Nations Unies A/73/438

Assemblée générale

Distr. générale
17 octobre 2018
Français
Original : anglais

Soixante-treizième session
Point 74 b) de l'ordre du jour
Promotion et protection des droits de l'homme : questions relatives aux droits de l'homme, y compris les divers moyens de mieux assurer l'exercice effectif des droits de l'homme et des libertés fondamentales

Droit à la vie privée*

Note du Secrétaire général

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

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

18-17254 (F) 251018 091118

Rapport du Rapporteur spécial sur le droit à la vie privée

Résumé

Le présent rapport est divisé en deux parties : un résumé des activités menées au cours de la période 2017-2018 et le rapport final sur les travaux de l'équipe spéciale chargée des mégadonnées et des données ouvertes créée par le Rapporteur spécial.

I. Aperçu des activités du Rapporteur spécial sur le droit à la vie privée

1. La période d'octobre 2017 à octobre 2018 a été extrêmement productive pour le Rapporteur spécial sur le droit à la vie privée, marquée par des contacts avec la société civile, les gouvernements, les services chargés de l'application des lois, les services de renseignement, les autorités de protection des données, les autorités de contrôle des services de renseignement, le milieu universitaire, le milieu des entreprises et d'autres parties prenantes.

2. En mars 2018, le Rapporteur spécial a présenté au Conseil des droits de l'homme un examen complet de son premier mandat de trois ans au poste créé par le Conseil en mars 2015[1]. Il y a rendu compte des activités qu'il avait menées dans chacun des domaines thématiques du mandat. Il tient à dire que c'est pour lui un grand honneur d'avoir vu son mandat prorogé jusqu'en 2021 et de pouvoir poursuivre l'œuvre utile qu'il accomplit.

3. Le Rapporteur spécial dû interrompre ses travaux pour subir une intervention chirurgicale en avril 2018. Le Rapporteur spécial remercie le Haut-Commissariat aux droits de l'homme pour le soutien et l'aide qu'il lui a apportés durant cette période. Le Rapporteur spécial s'est bien rétabli et a repris ses fonctions en juin 2018.

A. Activités de l'équipe spéciale chargée de la confidentialité des données de santé

4. L'Équipe spéciale chargée de la confidentialité des données de santé a travaillé sous la direction de Steve Steffensen, de la Dell Medical School de l'Université du Texas (États-Unis d'Amérique). Un projet de rapport a été entamé mais des imprévus ont fait que la consultation prévue pour 2018 a été reportée à 2019. Le Vice-Président, M. Nikolaus Forgo, a accepté d'assumer la charge de Président.

B. Activités de l'équipe spéciale chargée de l'utilisation des données personnelles par les entreprises

5. Le droit au respect de la vie privée n'a jamais été autant au centre des préoccupations politiques, judiciaires ou personnelles que depuis que les tensions entre sécurité, modèles d'entreprise et vie privée occupent le devant de la scène.

6. Face aux événements survenus au cours de l'année écoulée, notamment l'affaire Cambridge Analytica, l'introduction de textes législatifs tels que la loi de clarification de l'utilisation licite de données à l'étranger, aux États-Unis, et la loi de 2018 portant modification de la législation sur les télécommunications et autres, en Australie, ainsi que le procès *États-Unis* c. *Microsoft* devant la Cour suprême des États-Unis, le Rapporteur spécial a avancé le début des travaux de l'Équipe spéciale chargée de l'utilisation des données personnelles par les entreprises.

7. L'équipe spéciale s'est réunie pour la première fois en Malte en septembre 2018. Ses membres proviennent de grandes entreprises à la pointe du numérique ou sont d'importants acteurs de la protection du droit à la vie privée dans le monde de la technologie. Elle conseillera le Rapporteur spécial en ce qui concerne les difficultés et possibilités nouvelles en matière de promotion du droit à la vie privée, et notamment leurs incidences pour les hommes et les femmes.

[1] A/HRC/37/62.

C. Activités de l'équipe spéciale pour une meilleure compréhension de la vie privée

8. L'Équipe spéciale pour une meilleure compréhension de la vie privée étudie la reconnaissance par le Conseil des droits de l'homme que le respect de la vie privée concourt au développement de la personne et les obstacles à cette fonction. Il collaborera avec des initiatives dans le monde entier, telles que celle de la Commission australienne des droits de l'homme, qui vise à examiner l'incidence de l'ère numérique sur les droits de l'homme[2].

9. Chacun doit pouvoir jouir de la protection que prévoit le droit international des droits de l'homme mais il apparaît que l'exercice du droit à la vie privée n'est ni égal ni universel. La protection et le respect de la vie privée et les atteintes à celle-ci peuvent avoir des effets différents selon le sexe.

10. À cet égard, la Cour suprême de l'Inde a abrogé l'article 377 du Code pénal indien, qui érigeait en infraction les rapports sexuels librement consentis entre adultes, dans un arrêt où elle a reconnu les droits des lesbiennes, gays, bisexuels, transgenres, personnes en questionnement et intersexes en Inde. Ce jugement, qui aura un effet considérable sur le discours concernant l'égalité des sexes et le respect de la vie privée en Inde, découle de l'arrêt de 2017 sur le droit à la vie privée en l'affaire *Puttaswamy*[3].

11. Le Rapporteur spécial a lancé une consultation en ligne sur le droit à la vie privée à l'ère du numérique du point de vue de la problématique femmes-hommes, portant sur des questions telles que :

a) Quels problèmes femmes-hommes se posent à l'ère numérique ? Quels défis faut-il relever et quelles expériences positives peuvent être diffusées plus largement ?

b) L'ère numérique a-t-elle produit de nouvelles façons de vivre la vie privée différant sensiblement selon le sexe (notamment l'orientation sexuelle, l'identité de genre, l'expression du genre et les caractéristiques sexuelles) ? Si oui, quelles sont-elles ?

c) Quelles sont les répercussions des atteintes à la vie privée sur les femmes et les hommes et les personnes de diverses orientations et identités sexuelles, expressions de genre et caractéristiques sexuelles, notamment en ce qui concerne la santé ou la discrimination à l'emploi ?

d) Quelles sont dans la législation et les dispositifs de prestation de services les bonnes pratiques tenant compte des différences entre femmes et hommes dans l'exercice du droit à la vie privée ?

12. Les réponses ont été demandées pour le 30 septembre 2018, de sorte qu'elles puissent être présentées au Conseil des droits de l'homme en 2019. Le Rapporteur spécial recevra les réponses tardives des États Membres jusqu'au 30 novembre 2018.

13. Cette initiative fait suite aux consultations sur le thème « Vie privée, personnalité et circulation de l'information », menées dans le monde entier en juillet 2016, mai 2017 et septembre 2017. La quatrième de ces consultations, qui portera sur les aspects sexospécifiques et était prévue pour mai 2018 en Amérique latine, a été reportée car le Rapporteur spécial ne pouvait s'y rendre et aura lieu à la mi-2019.

---

[2] Commission australienne des droits de l'homme, « Major project to focus on human rights and technology », 22 mai 2018, disponible à l'adresse www.humanrights.gov.au/news/stories/major-project-focus-human-rights-and-technology.

[3] Communication de Smitha Krishna Prasad, Université nationale de droit de Delhi (Inde), 24 septembre 2018.

D. Activités de l'équipe spéciale chargée de la sécurité et de la surveillance

14. Après les révélations d'Edward Snowden sur les programmes de surveillance et de partage de renseignements utilisés par les services de renseignements des États-Unis et du Royaume-Uni de Grande-Bretagne et d'Irlande du Nord, la Cour européenne des droits de l'homme a été saisie de requêtes concernant l'interception massive de communications, le partage de renseignements avec des États étrangers et l'obtention de données de communication auprès de fournisseurs de services de communication en vertu de la loi britannique de 2000 régissant les pouvoirs d'enquête.

