait preuve en se gardant d'autoriser légalement la conception de portes dérobées dans les communications. Le 4 janvier 2016, il a été annoncé que le Gouvernement néerlandais s'était formellement opposé à l'introduction de portes dérobées

[d] www.bigbrotherawards.org.

dans les outils de chiffrement. Dans une note d'information[e] publiée par le Ministère de la sécurité et de la justice et signée par les Ministres de la sécurité et de l'économie, le Gouvernement a déclaré qu'il n'y avait pas lieu d'adopter à l'heure actuelle de mesure législative restreignant le développement, la disponibilité et l'utilisation du chiffrement aux Pays-Bas. Cette décision concluait cinq pages passant en revue les arguments en faveur d'un chiffrement plus généralisé et les contre-arguments prônant l'accès des autorités aux informations. Introduire dans les outils de chiffrement une porte dérobée à l'intention des autorités aurait aussi pour effet de rendre les fichiers chiffrés plus facilement accessibles pour les cybercriminels, les terroristes et les services de renseignement étrangers. Cela pourrait également avoir des conséquences indésirables pour la sécurité des informations communiquées ou stockées ainsi que pour l'intégrité des systèmes fondés sur les technologies de l'information et de la communication, alors même que la sécurité et l'intégrité revêtent une importance croissante pour le bon fonctionnement de la société.

30. La position du Gouvernement néerlandais semble être plus tranchée que celle du Gouvernement américain, prise environ trois mois plus tôt. Au début du mois d'octobre 2015, James Comey, Jr., Directeur du Federal Bureau of Investigation, a déclaré devant le Congrès que l'administration ne demandait pas pour le moment que soit adoptée une loi qui forcerait les entreprises à déchiffrer les données de leurs clients. Ce qui est plus préoccupant, et qui est apparu lors de la récente affaire concernant Apple, c'est que les autorités américaines continueront d'essayer de persuader les entreprises qui ont commencé à chiffrer les données de leurs clients de faire en sorte que le Gouvernement puisse encore avoir accès aux données lorsque celles-ci sont nécessaires dans le cadre d'une enquête pénale ou d'une enquête pour terrorisme. La position du Rapporteur spécial concernant cette affaire a été largement, mais indépendamment, exprimée dans la déclaration du Haut-Commissaire des Nations Unies aux droits de l'homme du 4 mars 2016[f]. La dernière déclaration en date d'Ashton Carter, Secrétaire américain à la défense, selon laquelle un chiffrement fort était essentiel à la sécurité de la nation est encourageante. Lors d'une allocation devant un public composé de spécialistes du secteur des technologies, le 2 mars 2016, M. Carter a dit qu'il n'était pas partisan des portes dérobées et des programmes de chiffrement qui offrent à des personnes extérieures la possibilité de décoder des fichiers chiffrés. Cette position est cohérente avec ses déclarations d'octobre 2015[g] et elle devrait être encouragée et pérennisée.

2. La question de fond : le début de la fin judiciaire de la surveillance de masse

31. Le 6 octobre 2015, la Cour de justice de l'Union européenne a rendu son jugement dans l'affaire *Maximillian Schrems* c. *Data Protection Commissioner*. La Cour a déclaré invalide la décision de la Commission européenne qui établissait une « sphère de sécurité » et sur laquelle était fondée la directive 95/46/CE. Le Rapporteur spécial voudrait s'attarder sur ce qui est probablement l'une des parties les plus importantes de la décision du point de vue de la confirmation (et de l'établissement) de précédents :

> « 94. En particulier, une réglementation permettant aux autorités publiques d'accéder de manière généralisée au contenu de communications électroniques doit être considérée comme portant atteinte au contenu essentiel du droit fondamental au respect de la vie privée, tel que garanti par l'article 7 de la Charte. ».

[e] Disponible sur www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id= 2016Z00009&did= 2016D00015 (consulté le 23 août 2016).

[f] Voir www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=17138&LangID=E.

[g] Voir http://europe.newsweek.com/us-defense-secretary-ashton-carter-doesnt-believe-encryption-backdoors-432811?rm=eu.

32. La signification précise de l'expression « accéder de manière généralisée » sera inévitablement source de discussions. Il apparaît clairement que la Cour fait ici référence au contenu des communications, par opposition aux métadonnées, mais il serait intéressant de voir si une loi européenne légitimant la surveillance de masse résisterait à l'épreuve d'une telle norme dans l'éventualité où la Cour serait disposée à continuer de l'appliquer strictement. Cependant, l'ambiguïté est, au moins partiellement, dissipée lorsque l'arrêt *Schrems* est lu conjointement avec la décision *Zakharov* mentionnée ci-dessous, qui constitue le droit de l'Union européenne autant que celui d'autres États membres du Conseil de l'Europe.

3. L'importance d'avoir accès à une voie de recours : questions de procédure et d'application de la loi

33. Se référant de nouveau à l'arrêt *Schrems*, le Rapporteur spécial note avec satisfaction que la Cour de justice est devenue une tribune pour les personnes telles que le requérant, qui a soumis l'affaire en tant que particulier préoccupé par les conséquences du développement des technologies modernes de l'information sur sa dignité en tant qu'être humain dans une société démocratique. Il est essentiel que les individus puissent faire valoir leur point de vue et défendre leurs droits devant une institution publique supranationale, remettant ainsi en cause les relations de pouvoir existantes, pour créer des connaissances afin d'améliorer le bien-être de la société, et cela va dans le sens du développement du droit international des droits de l'homme. L'existence de ces mécanismes est absolument cruciale pour protéger les droits de l'homme et restaurer la confiance de la population dans l'usage que font les États et les autres acteurs de la technologie.

34. Ces mécanismes sont également précurseurs d'un fait nouveau dans la société : ils appellent l'attention sur le fait que les droits doivent être respectés et exercés partout, et pas seulement dans les endroits hébergeant des serveurs.

35. La décision de la Cour de justice démontre également la valeur ajoutée des approches régionales, car celles-ci pourraient à l'avenir permettre de promouvoir des instruments juridiques ascendants et participatifs ayant une plus large portée.

4. La simple existence d'une mesure de surveillance secrète est une violation du droit au respect de la vie privée

36. Dans son arrêt *Roman Zakharov* c. *Russie*[h] du 4 décembre 2015, la Grande Chambre de la Cour européenne des droits de l'homme a reconnu à l'unanimité que le système d'interception secrète des communications de téléphonie mobile en Russie constituait une violation de l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales. En outre, il est très intéressant de noter que la Grande Chambre a admis que, si certaines conditions sont remplies, un requérant peut se prétendre victime d'une violation de l'article 8 entraînée par la simple existence de mesures de surveillance secrète. La déclaration de la Grande Chambre proscrivant les systèmes de surveillance de masse d'une manière encore plus explicite que dans l'arrêt *Schrems* de la Cour de justice est peut-être encore plus importante :

> « 270. La Cour estime que le mode de fonctionnement du système de surveillance secrète en Russie donne aux services de sécurité et à la police les moyens techniques de contourner la procédure d'autorisation et d'intercepter n'importe quelle communication sans mandat judiciaire préalable. Si l'on ne peut jamais, quel que soit le système, écarter complétement l'éventualité qu'un fonctionnaire malhonnête, négligent ou trop zélé commette des actes irréguliers (*Klass et autres*, précité, par. 59), la Cour considère néanmoins qu'un système tel que le système russe, qui

[h] *Roman Zakharov* c. *Russie* [GC], 4 décembre 2015, n° 47143/06, Recueil des arrêts et décisions.

