Nations Unies A/HRC/40/63

Assemblée générale

Distr. générale
16 octobre 2019
Français
Original : anglais

Conseil des droits de l'homme
Quarantième session
25 février-22 mars 2019
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

Droit à la vie privée

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

Résumé

Dans son rapport, établi en application des résolutions 28/16 et 37/2 du Conseil des droits de l'homme, le Rapporteur spécial sur le droit à la vie privée met l'accent sur les questions relatives au contrôle des services de renseignement et expose les liens avec le premier rapport de l'Équipe spéciale sur la vie privée et la personnalité qui rend compte de ses travaux concernant la vie privée et le genre et avec le rapport de l'Équipe spéciale chargée des données sur la santé.

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

GE.19-17878 (F) 061119 081119
1917878

Merci de recycler

Table des matières

I. Aperçu des activités

1. Depuis mars 2018, afin de s'acquitter de son mandat, le Rapporteur spécial sur le droit à la vie privée a mené les activités suivantes : examen des informations pertinentes, notamment des problèmes que posent les nouvelles technologies ; visites officielles et « non officielles » dans des pays ; promotion de la protection du droit à la vie privée ; défense des principes de la vie privée ; contribution à des manifestations internationales pour promouvoir une approche cohérente du droit à la vie privée ; sensibilisation au droit à la vie privée et aux recours utiles ; et signalement des violations présumées.

2. En octobre 2018, le Rapporteur spécial a présenté à l'Assemblée générale un rapport sur les mégadonnées et les données ouvertes (A/73/438).

3. Depuis son rapport annuel de 2018 au Conseil des droits de l'homme (A/HRC/37/62), le Rapporteur spécial a notamment mené les activités suivantes :

a) Faire progresser, en collaboration avec les présidents de ces organes, les travaux thématiques de cinq équipes spéciales sur les mégadonnées et les données ouvertes, les données relatives à la santé, le droit à la vie privée et la personnalité, la sécurité et la surveillance et l'utilisation de données à caractère personnel par les entreprises ;

b) Élaborer, au total, 24 communications aux États membres soulevant des questions relatives au droit à la vie privée et 14 communiqués de presse et déclarations[1] ;

c) Effectuer des visites officielles au Royaume-Uni de Grande-Bretagne et d'Irlande du Nord (en juin 2018) et en Allemagne (en novembre 2018) ;

d) Prononcer des discours liminaires ou présenter des exposés lors de manifestations internationales[2] ;

e) Consulter un certain nombre d'organismes, par exemple, l'Irish Council for Civil Liberties (Conseil irlandais pour les libertés civiles), l'Union japonaise pour les libertés civiles, la Japan Federation of Bar Associations, Privacy International et la Commission des droits de l'homme de l'Irlande du Nord, et participer à divers ateliers, notamment dans le cadre du Forum sur la gouvernance d'Internet et de la conférence RightsCon ;

f) Échanger des informations avec différents acteurs : des gouvernements (aux niveaux national et infranational), des commissaires à la protection des données et de la vie privée ; le Président du groupe de travail de l'Union européenne sur la protection des données créé par l'article 29 ; le Président du Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du Conseil de l'Europe (Convention n° 108) ; des organismes de normalisation, tels que l'Union internationale des télécommunications ; l'Institute of Electrical and Electronic Engineers ; des organisations de la société civile ; des missions permanentes auprès de l'Office des Nations Unies à Genève ; des titulaires de mandat au titre des procédures spéciales du Haut-Commissariat des Nations Unies aux droits de l'homme ; des chercheurs ; des universitaires et des organismes professionnels.

II. La protection de la vie privée dans divers contexte

4. Le droit à la vie privée peut faciliter la jouissance des autres droits de l'homme, tout comme les violations de ce droit entravent l'exercice d'autres droits de l'homme.

5. L'histoire offre plusieurs exemples d'États membres qui ont ratifié des instruments internationaux relatifs aux droits de l'homme sans avoir réellement la volonté de prendre les mesures nécessaires à leur mise en œuvre. C'est le cas de la République démocratique allemande qui, en ratifiant le Pacte international relatif aux droits civils et politiques le 8 novembre 1973, s'est notamment engagée à respecter le droit à la vie privée (art. 17),

[1] Au total, 18 lettres et 6 communiqués de presse ont été publiés conjointement avec d'autres rapporteurs spéciaux.

[2] Voir https://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2019_HRC_Annex1_Keynotes.pdf.

mais a cependant maintenu un régime de surveillance connu pour ses violations généralisées et systématiques de la vie privée d'un grand nombre de ses citoyens.

6. De nos jours, malheureusement, le Rapporteur spécial constate souvent des contradictions similaires : la plupart des États Membres s'engagent sans équivoque à protéger le droit à la vie privée mais nombre d'entre eux prennent des mesures qui menacent de plus en plus ce droit, en utilisant de nouvelles technologies, comme les mégadonnées et les données sur la santé, qui sont incompatibles avec le droit à la vie privée, en portant atteinte à la dignité de leurs citoyens au motif du genre ou de l'identité et de l'expression de genre, et en enquêtant de façon arbitraire sur leurs propres ressortissants.

7. Le droit de tous les peuples à disposer d'eux-mêmes, tel qu'il est énoncé au paragraphe 1 de l'article premier du Pacte international relatif aux droits civils et politiques, signifie la capacité pour eux de déterminer leur statut politique et d'assurer librement leur développement. De même, toutes les libertés fondamentales énoncées dans le Pacte, notamment le droit à la liberté de circulation (art. 12) ou le droit à la liberté d'association (art. 22), le droit à la liberté de religion (art. 18), le droit à la liberté d'expression (art. 19) et le droit à la vie privée (art. 17), protègent le droit de chacun à son autonomie personnelle. Le droit d'un citoyen de choisir ce qu'il veut être, quand agir, où, comment et avec qui, et de penser et s'exprimer comme il l'entend, fait partie des droits inaliénables que les pays ont convenu de protéger en vertu du Pacte.

8. Le droit à la vie privée fait partie intégrante des débats sur l'autonomie personnelle. Dès 1976, Paul Sieghart a mis en évidence les liens ci-après entre la vie privée, les flux d'information, l'autonomie et le pouvoir :

> Dans une société où les technologies modernes de l'information évoluent rapidement, bien des tiers peuvent être en mesure de découvrir comment nous nous comportons. Cette faculté peut, à son tour, réduire notre liberté d'agir comme bon nous semble, parce qu'une fois que les autres découvrent comment nous agissons, ils peuvent penser qu'il est dans leur intérêt, ou dans l'intérêt de la société, ou même dans notre propre intérêt, de nous dissuader, de nous décourager ou même de nous empêcher de faire ce que nous voulons faire, et chercher à nous manipuler pour faire ce qu'ils veulent faire[3].

9. Le Rapporteur spécial a établi le lien suivant entre ce constat et la protection de la vie privée :

> Dépourvu de la protection que lui offre le respect de la vie privée, un individu devient transparent et donc manipulable. Un individu manipulable est à la merci de ceux qui contrôlent les informations sur sa personne, et sa liberté, bien souvent relative dans le meilleur des cas, diminue de façon directement proportionnelle au rétrécissement du champ des options et alternatives que lui laissent ceux qui contrôlent les informations[4].

10. C'est la raison pour laquelle la protection de la vie privée est si étroitement liée à une autonomie personnelle digne de ce nom. L'atteinte à la vie privée fait souvent partie d'un système qui menace d'autres libertés. Elle est souvent pratiquée par des acteurs étatiques, afin de s'assurer un pouvoir et de le conserver, mais aussi par des acteurs non étatiques, tels que des individus ou des sociétés souhaitant continuer à contrôler autrui. Ainsi, dans bien des cas, le Rapporteur spécial doit examiner de quelle manière les violations du droit à la vie privée sont liées à d'autres violations.

La protection de la vie privée en tant que droit limité et le critère de nécessité dans une société démocratique

11. Le droit à la protection de la vie privée n'est pas un droit absolu mais un droit limité. Il peut être restreint, mais toujours de façon très soigneusement délimitée. Conformément à la norme établie dans l'article 17 du Pacte international relatif aux droits civils et politiques,

[3] Paul Sieghart, *Privacy and Computers* (London, Latimer New Dimensions, 1976), p. 24.

[4] Joseph A. Cannataci, *Privacy and Data Protection Law: International Development and Maltese Perspectives* (Oslo, Norwegian University Press, 1986), p. 60.

le droit international des droits de l'homme n'autorise les immixtions dans la vie privée que si elles ne sont ni arbitraires ni illégales. Dans son observation générale nº 16 (1988) sur le droit au respect de la vie privée, le Comité des droits de l'homme a expliqué que le terme « illégal » signifiait qu'il ne pouvait y avoir d'immixtion que dans les cas envisagés par la loi, et que la loi devait elle-même être conforme aux dispositions, aux buts et aux objectifs du Pacte. Quant à la notion d'arbitraire, elle avait pour objet, selon le Comité, de garantir que même une immixtion prévue par la loi soit conforme aux dispositions, aux buts et aux objectifs du Pacte et soit, dans tous les cas, raisonnable eu égard aux circonstances particulières.

12. Dans son observation générale nº 31 (2004) sur la nature de l'obligation juridique générale imposée aux États parties au Pacte, le Comité des droits de l'homme précise que les États parties doivent s'abstenir de violer les droits reconnus par le Pacte et que toute restriction à leur exercice doit être autorisée par les dispositions pertinentes du Pacte. Dans les cas où des restrictions sont formulées, les États doivent en démontrer la nécessité et ne prendre que des mesures proportionnées aux objectifs légitimes poursuivis afin d'assurer une protection véritable et continue des droits énoncés dans le Pacte. Le Comité souligne en outre que de telles restrictions ne peuvent en aucun cas être appliquées ou invoquées d'une manière qui porterait atteinte à l'essence même d'un droit énoncé dans le Pacte.

13. L'expression « nécessaires dans une société démocratique » est explicitement mentionnée dans deux articles du Pacte international relatif aux droits civils et politiques : l'article 21 (droit de réunion pacifique) et l'article 22 (liberté d'association), mais pas dans l'article 17.

14. Le paragraphe 2 de l'article 8 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales (Convention européenne des droits de l'homme) est explicite quant à la nature de la limitation :

> Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui.