15. La Cour a conclu récemment que le régime britannique d'interception massive avait emporté violation de l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (Convention européenne des droits de l'homme) sur le droit au respect de la vie privée et familiale, à raison de l'insuffisance de la surveillance appliquée au choix de « porteurs » Internet pour l'interception ainsi qu'au filtrage, à la recherche et à la sélection des communications interceptées pour examen, et à raison du caractère inadéquat des garanties liées à la sélection des « données de communication pertinentes » pour examen.

16. La Cour a considéré que le système d'obtention de données de communication auprès de fournisseurs de services avait emporté violation de l'article 8 ; et que les systèmes d'interception massive et d'obtention de données de communication auprès de fournisseurs de services de communication avaient emporté violation de l'article 10 de la Convention en raison de l'insuffisance des garanties appliquées aux informations journalistiques confidentielles. Elle a conclu en outre que le dispositif de partage de renseignements avec des États étrangers n'avait emporté violation ni de l'article 8 ni de l'article 10 de la Convention[4].

17. Même si cet arrêt concernait le cadre juridique antérieur en matière de surveillance au Royaume-Uni, ses conclusions sont importantes et portées à l'attention des États Membres afin qu'ils revoient leurs pratiques et leur législation.

18. En ce qui concerne l'arrêt de décembre 2016 de la Cour de justice de l'Union européenne concernant la conservation de données sur les communications et la consultation du Gouvernement du Royaume-Uni concernant son projet de réponse, le Rapporteur spécial a apporté au début de 2018 une contribution qui sera disponible sur la page Web du Haut-Commissariat consacrée au titulaire du mandat[5].

19. En septembre 2018, le Gouvernement australien a présenté le projet de loi portant modification de la législation sur les télécommunications et autres, qui a de profondes incidences sur les droits de l'homme et la cybersécurité aux niveaux international et national.

20. Ce projet de loi comporte des lacunes rédhibitoires. C'est une mesure de sécurité nationale mal conçue pouvant tout aussi bien menacer la sécurité que ne pas la menacer ; d'un point de vue technique, on peut douter qu'il puisse atteindre ses objectifs et éviter d'introduire des failles dans la cybersécurité de l'ensemble des appareils, qu'il s'agisse de téléphones mobiles, tablettes, montres, voitures ou caméras de télévision en circuit fermé, et il nuit indûment aux droits de l'homme, notamment au droit à la vie privée. Les assurances qu'il ne soit pas un « accès

[4] 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, note d'information sur l'Arrêt du 13 septembre 2018, disponible à l'adresse https://hudoc.echr.coe.int/eng#{"itemid":["002-12080"]}.

[5] www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx.

dérobé » à des communications chiffrées ne sont pas fiables car il pourrait en fait multiplier les clefs de l'accès principal ou même créer d'autres accès.

21. Le projet de loi crée une trop grande latitude d'utilisation de pouvoirs exceptionnels. La responsabilité ne revient pas au Parlement mais aux services concernés et au Procureur général. Le texte ne prévoit pas de contrôle judiciaire ni indépendant, son manque de transparence est extrêmement préoccupant et la proposition d'introduire un logiciel dans les appareils ressemble de manière troublante à un piratage par les autorités. Il a été présenté au Parlement à l'issue de consultations trop brèves, alors que de plus de 14 000 réactions ont été reçues dans les deux semaines qui les ont suivies[6].

22. Le Rapporteur spécial est d'autant plus préoccupé que le Gouvernement australien entend limiter les recours pour atteintes graves à la vie privée à la protection limitée existant en matière de droits de l'homme et de vie privée : il n'y a pas de protection constitutionnelle de la vie privée, pas de charte des droits consacrant le respect de la vie privée, pas de délit d'atteinte à la vie privée et, à l'inverse de la législation du voisin néo-zélandais, la législation australienne n'a pas été reconnue comme adéquate par l'Union européenne.

23. Il faut s'attaquer autrement aux difficultés que le codage présente pour l'application de la loi et la sécurité nationale. Certes, la technologie pose des problèmes aux services d'application de la loi et de renseignements et il importe de lutter contre les abus pédosexuels en ligne et les menaces terroristes, mais la protection des droits fondamentaux des citoyens est également légitime et nécessaire dans une société démocratique. Les technologies qui permettent à des criminels et à des terroristes d'échapper à la détection ou de lancer des attaques malveillantes présentent aussi d'énormes avantages pour la cybersécurité, la protection de la vie privée et l'économie[7]. Un affaiblissement des technologies de chiffrement met en péril la sécurité de l'économie moderne de l'information[8].

24. En résolvant les difficultés que le chiffrement pose aux enquêtes policières et à la collecte de renseignements, il faut éviter de l'affaiblir et préserver la sécurité nationale d'autres pays.

25. Je recommande aux États Membres de s'inspirer de l'approche des Pays-Bas, qui considèrent que les mesures nationales doivent tenir compte du contexte international et du manque de possibilités d'affaiblir les produits de chiffrement sans compromettre la sécurité des systèmes numériques qui y recourent[9].

26. Le Forum international de contrôle des services de renseignement, initiative du Rapporteur spécial, se réunira à Malte à la fin de novembre 2018. L'intérêt est tel qu'il est débordé de demandes d'inscription.

---

[6] Justin Hendry, « Decryption laws enter parliament », *IT News*, 20 septembre 2018, disponible à l'adresse www.itnews.com.au/news/decryption-laws-enter-parliament-512867?eid=1&edate=20180921&utm_source=20180921_AM&utm_medium=newsletter&utm_campaign=daily_newsletter.

[7] James A. Lewis, Denise E. Zheng and William A. Carter, *The Effect of Encryption on Lawful Access to Communications and Data* (Washington, Center for Strategic and International Studies, 2017), disponible à l'adresse https://csis-prod.s3.amazonaws.com/s3fs-public/publication/170221_Lewis_EncryptionsEffect_Web.pdf?HQT76OwM4itFrLEIok6kZajkd5a.r.rE.

[8] New America, « Coalition raises serious concerns about Australian draft bill and encryption backdoors », communiqué de presse, 10 septembre 2018 ; Michelle Mosey and Adam Henschke, « Defining thresholds in law – sophisticated decryption and law enforcement », document d'orientation nº 8, Collège de sécurité nationale, Université nationale australienne, avril 2018.

[9] G. A. Van der Steur, Ministre de la sécurité et de la justice, et H. G. J. Kamp, Ministre des affaires économiques des Pays-Bas, « Cabinets view on encryption », prise de position présentée au Président de la Chambre des représentants, 4 janvier 2016.

E. Communications

27. Le Rapporteur spécial a présenté 17 communications depuis le 22 septembre 2017, dont 8 « lettres d'allégation », 7 « autres lettres » et 2 « appels urgents ». Sur ces 17 communications, 15 ont été présentées conjointement avec d'autres titulaires de mandat et deux par lui seul.

F. Promotion du droit à la vie privée

28. Le Rapporteur spécial a collaboré avec d'autres titulaires de mandat au titre de procédures spéciales dans le cadre de communiqués de presse et de déclarations communes, et d'échanges de vues et d'informations. Il a tenu des consultations constructives avec la Rapporteuse spéciale sur la violence contre les femmes, ses causes et ses conséquences.