> permet aux services secrets et à la police d'intercepter directement les communications de n'importe quel citoyen sans leur imposer l'obligation de présenter une autorisation d'interception au fournisseur de services de communication ou à quiconque, est particulièrement exposé aux abus. La nécessité de disposer de garanties contre l'arbitraire et les abus apparaît donc particulièrement forte. ».

37. L'arrêt constitue un jalon déterminant car il met en lumière les exigences de soupçon raisonnable et de mandat judiciaire préalable ainsi que la nature inacceptable d'un « système […] qui permet aux services secrets et à la police d'intercepter directement les communications de n'importe quel citoyen sans leur imposer l'obligation de présenter une autorisation d'interception ». Il devrait donc servir de pierre de touche pour tous les textes législatifs existants et projets de loi relatifs à la surveillance dans tous les pays d'Europe. En outre, le Rapporteur spécial est profondément préoccupé par diverses informations faisant état d'une décision prise par la Douma (Chambre du Parlement russe) qui permettrait d'annuler les décisions de la Cour européenne des droits de l'homme[i]. Si ces informations sont avérées, cela pourrait, dans la pratique, supprimer une voie de recours très importante ouverte aux citoyens des pays qui ont ratifié la Convention européenne des droits de l'homme, notamment les recours en cas de violation du droit au respect de la vie privée. Le Rapporteur spécial invite le Gouvernement de la Fédération de Russie à l'aider à vérifier plus avant la véracité de ces allégations, à examiner plus en profondeur la loi en question pour la nuancer et, si les informations sont fondamentalement justes, à persuader la Douma d'abroger la loi du 4 décembre 2015 et de rétablir l'utilité des voies de recours ouvertes aux citoyens russes en vertu de la Convention européenne des droits de l'homme, notamment les recours contre l'État en cas de violation de leur droit à la vie privée.

5. Projet de loi du Royaume-Uni de Grande-Bretagne et d'Irlande du Nord relatif aux pouvoirs d'enquête

38. Il convient de rendre hommage à trois commissions parlementaires britanniques − la Commission sur les sciences et les technologies (le 1er février 2016), la Commission du Parlement sur les renseignements et la sécurité (le 9 février 2016) et, surtout, la Commission mixte du projet de loi relatif aux pouvoirs d'enquête elle-même (le 11 février 2016) − pour leur critique constante et argumentée, bien que parfois trop polie, du projet de loi qui est actuellement en cours d'examen au Parlement. Dans son rapport, la Commission mixte du projet de loi a recommandé 86 modifications, essentiellement axées sur des points à clarifier et sur la question du contrôle judiciaire et de la justification des différents pouvoirs. Il faut également rendre hommage au Gouvernement britannique, qui tient compte des conseils formulés par différentes parties et qui utilise ce projet de loi aux fins du renforcement, plus que nécessaire, des mécanismes de contrôle. Même s'il y a encore une marge d'amélioration, les mesures prises vont dans la bonne direction. Cependant, au moment de la soumission du présent rapport, le Rapporteur spécial s'interroge sur l'utilité de certaines révisions tout récemment apportées à la dernière version du projet de loi, publiée le 1er mars 2016. Au moment de la rédaction du présent rapport, certaines propositions du Gouvernement semblent non seulement aller à l'encontre du raisonnement et des conclusions du Rapporteur spécial sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste dans son rapport de 2014, qui traite notamment de la surveillance de masse[j], mais aussi, à première vue, s'écarter des normes fixées par la Cour de justice dans l'affaire *Schrems* et par la Cour européenne des droits de l'homme dans l'affaire *Zakharov*. Le Rapporteur spécial encourage vivement les trois Commissions dont l'action a été précédemment saluée à continuer d'exercer leur influence, avec une vigueur et une détermination renouvelées, afin que des mesures disproportionnées et intrusives, telles que la surveillance de masse et le piratage massif qui

[i] Voir www.bbc.com/news/world-europe-35007059.
[j] A/69/397.

sont envisagés dans le projet de loi, soient interdites et non légitimées. Il semble que le Gouvernement n'ait pas pleinement pris la mesure de la gravité des conséquences, même involontaires, que pourrait avoir la légitimation de l'interception et du piratage massifs. Compte tenu de l'immense influence qu'a encore la législation du Royaume-Uni sur plus d'un quart des États Membres de l'ONU, qui font toujours partie du Commonwealth, ainsi que de la tradition dont le Royaume-Uni s'enorgueillit en tant que démocratie et membre fondateur des principaux organes régionaux des droits de l'homme, comme le Conseil de l'Europe, le Rapporteur spécial invite le Gouvernement à se saisir de cette occasion idéale pour montrer l'exemple et renoncer à adopter des mesures disproportionnées qui pourraient avoir des effets préjudiciables bien au-delà des rivages du Royaume-Uni. Il l'invite en particulier à s'engager davantage en faveur de la protection du droit fondamental des Britanniques et de la population des autres États à la vie privée, ainsi qu'à renoncer à donner un mauvais exemple à d'autres États en continuant de proposer des mesures, telles que l'interception et le piratage massifs, qui ne répondent à première vue pas aux normes fixées par plusieurs commissions parlementaires britanniques, vont à l'encontre des arrêts les plus récents de la Cour de justice et de la Cour européenne des droits de l'homme et menacent l'esprit même du droit à la vie privée. Enfin, le Rapporteur spécial invite le Gouvernement à travailler en étroite collaboration avec lui, en particulier dans le cadre de son étude thématique sur la surveillance, afin de définir des mesures proportionnées qui renforcent la sécurité sans être trop intrusives.

6. Un premier pas vers la cyberpaix ?

39. Il convient de reconnaître l'action de la Chine et des États-Unis, qui sont les premiers à tenter d'apaiser la situation dans le cyberespace.

40. On peut établir trois grandes dimensions dans le cyberespace, qui sont toutes menacées par l'espionnage en ligne :

a) Le sabotage et la guerre ;

b) Les droits de propriété intellectuelle et l'espionnage économique ;

c) Les droits civils et la surveillance.

41. S'il est vrai que la question de la vie privée se pose davantage en rapport avec la troisième dimension, elle apparaît souvent dans des discussions sur les deux autres. En septembre 2015, les États-Unis et la Chine ont annoncé qu'ils étaient convenus qu'ils n'appuieraient ni ne commettraient aucun cybervol de propriété intellectuelle et qu'ils étaient déterminés à définir des normes appropriées pour régir le comportement des États dans le cyberespace au sein de la communauté internationale. Ils ont également décidé de créer un groupe d'experts de haut niveau chargé de discuter des questions relatives à la cybernétique[k]. Non seulement les États-Unis et la Chine ont donné suite à cette importante avancée, en tenant des discussions sur la cybernétique en décembre 2015, mais il semble aussi qu'ils ont montré l'exemple à d'autres pays : cette annonce a été suivie d'un accord similaire entre le Royaume-Uni et la Chine et de l'annonce que Berlin signerait avec Beijing un accord contre le cybervol en 2016. En novembre 2015, la Chine, le Brésil, la Russie, les États-Unis et d'autres membres du G20 ont accepté la norme interdisant la commission et le soutien des cybervols de propriété intellectuelle[l]. Il ne s'agit pas encore d'accords complets sur la cyberguerre ou la surveillance en ligne et sur les effets de l'espionnage sur la vie privée des citoyens, mais c'est un début, et le Rapporteur spécial ne peut que tenter de convaincre l'ensemble des parties concernées que les discussions devraient également porter sur des mesures concrètes garantissant le respect de la vie privée en ligne.