15. La démocratie a été considérée comme faisant partie du contexte essentiel à la jouissance des droits de l'homme dans la Déclaration universelle des droits de l'homme de 1948, où la notion de « bien-être général dans une société démocratique » figurait à l'article 29. L'interaction entre les auteurs et les signataires de la Convention européenne des droits de l'homme, adoptée en 1950, et les auteurs du Pacte international relatif aux droits civils et politiques s'est poursuivie pendant près de quinze ans, jusqu'à l'adoption du Pacte en 1966. L'expression « nécessaire dans une société démocratique » figure dans au moins six articles de la Convention européenne, dont l'article 8 précité, et apparaît transposée dans le Pacte, le meilleur exemple étant le paragraphe 1 de l'article 22 :

> L'exercice de ce droit ne peut faire l'objet que des seules restrictions prévues par la loi et qui sont nécessaires dans une société démocratique, dans l'intérêt de la sécurité nationale, de la sûreté publique, de l'ordre public, ou pour protéger la santé ou la moralité publiques ou les droits et les libertés d'autrui.

16. Cependant, l'article 22 porte sur la liberté de réunion et non sur le droit à la vie privée. Il appartient aux historiens qui étudient la genèse de la Déclaration universelle des droits de l'homme et du Pacte international relatif aux droits civils et politiques d'expliquer pourquoi l'expression « nécessaire dans une société démocratique » est explicite dans les articles 21 et 22 et non dans l'article 17. Cependant, le Rapporteur spécial est raisonnablement tenu d'appliquer la même norme, à savoir que le droit ne peut être limité que par des mesures prévues par la loi (par. 2 de l'article 17) et que ces mesures doivent être nécessaires dans une société démocratique, lorsqu'il s'agit d'interpréter les termes « immixtions arbitraires ou illégales », conformément aux articles 14, 21 et 22 du Pacte.

17. Cette interprétation est conforme au paragraphe 2 de la résolution 34/7 du Conseil des droits de l'homme, dans laquelle le Conseil réaffirme que les États devraient veiller à ce que toute immixtion dans la vie privée soit conforme aux principes de légalité, de nécessité et de proportionnalité, en accord avec les termes utilisés dans la jurisprudence du Comité des droits de l'homme (CCPR/C/USA/CO/4, par. 22).

18. Ainsi, le quadruple critère essentiel est que toute immixtion légitime dans la vie privée : a) ne peut être arbitraire et doit être prévue par la loi ; b) ne peut viser qu'un but nécessaire dans une société démocratique ; c) ne peut être envisagée à d'autres fins que pour servir « l'intérêt de la sécurité nationale, de la sûreté publique, de l'ordre public, ou pour protéger la santé ou la moralité publiques ou les droits et les libertés d'autrui » ; et d) doit être proportionnée à la menace ou au risque à gérer.

19. Le double critère de « nécessité » et de « nécessité dans une société démocratique » est essentiel concernant toute mesure prise par un État membre qui pourrait être considérée comme une atteinte à la vie privée. Il doit également être pris en compte lors de l'examen des atteintes à d'autres droits dont l'exercice dépend du droit à la vie privée.

20. Le contexte du droit à la vie privée, ainsi que les liens entre l'autonomie, la vie privée et les mesures nécessaires dans un État démocratique expliquent pourquoi le Rapporteur spécial accorde la priorité aux États dotés d'institutions et de garanties démocratiques solides, car c'est dans ces contextes que son intervention est la plus susceptible d'avoir un impact positif sur l'exercice du droit à la vie privée. Dans les pays où les garanties démocratiques sont plus fragiles, il s'efforce de déceler des possibilités d'intervenir de façon constructive.

21. En 2019 et 2020, le Rapporteur spécial mettra davantage l'accent sur l'Afrique, l'Asie et l'Amérique du Sud et a prévu d'effectuer une visite dans chacune de ces régions. Il continuera néanmoins de suivre la situation dans d'autres pays, notamment avec le concours de la société civile. Cette démarche ne traduit pas une insensibilité à l'égard du droit à la vie privée dans d'autres régions du monde. Le Rapporteur spécial n'est pas en mesure d'enquêter sur le respect de ce droit de façon aussi détaillée ou selon la méthode qu'il souhaiterait, et ce, en raison des limitations dues à trois facteurs : le temps, les ressources et la possibilité de mener des enquêtes sérieuses sur le terrain. Le Rapporteur spécial continuera donc de surveiller les États où le « gouvernement par la loi » remplace la primauté du droit et où le droit devient un instrument de contrôle et d'oppression du régime. Dans la région du Moyen-Orient et de l'Afrique du Nord, il examinera l'élaboration d'une législation sur la cybercriminalité qui pourrait présenter un risque pour l'exercice du droit à la vie privée[5].

Protection de la vie privée, outils technologiques et autres droits fondamentaux liés aux questions de genre

22. Le présent rapport rend compte des premiers résultats des travaux actuellement menés par le Rapporteur spécial concernant la protection de la vie privée et la prise en compte des questions de genre. L'Équipe spéciale sur la vie privée et la personnalité poursuivra ses travaux sur le lien entre la vie privée et l'égalité des genres, quel que soit le genre ou l' expression du genre. En plus des consultations sur le rapport[6], le Rapporteur spécial prévoit d'accorder davantage d'attention à ce domaine au cours des trois prochaines années, notamment aux liens entre la vie privée, l'autonomie et le système de tutelle masculine présent à des degrés divers dans un certain nombre de pays.

23. Les États membres qui souhaitent participer aux consultations sur la protection de la vie privée et la prise en compte des questions de genre sont priés de faire part de leur intérêt avant le 31 mars 2019.

[5] Wafa Ben-Hassine et Dima Samaro, "Restricting cybersecurity, violating human rights: cybercrime laws in MENA region", Open Global Rights, 10 janvier 2019.

[6] Voir https://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2019_HRC_Annex2_GenderReport.pdf.

Protection de la vie privée et données sur la santé

24. Le présent rapport fournit également des précisions sur les travaux que le Rapporteur spécial poursuit concernant la protection de la vie privée et les données sur la santé. Comme dans ses travaux sur la prise en compte des questions de genre, il aborde des thèmes importants qui se font jour, notamment la génétique, la recherche sur le génome et la mise en banque de matériel biologique. L'une des questions soumises à l'examen du Rapporteur spécial est celle de savoir s'il est nécessaire et proportionné de collecter les données génétiques de toute la population d'un pays donné. Il incombera au Rapporteur spécial de nouer un dialogue à ce propos avec les États qui envisagent de légiférer sur ces questions.

25. L'Équipe spéciale chargée des données sur la santé a mis en évidence un certain nombre de questions concernant notamment la souveraineté sur les données locales, les populations carcérales, les bases de données médico-légales, les dispositifs médicaux « intelligents » implantés et les dispositifs ou prothèses qui transmettent en continu des données réelles aux entreprises, notamment, faisant ainsi du corps humain un ensemble de données susceptibles d'être utilisées dans des procédures juridiques, ou encore les processus d'intelligence artificielle ou d'apprentissage automatique et les traitements automatisés. Ces questions feront l'objet de consultations en 2019.

III. Sécurité et surveillance

26. Le mandat du Rapporteur spécial a été créé à la suite du tollé international suscité par les révélations d'Edward Snowden sur les activités des services de renseignement, notamment en ce qui concerne la protection de la sécurité nationale.

27. Afin de renforcer la protection de la vie privée dans le domaine du renseignement, le Rapporteur spécial a créé le Forum international de contrôle des services de renseignement, qui a tenu des conférences à Bucarest en 2016, à Bruxelles en 2017 et à La Valette en 2018. À la suite de la conférence de 2018, le Rapporteur spécial fait part des éléments suivants :

a) Les initiatives régionales récentes telles que le Règlement général de l'Union européenne relatif à la protection des données[7] (entré en vigueur le 25 mai 2018) et la directive sur le même sujet[8] (entrée en vigueur le 6 mai 2018) sont importantes mais insuffisantes pour étendre la protection de la vie privée au domaine de la sécurité nationale, notamment au contrôle des activités de renseignement menées à des fins de sécurité nationale[9] ;

b) La modernisation de la Convention 108[10], une récente initiative mondiale officiellement lancée le 10 octobre 2018, à laquelle 70 des 193 États Membres de l'Organisation des Nations Unies (ONU) ont participé, est saluée pour son article 11, lequel contient un ensemble de principes et de garanties de haut niveau qui, contrairement au Règlement général relatif à la protection des données, sont également applicables aux activités menées à des fins de sécurité nationale.

28. Dans son rapport de 2018 à l'Assemblée générale (A/73/438), le Rapporteur spécial a recommandé d'encourager tous les États Membres à ratifier la Convention modernisée (Convention 108+). S'agissant du contrôle des services de renseignement et des activités liées à la sécurité nationale susceptibles de porter atteinte à la vie privée, la mise en place immédiate par les États Membres de l'ONU des normes et garanties énoncées à l'article 11 de la Convention 108+ est appropriée pour protéger le droit fondamental à la vie privée.

[7] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016.

[8] Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016.

[9] L'Union européenne n'a pas compétence dans le domaine de la sécurité nationale et ne peut donc pas étendre comme il convient la protection de la vie privée aux activités menées dans ce domaine, notamment le contrôle des activités de renseignement à des fins de sécurité nationale.

[10] Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel.

29. Ces garanties et normes essentielles, en particulier celles de proportionnalité et de nécessité, ont inspiré le raisonnement suivi dans deux arrêts historiques de la Cour européenne des droits de l'homme en 2018, tous deux étroitement liés aux activités des services de renseignement : *Centrum för Rättvisa c. Suède* (19 juin 2018) et *Big Brother Watch et autres c. Royaume-Uni* (13 septembre 2018).

30. Compte tenu du nombre élevé de membres du Conseil de l'Europe, soit 47 États, et de la portée mondiale des services de renseignement de cette région, ces arrêts sont susceptibles d'avoir une incidence à l'échelle mondiale.