29. Le Rapporteur spécial a publié 11 communiqués de presse et déclarations, dont deux conjointement avec d'autres titulaires de mandat : une sur les droits des défenseurs de l'environnement en prévision de la vingt-quatrième Conférence des Parties à la Convention-cadre des Nations Unies sur les changements climatiques[10] et une sur le projet de loi concernant la sécurité[11].

30. Les 19 et 20 février 2018, le Rapporteur spécial a fait un exposé sur le rôle du droit à la vie privée dans le cadre des droits de l'homme et de la protection de l'espace civique et animé une session sur les tendances nouvelles lors de l'atelier d'experts sur le droit à la vie privée à l'ère du numérique, organisé à Genève par le Haut-Commissariat aux droits de l'homme.

G. Visites de pays

31. En juin 2018, le Rapporteur spécial s'est rendu au Royaume-Uni. Dans la déclaration qu'il a prononcée à la fin de la mission, il a formulé des observations préliminaires[12]. Le rapport final sera présenté au Conseil des droits de l'homme à sa quarantième session.

32. En 2015, le Rapporteur spécial a critiqué les projets de loi augmentant les pouvoirs de surveillance du Gouvernement du Royaume-Uni. Depuis, d'importantes améliorations ont été apportées au dispositif de contrôle des services de renseignement, notamment la création d'un commissariat des pouvoirs d'enquête disposant de moyens accrus et d'un système de double verrouillage, où cinq commissaires judiciaires à plein temps examinent les autorisations les plus sensibles signées par de hauts responsables tels que le Ministre de l'intérieur ou le Ministre des affaires étrangères. Un point positif est que ces garanties contre la surveillance arbitraire ou illégale s'appliquent de manière égale à toute personne surveillée par les autorités britanniques sur le territoire national, indépendamment de sa nationalité ou de sa résidence.

33. Le Rapporteur spécial demeure préoccupé par les lacunes que pourrait comporter la nouvelle loi de 2016 sur les pouvoirs d'enquête, notamment le fait que

---

[10] Haut-Commissariat des Nations Unies aux droits de l'homme (HCDH), « UN experts urge Poland to ensure free and full participation at climate talks », 7 mai 2018, disponible à l'adresse www.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=23042&LangID=E.

[11] HCDH, « Mexico draft security law threatens rights and should be rejected, UN rights experts warn », 14 décembre 2017, Disponible à l'adresse www.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=22535&LangID=E.

[12] Voir www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=23296&LangID=E.

le commissariat des pouvoirs d'enquête soit chargé à la fois d'autoriser la surveillance et de la superviser, ce qui peut nuire à l'indépendance du contrôle a posteriori.

34. Le Rapporteur spécial a estimé qu'il fallait des directives plus claires concernant tout accord de partage de données au Service national de santé et un contrôle plus strict en la matière, et recommandé vivement que ces directives soient publiées dans les meilleurs délais. Il ressort de discussions avec le National Data Guardian qu'elles pourraient être publiées dans les 12 à 24 mois. Le Rapporteur spécial a recommandé que le rôle du Data Guardian soit légalement défini le plus rapidement possible.

35. Dans la déclaration qu'il a prononcée à la fin de sa mission, le Rapporteur spécial a également traité des mesures de lutte contre la radicalisation et du programme Prevent et de leurs incidences sur les musulmans ; des propositions de criminaliser l'accès aux contenus extrémistes ; et de questions soulevées par les organisations de la société civile.

Visites de pays prévues

36. La prochaine visite officielle est prévue en Allemagne, du 29 octobre au 9 novembre 2018, et sera précédée d'un appel à contributions de parties intéressées, sur la page Web du Haut-Commissariat consacrée au titulaire de mandat.

Visites informelles et manifestations internationales

37. Alors qu'il était en Australie à l'occasion des consultations sur les mégadonnées et les données ouvertes, le Rapporteur spécial s'est rendu dans trois États et s'est entretenu avec des membres d'organisations de la société civile, un membre du Gouvernement, le porte-parole de l'opposition pour la justice, des fonctionnaires gouvernementaux, des représentants d'entreprises et d'associations professionnelles, des universitaires et d'autres personnes. Il a également rencontré le Commissaire australien aux droits de l'homme et Président de la Commission, et donné des conférences publiques à l'université de Nouvelle-Galles du Sud, à Sydney ; à l'université de Melbourne ; à l'université de La Trobe ; et à l'université Edith Cowan. Le Cyber Security Hub de l'université Optus Macquarie a organisé une séance d'information avec le Rapporteur spécial et les principales sociétés cotées en bourse. La section Australie et Nouvelle-Zélande de l'Association internationale des professionnels de la protection de la vie privée (iappANZ) a organisé des réunions avec des praticiens de la protection de la vie privée.

38. Le Rapporteur spécial a également participé à la seizième Conférence internationale sur le cyberespace, tenue en Tchéquie en novembre 2017 ; à la onzième Conférence internationale sur les ordinateurs, la vie privée et la protection des données, tenue à Bruxelles en janvier 2018 ; à un atelier d'experts sur le droit à la vie privée à l'ère du numérique, tenu à Genève en février 2018 ; à la Conférence mondiale d'Internet And Jurisdiction, tenue à Ottawa en février 2018 ; et à la Conférence MAPPING tenue à Malte en février 2018.

H. Faits nouveaux concernant le droit à la vie privée

Possibilité de demander réparation

39. Le Rapporteur spécial a continué d'appeler l'attention d'États Membres concernés sur des allégations de violations du droit à la vie privée et, dans son rapport de 2018, a signalé au Conseil des droits de l'homme des violations de l'article 12 de la Déclaration universelle des droits de l'homme et de l'article 17 du Pacte international relatif aux droits civils et politiques.

40. Le Rapporteur spécial reste convaincu que la réparation du préjudice causé par une atteinte à la vie privée suppose de pouvoir compter sur une procédure équitable et une possibilité de recours. La possibilité de recours est cruciale pour la protection des droits de l'homme et demeure une des priorités du Rapporteur spécial.

Intelligence artificielle

41. De plus en plus de décisions touchant la vie de toutes les personnes sont prises à l'aide d'algorithmes et de l'apprentissage automatique. Il convient donc d'évaluer soigneusement et en permanence leurs incidences sur les droits de l'homme.

42. Ces technologies sont tellement répandues qu'elles sont même utilisées comme éléments de preuve dans des procédures judiciaires. Or, on en sait peu sur la façon dont fonctionnent les algorithmes complexes et la façon dont ils se développent dans le cas de l'apprentissage automatique. Un examen de la question du point de vue des droits de l'homme doit se faire avant d'encourager ou de permettre la mise au point et le déploiement de produits fondés sur l'intelligence artificielle, ou au plus tard en même temps[13]. Des cadres juridiques et déontologiques solides sont cruciaux pour protéger les droits de l'homme concernés.

Introduction de législation sur la vie privée et la protection des données à l'échelle mondiale

43. Le nombre de pays adoptant des lois sur la protection des données et le respect de la vie privée a augmenté[14] et 2018 a été une année particulièrement active sur ce point dans le monde entier.

44. On mentionnera en Inde le projet de loi faisant suite à la décision rendue par la Cour suprême en l'affaire *Puttaswamy*[15]. Ce projet de loi, promulgué à la mi-2018, présente de nombreux éléments positifs également présents dans le Règlement 2016/679 de l'Union européenne, ou Règlement général sur la protection des données, tels que les évaluations d'impact de la protection des données, le droit à l'oubli et des sanctions effectives en cas de non-respect. Il suscite également des préoccupations, notamment pour ce qui est des restrictions concernant la recherche sur la ré-identification de personnes dans des ensembles de données prétendument anonymisés. En outre, alors que l'utilisation de données personnelles par les forces de l'ordre doit être « nécessaire et proportionnée », leur divulgation lors de procédures judiciaires ouvre la voie à de larges exceptions[16]. Le Rapporteur spécial demande instamment au Gouvernement indien de dialoguer avec les universitaires, les chercheurs et les organisations de la société civile qui soulèvent de telles questions.