[k] Voir www.cnbc.com/2015/09/25/us-china-agree-to-not-conduct-cybertheft-of-intellectual-property-white-house.html.

[l] Voir http://blogs.cfr.org/cyber/2016/01/04/top-5-us-china-cyber-agreement.

IV. Principales activités du Rapporteur spécial

A. Ressources allouées aux activités du Rapporteur spécial

42. Étant donné qu'il s'agit d'un nouveau mandat, que le budget officiel y afférent n'a été approuvé qu'en janvier 2016 et que le mandat a débuté le 1er août 2015, c'est-à-dire alors que la plus grande partie de l'Europe était en vacances, le Rapporteur spécial n'a pu bénéficier d'une forme d'appui du Haut-Commissariat aux droits de l'homme qu'au bout de plusieurs semaines. Pour l'instant, ce soutien administratif est fourni de manière temporaire, en attendant que du personnel soit recruté, ce qui devrait être fait d'ici à juin 2016. Après avoir évalué la situation en matière de ressources, le Rapporteur spécial a pris immédiatement des mesures pour trouver des financements externes à l'ONU. Un chercheur postdoctoral (titulaire d'un doctorat sur le droit au respect de la vie privée et le droit à l'oubli) a été recruté à compter d'octobre 2015 à temps partiel puis, à partir de janvier 2016, à temps plein, pour offrir son aide sur les questions de fond. Le financement par des sources externes sera maintenu jusqu'à ce que la situation en matière de ressources humaines soit réglée. En outre, des experts et des membres d'institutions pour lesquelles le Rapporteur spécial travaille, à savoir le Département de la politique de l'information et la gouvernance de la faculté des médias et des connaissances de l'Université de Malte et le Groupe de recherche sur la sécurité, la technologie et la vie privée en ligne de la faculté de droit de l'Université de Groningen (Pays-Bas), apportent aussi très aimablement leur concours bénévole. Cette assistance, vivement appréciée, tout comme celle du personnel des Nations Unies à Genève, permet au Rapporteur spécial de s'acquitter de ses fonctions jusqu'à ce que les capacités soient portées à un niveau acceptable et qu'une structure d'appui plus adéquate, adaptée au mandat, puisse être mise en place.

B. Feuille de route pour le mandat du Rapporteur spécial : élaboration du plan en dix points

43. Outre les activités quotidiennes énoncées dans la section II, le Rapporteur spécial a consacré un temps considérable à l'élaboration du plan en dix points exposé dans la section V et aux consultations avec les nombreuses parties prenantes.

C. Participation à diverses manifestations

44. Le Rapporteur spécial a accepté des invitations à des réunions, à des conférences, à des tables rondes et à des consultations individuelles, en particulier à celles qui contribuaient à maintenir une participation continue aux sept études thématiques précédemment évoquées. On trouvera ci-après une liste non-exhaustive des manifestations auxquelles il a participé :

a) Réunion-débat intitulée « Inextricably intertwined: freedom of expression and privacy in Internet governance » (Liberté d'expression et vie privée en matière de gouvernance de l'Internet : un lien inextricable), MAPPING, première Assemblée générale, Hanovre (Allemagne), 22 septembre 2015 ;

b) Réunion avec la Directrice des affaires mondiales de Human Rights Watch, 30 septembre 2015 ;

c) Participation et prise de parole au séminaire sur la protection des données et la vie privée dans le domaine de la statistique, Genève, 13 et 14 octobre 2015 ;

d) Réunion avec le Vice-Secrétaire général de l'UIT, Genève, 14 octobre 2015 ;

e) Organisation et présidence de la table ronde sur la vie privée et la surveillance lors de la Conférence sur le renseignement dans la société de la connaissance, Bucarest, 16 octobre 2015 ;

f) Allocution sur la vie privée à l'ère du numérique lors de la Conférence internationale des Commissaires à la protection des données et de la vie privée, réunion privée, Amsterdam, 27 octobre 2015 ;

g) Participation à la table ronde intitulée « tour du monde » lors de la Conférence internationale des Commissaires à la protection des données et de la vie privée, Amsterdam, 29 octobre 2015 ;

h) Participation à plusieurs séances, publiques et bilatérales, du Forum sur la gouvernance d'Internet, João Pessoa (Brésil), 9-13 novembre 2015[m] ;

i) Discours principal lors d'une réunion privée, *Big Data in the Global South International Workshop*, Rio de Janeiro (Brésil), 16 et 17 novembre 2015[n] ;

j) Réunions avec des fonctionnaires du Ministère brésilien de la justice lors d'une analyse approfondie d'un nouveau projet de loi brésilien sur la vie privée, Brasilia, 18 novembre 2015 ;

k) Réunion conjointe avec des fonctionnaires des Ministères brésiliens des télécommunications, de la justice et de l'intérieur au sujet d'un nouveau projet de loi brésilien sur la vie privée, Brasilia, 18 novembre 2015 ;

l) Réunion au bureau du Procureur général, Brasilia, 18 novembre 2015 ;

m) Réunion avec le Directeur des droits de l'homme, Ministère des affaires étrangères du Brésil, Brasilia, 19 novembre 2015 ;

n) Discours (par visioconférence) lors du Congrès mondial de Consumers International, Brasilia, 19 novembre 2015[o] ;

o) Réunions et consultations approfondies avec le fondateur et directeur de Patient Privacy Rights, Malte, 25 novembre 2015 ;

p) Allocution lors de la séance consacrée à la contextualisation des débats de la Conférence de haut niveau sur la protection de la vie privée en ligne grâce à l'amélioration de la sécurité de l'information et au renforcement de l'autonomie de l'UE en matière de technologies de l'information, conjointement organisée par la Commission des libertés civiles, de la justice et des affaires intérieures et le groupe d'évaluation des choix scientifiques et techniques du Parlement européen, Bruxelles, 8 décembre 2015[p] ;

q) Allocution lors d'une conférence sur la sécurité et la vie privée dans le contexte d'une sphère de sécurité 2.0, Rome, 9 décembre 2015[q] ;

r) Discours principal sur la vie privée, l'identité, la sécurité et la liberté lors du congrès annuel du Privacy and Identity Lab, Utrecht (Pays-Bas), 11 décembre 2015[r] ;

s) Participation à une séance de formation initiale des Rapporteurs spéciaux, Genève, 14-16 décembre 2015 ;

t) Réunion avec une délégation du Royaume-Uni, Genève, 17 décembre 2015 ;

[m] Voir www.intgovforum.org/cms/igf-2015-schedule.

[n] Voir http://itsrio.org/en/2015/11/05/encontro-fechado-workshop-internacional-big-data-no-sul-global.

[o] Voir http://congressprogramme.consumersinternational.org/speakers.html.

[p] Voir www.europarl.europa.eu/stoa/cms/cache/offonce/home/events/workshops/privacy.

[q] Voir www.dimt.it/tag/cannataci.