31. Le Rapporteur spécial est favorable à l'application stricte des critères de proportionnalité et de nécessité dans une société démocratique, car elle constitue une référence importante ayant des répercussions mondiales. Les services de renseignement d'autres régions sont susceptibles d'être influencés par les normes de plus en plus strictes appliquées en Europe. Par conséquent, il importe de soumettre l'analyse de renseignements contenant des informations personnelles et d'autres données à caractère personnel transférées depuis et vers l'Europe à un contrôle strict, afin de garantir l'application, en Europe, de ces normes respectueuses de la vie privée et de proposer ainsi un modèle et des bonnes pratiques transposables dans le monde entier.

32. Il est important de noter que l'expression « une société démocratique » est un élément fondamental des critères d'évaluation des protections juridiques accordées dans tout État Membre de l'ONU. Un certain nombre de nouvelles technologies, en particulier Internet, les smartphones, l'analyse de mégadonnées, les accessoires intelligents, l'énergie intelligente et les villes intelligentes, exposent davantage les individus et les collectivités à la surveillance par des entreprises ou des organismes publics dans leur pays, ainsi que par des services de renseignement et des entreprises d'États étrangers.

33. La possibilité que les États utilisent les nouvelles technologies de cette manière constitue un risque important pour la vie privée et pour d'autres droits de l'homme, comme la liberté d'expression, la liberté d'association et la liberté de religion ou de conviction. Les effets distincts et cumulés de ces technologies donnent aux États la capacité de surveiller de près le comportement des individus et d'établir des profils, selon des méthodes nouvelles et avec une ampleur sans précédent.

34. Ces technologies peuvent être exploitées pour porter atteinte aux droits de l'homme et à la démocratie. La démocratie est peut-être un mécanisme imparfait mais, historiquement, elle a fourni le meilleur écosystème possible pour protéger les droits de l'homme. Par conséquent, les effets sur la démocratie constituent un repère essentiel qui doit être pris en compte pour évaluer les mesures intrusives portant atteinte à la vie privée.

35. Le Rapporteur spécial continuera de s'acquitter de son mandat mondial en coopération avec tous les États Membres, même s'il est conscient que cette coopération a plus de chances de donner des résultats et, en définitive, de contribuer au respect du droit à la vie privée dans les pays qui bénéficient d'institutions démocratiques et de garanties solides.

36. Tout au long de l'année 2018, l'une des principales préoccupations a été de savoir ce qu'il advenait de l'analyse de renseignements contenant des données personnelles une fois que le service de renseignement ou les services de répression d'un pays la transmettaient aux services correspondants d'un autre pays. Les données, et donc la vie privée des personnes concernées, sont-elles protégées par les mêmes normes dans l'État destinataire et dans l'État qui transmet ? L'importance de ce point impose d'appliquer les mesures recommandées.

37. Le 14 novembre 2018, cinq organes de contrôle de la Belgique, du Danemark, de la Norvège, des Pays-Bas et de la Suisse, tous parties à la Convention 108 et donc liés par ses dispositions imposant des contraintes sur l'utilisation de données personnelles à des fins de sécurité nationale, ont publié une déclaration commune sur une lacune potentielle en matière de contrôle et sur les moyens de limiter le risque correspondant lors de la surveillance des échanges internationaux de données entre les services de renseignement et

de sécurité[11]. Il s'agit là d'une évolution importante et bienvenue à porter à l'attention de la communauté internationale.

38. Les participants au Forum international de contrôle des services de renseignement de 2018 ont estimé que cette initiative constituait une évolution importante, en parallèle de la création du Five Eyes Intelligence Oversight and Review Council, le Conseil d'examen et de contrôle regroupant les services de renseignement des pays membres de l'alliance Five Eyes (Australie, Canada, États-Unis, Nouvelle-Zélande et Royaume-Uni). Le Rapporteur spécial se félicite de la création de ce Conseil et des activités qu'il mène, en particulier compte tenu de la situation géographique et de la portée mondiale des cinq États qui composent l'alliance. Depuis 2013, chacun de ces États a introduit une réforme législative en vue de renforcer le contrôle et les mesures de protection de la vie privée dans le domaine des activités de renseignement à des fins de sécurité nationale et dans d'autres secteurs. Les réformes menées par certains de ces États ont été plus complètes que d'autres. À titre d'exemple, le titulaire du mandat a estimé que s'agissant de la protection de la vie privée, les dernières dispositions adoptées en Australie étaient préoccupantes[12].

39. Dans une déclaration[13], le United Kingdom Investigatory Powers Commissioner's Office (Bureau du commissaire chargé des pouvoirs d'enquête du Royaume-Uni) a accueilli avec satisfaction la déclaration des organismes de surveillance de la Belgique, du Danemark, de la Norvège, des Pays-Bas et de la Suisse. Le Bureau a le potentiel, et peut-être même une responsabilité particulière inhérente à sa situation géographique, pour faire le lien entre les organismes de contrôle de l'Europe continentale et ceux qui collaborent au sein du Conseil de l'alliance Five Eyes.

40. Le Rapporteur spécial favorisera et appuiera cette initiative, ainsi que d'autres, dans la mesure où elles aboutissent à l'intégration de normes et de garanties internationales relatives aux droits de l'homme concernant l'échange de données personnelles entre les services de renseignement et les services de répression d'un pays à l'autre.

41. Le contrôle des services de renseignement a été le thème principal de la contribution du Rapporteur lors de la procédure d'examen, par le Comité européen de la protection des données, de l'adéquation de la législation nationale du Japon et des garanties qu'elle comporte. Lors du débat, l'examen des observations et preuves présentées par le Rapporteur spécial a abouti au refus[14], le 5 décembre 2018, de conclure pour le moment que le cadre juridique japonais offrait une telle adéquation.

42. En septembre 2018, la Cour européenne des droits de l'homme a conclu que le régime d'interception en masse du Royaume-Uni violait l'article 8 de la Convention européenne des droits de l'homme (droit au respect de la vie privée et familiale et de la correspondance), en raison d'un contrôle insuffisant de la sélection des canaux de transmission Internet à intercepter et du filtrage, de la recherche et de la sélection des communications interceptées à examiner, ainsi que de garanties insuffisantes pour la sélection des « données de communication associées » à examiner[15] :

a) La Cour a considéré que le régime d'obtention de données de communication auprès des fournisseurs de services de communication enfreignait l'article 8 de la Convention et que les régimes d'interception en masse et d'obtention de données de communications auprès des fournisseurs de services de communication enfreignaient l'article 10 de la Convention en raison de l'insuffisance de garanties concernant les éléments journalistiques confidentiels ;

[11] Voir https://english.ctivd.nl/documents/publications/2018/11/14/index.

[12] Communication du Rapporteur spécial à l'Australian Joint Parliamentary Committee Intelligence and Security (commission parlementaire mixte australienne sur le renseignement et la sécurité), n° 81. 2018, disponible à l'adresse https://www.aph.gov.au/Parliamentary_Business/Committees/%20Joint/Intelligence_and_Security/TelcoAmendmentBill2018/Report_1/section?id=committees%2freportjnt%2f024247%2f26914.

[13] Voir http://www.ipco.org.uk/docs/IPCO%20Statement%20re%205%20oversight%20bodies.docx.

[14] Voir https://edpb.europa.eu/news/news_fr.

[15] Cour européenne des droits de l'homme (première section), *Big Brother Watch et autres c. Royaume-Uni*, requêtes nos 58170/13, 62322/14 et 24960/15, arrêt du 13 septembre 2018.

b) La Cour a également conclu que le régime d'échange de renseignements avec les gouvernements étrangers n'était contraire ni à l'article 8 ni à l'article 10 de la Convention.

43. Bien que cet arrêt concerne le précédent cadre de surveillance réglementaire du Royaume-Uni, ses conclusions sont très importantes et sont portées à l'attention des États membres afin qu'ils réexaminent leurs propres cadres et pratiques.

44. Cette évolution souligne l'importance de disposer de garanties précises et efficaces, tant juridiques que procédurales, dans la législation nationale et dans les pratiques des services de renseignement et de leurs autorités de contrôle.

45. Lors de la visite officielle du Rapporteur spécial en Allemagne, en novembre 2018, les bonnes pratiques dans l'exercice des pouvoirs de surveillance massive ont fait l'objet d'un débat, puis d'un recueil élaboré par la Stiftung Neue Verantwortung[16] (novembre 2018). Il est recommandé aux États d'étudier ce recueil.

Recommandations

46. Le Rapporteur spécial recommande les mesures suivantes :

a) L'incorporation par les États membres dans leurs juridictions nationales des normes et garanties énoncées à l'article 11 de la Convention 108+ pour la protection du droit fondamental à la vie privée, en particulier par les initiatives suivantes :

i) Créer la sécurité juridique en garantissant que toutes les mesures portant atteinte à la vie privée, y compris aux fins de la sécurité nationale, de la défense et de la sûreté publique, ainsi que de la prévention, des enquêtes et des poursuites en matière de criminalité, sont prévues par des lois qui font l'objet de consultations publiques et d'un contrôle parlementaire appropriés ;

ii) Faire de l'impératif d'une « mesure nécessaire et proportionnée dans une société démocratique » le critère clef, à appliquer par les unités internes chargées de la mise en œuvre au sein des services de renseignement et des services de répression à toute mesure qui porte atteinte à la vie privée, et au regard duquel les activités de ces organismes seront évaluées par les autorités de contrôle indépendantes et lesdits organismes devront répondre de leurs actes devant les tribunaux de la juridiction compétente ;

iii) Mettre en place une ou plusieurs autorités de contrôle indépendantes habilitées par la loi et dotées par l'État de ressources suffisantes pour procéder à un examen efficace de toute activité portant atteinte à la vie privée menée par les services de renseignement et les services de répression ;

b) L'adoption du principe « s'il est échangeable, alors il est contrôlable »[17] concernant tout renseignement personnel échangé entre les services de renseignement et les services de répression à l'intérieur d'un pays et au-delà des frontières :

i) Tous les États membres devraient modifier leur législation afin d'habiliter précisément et explicitement leurs autorités indépendantes chargées du contrôle des

[16] Voir https://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2019_HRC_Annex5_CompendiumBulkSurveillance.pdf.