45. Dans un arrêt du 26 septembre 2018, la Cour suprême indienne a confirmé la validité constitutionnelle de la loi Aadhaar, mais annulé : a) l'article 57, en vertu duquel les entreprises privées pouvaient demander aux consommateurs des informations issues du programme Aadhaar à des fins d'identification ; b) le

---

[13] Priyanar Bhunia, « Taskforce recommends establishment of national mission for coordinating AI-related activities across India », *Open Gov*, 9 avril 2018.

[14] Graham Greenleaf, « Global data privacy laws 2017: 120 national data privacy laws, including Indonesia and Turkey – 145 privacy laws and business international report 10, 2017 », University of New South Wales Law Research Series, nº 45 (2017).

[15] Cour suprême de l'Inde, juridiction civile du premier degré, *Justice K. S. Puttaswamy (Retired), and Another v. Union of India and Others*, requête nº 494 de 2012, arrêt du 24 août 2017, disponible à l'adresse http://supremecourtofindia.nic.in/pdf/jud/ALL%20WP(C)%20No.494%20of %202012%20Right%20to%20Privacy.pdf.

[16] Richard Chirgwin, « India mulls ban on probes into anonymized data use – with GDPR-style privacy laws », *The Register*, 31 juillet 2018, disponible à l'adresse www.theregister.co.uk/2018/07/31/india_privacy_boffin_ban/.

paragraphe 2 de l'article 33 sur le partage de données avec les organismes de sécurité pour raisons de sécurité nationale ; et c) l'article 47, en vertu duquel seul le Gouvernement peut intenter une action pour vol de données Aadhaar[17]. La Cour a prié le Gouvernement d'adopter une législation solide sur la protection des données.

46. Au sein de l'Union européenne, il y a eu d'importantes réformes. Le Règlement général sur la protection des données est entré en vigueur le 25 mai 2018 et une directive spécifique sur la protection des données dans les domaines de la police et de la justice, le 6 mai 2018. La Directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques doit être remplacée par un nouveau règlement en la matière[18]. Le Règlement (CE) 45/2001 énonce les règles de protection des données dans les institutions de l'Union et les devoirs du Contrôleur européen de la protection des données. La Commission européenne a adopté le 10 janvier 2017 une proposition abrogeant le Règlement et l'alignant sur le Règlement général sur la protection des données ; ces deux mesures devraient s'appliquer à partir de la fin de 2018. Par cette réforme, l'Union européenne va achever la première grande modernisation de son cadre de protection de la vie privée et de protection des données en plus de 20 ans[19].

47. Ces importantes mesures de consolidation au sein de l'Union européenne s'appliquent à tous les secteurs, sauf à la vie privée et à la « sécurité nationale », matière exclue de la compétence de l'Union en vertu du paragraphe 2 de l'article 4 du Traité sur l'Union européenne. La surveillance qui relève de la sécurité nationale et non du maintien de l'ordre est réglementée de manière beaucoup plus disparate au sein de l'Union par l'action que mènent des pays comme la Belgique, la France, les Pays-Bas et le Royaume-Uni pour actualiser leur législation.

48. À un niveau régional plus large, il est encourageant de noter que la version modernisée de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (ou « Convention 108 modernisée ») a été achevée en juin 2018 et que le Protocole d'amendement (STCE 223) a été ouvert à la signature le 10 octobre 2018. C'est une étape importante car, à la différence du Règlement général sur la protection des données, la Convention porte également sur la sécurité nationale et été ratifiée par plus de 55 États Membres de l'ONU, dont un nombre croissant d'États non européens.

49. Au Brésil, le Sénat a approuvé une loi générale de protection des données qui entrera en vigueur en février 2020. Elle porte principalement[20] sur la juridiction transfrontière ; les principes de protection de la vie privée et l'approche fondée sur le risque ; les nouveaux droits pour les individus ; davantage de bases juridiques pour le traitement des données à caractère personnel ; la cartographie des données et les études d'impact sur la protection des données ; la notification obligatoire des violations et un responsable de la protection des données ; et les restrictions au transfert transfrontière des données personnelles.

---

[17] Cour suprême de l'Inde, juridiction civile du premier degré, *Justice K. S. Puttaswamy (Retired), and Another v. Union of India and Others* ; *Economic Times*, « This is what the Supreme Court did not like about Aadhaar », 26 septembre 2018, disponible à http://economictimes.indiatimes.com/articleshow/65961697.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst.

[18] Voir Commission européenne, « Proposition de règlement du Parlement européen et du Conseil concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE (règlement "vie privée et communications électroniques") », 10 janvier 2017.

[19] Voir https://edps.europa.eu/data-protection/data-protection/legislation_fr.

[20] Voir www.onetrust.com/what-is-the-brazil-general-data-protection-law-lgpd/.

50. Le non-respect des dispositions peut entraîner des amendes s'élevant à 2 % du montant brut des ventes de la société ou du groupe de sociétés en cause ou à un montant maximum de l'ordre de 12,9 millions de dollars par infraction.

Peuples autochtones et données

51. Le Rapporteur spécial étudie la culture de la vie privée des aborigènes australiens depuis de nombreuses années. Étant donné que la vie privée y connaît l'une de ses formes les plus sophistiquées, exprimée au niveau individuel, familial et collectif par des comportements, des rites et des pratiques telles que les espaces privés et communautaires, le Rapporteur spécial se félicite de ce que la consultation sur les mégadonnées et les données ouvertes ait également porté sur la souveraineté des données autochtones, bien que de façon modeste.

52. Le Rapporteur spécial engage les gouvernements et les entreprises à reconnaître la souveraineté inhérente des peuples autochtones sur les données les concernant ou recueillies auprès d'eux, qui relèvent de leurs systèmes de connaissances, coutumes ou territoires.

II. Consultations autour du rapport précédent du Rapporteur spécial à l'Assemblée générale

53. Dans le rapport qu'il a présenté en octobre 2017 à l'Assemblée générale (A/72/540), le Rapporteur spécial a passé en revue les problèmes que pose la garantie du respect du droit à la vie privée dans le contexte créé par les deux principales caractéristiques de l'ère numérique que sont les mégadonnées et les données ouvertes. Depuis lors, le Règlement général sur la protection des données a été promulgué et l'affaire impliquant Facebook et la société Cambridge Analytica a été révélée.

54. Des consultations sur le rapport se sont tenues en Australie avec des responsables gouvernementaux, des organisations de la société civile, des entreprises et des particuliers, les 26 et 27 juillet 2018. En amont de celles-ci, un appel à participations avait été lancé : il a été clos le 28 avril 2018 et les contributions ont été résumées en vue des consultations. Des contributions supplémentaires ont été obtenues lors de réunions avec des organisations de la société civile, organisées par l'Australian Privacy Foundation et grâce aux communications reçues après les consultations.