[r] Voir www.pilab.nl/index.php/2015/12/14/the-privacy-identity-lab-four-years-later-published.

u) Réunion avec une délégation de la Chine, Genève, 17 décembre 2015 ;

v) Réunion avec une délégation de la Fédération de Russie, 17 décembre 2015 ;

w) Participation par visioconférence à la réunion spéciale du Comité contre le terrorisme sur les moyens de prévenir l'exploitation d'Internet et des médias sociaux aux fins du recrutement de terroristes et de l'incitation à la commission d'actes terroristes, tout en respectant les droits de l'homme et les libertés fondamentales, New York, 17 décembre 2015 ;

x) Exposé et conduite des débats lors d'une table ronde de représentants d'ONG, dont Privacy International, Amnesty International, Reporters sans frontières, Internet Society, Human Rights Watch et American Civil Liberties Union, Genève, 18 décembre 2015 ;

y) Réunion avec le Directeur adjoint du Bureau de la normalisation des télécommunications de l'UIT (avec l'Unité des affaires juridiques de l'UIT), Genève, 18 décembre 2015 ;

z) Intervention et exposé par visioconférence sur la vie privée, la qualité de la vie et les villes intelligentes : développement du « surveillable » lors d'une conférence de l'UIT sur les villes intelligentes, Singapour, 18 janvier 2016 ;

aa) Réunion avec Helen Wallace et Andrew Jackson de GeneWatch UK, Malte, 3 février 2016 ;

bb) Allocution (par visioconférence) lors du cinquième atelier sur la protection des données dans les organisations internationales, Genève, 5 février 2016[s] ;

cc) Allocution et participation à une réunion générale du Ministère néerlandais des affaires étrangères pour les acteurs concernés, La Haye (Pays-Bas), 3 mars 2016.

V. Plan d'action en dix points

45. Afin d'examiner de manière plus approfondie les dimensions du droit à la vie privée et de ses liens avec d'autres droits de l'homme, le Rapporteur spécial a élaboré un bref plan d'action en dix points. Il convient de garder à l'esprit que ces points ne sont pas exposés dans un ordre particulier et que ce plan n'est donc pas un programme de travail énoncé selon un ordre de priorité. Le Rapporteur spécial estime que son rôle s'apparente à celui d'un pionnier. Autrement dit, il s'efforce de trouver la voie à suivre tout en déterminant les questions urgentes à traiter ou en réagissant aux besoins des individus ou des pays pour lesquels il convient d'agir en urgence en matière de responsabilité. Le plan d'action en dix points est une liste de mesures à prendre et non une simple liste de souhaits. Le Rapporteur spécial a déjà commencé à travailler sur chacun de ces dix points ; l'avancement des travaux dépendra du temps et des ressources disponibles.

1. Signification du « droit à la vie privée »

46. Pour dépasser le cadre juridique existant en vue de mieux comprendre ce que l'on s'est engagé à protéger, il convient de travailler à l'élaboration d'une meilleure définition, plus détaillée et plus universelle, du « droit à la vie privée ». Que signifie cette expression et que devrait-elle signifier au vingt et unième siècle ? Comment mieux protéger ce droit à l'ère du numérique ? Le Rapporteur spécial organisera des activités et appuiera des travaux de recherche en vue d'examiner les réponses qui pourraient être données à ces questions essentielles, réponses qui contribueront à établir des bases essentielles pour d'autres points du plan d'action du Rapporteur spécial.

[s] Voir www.icrc.org/en/event/5th-workshop-data-protection-within-international-organisations.

2. Renforcement de la prise de conscience

47. Il importe également de mieux sensibiliser les populations pour les aider à comprendre ce qu'est la vie privée. Il est important de tenir un discours général sur ce qu'est leur droit à la vie privée et sur la manière dont il peut être porté atteinte à ce droit, en particulier dans le cadre des nouvelles technologies et du fait du comportement des usagers dans le cyberespace. Les particuliers doivent savoir comment leurs données personnelles sont monétisées et connaître les garanties et les voies de recours qui sont à leur disposition pour protéger leur droit à la vie privée. Que peuvent-ils faire pour réduire au minimum le risque d'atteinte à leur droit à la vie privée ? Comment peuvent-ils dialoguer avec le législateur et le secteur privé pour améliorer la protection de la vie privée ? La sensibilisation est une entreprise considérable et le Rapporteur spécial souhaite y contribuer tout au long de son mandat en travaillant de manière continue avec l'ensemble des parties prenantes, en particulier la société civile.

3. Établissement d'un dialogue structuré et suivi au sujet de la vie privée

48. Il est indispensable qu'un dialogue plus structuré, ouvert, approfondi, concret et par-dessus tout, suivi, se noue entre les différentes parties prenantes. Pour protéger la vie privée, il faut tisser des liens. Le Rapporteur spécial compte mettre l'accent sur cette activité, en s'appuyant sur les espaces de discussion existants et en en créant de nouveaux. Il est particulièrement important, à cet égard, de faciliter l'établissement d'un dialogue structuré entre les organisations non gouvernementales, les commissaires à la protection des données et de la vie privée, les services chargés de l'application des lois et les services de sécurité et du renseignement. Il est tout aussi important d'œuvrer, avec toutes les catégories de parties prenantes, à améliorer les procédures internes et à renforcer les niveaux de protection, en tenant compte du respect de la vie privée dès la conception des technologies que ces entités utilisent et des procédures qu'elles suivent. Il importe également de développer au maximum la transparence et l'obligation de rendre des comptes, et de renforcer les contrôles neutres et efficaces, de sorte à en accroître considérablement l'efficacité et la crédibilité.

4. Une approche globale des garanties juridiques, procédurales et opérationnelles et des voies de recours

49. La mise en place de garanties appropriées et de recours effectifs est une des raisons d'être de la législation relative à la protection des données depuis sa création. Cette législation a pour objet d'offrir des orientations et des garanties de protection adéquates dans un monde que l'évolution constante de la technologie rend plus complexe. Des garanties de protection plus claires et efficaces devraient être proposées pour prévenir toute atteinte à la vie privée. En cas d'atteinte, les personnes concernées devraient toutes avoir accès à de véritables recours. La recherche de garanties et de recours est transversale et sous-tend l'ensemble des études thématiques du Rapporteur spécial, qui sont présentées dans la section II ci-dessus.

5. Un intérêt accru pour les garanties techniques

50. Les garanties et les recours offerts aux citoyens ne peuvent jamais être uniquement juridiques ou opérationnels. À elle seule, la loi ne suffit pas. Le Rapporteur spécial continuera de coopérer avec les milieux techniques en vue de promouvoir le développement de garanties techniques efficaces, notamment le chiffrage, des logiciels de recouvrement (overlay) et d'autres méthodes techniques assurant une application réelle du concept de protection de la vie privée dès la conception.

6. Un dialogue ciblé avec le monde des entreprises

51. De nos jours, un nombre croissant d'entreprises collectent déjà bien plus de données personnelles que ne peuvent ou ne pourront jamais le faire la plupart des États. Avec les business models actuels, on assiste à une monétisation à outrance des données personnelles. Quels grands changements la société peut-elle espérer voir émerger de ces modèles et quels modèles acceptables peut-elle espérer voir se développer ? Quelles sont les garanties qui s'appliquent lorsque les autorités étatiques demandent à des entreprises privées de leur transmettre les données qu'elles détiennent ? L'aspect du mandat touchant à ces questions mérite qu'on lui consacre du temps et de l'attention. Le Rapporteur spécial a déjà commencé à établir des contacts directs avec des représentants du monde des entreprises et continuera d'entretenir avec eux un dialogue axé sur la vie privée, dans l'objectif de rester au fait des évolutions dans le secteur et de leur communiquer d'autres informations relatives à son mandat.