[17] Les services de renseignement situés dans différents États échangent régulièrement des données à caractère personnel, mais celles-ci ne sont pas nécessairement soumises à la surveillance des organismes de contrôle indépendants situés soit dans l'État expéditeur soit dans l'État destinataire. En outre, certaines législations empêchent, de fait, un tel contrôle ou même une consultation à ce sujet entre les autorités de contrôle indépendantes de l'État expéditeur et de l'État destinataire. Les États sont encouragés à modifier leur législation pour habiliter leurs autorités de contrôle indépendantes à consulter d'autres autorités de contrôle indépendantes dans d'autres États et à assurer un suivi de tous les cas de données échangées avec un autre État, qu'elles se trouvent dans l'État destinataire ou dans l'État expéditeur, notamment les données personnelles brutes non traitées ou celles qui figurent dans des analyses classées par produit de renseignement. Les services de renseignement et les services de répression échangent les deux catégories de données à caractère personnel et ces deux services devraient faire l'objet d'un contrôle indépendant tant dans l'État expéditeur que dans l'État destinataire.

services de renseignement à surveiller toutes les informations personnelles échangées entre les services de renseignement des pays qui relèvent de leur compétence ;

ii) Chaque fois que cela est possible et approprié, les autorités de contrôle indépendantes des États expéditeurs et des États destinataires devraient avoir un accès immédiat et automatique aux données à caractère personnel échangées entre les services de renseignement ou les services de répression de leurs États respectifs ;

iii) Tous les États membres devraient modifier leur législation afin d'habiliter spécifiquement leurs autorités nationales et étatiques de contrôle des services de renseignement à partager des informations, à se concerter et à débattre des meilleures pratiques de surveillance avec les autorités de contrôle des États auxquels des données personnelles ont été transmises ou qui ont échangé de telles données par l'intermédiaire de leurs services de renseignement respectifs ;

iv) Lorsqu'un service de renseignement transmet à un État tiers ou à un groupe d'États tiers une analyse contenant des informations personnelles ou d'autres formes de données personnelles reçues d'un autre État, cet échange devrait être soumis à l'examen des autorités de contrôle du renseignement de ces États.

47. Lorsque les autorités compétentes des États membres envisagent d'utiliser des pouvoirs de surveillance massive, elles devraient d'abord examiner, puis hiérarchiser et adopter, dans toute la mesure possible, les mesures visant à introduire les bonnes pratiques recommandées dans le recueil de la Stiftung Neue Verantwortung[18], en plus d'appliquer les critères de mise en place et les garanties adoptés par la Cour européenne des droits de l'homme dans l'affaire *Big Brother Watch et autres* en septembre 2018.

IV. Droit à la vie privée : prise en compte des questions de genre

48. Le Conseil des droits de l'homme, dans sa résolution 34/7, et l'Assemblée générale, dans sa résolution 71/199, ont demandé aux États de « renforcer ou de maintenir les mesures préventives et les voies de recours existant contre les violations du droit à la vie privée à l'ère du numérique et les atteintes à ce droit pouvant toucher toutes les personnes, notamment lorsqu'elles ont des conséquences particulières sur les femmes, les enfants, les personnes vulnérables ou les groupes marginalisés ».

49. En 1994, dans l'affaire *Toonen c. Australie*, le Comité des droits de l'homme a conclu à une violation du droit à la vie privée du fait que des relations homosexuelles consenties entre adultes avaient été érigées en infraction. En 2017, le Comité a réaffirmé que le droit à la vie privée englobait la notion d'identité de genre (CCPR/C/119/D/2172/2012, par. 7.2).

50. Bien qu'il ne s'agisse pas d'un droit inaliénable, le droit à la vie privée est essentiel pour garantir le libre développement de la personnalité et de l'identité de chacun. Ce droit découle de la dignité intrinsèque de chacun tout en la conditionnant, en plus de favoriser l'exercice et la jouissance des autres droits de l'homme[19]. En outre, il ne se limite pas à la sphère publique.

51. Le droit à la vie privée, condition indispensable à la protection de valeurs fondamentales telles que la liberté, la dignité, l'égalité et le droit de ne pas subir l'ingérence de l'État, est un élément essentiel de toute société démocratique, et il importe de le protéger

[18] Thorsten Wetzling et Kilian Vieth, *Upping the Ante on Bulk Surveillance: An International Compendium of Good Legal Safeguards and Oversight Innovations*, Publication Series on Democracy, vol. 50 (Berlin, Heinrich Böll Stiftung, 2018).

[19] L'Assemblée générale, le Haut-Commissaire des Nations Unies aux droits de l'homme et les titulaires de mandat au titre des procédures spéciales ont reconnu que le respect de la vie privée était une passerelle vers l'exercice d'autres droits. Voir la résolution 68/167 de l'Assemblée générale, A/HRC/13/37 et la résolution 20/8 du Conseil des droits de l'homme.

comme il se doit[20]. Le Conseil des droits de l'homme a adopté des résolutions qui faisaient ressortir les liens d'interdépendance entre démocratie et droits de l'homme et la façon dont ils se renforçaient mutuellement[21].

52. Le Rapporteur spécial prend en compte les questions de genre dans toutes les activités relevant de son mandat[22]. À l'issue de trois consultations régionales fructueuses sur la vie privée, la personnalité et la circulation de l'information, une consultation en ligne a été organisée autour des questions de genre à l'ère du numérique et de leurs incidences sur les femmes, les hommes et les personnes de diverses orientations sexuelles, identités de genre, expressions du genre et caractéristiques sexuelles.

53. Le premier rapport complet de la ligne d'action thématique sur la vie privée et la personnalité regroupe un ensemble d'informations[23] reçues par le Rapporteur spécial, ainsi que des travaux de recherche subsidiaires. Exception faite des recommandations, cet ensemble d'informations ne reflète pas nécessairement les vues de son auteur principal, Elizabeth Coombs, présidente de l'Équipe spéciale sur la vie privée et la personnalité, ni celles du Rapporteur spécial.

Ligne d'action thématique sur la vie privée et la personnalité

54. Les communications reçues par le Rapporteur spécial à ce propos préconisaient de conduire une analyse transversale axée sur les forces économiques, la classe sociale, la religion, la race et le genre pour recenser les domaines méritant examen en dehors du courant dominant[24] et prendre acte des liens d'interdépendance entre droit à la vie privée et démocratie[25].

55. On a indiqué que le rapport des individus aux technologies numériques et à la protection de la vie privée était influencé par leur genre, et par des facteurs tels que l'appartenance ethnique, la culture, la race, l'âge, l'origine sociale, la richesse, l'autonomie économique, l'éducation et les cadres juridiques et politiques[26]. Le droit à la vie privée revêtait une importance particulière pour ceux qui devaient faire face aux inégalités, à la discrimination ou à la marginalisation en raison de leur genre, de leur orientation sexuelle, de leur identité de genre, de leurs caractéristiques sexuelles ou de l'expression de celles-ci. Internet, du fait de sa portée et de l'anonymat relatif qu'il permet, a offert aux lesbiennes, aux gays, aux bisexuels, aux transgenres, aux queers et aux intersexes (LGBTQI) de nouvelles possibilités d'interaction et d'entraide.

56. Il ressortait des informations communiquées que les technologies numériques avaient des incidences non négligeables sur la vie privée en ce qu'elles amplifiaient les expériences vécues en dehors du monde numérique. On indiquait que les avantages liés aux technologies numériques n'étaient pas les mêmes pour tous, et ce en raison d'inégalités structurelles et de normes de genre discriminatoires pesant lourdement sur les femmes, les personnes non binaires et non cisnormatives, les pauvres et les communautés religieuses ou culturelles minoritaires. Les nouvelles technologies permettent la misogynie en ligne[27] et,

[20] Daniel Therrien, Commissaire canadien à la protection de la vie privée, Mémoire à l'intention d'Innovation, Sciences et Développement économique Canada, consultations nationales sur le numérique et les données, 23 novembre 2018.

[21] Résolutions 19/36 et 28/14 sur les droits de l'homme, la démocratie et l'état de droit.

[22] Voir https://www.ohchr.org/FR/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx.

[23] Voir https://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2019_HRC_Annex2_GenderReport.pdf.

[24] Par exemple, les informations communiquées par l'Association pour le progrès des communications en 2018.

[25] Par exemple, les informations communiquées par le Commissaire canadien à la protection de la vie privée en 2018.

[26] Phoenix Strategic Perspectives, « Sondage auprès des Canadiens sur la protection de la vie privée de 2016 », rapport final établi pour le Commissariat à la protection de la vie privée du Canada, décembre 2016.

[27] West Coast Women's Legal Education and Action Fund (West Coast LEAF), *#CyberMisogyny : Using and Strengthening Canadian Legal Responses to Gendered Hate and Harassment Online* (Vancouver, 2014).

de manière générale, la violence en ligne contre des personnes de genre non binaire[28], agissements qui ont une portée, notamment dans le temps, et des incidences infiniment plus grandes qu'auparavant.

57. Dans les communications reçues, on soutenait vivement qu'il pouvait en être autrement, et que la technologie numérique pouvait être vecteur d'égalité dans l'exercice du droit à la vie privée.

58. On prenait acte, dans ces communications, des avantages que présentaient les dispositifs intelligents, les applications, les moteurs de recherche et les réseaux sociaux, sans pour autant ignorer leur capacité de porter atteinte à la vie privée des utilisateurs sur la base de leur genre. Les jeunes LGBTQI, par exemple, utilisaient Internet plus souvent que les jeunes qui ne l'étaient pas pour fréquenter les réseaux sociaux et faire du réseautage mais couraient également plus de risques que ces derniers d'être victimes d'intimidation ou de harcèlement en ligne (42 % contre 15 %)[29].

59. Malgré les avantages des technologies numériques[30], les personnes perçues comme étant les plus exposées étaient les femmes, les filles, les enfants et les personnes et communautés LGBTQI[31], en particulier les personnes transgenres, les militants, les enseignants homosexuels, les défenseurs des droits de l'homme, les travailleurs du sexe et les femmes journalistes.

60. Les personnes LGBTQI peuvent également être exposées à des risques particuliers, tels que l'« outing » et à des violations directement liées à leur identité de genre[32].

61. On a établi au Canada que les réseaux sociaux, tout en offrant aux femmes et aux filles la possibilité de nouer des liens sociaux, amplifiaient les normes sociales en intensifiant la surveillance commerciale, ce qui contribuait à renforcer les normes existantes et à accroître la surveillance exercée par les membres de la famille et les pairs[33].