A. Résumé des observations reçues

55. Lors des consultations publiques, un certain nombre d'éléments ont été examinés : les origines et les utilisations des mégadonnées et des données ouvertes ; les avantages et les effets nocifs potentiels de chacun de ces types de données ; l'incidence de l'utilisation des données personnelles sur d'autres droits de l'homme ; l'adéquation des techniques de désidentification ; les bonnes pratiques concernant l'utilisation des données personnelles ; l'importance des droits de l'homme et de l'éthique dans les technologies automatisées de prise de décisions ; la souveraineté des peuples autochtones sur les données les concernant ; les questions liées aux consommateurs et à la problématique femmes-hommes ; et les points de vue des pays non européens[21]. Une grande partie des débats ont concerné les données ouvertes et les conséquences pour la vie privée de leur interaction avec les mégadonnées.

[21] Amanda Lo, « The Right to Privacy in the Age of Big Data and Open Data », The Allens Hub for Technology, Law and Innovation, Université de Nouvelle-Galles du Sud, 21 août 2018.

B. Données ouvertes

56. Si elles offrent des avantages, l'analyse des mégadonnées et les techniques de calcul fondées sur l'intelligence artificielle créent des risques potentiels pour la confidentialité des informations relatives à des individus et à des communautés, et pour le tissu même des sociétés démocratiques. L'ouverture des informations détenues par les autorités publiques, en particulier la divulgation répétée d'ensembles de données contenant des informations personnelles, doit faire l'objet d'un examen plus nuancé et plus approfondi[22].

57. Au cours des consultations, la proposition selon laquelle l'analyse des mégadonnées pouvait révéler l'identité des personnes en dépit de la désidentification a été examinée[23]. Les participants ont entendu des exposés expliquant que la réponse à la question de savoir si des données ou les résultats d'un projet d'analyse de données contenaient des informations personnelles dépendait des circonstances de l'utilisation ou de la divulgation des données en question et que d'autres facteurs pouvaient faire évoluer la situation. Par conséquent, il est préférable de décrire la ré-identification en termes de niveaux de risque plutôt que comme un absolu. La détermination des niveaux de risque tient compte de plusieurs facteurs : qui a accès aux données en question, quel est le niveau de granularité des données (la taille du plus petit élément dans ces données), quels autres ensembles de données peuvent être correctement reliés aux données en question et quel est le contexte extérieur associé.

58. L'expression « informations personnelles » appliquée aux données recouvre un champ très vaste et les définitions qui y sont rattachées varient d'une juridiction à l'autre. La plupart des définitions s'accordent cependant sur le fait que la portée du terme peut être très large, et qu'il s'agit de savoir si les données donnent la possibilité d'identifier une personne, pas seulement si les données en elles-mêmes identifient la personne.

59. Pour déterminer si des données contiennent des informations personnelles, deux aspects sont fondamentaux : a) soit les données en elles-mêmes permettent d'identifier une personne ; b) soit il est raisonnablement possible d'identifier une personne à partir des données en question.

60. À chacun des trois principaux mécanismes de partage de données (explicite, dérivé et induit) correspondent des considérations relatives au niveau d'informations personnelles contenues, ainsi que des obligations s'appliquant à l'organisation qui saisit, utilise et conserve ces données.

61. Les données relatives à la consultation de contenus et aux achats en ligne peuvent être utilisées pour proposer des services toujours plus personnalisés sans connaître l'identité de l'utilisateur, mais des préoccupations ont été exprimées quant à la question de savoir si des éléments d'identification anonymes mais extrêmement ciblés ne constituaient pas des informations personnelles. Les données relatives au réseau mobile ont été utilisées à des fins allant au-delà de l'optimisation du réseau, notamment pour prévoir le taux d'attrition des clients et même pour révéler les relations entre les divers utilisateurs du réseau mobile sans connaître l'identité des personnes concernées[24].

---

[22] Contribution de M. Paterson, Monash University, août 2018.

[23] Voir Bureau du Commissaire à l'information de l'État de Victoria, « Protecting unit-record level personal information: the limitations of de-identification and the implications for the Privacy and Data Protection Act 2014 », mai 2018. Document disponible à l'adresse https://ovic.vic.gov.au/resource/protecting-unit-record-level-personal-information/.

[24] Contribution de Ian Opperman, Centre de l'analyse des données du Gouvernement de Nouvelle-Galles du Sud, Australie, 31 août 2018.

62. L'un des principaux problèmes qui se posent en matière de partage de données est qu'il n'existe actuellement aucun moyen de déterminer avec certitude si des informations personnelles figurent dans des données agrégées, ou si des données désagrégées pourront à nouveau être regroupées. Le risque de ré-identification dépend de l'accès à des ensembles de données connexes (et de l'aptitude à les relier), des techniques de désidentification utilisées et du niveau d'agrégation ou de perturbation des données. En conséquence, les organisations recourent à différentes techniques et à différents niveaux d'agrégation des données en fonction de la façon dont elles perçoivent le risque associé aux données qui sont partagées.

63. Il serait utile de mettre au point des normes permettant de déterminer ce qui constitue des données « désidentifiées » pour s'attaquer aux problèmes liés à la protection de la vie privée. Au niveau international, il n'existe actuellement que des directives de très haut niveau, et en tous cas rien sur le plan quantitatif, sur la signification du terme « désidentifié » ; par conséquent, de nombreuses organisations doivent fixer leur propre définition du terme, au cas par cas, en fonction des différents ensembles de données qu'elles gèrent et de la manière dont ces ensembles peuvent raisonnablement être utilisés ou combinés avec d'autres données.

64. En 2017, la Australian Computer Society a publié un livre blanc dans lequel elle s'est penchée sur les défis entourant le partage de données et a souligné qu'une des difficultés fondamentales en matière de création de services intelligents était la question de savoir si un ensemble de données contenait ou non des informations personnelles. Répondre à cette question est un défi majeur sachant que le fait de combiner des ensembles de données crée des informations. Les auteurs du livre blanc y proposent en outre une version modifiée des cinq principes de sécurité, ou cadre « Five safes », qui vise à réglementer le partage de données, en suggérant différents seuils mesurables de sécurité. Ce travail, qui se poursuit avec l'appui de l'organisation Standards Australia, vise à s'atteler à la création de normes internationales relatives à la protection de la vie privée et au partage de données. Un deuxième livre blanc, prévu pour octobre 2018, devrait constituer la base des activités de normalisation au niveau international, le but étant à terme de définir des cadres solides en matière de protection de la vie privée et de partage de données[25].

65. Un exemple des limites de la désidentification s'agissant de la protection des données unitaires a été la publication en ligne, en août 2016, d'un vaste ensemble de données longitudinales concernant un échantillon de 10 % des Australiens ayant bénéficié de l'assurance maladie Medicare depuis 1984 ou de prestations pharmaceutiques depuis 2003[26]. Les données médicales d'environ 2,9 millions d'Australiens ont été concernées, y compris les ordonnances, les interventions chirurgicales, les tests (sans les résultats) et les consultations chez des médecins généralistes et des spécialistes (sans les observations des médecins)[27]. L'ensemble de données avait été téléchargé 1 500 fois avant d'être mis hors ligne à la suite

[25] Ibid., y compris Australian Computer Society, *Data Sharing Frameworks*, livre blanc technique, Sydney, 2017. Texte disponible en anglais à l'adresse www.acs.org.au/content/dam/acs/acs-publications/ACS Data-Sharing-Frameworks_FINAL_FA_SINGLE_LR.pdf.

[26] Contribution de Vanessa Teague au Rapporteur spécial pendant les consultations sur le thème des mégadonnées et des données ouvertes, tenues les 26 et 27 juillet 2018, à l'Université de Nouvelle-Galles du Sud à Sydney. Voir aussi Bureau du Commissaire australien à l'information, « Publication of MBS/PBS data », rapport d'enquête établi à l'initiative du Commissaire, 20 mars 2018, p. 7 à 9. Texte disponible en anglais à l'adresse www.oaic.gov.au/resources/privacy-law/commissioner-initiated-investigation-reports/0publication-of-mbs-pbs-data.pdf.