7. Promouvoir le progrès, aux niveaux national et régional, en ce qui concerne les mécanismes de protection de la vie privée

52. L'utilité des progrès réalisés aux niveaux national et régional dans le domaine des mécanismes de protection de la vie privée devrait être davantage appréciée au niveau mondial. Le Rapporteur spécial est investi d'un rôle complémentaire important lorsqu'il travaille en relation étroite avec les Commissaires à la protection des données et à la vie privée de différents pays. Par la coopération et le dialogue, les normes qui régissent, sur le plan mondial, la protection de la vie privée pourraient être sensiblement renforcées. Le Rapporteur spécial a commencé à mener, à l'échelle mondiale, une série d'activités planifiées et mises en œuvre avec le concours des autorités chargées de la protection des données. Il est notamment prévu d'organiser des manifestations en Australie, au Maroc, en Nouvelle-Zélande, en Tunisie et en Irlande du Nord en 2016, et d'autres devraient avoir lieu dans les années à venir.

8. Mettre à profit le dynamisme et l'influence de la société civile

53. Le Rapporteur spécial, qui a déjà rencontré les représentants de 40 organisations non gouvernementales au cours des six premiers mois de son mandat, entend bien continuer de consacrer un temps considérable à écouter les représentants de la société civile et à travailler avec eux, qui déploient tant d'énergie pour qu'à travers le monde, le droit à la vie privée soit mieux respecté.

9. Cyberespace, cyberespionnage, cyberguerre, cyberpaix et respect de la vie privée sur Internet

54. La communauté internationale doit faire preuve de curiosité, de franchise et d'ouverture s'agissant de ce qui se passe réellement dans le cyberespace, en particulier à propos de la réalité de la surveillance de masse, du cyberespionnage et de la cyberguerre. En s'attaquant à ces phénomènes, elle renforcera les mesures décrites précédemment et les résultats des études thématiques évoquées à la section II ci-dessus. Le Rapporteur spécial s'attend à ce que ces questions soient soulevées dans beaucoup de ses rapports et dans le cadre de nombreuses visites de pays. En communiquant en toute transparence avec les différentes parties prenantes sur ces questions, il espère contribuer, de façon constructive, à l'amélioration de la protection de la vie privée à l'ère du numérique.

10. Investir davantage dans le droit international

55. Si le droit ne suffit pas à lui seul, il n'en demeure pas moins d'une grande importance. Les possibilités de développer le droit international applicable à la vie privée devraient toutes être explorées ; le Rapporteur spécial est disposé à examiner la valeur

de tout instrument juridique, qu'il soit considéré comme relevant de la *soft law* ou de la *hard law*. Il faudrait commencer par une question prioritaire comme l'actualisation des instruments juridiques, afin qu'ils tiennent compte d'une approche plus large du droit à la vie privée. Il semblerait que plusieurs parties prenantes se soient accordées sur le fait qu'un tel instrument pourrait prendre la forme d'un protocole additionnel à l'article 17 du Pacte international relatif aux droits civils et politiques[t]. Le Rapporteur spécial a d'ailleurs été instamment invité à « promouvoir l'ouverture de négociations sur un tel protocole pendant son premier mandat »[u]. La date précise à laquelle il pourra s'atteler à cette tâche dépendra toutefois sûrement de la durée et de l'issue des discussions vastes et approfondies à mener sur les aspects évoqués au point 1 − parvenir à une meilleure conception universelle de ce que sont, ou pourraient être, les aspects fondamentaux du droit à la vie privée. D'autres questions relatives à la vie privée, en particulier la question de la compétence et de la territorialité dans le cyberespace, ne peuvent être traitées comme il se doit en l'absence d'un accord international clair à ce sujet. Un tel accord prendrait normalement la forme d'un traité multilatéral, portant très probablement sur une question ou une série de questions précises. Afin de dissiper tout malentendu, il convient de préciser que l'idée n'est pas d'élaborer une nouvelle convention internationale de portée mondiale et générale, couvrant tous les aspects du droit à la vie privée et de la gouvernance d'Internet. Il est bien plus réaliste de considérer qu'un meilleur respect du droit à la vie privée passera par le développement progressif du droit international, c'est-à-dire par la clarification et, à terme, par l'élargissement, des instruments juridiques existants. À moyen et long termes, cela pourrait conduire à l'élaboration d'instruments juridiques entièrement nouveaux. En outre, le Rapporteur spécial suivra les discussions en cours sur le droit international et les nouveaux instruments juridiques relatifs à la gouvernance d'Internet, afin de définir le calendrier des activités que doivent mener les divers organes des Nations Unies et de déterminer la nature et le champ d'application de l'instrument juridique qu'il pourrait, à terme, souhaiter recommander au Conseil des droits de l'homme et à l'Assemblée générale.

VI. Conclusions

56. **Le Rapporteur spécial a été impressionné par l'accueil particulièrement chaleureux et enthousiaste que lui ont réservé la plupart des secteurs de la société et des catégories de parties prenantes.**

57. **La question de la vie privée n'a jamais été aussi présente aux plans politique, judiciaire et individuel qu'en 2016.**

58. **Les tensions entre la sécurité, les business models des entreprises et le respect de la vie privée continuent d'occuper le devant de la scène, mais les douze derniers mois ont été marqués par des tendances contradictoires : alors que certains États ont continué d'afficher, dans la pratique ou par l'intermédiaire de leurs Parlements, de l'hostilité vis-à-vis de la protection de la vie privée, des tribunaux dans le monde entier, et en particulier aux États-Unis et en Europe, ont fait clairement avancer la lutte en faveur du droit à la vie privée et se sont opposés, en particulier, aux mesures disproportionnées qui portent atteinte à ce droit, comme la surveillance de masse et le déchiffrement.**

59. **Des signaux forts portent à croire que la vie privée revêt à présent un grand intérêt commercial, certaines grandes entreprises en ayant même fait un argument de vente. S'il existe un marché de la vie privée, les lois du marché ne manqueront pas de l'alimenter. L'augmentation rapide de l'offre de dispositifs chiffrés et des services**

[t] Voir https://icdppc.org/wp-content/uploads/2015/02/R%C3%A9solution-sur-le-Rapporteur-sp%C3%A9cial-de-lONU-sur-le-droit-%C3%A0-la-vie-priv-VF.pdf

[u] Ibid.

logiciels montre que, dans le monde entier, les consommateurs sont de plus en plus conscients des risques qui pèsent sur leur vie privée et qu'ils vont de plus en plus donner la préférence aux produits et aux services qui protègent leur vie privée plutôt qu'à ceux qui n'en tiennent pas compte ou qui lui sont préjudiciables.

60. **Si certains États continuent, de façon mal inspirée, inconsidérée, intempestive, inopportune et parfois déplacée, de légitimer ou de maintenir des mesures disproportionnées et injustifiables, qui portent atteinte à la vie privée, comme la collecte massive de données, le piratage massif et l'interception injustifiée de données, d'autres − en tête desquels figurent en l'occurrence les Pays-Bas et les États-Unis − se sont quant à eux orientés plus ouvertement vers une politique d'interdiction des portes dérobées dans les programmes de chiffrement. Le Rapporteur spécial souhaiterait encourager davantage d'États à se ranger derrière cette politique.**

61. **Les États, partout dans le monde, ne sont pas seulement en train de prendre conscience de leurs responsabilités et de l'existence de garanties techniques telles que le chiffrement, ils sont également en train de se rendre compte, lentement mais sûrement, du peu de bénéfices qu'ils tireraient et de l'ampleur des risques qu'ils prendraient s'ils contribuaient, par la cyberguerre et le cyberespionnage, à la destruction du cyberespace. S'il reste encore des progrès à faire, des avancées importantes ont été réalisées en 2015. Le Rapporteur encourage par conséquent les États − et non uniquement le Groupe des Vingt − à se réunir pour discuter de la politique étatique adéquate à adopter en matière de cyberespace, et des mesures qui l'accompagneront, notamment du point de vue des droits civils, en particulier du droit à la vie privée, du droit à la liberté d'expression et de la surveillance.**