62. De faux comptes sur des applications de rencontre LGBTI et d'autres médias sociaux auraient été utilisés par des acteurs étatiques et non étatiques pour piéger des homosexuels et les arrêter ou les soumettre à des traitements cruels et dégradants, ou à du chantage[34].

63. Il a été signalé que des médias, y compris de nouveaux médias, publiaient les données personnelles de personnes LGBTQI et de défenseurs des droits de la personne, ce qui compromettait leur sécurité[35].

64. Internet permet non seulement de créer des récits contemporains, mais aussi de perpétuer des récits datant de l'ère prénumérique, en plus d'ouvrir la voie à d'autres atteintes à la vie privée du même ordre[36].

---

[28] Informations communiquées par la Eastern European Coalition for LGBT+ Equality, "Gender perspectives on privacy in Eastern partnership countries and Russia" en 2018 ; voir également https://www.ucl.ac.uk/steapp/research/digital-technologies-policy-laboratory/gender-and-iot.

[29] David Brian Holt, "LGBTIQ teens - plugged in and unfiltered: how Internet filtering impairs construction of online communities, identity formation, and access to health information", 2009.

[30] Informations communiquées (par une source dont le nom n'a pas été révélé) en 2018, citant Valerie Horres, "Online and enabled: ways the Internet benefits and empowers women", *Interface: The Journal of Education, Community and Values*, vol. 10, nº 4 (2010).

[31] Informations communiquées en 2018 par l'Initiative féministe kazakh « Feminita », l'Office for the Defense of Rights and Intersectionality, "Stimul" LGBT Group and Transgender Legal Defense Project (Russie), Richard Lusimbo, MPact Global Action for Gay Men's Health and Rights, Transgender Europe, Federatie van Nederlandse Verenigingen tot Integratie Van Homoseksualiteit et l'Association internationale des personnes lesbiennes, gays, bisexuelles, trans et intersexe.

[32] Eastern European Coalition for LGBT+ Equality, Gender Perspectives on Privacy in Eastern Partnership Countries and Russia.

[33] Valerie Steeves et Jane Bailey, "Living in the mirror: understanding young women's experiences with online social networking", dans Emily van de Muelen et Robert Heynen, éd., *Expanding the Gaze: Gender and the Politics of Surveillance* (Toronto, University of Toronto Press, 2016). Voir également https://egirlsproject.ca/ et http://www.equalityproject.ca/.

[34] Informations communiquées par l'Initiative féministe kazakhe « Feminita » en 2018.

[35] Ibid.

65. Certaines communications portaient sur la reconnaissance de l'identité de genre, de l'autonomie et de l'intégrité corporelle et sur l'expression de celles-ci et faisaient état de préoccupations quant à une gestion inadéquate de la vie privée lors de la procédure de changement de nom et de sexe sur les documents d'identité[37]. Des activités ordinaires et quotidiennes supposant de présenter des documents d'identité − voyages, opérations bancaires ou rendez-vous médicaux, par exemple − sont souvent synonymes, pour les personnes transgenres, d'intrusions dans la vie privée profondément embarrassantes et pénibles que les personnes de genre binaire ne connaissent pas.

66. La Cour européenne des droits de l'homme a jugé que des États avaient violé l'article 8 de la Convention européenne des droits de l'homme en instaurant des procédures de reconnaissance du genre qui portaient atteinte au droit à la vie privée des personnes transgenres[38].

67. La disponibilité en ligne de registres publics, d'avis judiciaires et de décisions concernant l'identité de genre suscitait des préoccupations quant à la protection de la vie privée, en particulier compte tenu des mégadonnées et de la capacité des moteurs de recherche[39].

68. Dès leur naissance, les personnes intersexes peuvent être victimes d'ingérences dans leur vie privée, notamment lorsqu'elles font l'objet d'une procédure chirurgicale de réassignation sexuelle ou qu'elles reçoivent des traitements hormonaux destinés à leur assigner l'un ou l'autre sexe. La chirurgie visant à « faire entrer dans la norme » les nourrissons intersexes peut avoir des incidences préjudiciables sur les droits de la personne, y compris sur le droit à la vie privée, car elle porte atteinte au droit à l'autonomie personnelle et à la liberté de choix face aux traitements médicaux. D'après les informations communiquées, les pays réagiraient de diverses façons à cette question[40].

69. Les communications, y compris la communication de la Rapporteuse spéciale sur la violence contre les femmes, mentionnaient l'ensemble croissant de recherches sur la violence numérique fondée sur le genre menées au plan international, régional et national.

70. La technologie numérique et les dispositifs intelligents offrent des moyens presque illimités de harceler et de contrôler les autres[41]. La violence facilitée par la technologie fait intervenir les problématiques de l'inégalité entre les sexes, de la violence sexualisée, de la réglementation d'Internet, de l'anonymat sur Internet et du respect de la vie privée (voir A/HRC/38/47).

71. Le phénomène des abus liés aux images ou de la vengeance pornographique − le partage d'images et de vidéos privées à caractère sexuel sans le consentement de la personne concernée dans le but de causer du tort − est largement connu comme une forme de violence en ligne. Des recherches menées en Australie ont fait apparaître que les hommes et les femmes avaient autant de risques de subir des abus liés aux images tandis que les lesbiennes, les gays ou les bisexuels avaient plus de risques d'être victimes de ce phénomène (36 %) que les hétérosexuels (21 %)[42].

72. La violence domestique fait de plus en plus intervenir l'utilisation d'appareils domestiques intelligents contre des femmes et des personnes à charge[43], ce qui crée de

[36] Faculté de droit d'Osgoode, informations communiquées à titre confidentiel en décembre 2018.

[37] Informations communiquées par Eastern European Coalition for LGBT+ Equality en 2018.

[38] Cour européenne des droits de l'homme (deuxième section), *L. c. Lituanie*, requête n° 27527/03, arrêt définitif du 31 mars 2008 ; Cour européenne des droits de l'homme (cinquième section), *A. P., Garçon et Nicot c. France*, requêtes n^{os} 79885/12, 52471/13 et 52596/13, arrêt du 6 avril 2017.

[39] Informations communiquées par l'Initiative féministe kazakhe « Feminita » en 2018.

[40] Susan Miller, "California becomes first state to condemn intersex surgeries on children", *USA Today*, 28 août 2018.

[41] Informations communiquées par Dejusticia en septembre 2018.

[42] Nicola Henry, Anastasia Powell et Asher Flynn, "Not just 'revenge pornography': Australians' experiences of image-based abuse", mai 2017.

[43] Makda Ghebreslassie, "Stalked within your own home': woman says abusive ex used smart home technology against her", CBC News, 1er novembre 2018 ; Nellie Bowles "Thermostats, locks and lights: digital tools of domestic abuse", *New York Times*, 23 juin 2018.

nouvelles possibilités de porter atteinte à la vie privée et de réduire l'autonomie et la maîtrise de son propre destin au sein du foyer[44] ou lors d'échanges[45]. Parfois, la protection juridique offerte est inadaptée[46] ou les mesures prises par les services de police en cas de violation sont insuffisantes[47].

73. La misogynie en ligne est apparue sur les plateformes numériques[48]. On a indiqué que Twitter était la principale tribune utilisée pour véhiculer des campagnes de haine contre les femmes et diffuser du contenu à caractère sexuel, et c'est sur Facebook que l'on dénombrerait le plus d'attaques dirigées contre les femmes défendant leurs droits[49].

74. Les phénomènes d'ingérence dans la vie privé et la violence en ligne touchent davantage les hommes qui ne se conforment pas aux stéréotypes masculins conventionnels ainsi que les lesbiennes, les gays ou les bisexuels[50].

75. Les atteintes genrées au droit à la vie privée ont également des incidences sur l'exercice d'autres droits ; ainsi, les femmes sont censurées et fichées en ligne dans le cadre de campagnes prenant pour cible les militantes et les femmes journalistes[51].

Ligne d'action thématique sur la sécurité et la surveillance

76. La surveillance, à moins qu'elle ne soit exercée par nécessité et de manière légale et proportionnée, constitue une atteinte au droit à la vie privée. Le genre, la race, la classe sociale, l'origine sociale, la religion, les opinions, ainsi que leur expression, peuvent devenir des critères permettant de déterminer qui surveiller dans la société, certains individus étant exposés de ce fait à un risque plus grand de voir leur droit à la vie privée bafoué[52].

77. Dans plusieurs pays, les préjugés fondés sur le genre sont rendus apparents par le degré de surveillance plus élevé auquel sont soumis les membres de groupes LGBTQI[53]. Dans certains pays, les activités de surveillance étatique visant la communauté LGBTQI ont été favorisées par la législation. La loi contre la cybercriminalité promulguée en Égypte en 2018 figure parmi les exemples qui ont été donnés[54].

78. On présente généralement la surveillance étatique comme étant un phénomène qui vise les hommes[55], mais il ressort de certaines informations communiquées que les mesures de lutte antiterroriste touchent de manière disproportionnée les femmes et les demandeurs d'asile, réfugiés et migrants transgenres[56].

79. Les femmes peuvent s'attendre à ce que presque tous les détails de leur vie intime soient soumis à différentes formes de surveillance exercées par les autorités publiques et les

[44] Bowles, "Thermostats, locks and lights".

[45] Corinne Lysandra Mason et Shoshana Magnet, "Surveillance studies and violence against women", *Surveillance and Society*, vol. 10, nº 2 (2012) ; Informations communiquées par l'Association pour le progrès des communications.

[46] Bowles, "Thermostats, locks and lights".

[47] Al-Alosi Hadeel, "Cyber-violence: digital abuse in the context of domestic violence", *University of South Wales Law Journal*, vol. 40, nº 4 (2017).

[48] West Coast LEAF, *#CyberMisogyny*.

[49] Informations communiquées par l'Instituto nacional de la mujeres (Mexico) et l'Association pour le progrès des communications en 2018.

[50] Irish Council For Civil Liberties.

[51] Informations communiquées par Dejusticia en 2018.

[52] Mary Anne Franks, "Democratic surveillance", *Harvard Journal of Law and Technology*, vol. 30, nº 2 (printemps 2017).

[53] Informations communiquées par l'Association pour le progrès des communications en 2018.

[54] Informations communiquées par Joint International en 2018 ; voir aussi George Sadek, "Egypt: President ratifies Anti-Cybercrime Law", Global Legal Monitor, 5 octobre 2018.