[27] Vanessa Teague, Chris Culnane et Ben Rubinstein, « The simple process of re-identifying patients in public health records », Université de Melbourne, publication *Pursuit*, 18 décembre 2017. Texte disponible en anglais à l'adresse https://pursuit.unimelb.edu.au/articles/the-simple-process-of-re-identifying-patients-in-public-health-records.

d'informations indiquant que les identifiants des médecins pouvaient facilement être décryptés[28] et, par la suite, que les patients pouvaient être identifiés[29]. La publication, effectuée par le Ministère australien de la santé, visait à faciliter la recherche médicale.

66. Ces exemples soulèvent un certain nombre de questions importantes, et notamment les suivantes : faut-il publier en externe des ensembles de données détenus par les autorités publiques et contenant des informations personnelles alors qu'il existe des risques croissants d'atteintes à la vie privée à grande échelle en raison de la ré-identification, elle-même rendue possible, en partie, par la disponibilité d'autres informations rendues publiques et par le fait que les organisations ne disposent pas de moyens technologiques adéquats ; une autre question importante est celle de savoir quelle réponse permettrait d'éviter la répétition de tels incidents.

67. Il est clairement ressorti des informations recueillies lors des consultations que la publication d'informations détenues par les autorités publiques nécessite l'adoption de mesures de protection de la vie privée et de mesures réglementaires adéquates. Plusieurs participants ont estimé, de façon catégorique, que l'accès sans restriction à des données unitaires ainsi qu'à d'autres données personnelles ne pouvant être divulguées en toute sécurité sous forme agrégée, est incompatible avec le droit à la vie privée. L'idée d'instaurer des mesures réglementaires reposant sur la criminalisation des procédures de ré-identification effectuées pour tester la sécurité des ensembles de données publiés a reçu un accueil défavorable[30].

68. Les participants ont décrit des mécanismes existants qui permettent l'utilisation de données personnelles identifiables à des fins de recherche[31], en faisant valoir que le recours à ces mécanismes pourrait être élargi, selon qu'il conviendra, à de nouvelles utilisations d'intérêt public[32].

69. Il semblerait que la question soit de savoir si nous aurions des pratiques plus durables si les données utiles étaient considérées comme une ressource limitée plutôt que comme une ressource illimitée et inexploitée[33].

70. Les pratiques actuelles qui dépossèdent de tout pouvoir le sujet sur lequel portent les données ont été décrites métaphoriquement comme le fait de « tuer la poule aux œufs d'or », étant donné que la méfiance concernant la capacité des autorités publiques ou des acteurs privés à gérer de façon appropriée les informations personnelles pousse les populations soit à s'abstenir d'utiliser les services proposés – phénomène qui à son tour expose au risque d'impacts sociaux néfastes, comme par exemple en matière de santé publique –, soit à fournir des informations incomplètes

---

[28] Chris Culnane, Benjamin Rubinstein et Vanessa Teague « Health data in an open world », rapport sur la ré-identification des patients dans l'ensemble de données MBS/PBS et sur son incidence sur les publications de données du Gouvernement australien à l'avenir, Université de Melbourne, 18 décembre 2017. Document disponible à l'adresse https://arxiv.org/ftp/arxiv/papers/1712/1712.05627.pdf.

[29] D'après les constatations du Bureau du Commissaire australien à l'information, les médecins étaient identifiables et les patients pouvaient également être identifiés, sans pour autant être « raisonnablement identifiables » selon les termes de la loi australienne sur la vie privée (*Australian Privacy Act*). Les personnes touchées n'en ont apparemment pas été informées.

[30] Contributions de M. Paterson, entre autres.

[31] Ces mécanismes sont en général placés sous la supervision de comités d'éthique et l'accès est limité à des chercheurs soumis à une obligation de confidentialité.

[32] Il s'agirait, par exemple, de se fonder sur des cadres tels que les cinq principes de sécurité : voir Bureau de statistique australien, « Managing the risk of disclosure: the five safes framework », Confidentiality Series, partie 3, août 2017. Texte disponible en anglais à l'adresse www.abs.gov.au/ausstats/abs@.nsf/Latestproducts/1160.0Main%20Features4Aug%202017?opendocument&tabname=S.

[33] Contribution de Theresa Dirndorfer Anderson, University of Technology, Sydney.

ou inexactes[34]. Ces actions sapent également la qualité des données et, en fin de compte, la précision des algorithmes d'apprentissage automatique.

71. Une écrasante majorité des participants aux consultations a estimé que les pratiques de gestion des données sont beaucoup plus durables si les sujets concernés sont reconnus comme des partenaires à part entière dans les opérations relatives à ces données[35]. Comme les participants ont pu l'entendre, la meilleure illustration de l'évidence et de l'importance de cette idée est le cas des peuples autochtones.

C. Souveraineté des peuples autochtones sur les données les concernant

72. Les données constituent une ressource culturelle, stratégique et économique pour les peuples autochtones. Or, ces peuples demeurent largement tenus à l'écart de la collecte, de l'utilisation et de l'application des données les concernant ou concernant leurs terres et leurs cultures[36]. Les données et infrastructures de données existantes ne prennent pas en compte et ne mettent pas en valeur les connaissances et la vision du monde des peuples autochtones ; elles ne répondent par ailleurs pas aux besoins actuels et futurs de ces populations en matière de données. Les pratiques actuelles en matière de gestion des mégadonnées et des données ouvertes, que ce soit sous l'égide des autorités publiques ou des entreprises, éloigneront sans doute encore plus les intérêts des peuples autochtones en matière de données des instances qui prennent des décisions ayant une incidence sur les données relatives à ces peuples.

73. Le mouvement en faveur de la souveraineté des peuples autochtones sur les données les concernant est un mouvement mondial qui vise à défendre les droits de ces peuples d'avoir accès aux données qui émanent d'eux et qui ont trait à leurs membres, à leurs systèmes de connaissances, à leurs coutumes et à leurs territoires et de les posséder et de les contrôler[37]. Il se fonde sur les droits des peuples autochtones à l'autodétermination et à la gouvernance de leurs terres, de leurs territoires et de leurs cultures, droits consacrés dans la Déclaration des Nations Unies sur les droits des peuples autochtones. La défense de cette souveraineté a pour corollaire implicite la volonté de faire en sorte que les données soient utilisées d'une manière qui soutienne et améliore le bien-être collectif des peuples autochtones.

74. La souveraineté des peuples autochtones sur les données les concernant doit être un principe qui sous-tend les dispositifs de gouvernance relatifs aux mégadonnées et aux données ouvertes. La mise en pratique de ce principe passe par l'instauration d'un dispositif de gouvernance des données par les peuples autochtones, fondé sur des principes, des structures, des mécanismes de responsabilisation, des politiques relatifs

---

[34] Bureau du Commissaire australien à l'information, *Australian Community Attitudes to Privacy Survey, 2017*, Canberra, 2017. Texte disponible en anglais à l'adresse www.oaic.gov.au/engage-with-us/community-attitudes/australian-community-attitudes-to-privacy-survey-2017 ; Bureau du Commissaire australien à l'information, *Community Attitudes to Privacy Survey: Research Report 2013*, Canberra, 2013. Texte disponible en anglais à l'adresse www.oaic.gov.au/images/documents/privacy/privacy-resources/privacy-reports/2013-community-attitudes-to-privacy-survey-report.pdf.