62. **Les méthodes de travail du Rapporteur spécial et son plan d'action en dix points devraient permettre d'appréhender de façon globale la question de la protection et de la promotion du droit à la vie privée à l'ère du numérique. Une approche globale contribue à donner une vue d'ensemble de ce qui doit être fait, même si la question de savoir selon quel échéancier, par qui et quand exactement sera fonction de deux grands facteurs : premièrement, les ressources dont le Rapporteur spécial disposera pour mettre en œuvre son plan d'action et mener à bien ses études thématiques ; deuxièmement, la volonté des différentes parties prenantes d'adopter et de promouvoir un programme respectueux de la vie privée, au lieu de rester enfermées dans une logique d'emprise et de contrôle. Le Rapporteur spécial souhaite adresser un message clair et simple à ceux qui pourraient trouver, à première vue, que ce plan d'action n'est pas seulement ambitieux mais peut-être excessivement ambitieux : si vous adhérez aux objectifs de ce plan et à la manière dont des questions complexes mais intimement liées y sont présentées, faites-vous connaître et allouez des ressources supplémentaires à sa mise en œuvre. Cela contribuerait à le rendre plus réalisable. Pour élaborer une stratégie permettant d'accroître les ressources mises à sa disposition, le Rapporteur spécial s'appuie sur son expérience en tant que chargé de projet qui a réussi à lever des millions de dollars pour la recherche dans le domaine de la vie privée. De fait, la réalisation du plan d'action en dix points dépend du succès de cette stratégie. Même si elle s'avérait être une réussite totale, le Rapporteur spécial ne serait absolument pas étonné que le prochain titulaire de mandat doive reprendre et, éventuellement, compléter certains aspects du plan d'action. L'objectif, à ce stade, est de définir une vision claire et globale et de poser des fondements solides, en vue de jeter les bases d'une politique robuste, reposant sur des données probantes en matière de protection de la vie privée.**

Annex I

Challenges faced by the Special Rapporteur and his vision for the mandate

1. The Special Rapporteur immediately set about building up his team composed of persons working for the mandate on a part-time or full-time basis. One of these persons is currently a full-time United Nations (UN) Human rights officer, hired on a temporary contract, while the position is under recruitment. The work of this person is supervised by a more senior UN employee who is also responsible for supporting the work of six other mandate holders. A second part time professional and a part time administrative officer will soon be recruited, as well as a part-time consultant. The SRP is grateful that the Human Rights Council endowed his mandate with this still limited (given the scope of his mandate) but unprecedented level of support to a mandate holder. The other persons in the SRP team are not employed by the UN but are resourced by extra-mural funding obtained by the SRP or may be volunteers. The team is often physically spread across at least three geographical locations (currently Malta, the Netherlands and Switzerland) and, as befits the digital age, most of the team meetings are carried out in cyber-space with the working day being opened by an on-line conference call involving all team-members who may be available. During the "morning meeting" team members typically report on work carried out in the previous day, consult about tasks planned for the rest of the working day and plan tasks and events for the following weeks and months. When doing so, their tasks reflect the fact that the work of the SRP may be broadly divided into four categories and any team member may be working concurrently on tasks from each of these categories.

2. The fact that the mandate on privacy is a new one presents both advantages and disadvantages. Amongst other things it means that the Special Rapporteur on Privacy (SRP) had no roadmap to follow and indeed one of his first priorities in this case is to work on designing and developing such a roadmap. This means that some of the issues identified in this and later reports are not necessarily capable of being resolved within the time-constraints imposed by one or even two three-year mandates. They are mentioned however in order to provide a more holistic picture of what needs to be done in the short, mid and long-term. In doing so, this incumbent is conscious of possibly identifying issues which may possibly be more appropriately tackled in a more timely manner by later holders of the mandate.

3. One of the recurring themes of this and later reports will undoubtedly be the time dimension. The rapid pace of technology and its effects on privacy means that action on some already-identified issues may increase or decrease in priority as time goes by while new issues may emerge fairly suddenly. It may also mean that sometimes it may be more opportune to launch or intensify action on a particular issue not necessarily because it is much more important than other issues but rather because the timing is right, because the different international audiences and classes of stakeholders may be far more sensitive and receptive to that particular issue for reasons and circumstances over which the Special Rapporteur may have absolutely no control but in which case it would be foolish not to take advantage of favourable opportunities which may result in the creation or improvement of privacy safeguards and remedies.

4. The later prioritisation of action will also depend on the extent of the resources made available to the Special Rapporteur and the extent to which he can succeed in attracting fresh resources to support the mandate on privacy. This resource issue is fundamentally important and will directly affect the extent of the impact the mandate on Privacy may have

in practice in real life. It is clear that, however good in quality in some respects, the quantity of resources provided to the mandate by the UN is woefully inadequate and even if the mandate's human and financial resources are increased tenfold, it would still be hard-pressed to achieve the minimum required to persuade the incumbent that the work of the mandate is really making a difference to the protection of privacy of ordinary citizens around the world. The experience of the first six months in office has persuaded the mandate-holder that not only must the SRP be omni-present 24/7 on the many privacy-related issues which arise literally every day in many countries around the world but that he must also act as rainmaker, somehow attracting funds and human resources in order to make the work of the mandate both possible and sustainable in the short, mid and long-term. The effort required by what is, in essence, a part-time, un-paid position which must, by definition, co-exist with a demanding day-job, should not be under-estimated. This effort can be encouraged by the positive response of all stakeholders not least that of the nation-states, members of the UN to whom this report is addressed. If these stakeholders do not support the mandate adequately, if they do not put their money where their mouth is, then this will only serve to increase the frustrations already inherent to any work being carried out within the UN's systems and bureaucracy.

5. The incumbent's vision of the mandate is therefore analogous to the process required to design, finance, project manage and complete the building of a house or other building suitable for human beings to live and/or work in safely. Firstly we need to understand the function of the building: is it a residence for an individual living alone or for one nuclear family, or for a large and extended family or indeed for several of such individuals and families? Should it include a working space and if so for what type of work: is this to be a farm-house, a baker's *casa bottega* or a black-smith's lodge or an urban block of multi-rise apartments? Form follows function so the function or functions must be clearly identified and understood in-depth. Secondly, form follows function so the design of the house — or the mandate's range of activities — must be completed on the basis of the function. Thirdly, the size of the building and its interior may be basic, cramped, spartan i.e. just barely enough to provide basic shelter and sanitation or else it may be more comfortable and spacious and functional or else it may be downright luxurious. Whether it is one or the other will depend on the resources and especially the finances which can be projected to be available to the builder — and these will influence the final design of the plan for the building — and the mandate. Fourthly, the time available to complete essential parts of the building will also influence the design of the plan. Fifth, it will need to be borne in mind that life gets in the way of the best-laid plans and the design may, from time to time, have to be more of an emergent design process rather than the fulfilment of a rigid, prescriptive pre-ordinate design. This analogy is useful to explaining the scope of this report especially to emphasize that while the building itself may not necessarily be capable of completion within the time-frame of one or even two three-year mandates, it is very important to decide on what the final building needs to be like, otherwise we would be unable to design the type of the foundations we require to build... and unless the foundations are sound and fit-for-purpose the building will ultimately prove to be unsustainable and collapse.