[55] Privacy International, 2017.

[56] Rapport du Rapporteur spécial sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste (A/64/211).

acteurs privés, qu'il s'agisse de violence domestique, de chosification sexuelle ou de reproduction[57].

80. De grands fournisseurs de plateformes proposent désormais des outils de gestion de l'identité par l'intermédiaire de mécanismes d'authentification de l'identité en ligne. Certains sites Web, certaines applications et certains services requièrent à présent des informations de connexion et considèrent que les informations d'identification d'une personne ne font foi qu'après qu'elle se soit connectée via son compte Facebook ou Google[58]. Facebook détient 60 % de ce marché du « login social »[59], qui donne accès à une grande quantité d'informations permettant d'établir des profils, ce qui permet de mieux cerner les comportements des individus, des familles, des groupes et des communautés, processus dans le cadre duquel le genre est une variable.

Ligne d'action thématique sur les mégadonnées et les données ouvertes

81. Le développement de la collecte, du stockage et de la manipulation des données a augmenté les possibilités d'atteintes à la vie privée, qui peuvent avoir des conséquences différentes selon le genre.

82. Le traitement des données peut intégrer des biais liés aux rôles et identités de genre, d'autant plus que la modélisation des données aux fins d'interventions sociales dépasse de plus en plus l'individu pour cibler des groupes ou des communautés[60].

83. Les analyses de données qui permettent de tirer des conclusions sur des individus ou des groupes selon leur genre, et qui conduisent à une discrimination, sont contraires au droit des droits de l'homme.

Ligne d'action thématique sur les données relatives à la santé

84. Les personnes LGBTQI jugent particulièrement préoccupant le partage non consenti de données sur la santé, en particulier sur le statut VIH[61]. On a par exemple découvert que l'application Grindr contenait des trackers et partageait des informations personnelles, y compris le statut VIH de ses utilisateurs, avec de tierces parties[62].

85. On a constaté que les expériences vécues en matière de vie privée dans les établissements de soins avaient des incidences sur la décision d'avoir recours ou non aux services de santé, ce qui avait à son tour des conséquences sur le plan de la santé individuelle et publique.

86. La peur de subir des humiliations ou des discriminations du fait d'intrusions dans leur vie privée peut amener les personnes transgenres à ne pas utiliser des services de santé ou à y avoir moins recours[63].

87. Les atteintes au droit à la vie privée dont sont victimes les femmes lors de l'accouchement peuvent grandement dissuader celles-ci de solliciter des soins dans le cadre d'accouchements futurs[64].

[57] Franks, "Democratic surveillance"; Informations communiquées par l'Association pour le progrès des communications en 2018.

[58] "The Economist essay", *The Economist*, éd. de Noël, 22 décembre 2018.

[59] Ibid.

[60] Khiara M. Bridges, *The Poverty of Privacy Rights* (Stanford University Press, 2017) ; David Lyon, éd., *Surveillance as Social Sorting : Privacy, Risk and Digital Discrimination* (Londres et New York, Routledge, 2003).

[61] Informations communiquées par l'Initiative féministe kazakhe « Feminita » en 2018.

[62] Informations communiquées par l'Association pour le progrès des communications en 2018.

[63] "New health care clinic for transgender people in pipeline", *Times of Malta*, 7 avril 2018.

[64] White Ribbon Alliance for Safe Motherhood, "Respectful maternity care: the Universal Rights of Childbearing Women Charter", 2011 ; Meghan A. Bohren *et al.*, "The mistreatment of women during childbirth in health facilities globally: a mixed-methods systematic review", *PLOS Medicine*, vol. 12, nº 6 (2015). Informations communiquées par Dejusticia et par l'Association pour le progrès des communications.

88. Des technologies telles que Google Street View peuvent avoir des incidences sur le recours aux dispositifs de santé par les femmes, en suscitant chez elles la crainte d'être reconnues lorsqu'elles utilisent certains services de santé[65].

Ligne d'action thématique sur l'utilisation de données à caractère personnel par les entreprises

89. On s'accorde de plus en plus à reconnaître que le secteur privé a des obligations au titre du droit des droits de l'homme, comme l'illustre le cadre « protéger, respecter et réparer » proposé par le Représentant spécial du Secrétaire général chargé de la question des droits de l'homme et des sociétés transnationales et autres entreprises, John Ruggie, en 2008 (A/HRC/8/5)[66].

90. Le mécanisme de prise de décisions automatisée utilisé par les plateformes numériques peut produire des résultats ayant des incidences différentes en fonction du sexe de l'utilisateur. On a indiqué que des poursuites judiciaires, toujours en cours, auraient été intentées contre Facebook, qui aurait permis aux propriétaires et aux courtiers d'exclure l'affichage de certaines publicités sur la base du sexe de l'utilisateur[67].

91. On a noté avec préoccupation que le nombre de pages et de groupes, sur les réseaux sociaux, qui encourageaient la violence à l'égard des femmes, le sexisme et les stéréotypes nuisibles fondés sur le genre augmentait, et que la communauté devait exercer des pressions considérables pour faire supprimer ces pages.

92. On a indiqué ne pas avoir connaissance des éléments suivants : le processus de prise de décisions des plateformes en ligne après réception de plaintes pour violence en ligne, le nombre et la nature des cas signalés par pays, et les mesures prises. Amnesty International a constaté que Twitter n'avait pas mené d'enquête adéquate sur les signalements de violences et d'abus et a demandé à plusieurs reprises à l'entreprise de diffuser des informations utiles concernant les violences et les abus qui viseraient des femmes − et d'autres groupes − sur la plateforme, et les mesures prises pour combattre ces phénomènes[68].

93. Il a été rapporté dans une des communications que l'application Grindr avait pris des mesures concrètes pour réduire toute utilisation abusive visant à piéger les homosexuels[69]. Cependant, on indiquait que l'impunité et l'opacité étaient généralement la seule réponse des plateformes numériques (Facebook, Twitter, les médias, etc.) face aux violences en ligne fondées sur le genre, et que les victimes se sentaient généralement abandonnées[70].

94. On indiquait que les préjudices subis par des individus en raison d'atteintes à leur droit à la vie privée fondées sur leur genre et liées aux technologies avaient des incidences graves et amplement démontrées telles que l'escroquerie, la perte d'emploi et de possibilités de suivre un enseignement, les restrictions à la liberté de mouvement, à la liberté d'association et à la liberté de se vêtir à sa guise, l'ingérence dans la manière d'élever ses enfants, les coups portés à la réputation et à la confiance de manière générale, la violence (voire la mort) et la détention[71].

[65] Melissa L. Davey, "Protect us from anti-abortion protesters, say women's clinics in WA", *The Guardian*, 25 janvier 2018.

[66] Internet Rights and Principles Coalition, "The Charter of Human Rights and Principles for the Internet", 2014 ; Informations communiquées par l'Association pour le progrès des communications en 2018.

[67] Informations communiquées par Consumer Policy Research Centre, qui cite un article intitulé « Money », CNN News, mars 2018.

[68] Voir https://decoders.amnesty.org/projects/troll-patrol/findings.

[69] Informations communiquées par l'Initiative féministe kazakhe « Feminita » en 2018.

[70] Electronic Media cité par Dejusticia dans une communication de 2018.

[71] Informations communiquées par l'Association pour le progrès des communications en 2018. Informations communiquées par N. Pushkarna et M.M. Ren en 2018 ; Commissariat à la protection de la vie privée du Canada, "Online reputation: what are they saying about me?", janvier 2016 ; soumission de cas à Transgender Europe ; Agence des droits fondamentaux de l'Union européenne, *Violence against Women: an EU-Wide Survey − Main Results* (Luxembourg, Office des publications de l'Union européenne, 2015).

95. Les répercussions en cas d'atteinte à la vie privée ne sont pas homogènes ; ces atteintes peuvent entraîner une augmentation de la violence domestique pour les femmes et une discrimination accrue pour les personnes LGBTQI[72].

96. Les immixtions dans la vie privée constituent des atteintes à la personnalité humaine en tant que telle et ont des incidences plus larges sur le plan sociétal. Les formes extrêmes de violences en ligne et d'atteintes à la vie privée personnelle et familiale infligées aux femmes très en vue dissuadent les filles et les femmes d'endosser des rôles publics, ce qui compromet le droit des femmes de participer aux affaires publiques et donc, le caractère représentatif des institutions démocratiques[73].

97. Les informations communiquées faisaient état d'une diversité de bonnes pratiques qui garantissaient la protection de la vie privée dans une perspective de genre : réformes législatives, adoption de cadres généraux s'appliquant indifféremment aux deux sexes et fondés sur des données probantes, décisions judiciaires prononcées, participation des organisations de la société civile et mise à profit de leur expérience, programmes communautaires de protection de la vie privée tenant compte des questions de genre, ou encore élaboration de ressources pédagogiques.

98. On considérait que les pratiques permettant de traiter de manière optimale les questions d'atteintes à la vie privée liées à l'orientation sexuelle et à l'identité de genre étaient consacrées par les Principes additionnels et obligations additionnelles des États relatifs à l'application du droit international des droits de l'homme en matière d'orientation sexuelle, d'identité de genre, d'expression de genre et de caractéristiques sexuelles venant compléter les Principes de Jogjakarta[74].

V. Conclusions

99. **La Déclaration universelle des droits de l'homme engage tous les individus et tous les organes de la société à promouvoir et à respecter les droits de l'homme[75]. Les États, les entreprises, les organismes religieux, la société civile, les organisations professionnelles et les particuliers ont tous un rôle important à jouer.**

100. **Le fait que les individus puissent partager des idées et se rassembler en toute confiance est également d'une importance capitale pour la bonne santé des sociétés et de la démocratie. Les atteintes à la vie privée risquent de conduire à la perte de cette confiance, notamment envers les autorités et les institutions créées pour représenter l'intérêt public, et au retrait du processus participatif, ce qui peut avoir des effets préjudiciables sur les régimes représentatifs et les compromettre.**

101. **Bien que le droit à la vie privée ait un coût et ne soit pas sans risques pour les autorités, l'intérêt collectif que nous portons à la démocratie l'emporte sur les défis à relever. Le droit à la vie privée des femmes, ainsi que des enfants et des personnes de diverses orientations sexuelles, identités de genre, expressions de genre et caractéristiques sexuelles, est d'une importance cruciale pour toutes les raisons exposées ci-dessus et dans les communications[76].**

102. **Les atteintes à la vie privée fondées sur le genre sont une forme systémique de déni des droits humains, sont discriminatoires par nature et contribuent souvent au maintien de structures sociales, économiques, culturelles et politiques qui ne sont pas égalitaires.**

[72] Gay, Lesbian and Straight Education Network, *Out Online : The Experiences of Lesbian, Gay, Bisexual and Transgender Youth on the Internet* (New York, 2013), dans une communication conjointe internationale, 2018.