[35] Contribution de Theresa Dirndorfer Anderson.

[36] Tahu Kukutai et Maggie Walter, « Recognition and indigenizing official statistics: reflections from Aotearoa New Zealand and Australia », *Statistical Journal of the IAOS*, vol. 31, nº 2 (2015).

[37] Tahu Kukutai et John Taylor, « Data sovereignty for indigenous peoples: current practice and future needs » et C. Matthew Snipp, « What does data sovereignty imply: what does it look like? » *in* Kukutai et Taylor (dir.), *Indigenous Data Sovereignty: Towards an Agenda*, Research Monograph, 2016/38, Canberra, Australian University Press, 2016. Texte disponible en anglais à l'adresse https://press.anu.edu.au/publications/series/centre-aboriginal-economic-policy-research-caepr/indigenous-data-sovereignty.

à la gouvernance des données, à la protection de la vie privée et à la sécurité, ainsi que sur des instruments juridiques. Les cadres de protection de la souveraineté des peuples autochtones sur les données les concernant peuvent s'appliquer aux données contrôlées en interne et appartenant aux nations ou tribus, ainsi qu'aux données conservées ou gérées en externe. En Australie et en Nouvelle-Zélande, les réseaux de défense de la souveraineté des peuples autochtones sur les données les concernant travaillent à l'élaboration de protocoles relatifs à cette question de la gouvernance autochtone[38].

75. Le concept de souveraineté autochtone sur les données montre que les bonnes pratiques en matière de mégadonnées et de données ouvertes exigent une prise de conscience s'agissant des données manquantes, sous-représentées ou mal représentées[39], ainsi que des intérêts servis, ou non, par ces pratiques.

D. Questions relatives à la problématique femmes-hommes

76. Les participants aux consultations ont pu entendre que le concept de vie privée peut avoir une signification différente selon le sexe ou l'identité de genre d'une personne.

77. La notion d'intimité est une préoccupation qui revêt une importance toute particulière pour les lesbiennes, les gays, les bisexuels, les transgenres et les personnes intersexes, par exemple, et son respect peut par ailleurs être crucial pour assurer la sécurité des personnes, généralement des femmes, qui fuient des violences familiales, domestiques ou religieuses.

78. Si les pratiques de collecte de données fondées sur l'inclusion promeuvent l'acceptation et le respect, les pratiques de collecte intrusives peuvent constituer un obstacle important à l'accès aux services, étant donné que les lesbiennes, gays, bisexuels, transgenres, les personnes en questionnement et les personnes intersexes et d'autres se préoccupent légitimement de la protection de leur vie privée à la suite d'expériences d'actes de discrimination, de stigmatisation et de violence ciblée.

79. Cette question sera examinée plus avant par l'équipe spéciale chargée du droit à la vie privée et de la personnalité. Toutefois, en ce qui concerne les mégadonnées et les données ouvertes, les bonnes pratiques nécessitent l'examen de la façon dont les données sont collectées et une prise de conscience quant aux incidences possibles des mauvaises pratiques en termes de respect du droit à la vie privée et des conséquences particulières qu'elles peuvent avoir selon le sexe ou l'identité de genre des personnes concernées.

E. Droits des consommateurs et collecte et utilisation des données personnelles

80. Dans un monde où les marchés de consommation reposent sur la gestion de données, l'utilisation de plus en plus massive qui est faite de celles-ci aux fins de l'élaboration, de la vente et de la promotion de produits de consommation fait que de nombreuses questions relatives à la protection des données aussi deviennent des questions relatives à la protection du consommateur, et vice-versa. La distinction entre le droit de la consommation et la législation relative à la protection des données tend désormais à s'estomper[40].

---

[38] Contribution de Maggie Walter, Université de Tasmanie, Australie.

[39] Contribution de Theresa Dirndorfer Anderson.

[40] Natali Helberger, Frederik Zuiderveen Borgesius et Agustin Reyna, « The perfect match? A closer

81. L'utilisation des données personnelles des consommateurs dans le cadre de services financiers et d'autres secteurs a fait naître des inquiétudes tant au niveau des politiques publiques qu'au niveau individuel[41]. Le traitement approprié des données personnelles occupe une place de plus en plus importante dans les attentes raisonnables que peuvent avoir les consommateurs concernant les services et produits qu'ils utilisent[42].

82. Au cours des consultations, les participants ont comparé l'approche axée sur le droit de la consommation et celle axée sur la législation relative au respect de la vie privée et à la protection des données, en notant que certains pays mettaient en place des initiatives visant à protéger la vie privée des consommateurs.

83. À la suite du scandale impliquant Cambridge Analytica, l'État de Californie (États-Unis) a promulgué en juin 2018 la loi sur la protection de la vie privée des consommateurs (*Consumer Privacy Act*) qui doit prendre effet en janvier 2020 : l'objectif est de protéger la confidentialité des données des utilisateurs d'applications technologiques, entre autres, en imposant de nouvelles règles aux entreprises qui collectent, utilisent et partagent des données personnelles[43]. La loi proclame quatre droits individuels fondamentaux : une personne a le droit de savoir de quelles informations personnelles la concernant une entreprise dispose, d'où proviennent ces informations et à qui elles ont été transmises ; elle a le droit de supprimer des informations personnelles la concernant qu'une entreprise a collectées auprès d'elle ; elle a le droit de s'opposer à la vente des informations personnelles la concernant ; enfin, elle a le droit de bénéficier des mêmes services et tarifs que les autres utilisateurs d'une entreprise, même si elle fait valoir les droits que lui accorde la loi sur la protection de la vie privée[44]. La loi crée également un droit limité pour les consommateurs d'intenter une action en justice contre des entreprises pour atteinte à la sécurité des données, sur la base de la loi californienne existante relative à la notification des failles dans la sécurité des données.

84. Toutefois, il a été signalé que les droits consacrés par la loi doivent être renforcés, pour les raisons suivantes :

a) Le terme « entreprise » est défini de façon trop restreinte[45]. À l'ère du numérique, les petits acteurs du secteur technologique et des individus lambda peuvent eux aussi compromettre le respect de la vie privée de mille et une façons,

---

look at the relationship between EU consumer law and data protection law », *Common Market Law Review*, vol. 54 (2017).

[41] Lee Rainie et Maeve Duggan, « Privacy and information sharing », 14 janvier 2016 ; (il ressort de cette étude que le niveau de confort des utilisateurs dépend de leur perception de la fiabilité de l'entité concernée, de ce qui se passe après la collecte des données et de la durée de la conservation des données). Phuong Nguyen et Lauren Solomon, *Consumer Data and the Digital Economy – Emerging Issues in Data Collection, Use and Sharing*, Consumer Policy Research Centre, 2018 ; (il ressort de cette étude que les consommateurs souhaitent bénéficier d'un plus grand nombre d'options s'agissant du type de données collectées et de l'utilisation de ces données, et que le Gouvernement participe au renforcement du contrôle des consommateurs sur les données ainsi que des mesures de protection contre l'utilisation abusive des données).

[42] Helberger, Zuiderveen Borgesius et Reyna, « The perfect match? ».

[43] Voir https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375.

[44] Adam Schwartz, Lee Tien et Corynne McSherry, « How to improve the California Consumer Privacy Act of 2018 », Electronic Frontier Foundation, 8 août 2018.