Annex II

A more in-depth look at open data and big data

1. One of the most important issues in information policy and governance in the second decade of the twenty-first century deals with determining the *medio stat virtus* between, on the one hand, use of data for the benefit of society under the principles of Open Data and, on the other hand, the established principles we have developed to date with a view to protecting fundamental rights like privacy, autonomy and the free development of one's personality.

2. At first sight Open Data sounds fine as a concept, a noble and altruistic approach to dealing with data as a common good, if not quite "common heritage of mankind". Who could object to data sets being used and re-used in order to benefit various parts of society and eventually hopefully all of humanity? It is what you can do with Open Data that is of concern, especially when you deploy the power of Big Data analytical methods on the data sets which may have been made publicly available thanks to Open Data policies. Of course, it is important to differentiate between data sets of one type and another. If what is put into the public domain consists of, say, the raw data arising out of tens of thousands of questionnaire responses about perceptions of privacy which responses would have been gleaned from across 27 EU member states and processed in an anonymised manner, the risk to individual privacy from aggregated data sets would appear to be very low if not non-existent. If, on the other hand, one uses Big Data analytical methods to develop links between supposedly anonymized medical data and publicly available electoral registers in a way that links identified or identifiable individuals to sensitive patient information then society has genuine cause for concern. Pioneers like Latanya Sweeney in the USA have demonstrated these abilities and exposed these risks on numerous occasions over the past two decades but the question remains: how should society intervene? More precisely how should policy-makers act in the face of such risks? Which is the correct information policy to develop and adopt? Especially since society has already intervened in a number of ways. Open Data is an information policy born out of specific information politics. For example, the EU legislated in favour of re-utilising public data more than 12 years ago (Directive 2003/98/EC), indeed five years after Prof Sweeney's first eye-opening discoveries.[v] Is this one of many cases where Open Data Policies were embraced before unintended consequences were properly understood and may now need to be remedied?

3. It is sometimes not widely appreciated how fundamental a challenge Open Data represents to the most important principles in data protection and privacy law world-wide. For the best part of forty years, our entire *forma mentis* has been founded upon something we call the purpose-specification principle. Put simply, personal data should be collected,

[v] "In 2000, Sweeney analyzed data from the 1990 census and revealed that, surprisingly, 87 percent of the U.S. population could be identified by just a ZIP code, date of birth, and gender" according to Caroline Perry, SEAS Communications "You're not so anonymous" October 18, 2011 last accessed on 13 Jan 2016 at http://news.harvard.edu/gazette/story/2011/10/you%E2%80%99re-not-so-anonymous/. However, in testimony to the Privacy and Integrity Advisory Committee of the Department of Homeland Security ("DHS") on 15 June 2005 Sweeney states that it was in 1997 that she "was able to show how the medical record of William Weld, the governor of Massachusetts of the time could be re-identified using only his date of birth, gender and ZIP. In fact, 87% of the population of the United States is uniquely identified by date of birth (e.g., month, day and year), gender, and their 5-digit ZIP codes. The point is that data that may look anonymous is not necessarily anonymous". http://www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_06-2005_testimony_sweeney.pdf last accessed on 13 January 2016.

used, stored and re-used for a specified legitimate purpose or for a compatible purpose. Once the time required for the data to be stored by that specified purpose runs out then the data should be deleted permanently. Re-using personal data is not part of our privacy or data protection DNA.

4. The purpose-specification principle is not something invented by Europeans. One of the first places where it is articulated as such is in a 1973 report by an Advisory Committee to the US Department of Health[w] where it was held that "There must be a way for an individual to prevent personal information used for one purpose from being used or made available for other purposes without his or her consent". This quickly became a fundamental value in many other fora. The OECD Guidelines of 1980 have the Purpose specification Principle as the third out of eight principles "The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose". In this context it is also important to note the OECD's corollary fourth principle usually recognised as the Use Limitation Principle whereby "Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with 3 above except a) with the consent of the data subject; or b) by the authority of law" These principles are also found in the Council of Europe's influential Data Protection Convention of 1981 and the EU's Data Protection Directive (46/95).

5. In an important regional development, the European Union is now at an advanced stage of devising and implementing the next generation of its data protection laws. When one examines the texts produced by the EU between 2012 and 2015, it is not as if the European Union appears ready to abandon the principle of purpose limitation. In the latest available version[x] of the draft text of the EU's General Data Protection Regulation (GDPR) the importance of the purpose specification principle does not appear to be in any way to be diminished. Article 5 b retains the principle prominently, stipulating that personal data shall be

> (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes;

an approach reinforced by the next principle to be found in the GDPR's Article 5 which lays down that personal data shall be

> (c) adequate, relevant, and limited to the minimum necessary in relation to the purposes for which they are processed; they shall only be processed if, and as long as, the purposes could not be fulfilled by processing information that does not involve personal data;

[w] DHEW Secretary's Advisory Committee on Automated Personal Data Systems, *Records, Computers and the Rights of Citizens*, U S Govt. Printing Office, Washington USA 1973 at p. 41.

[x] s_2014_2019_plmrep_AUTRES_INSTITUTIONS_COMM_COM_2015_12-17_COM_COM(2012)0011_EN.pdf.

6. The meaning of these key principles had been similarly announced in the recitals of the GDPR

> (30) Any processing of personal data should be lawful, fair and transparent in relation to the individuals concerned. In particular, the specific purposes for which the data are processed should be explicit and legitimate and determined at the time of the collection of the data. The data should be adequate, relevant and limited to the minimum necessary for the purposes for which the data are processed; this requires in particular ensuring that the data collected are not excessive and that the period for which the data are stored is limited to a strict minimum. Personal data should only be processed if the purpose of the processing could not be fulfilled by other means. Every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted. In order to ensure that the data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review.

7. It is clear therefore that the current thinking in Europe on Data Protection still relies on the purpose specification principle taken in tandem with anonymization or deletion despite all the risks inherent in the use of Big Data Analytics and Open Data. Likewise, in the United States where on May 9, 2013, President Obama signed an executive order[y] that made open and machine-readable data the new default for government information",[z] some have attempted to downplay the concerns raised by Latanya Sweeney and have generally held that the risks of de-identification are not as great as previously made out.[aa] Yet, a detailed analysis of the output of Prof Sweeney's Data Privacy Lab[bb] and some of her more recent research[cc] persuade the SRP that we are running the risk of using outmoded safeguards, almost twenty years after our attention was drawn to the fact that stripping personal data of some basic identifiers may not be enough to protect privacy.

8. A careful examination of the pivotal thinking in Europe in 2015-2016 does not provide much reassurance especially if one carefully examines the pertinent part of the latest version[dd] available of the draft EU General Data Protection Regulation which holds that

> (23) The principles of protection should apply to any information concerning an identified or identifiable person. To determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the individual. The principles of data protection should not apply to data rendered anonymous in such a way that the data subject is no longer identifiable.

[y] https://www.whitehouse.gov/the-press-office/2013/05/09/executive-order-making-open-and-machine-readable-new-default-government- last accessed on 13 Jan 2016.

[z] https://www.whitehouse.gov/open last accessed on 13 January 2016.

[aa] See for example Barth-Jones, Daniel C. "The "Re-identification" of Governor William Weld's Medical Information: A Critical Re-examination of Health Data Identification Risks and Privacy Protections, Then and Now" June 2012 last accessed on 13th January at https://fpf.org/wp-content/uploads/The-Re-identification-of-Governor-Welds-Medical-Information-Daniel-Barth-Jones.pdf.