[73] Informations communiquées par Australian Women Against Violence Alliance submission en 2018.

[74] Communication conjointe d'organisations de la société civile, 2018 ; Peter Micek et Denis Nolasco, "The gender of surveillance: how the world can work together for a safer Internet", Access Now, blog, 6 février 2018.

[75] Voir le préambule de la résolution 217 A (III) de l'Assemblée générale.

[76] Haut-Commissariat des Nations Unies aux droits de l'homme, *Nés libres et égaux : orientation sexuelle et identité de genre en droit international des droits de l'homme* (New York et Genève, 2012).

103. **La lutte contre les atteintes à la vie privée fondées sur le genre suppose la mise en place de cadres aux niveaux international, régional et national.**

104. **Afin de prévenir les immixtions dans la vie privée fondées sur le genre, il est nécessaire que les États veillent à protéger comme il se doit la vie privée dans le cadre de l'élaboration de politiques, des réformes législatives, de la prestation de services, de l'action réglementaire, du soutien aux organisations de la société civile et des dispositifs liés à l'éducation et à l'emploi, en s'appuyant sur l'expérience des femmes, des hommes, des personnes transgenres, des personnes intersexes et de tous ceux qui ne se reconnaissent pas dans le genre binaire et la cisnormativité.**

105. **La protection des données à caractère personnel en ligne devrait être une priorité, et il importe que les pays qui ne sont pas parties au Règlement général sur la protection des données adoptent des dispositions équivalentes ou supérieures à celles qu'il contient. Il est essentiel que la question du genre soit prise en compte dans l'élaboration et l'application de cadres de protection de la vie privée.**

106. **Il est nécessaire que les entreprises privées communiquent en toute transparence sur la manière dont elles utilisent les données personnelles des utilisateurs**[77] **et donnent suite aux plaintes de harcèlement en ligne. En outre, il importe de renforcer la diversité de genre parmi ceux qui façonnent les expériences en ligne afin de rendre les produits et les plateformes plus sûrs et plus responsables sur le plan social.**

VI. Résumé des recommandations

107. **En ce qui concerne les organismes de l'ONU, toutes les procédures spéciales et autres mécanismes du Conseil des droits de l'homme ainsi que les organes conventionnels des droits de l'homme concernés devraient intégrer les questions de genre et le respect de la vie privée dans l'exécution de leurs mandats respectifs.**

108. **Il est recommandé aux États Membres :**

a) D'adopter une approche transversale qui tienne compte du fait que les avantages retirés du droit à la vie privée, l'expérience de ce droit et les menaces pesant sur son exercice ne sont pas les mêmes selon le genre et qui reconnaisse les principes fondamentaux des droits humains et du respect de la vie privée ;

b) De mener une évaluation du cadre législatif qu'ils ont mis en place pour prévenir et réprimer les atteintes à la vie privée fondées sur le genre, au regard des lois et traités pertinents aux niveaux mondial, régional et national ;

c) De prendre des mesures et d'adopter un cadre légal et réglementaire offrant une protection globale pour l'utilisation et le développement de communications numériques sécurisées ;

d) De promouvoir un accès suffisant à l'Internet et de combler l'écart numérique entre les sexes ;

e) De prendre toutes les mesures législatives, administratives et autres nécessaires pour prévenir les atteintes à la vie privée fondées sur le sexe, l'orientation sexuelle et l'identité de genre, mener une enquête le cas échéant et sanctionner leurs auteurs.

109. **Les entreprises devraient appliquer les Principes directeurs relatifs aux entreprises et aux droits de l'homme : mise en œuvre du cadre de référence « protéger, respecter et réparer » des Nations Unies, et éviter de porter atteinte aux droits fondamentaux de toutes les personnes touchées par leurs pratiques, en tenant dûment compte des incidences de leurs activités en fonction du genre.**

[77] Australian Competition and Consumer Commission, *Digital Platforms Inquiry: Preliminary Report* (Canberra, Australie, 2018).

VII. Protection des données relatives à la santé

110. La santé est le bien le plus précieux de chacun d'entre nous. Les altérations de l'état de santé entraînent toujours un changement de vie, souvent définitif. Nous sommes tous, à un moment de notre vie, des patients. Il arrive parfois aussi que notre état de santé ait une influence décisive sur notre vie. Protéger notre dignité et notre autonomie grâce à l'application des normes les plus exigeantes dans les scénarios impliquant des données relatives à la santé constitue donc pour nous tous un intérêt très légitime.

111. La relation entre un patient dont les données sont recueillies et un professionnel de la santé est très délicate : les patients sont, par définition, dans une position vulnérable. Leur situation peut être pénible et dangereuse, et avoir des conséquences à vie. Le rôle d'un professionnel de la santé est d'informer le patient de manière aussi exhaustive et précise que possible et de traiter ces informations de manière transparente et conforme aux normes.

112. La protection des patients (et de leurs parents) dans ces moments de vulnérabilité existentielle fait l'objet de considérations juridiques et éthiques depuis des millénaires et a donné naissance à des règles. Des principes comme le secret médical, l'obligation de recueillir un consentement en pleine connaissance de cause pour entreprendre un traitement, la mise à disposition d'une documentation appropriée sur le traitement et le libre choix du médecin traitant sont certains des résultats essentiels de siècles de réflexion sur la meilleure manière de protéger les droits des patients.

113. Chaque cas médical génère des données personnelles. Ces données sont importantes pour la prise en charge et doivent être traitées conformément aux normes juridiques et éthiques les plus élevées. La numérisation produit de plus en plus de données médicales, qui seront partagées de façon croissante par les professionnels de la santé, dans la mesure où ils ne cessent de se spécialiser et doivent collaborer en se conformant aux normes de qualité les plus élevées.

114. Les données traitées à des fins médicales sont également importantes pour de nombreuses autres parties prenantes et ont beaucoup d'autres finalités que la relation entre le professionnel de la santé et le patient, relation au demeurant susceptible de changer le cours de la vie de ce dernier. Tout d'abord, le patient ou la patiente peut avoir un intérêt légitime à contrôler ces données et accepter qu'elles soient partagées pendant le traitement et après celui-ci. Ensuite, d'autres parties prenantes, comme la famille du patient, les institutions auxquelles le patient doit rendre des comptes − institutions de sécurité sociale, compagnies d'assurance ou employeurs − ainsi que d'autres acteurs moins directement concernés, comme les chercheurs en médecine ou le grand public, qui comptent sur un système de santé efficace, peuvent avoir un intérêt à accéder à ces données.

115. Les tensions entre les intérêts et besoins de ces différentes parties prenantes posent d'épineux problèmes sur les plans juridiques et déontologiques.

Problèmes fondamentaux

Consentement éclairé

116. En général, les patients ont le droit d'accepter un traitement après avoir été correctement informés de ses risques et effets secondaires éventuels et des autres traitements possibles. Les critères de la procédure de consentement pour les traitements médicaux et la recherche médicale font l'objet d'une réglementation abondante, détaillée et controversée.

117. Ces règlements n'ont pas encore été harmonisés avec les prescriptions relatives aux informations communiquées aux patients dont les données ont été recueillies et les critères permettant d'établir le consentement éclairé comme base juridique du traitement des données. Les critères régissant le consentement éclairé sont souvent imprécis et contradictoires.

118. Les patients dont les données sont recueillies peuvent se sentir dépassés par les différentes procédures de consentement à un moment où la protection de leurs données n'est pas leur préoccupation immédiate. De même, ils ne souhaitent et ne peuvent pas

toujours comprendre pleinement toutes les conséquences des différents types de consentement qu'ils donnent. Il n'est pas facile de faire la différence entre un consentement donné pour des tests, pour un traitement, pour la recherche médicale et pour l'utilisation des données, procédures qui sont souvent soumises à des réglementations dont les champs d'application sont différents et parfois contradictoires et ne dépendent pas des mêmes autorités de contrôle. Les patients et leur famille sont ainsi soumis à une forte pression qui nuit à leur capacité de donner librement un consentement éclairé.

Utilisation secondaire pour la recherche médicale

119. Les données personnelles doivent être recueillies et traitées en tant que base du traitement médical, puis stockées à des fins de documentation du traitement, parfois pendant des décennies. Ces données constituent aussi souvent une ressource importante pour la recherche médicale. Des arguments de poids mettent en avant une justification, voire une nécessité, éthique de conserver ces données pour la recherche dans l'intérêt des générations futures de patients.

120. La recherche a une finalité différente de celle du traitement et requiert donc un fondement juridique différent pour l'exploitation des données. Les critères qui entrent ici en jeu sont très variés et peu clairs, dans la mesure où de nombreuses questions éthiques sous-jacentes ne sont pas clairement décrites ou analysées. En particulier, la question se pose de savoir si cette utilisation secondaire requiert là encore le consentement éclairé du patient et/ou l'autorisation d'un comité d'éthique compétent et/ou d'autorités de contrôle. Les interrogations portent également sur l'autonomie individuelle découlant de l'intégrité physique et la responsabilité à l'égard du « bien commun ».

121. Si un tel consentement était remplacé par un autre fondement juridique, il faudrait prendre d'autres mesures pour protéger les droits fondamentaux du patient dont les données sont recueillies. L'absence de législation internationale dans ce domaine aboutit à des situations dans lesquelles les médecins traitants doivent, ou pensent qu'ils doivent obtenir un consentement éclairé supplémentaire des patients concernés, consentement qui ne peut plus être obtenu dans certains cas, pour des raisons techniques ou déontologiques.