[bb] http://dataprivacylab.org/index.html.

[cc] Sweeney L, Matching Known Patients to Health Records in Washington State Data, 2012 last accessed on 13th January 2016 at http://dataprivacylab.org/projects/wa/1089-1.pdf.

[dd] http://www.emeeting.europarl.europa.eu/committees/agenda/201512/LIBE/LIBE%282015%291217_1/sitt-1739884 last accessed on 13th January 2016.

9. This latest version from December 2015 after negotiation with the Council is less detailed than the one approved by the Parliament in October 2013 which held that

> (23) The principles of data protection should apply to any information concerning an identified or identifiable natural person. To determine whether a person is identifiable, account should be taken of all the means reasonably likely to be used either by the controller or by any other person to identify or single out the individual directly or indirectly. To ascertain whether means are reasonable likely to be used to identify the individual, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration both available technology at the time of the processing and technological development. The principles of data protection should therefore not apply to anonymous data, which is information that does not relate to an identified or identifiable natural person. This Regulation does therefore not concern the processing of such anonymous data, including for statistical and research purposes.

10. Is the change an improvement, a factor which strengthens privacy protection in the era of Open Data or Big Data or is it a compromise which weakens protection? Whereas, it seems to the SRP that the very standard formulation of October 2013,[ee] dependant as it was on the costs and time required to identify an individual, is rapidly becoming archaic in the era of big data analytics, the rather vaguer 2015 version seems to be a bit more elastic, but that could be a double-edged sword. If we are to insist on maintaining information policies built around the principles of Open Data then we need to develop much stronger, complex algorithmic solutions and procedural safeguards. The application of the newest EU proposals pivot almost entirely on what constitutes anonymous data yet Latanya Sweeney[ff] and others have clearly demonstrated that there are huge limits to anonymization and it would seem that practically most personal data may actually be identifiable with such minimal effort that they would not meet eligibility criteria to qualify as anonymous data, thus bringing the GDPR into play.

11. Things get even more complicated when taking into consideration the factors legitimising research[gg]

> (88) For the purposes of processing for historical, statistical and scientific research purposes, the legitimate expectations of society for an increase of knowledge should be taken into consideration.

12. While the issue of sensitive data such as health information still presents a quandary within the EU's GDPR

> (42) Derogating from the prohibition on processing sensitive categories of data should also be allowed if done by a law, and subject to suitable safeguards, so as to protect personal data and other fundamental rights, where grounds of public interest so justify and in particular for health purposes, including public health and social protection and the management of health-care services, especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system, or for historical, statistical and scientific research purposes.

[ee] "inofficial consolidated version" https://www.janalbrecht.eu/fileadmin/material/Dokumente/DPR-Regulation-inofficial-consolidated-LIBE.pdf last accessed on 13th January 2016.

[ff] http://latanyasweeney.org/publications.html.

[gg] Though this recital 88 has been expanded in the latest 17 Dec 2015 version.

13. How do Open Data and Big Data analytical capabilities fit into the scenarios and thinking portrayed above? Which would be the suitable safeguards to apply in Open Data policies which would protect privacy in the era of Big Data? Are the latest legal innovations being contemplated in Europe the right response to the evidence presented by Sweeney and do they represent best practice for the world to follow or dubious practice for the world to shun? The only thing that is certain is that if we are to get things right then it is clear that we need much more in-depth analysis of both the risks of Open Data as well as existing and new safeguards. Moreover, in this field too there appears to be a huge need for increasing public awareness. Relatively few people seem to know about the existence of open data policies or the consequences of applying big data analytics to different data sets put into the public domain by Open Data policies. In the course of participating in debates about Open data and Big data during tenure as SRP, one reinforced the impression that Open Data policies and their privacy and autonomy implications remain very much an area of interest to a tiny group of domain specialists and then again may be restricted further by the language in which they are made available to the public. The SRP is very sensitive to and is working with NGOs interested in protecting personal data in a number of sectors, including medical data and will, during 2016-2017 be engaging in events aimed at promoting discussion and on-going, in-depth investigation of related matters. The SRP is also very concerned that entire nations or trading blocs including major nations or regional federations such as China, the European Union and the United States have adopted or are adopting Open Data and Big Data policies the far-reaching consequences of which may not as yet be properly understood and which may unintentionally put in peril long-standing social values as well as the fundamental rights to privacy, dignity and free development of one's personality. Some studies on posthumous privacy suggest that in 2016 the citizens of some countries may be better off dead from a privacy point of view since their rights to privacy are better protected by law if they are dead than if they are alive in a world where Open data and big data analytics are a way of life endorsed by the information policies of the countries concerned. These developments may well be unintentional but the impact on privacy, autonomy, dignity and free development of personality may be far-reaching.

Annex III

Further reflections on the notion of privacy

A. Core values and cultural differences

1. As a result of the processes described in Section III of the report, an improved, more detailed understanding of privacy should be developed by the international community. This understanding should possibly result in some flexibility when it comes to addressing cultural differences at the outer fringes of the right or in privacy-neighbouring rights while clearly identifying a solid and universally valid core of what privacy means in the digital age.

2. This global concept of privacy has to pass the test of being positively describable and definable as a precious substantive right on the one hand. On the other hand there also needs to be a negative understanding of the right which hints at legitimate limitations should it be legitimate and necessary to restrict privacy in a proportionate manner. The Special Rapporteur invites all actors in the field to contribute to the development of this urgently needed and improved understanding of the right to privacy and is convinced that significant progress is possible.

B. Enforcement

3. Apart from the absence of a clear universal understanding of privacy, the lack of effective enforcement of the right is an issue which is evident at most turns of the debate. Thus, not only is it not entirely clear what needs to be protected but also how to do it. Regretfully though perhaps hitherto inevitably, the super-fast development of privacy-relevant technologies and especially the Internet has led to a huge organic growth in the way in which personal data is generated and the exponential growth in the quantity of such data. This is especially evident in an on-line environment where, when seen from a global perspective, it would appear that the triangle of actors consisting of legislators, private (mostly corporate) actors and citizens all try to shape cyberspace using their possibilities in an uncoordinated manner. This may lead to a situation where none of the three is able to unleash the full potential of modern information technology.

4. In order to disentangle this triangular relationship an ongoing and open dialogue needs to be set up which eventually would provide for a more clear and harmonious regulation of cyberspace. This can only be achieved as a result of a sincere, open and committed dialogue of all parties which is to be held in a respectful and open manner. Sturdy and reliable bridges need to be built between all actors which are shaping the developments. It is the intention of the Special Rapporteur to listen closely to all parties and to facilitate this dialogue. In this way a basis for a positive and sustainable long-term development in the field of privacy protection should be achieved.

Annexe IV

A “State of the Union” approach to privacy

It would appear to be useful to, at least once a year, have the SRP present an independent stocktaking report on where the right to privacy stands and this may be one of the primary functions of both the reports to be made to the Human Rights Council (HRC) and the General Assembly (GA). Since these reports are constrained by a word-limit it is clear that they can be little more than an extended executive summary of the findings and activities of the mandate throughout the reporting period. It should follow that the reports will also reflect the working methods of the mandate as outlined in Section II of the main report, in particular the thematic investigations as well as salient developments identified in the country monitoring activities carried out by the SRP team. It is expected that the report presented to the March 2017 session of the Human Rights Council would be the first such report reflecting a “State of the Union” approach. The report to the March 2016 session of the HRC will not attempt to prioritise risks or landmark improvements in privacy protection but simply refer to a few cases which illustrate particular progress or difficulties.