Utilisation secondaire à d'autres fins

122. Les données médicales ont une grande valeur également à d'autres fins (sécurité sociale, santé publique, emploi et commerce). Les lois nationales ne disent souvent rien du traitement des données à ces fins, dont on ne sait pas si elles sont juridiquement et déontologiquement justifiables et lesquelles d'entre elles requièrent le consentement éclairé ou un autre fondement juridique légitime. Le principe obligatoire de finalité, qui exige que l'utilisation secondaire des données à caractère personnel ne puisse être faite que dans un but compatible avec l'objectif principal, est donc souvent ignoré ou n'est pas respecté.

123. L'hétérogénéité des législations dans ce domaine conduit à un nivellement par le bas, les services publics ou même les entreprises qui dépendent d'informations personnelles relatives à la santé ayant intérêt à exercer leurs activités dans des zones où le niveau de protection des données est faible.

124. La protection des droits des patients dont les données sont recueillies, notamment le droit à la transparence, qui comprend l'information et l'accès, pose problème, dans la mesure où ces utilisations secondaires sont le fait d'entités qui ne sont pas connues de l'intéressé, et servent bien souvent des fins qu'il ignore.

Propriété des données comme moyen de protection concurrent

125. Les situations décrites ci-dessus ont eu pour conséquence que certains juristes (et même des législateurs) ont commencé à plaider en faveur d'un droit de la propriété des données similaire au droit de la propriété intellectuelle, qui devrait contribuer à atténuer les problèmes de partage en ce qui concerne les données à caractère personnel et les autres données. Ces notions s'articulent très difficilement avec les fondements existants de la protection des données ; elles doivent reposer sur un raisonnement clair et une justification qui mettent en avant les conséquences prévisibles en se fondant sur des faits. Il n'existe pas à l'heure actuelle de modèle de faits et de preuves qui sous-tende ces notions.

Répartition peu claire des responsabilités

126. Les traitements médicaux et la recherche sont supervisés par des organismes de réglementation, notamment par des comités d'éthique composés d'experts et de parties prenantes, dont beaucoup ne sont pas juristes et n'ont pas de compétence particulière en matière de protection des données.

127. Nombre des exigences formulées par ces organes concernant l'exploitation des données pour les traitements médicaux et la recherche sont cependant liées à la protection des données, qu'il s'agisse des prescriptions spécifiques (et souvent contradictoires) sur les procédures de consentement, des informations à communiquer au patient ou à la personne dont les données sont recueillies, du droit du patient à savoir ou à ne pas savoir, et des conséquences qu'entraîne le retrait du consentement, entre autres aspects.

128. Les règlements proposés par ces organes peuvent entrer en conflit avec des règles de protection des données et la supervision qu'ils exercent peut interférer avec celle qu'assurent les personnels et les entités exclusivement chargés de veiller au respect de la protection des données, tels que les spécialistes indépendants et les autorités de protection des données.

Champ d'application peu clair : données personnelles, anonymes et sous pseudonyme

129. Le postulat de base selon lequel les lois relatives à la protection des données ne s'appliquent que lorsqu'il s'agit de données personnelles, propres à un individu donné, est très difficile à appliquer dans le domaine médical, dans la mesure où il est rare que les données médicales puissent être intégralement anonymisées. D'où la difficulté de savoir quelle mesure d'anonymisation est suffisamment efficace pour que des données restent en dehors du champ d'application de la législation sur la protection des données.

130. Ce problème est particulièrement difficile à résoudre lorsqu'il s'agit de déterminer si les données médicales devraient être incluses dans les initiatives de libre accès ou de données ouvertes qui exigent la communication de données (non personnelles) au public. Les responsables du traitement des données peuvent d'une part être obligés de garder les données sous leur contrôle pour en protéger l'anonymat, mais d'autre part être tenus de donner librement accès aux données, avec le risque de leur ré-identification. Le flou sur cette question peut faciliter la protection de facto des données médicales par des responsables du traitement des données qui pourront − de fait − décider qui a accès aux données (anonymisées selon une méthode ou une autre) et à quelles conditions.

131. Le Rapporteur spécial a déclaré sans ambiguïté dans son rapport de 2018 à l'Assemblée générale que les données d'enregistrement unitaire sensibles et de grandes dimensions concernant des individus ne devraient pas être publiées en ligne ou échangées à moins qu'il ne soit prouvé de manière convaincante qu'elles ont été anonymisées en toute sécurité et résisteront à une ré-identification à l'avenir.

Absence de portabilité des données et absence de numérisation

132. Les données médicales sont encore souvent collectées dans un format analogique. Les anamnèses sont souvent aléatoires et incomplètes et les diagnostics peuvent être fondés sur des données de mauvaise qualité.

133. La numérisation des données médicales, la normalisation des formats et des procédures, ainsi que l'établissement de critères minimaux pour la qualité des données peuvent aider tant les patients que les professionnels de la santé à contrôler et à gérer de manière responsable les données relatives à la santé.

134. Les États ont cependant tendance à mettre au point leurs propres systèmes de santé électronique sans la participation des citoyens et des professionnels de la santé et sans établir de normes. Cela peut rendre la portabilité des données impossible pour les patients, dont la capacité de contrôler leurs données médicales se trouve en outre réduite faute d'un outil normalisé qui permettrait le stockage et la gestion en toute sécurité de leurs propres données relatives à la santé, selon leurs propres règles.

Nuages informatiques

135. De plus en plus d'informations médicales sont stockées dans des nuages informatiques (comme n'importe quelles autres données), ce qui entraîne de nombreuses conséquences : transfert transfrontière de données personnelles pouvant entraîner des conflits de compétences, absence de contrôle pour les patients et incidents de sécurité à fort impact pouvant toucher des millions de personnes.

136. Cependant, les prescriptions minimales s'appliquant aux prestataires de services informatiques en nuage ne sont pas harmonisées, ce qui incite les utilisateurs à mener leurs activités dans des zones où la protection des données est faible.

Produits/dispositifs portables liés au mode de vie

137. Les données relatives à la santé ne sont plus (directement) liées à la morbidité et sont maintenant recueillies à des fins très différentes du traitement ou de la prévention des maladies. En particulier, les applications et gadgets liés au mode de vie (« dispositifs portables ») recueillent des quantités considérables de données relatives à la santé avec ou sans le consentement éclairé des intéressés. Ces dispositifs sont devenus de plus en plus populaires, bien que la base juridique autorisant la collecte des données et les prescriptions régissant leur exploitation ne soient pas clairement définies, qu'aucune norme minimale de transparence ne s'applique et que le principe obligatoire de finalité ne soit pas suffisamment pris en compte.

Sécurité et sûreté

138. Bien que les données relatives à la santé soient très sensibles, et que les failles des dispositifs traitant les données relatives à la santé puissent avoir des conséquences fatales, il n'existe pas de règles précises et détaillées concernant les normes minimales de sécurité et de sûreté. Il en résulte une série d'incidents de sécurité lourds de conséquences pour les intéressés qui en sont victimes.

Notification des atteintes à la protection des données, manque de transparence

139. Bien que des atteintes à la protection des données médicales se produisent régulièrement, il n'existe aucune norme déterminant quand et comment les personnes concernées, ainsi que le grand public, doivent être informés de tels incidents. Ce manque de transparence ne répond pas aux exigences de la population en matière de responsabilité.

Accès à la justice

140. La non-conformité à la législation sur la protection des données peut mettre en danger la vie des personnes dont les données sont recueillies. Cependant, depuis le début, la législation en la matière a manqué d'instruments de mise en œuvre efficaces. L'imprécision des règles définissant les compétences respectives des autorités de protection des données, des tribunaux, des médiateurs, des responsables de la protection des données et des autorités de contrôle dans le domaine médical, ainsi que la diffusion inégale des informations et des connaissances et la complexité des cadres réglementaires font qu'il est très difficile pour les personnes dont les données sont recueillies de faire appliquer leurs droits.

141. Ce défaut d'application de la loi aboutit à une défiance à l'égard du système médical qui se ressent notamment dans la relation entre le patient et le professionnel de santé et peut avoir un effet préjudiciable sur chaque patient. Il serait donc de la plus grande importance sur le plan stratégique que l'ONU formule des normes minimales.

Prochaines étapes

142. Le Rapporteur spécial a l'intention de fournir des orientations pour réglementer les données relatives à la santé afin de promouvoir la protection du droit à la vie privée et la protection des données personnelles, comme le prévoient 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.

143. Un projet d'orientations[78] contenant des principes directeurs pour le traitement des données relatives à la santé souligne l'importance qu'il y a à doter ce processus d'un fondement légitime qui tienne compte des questions soulevées ci-dessus. L'objectif de ces orientations est tout d'abord de servir de base de référence commune au plan international pour l'établissement de normes minimales de protection des données relatives à la santé destinées à être mises en œuvre au niveau national, et ensuite de fournir des points de repère pour le débat en cours sur la manière dont le droit à la vie privée peut être protégé s'agissant des données relatives à la santé, et promu conjointement avec d'autres droits de l'homme (comme le droit à la liberté d'expression, le droit à un procès équitable et la protection de la propriété) dans un contexte de traitement et de partage des données médicales à l'échelle mondiale.

144. Le projet d'orientations, qui est examiné actuellement par des experts de l'équipe spéciale, est ouvert à la consultation publique afin que des observations écrites puissent être formulées d'ici au 11 mai 2019 ; une réunion publique des parties prenantes se tiendra ensuite à Strasbourg les 11 et 12 juin 2019. Les États membres souhaitant participer à cette réunion devraient manifester leur intérêt avant le 11 mai.

145. Le groupe de rédaction formulera une recommandation finale, en s'inspirant des contributions des parties prenantes, qui sera communiquée au Rapporteur spécial et intégrée fin 2019 à son rapport annuel à l'Assemblée générale pour 2019.

VIII. Indicateurs de la vie privée

146. Le Rapporteur spécial mène également des consultations sur les « Metrics for privacy » (Indicateurs de la vie privée)[79]. Les particuliers ainsi que les représentants de la société civile et les gouvernements sont invités à lui adresser leurs observations et suggestions avant le 30 juin 2019. Il s'agirait d'utiliser ces indicateurs comme outil d'enquête normalisé pendant les visites de pays, officielles et non officielles.

[78] Voir https://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2019_HRC_Annex3_HealthData.pdf.

[79] Voir https://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2019_HRC_Annex4_Metrics_for_Privacy.pdf.