[45] Ibid. ; la loi définit une entreprise comme une personne morale à but lucratif qui : i) perçoit un revenu brut annuel d'au moins 25 millions de dollars ; ii) reçoit ou publie chaque année des informations personnelles concernant au moins 50 000 consommateurs, ménages ou appareils ; iii) tire au moins 50 % de ses revenus annuels de la vente d'informations personnelles [sect. 140 c)].

faute de disposer des connaissances, des compétences ou des ressources nécessaires à la mise en œuvre de mesures adéquates de protection des données[46] ;

b) Les entreprises peuvent toujours facturer un prix plus élevé aux utilisateurs qui font valoir leurs droits en matière de protection de la vie privée ;

c) Il est très difficile pour les utilisateurs de poursuivre en justice les contrevenants, à quelques rares exceptions près ;

d) Le consentement des utilisateurs n'est requis que pour la vente de données, et pas pour la collecte de celles-ci, et les utilisateurs doivent s'opposer expressément à la vente des données les concernant ;

e) Le « droit de savoir » ne permet pas d'obtenir des sources et des bénéficiaires précis, et le « droit de suppression » concerne les informations collectées auprès des utilisateurs uniquement, et non l'ensemble des informations les concernant détenues par l'entité concernée ;

f) La responsabilité de faire respecter la loi incombe pour la plus grande partie au Procureur général de Californie, et non pas à une entité indépendante.

85. En vertu du droit relatif à la protection des données de l'Union européenne, certains aspects du Règlement général sur la protection des données prévoient de nouvelles protections pour les consommateurs de l'Union européenne, en instaurant notamment une transparence et un contrôle des données collectées à leur sujet par des sociétés plus importants que ceux prévus par les directives de l'Union européenne sur la protection des consommateurs[47].

86. L'Australie travaille à l'établissement d'un « droit des consommateurs en matière de données », un droit relatif à la portabilité des données[48] qui reste en deçà des protections plus générales fournies en vertu des lois de protection de la vie privée ou des données pour les consommateurs australiens dont les données sont collectées, partagées et utilisées au quotidien[49]. Les participants aux consultations ont entendu que ce droit relatif à la portabilité des données, au lieu de protéger les données des consommateurs, risquait au contraire de les exposer à être plus largement utilisées par des tierces parties[50].

87. Il y a un avantage à établir un lien étroit entre le droit de la consommation et la législation relative à la protection de la vie privée, par exemple dans le cadre d'une action en justice coordonnée[51]. Le droit de la consommation peut être utile pour préserver l'équilibre général dans la relation commerciale entre le consommateur et le fournisseur et peut permettre d'évaluer le caractère équitable dans des situations où les sociétés exigent des consommateurs qu'ils consentent au traitement de volumes de données disproportionnés ou au partage de données avec des tierces parties.

---

[46] Contribution de Roland Wen, Université de Nouvelle-Galles du Sud, Sydney.

[47] Helberger, Zuiderveen Borgesius et Reyna, « The perfect match? ».

[48] Commission australienne de la concurrence et de la protection du consommateur, « Consumers' right to their own data is on its way », communiqué de presse, 16 juillet 2018. Texte disponible en anglais à l'adresse https://www.accc.gov.au/media-release/consumers-right-to-their-own-data-is-on-its-way.

[49] Nguyen et Solomon, *Consumer Data and the Digital Economy*.

[50] Contribution de Katherine Kemp, soumise au Rapporteur spécial pendant les consultations sur les mégadonnées et les données ouvertes, tenues les 26 et 27 juillet 2018, à l'Université de Nouvelle-Galles du Sud à Sydney.

[51] Des groupes de consommateurs des États-Unis et de l'Union européenne ont conjointement demandé à des organismes de protection du consommateur et aux autorités chargées de la protection des données d'examiner les infractions en matière de protection des données et au regard du droit de la consommation découlant de l'utilisation de jouets connectés. Helberger, Zuiderveen Borgesius et Reyna, « The perfect match? ».

88. Parmi les observations recueillies sur des mesures pratiques visant à aider les entités à améliorer leur relation de confiance avec les utilisateurs, il a été suggéré d'indiquer les conditions de l'utilisation des données au moyen de licences standard semblables aux six licences standardisées Creative Commons. On a fait valoir que cela permettrait de simplifier certains des problèmes liés aux politiques complexes régissant la protection de la vie privée, tout en facilitant et en harmonisant les méthodes utilisées pour communiquer avec les utilisateurs dans différents pays[52]. Les licences types pourraient être assorties de politiques de confidentialité plus détaillées présentant les « conditions contractuelles ».

89. La mise en place d'un système de notation des risques en matière de confidentialité pourrait faciliter les choix des consommateurs en matière de confidentialité des informations et aider les autorités chargées du contrôle des données à communiquer sur les risques relatifs à la vie privée de façon plus transparente et plus efficace[53].

F. Intelligence artificielle

90. L'apprentissage automatique et l'intelligence artificielle utilisent d'énormes quantités de données et créent à leur tour davantage de données. La combinaison de la disponibilité des données, de la puissance de calcul et des capacités d'analyse à l'aide d'algorithmes sophistiqués, couplée à l'apprentissage automatique et à l'intelligence artificielle, a le potentiel de révolutionner les sociétés de manière positive, mais pourrait également changer en profondeur notre monde, et pas nécessairement dans le bon sens, puisque cela pourrait même compromettre nos chances de survie[54].

91. Ce dernier scénario pourrait résulter de l'impact négatif potentiel de l'intelligence artificielle sur les droits de l'homme, y compris le droit à la vie privée. Les méthodes d'intelligence artificielle peuvent être et sont utilisées pour identifier des personnes qui souhaitent rester anonymes ; pour permettre le microciblage des messages ; pour produire, à partir de données non sensibles, des informations sensibles concernant des personnes ; aux fins du profilage de certaines personnes sur la base des données démographiques ; et pour prendre des décisions sur la base de ces données, ce qui a des répercussions profondes sur la vie des personnes[55].

92. Étant donné que de plus en plus de mesures et de décisions sont transférées aux machines, il est urgent de veiller à la transparence de la logique et des hypothèses sur lesquelles reposent l'apprentissage automatique et les algorithmes. Les algorithmes utilisés dans l'apprentissage automatique et l'intelligence artificielle sont de plus en plus complexes, et la transparence sera difficile à atteindre. Cela étant, cette complexité ne doit pas empêcher de procéder à des vérifications pour s'assurer de la légalité des procédés mis en œuvre[56]. À l'heure actuelle, l'utilisation des technologies liées aux mégadonnées ne fait pas l'objet d'un contrôle suffisant en ce qui concerne le respect du droit international des droits de l'homme, des règles de protection des

---

[52] Présentation du Allens Hub for Technology, Law and Innovation, 14 août 2018.

[53] Voir Lorrie Faith Cranor, « Necessary but not sufficient: standardized mechanisms for privacy notice and choice », *Journal on Telecommunications and High Technology Law*, vol. 10, n° 2 (été 2012).

[54] Toby Walsh, *2062: The World that AI Made*, Carlton, Victoria, Australie, La Trobe University Press, 2018.

[55] Privacy International et Article 19, « Privacy and freedom of expression in the age of artificial intelligence », avril 2018.

[56] Agence des droits fondamentaux de l'Union européenne, *#BigData: Discrimination in Data Supported Decision Making*, Luxembourg, Office des publications de l'Union européenne, 2018.

données, des réglementations sectorielles de protection de la vie privée, des codes de déontologie ou des normes sectorielles[57]. Il a été avancé que les machines devraient être soumises à des normes éthiques plus strictes que celles auxquelles sont soumis les êtres humains et que, si les bons choix sont faits, le respect de la vie privée ne sera pas une anomalie historique, mais plutôt un droit consacré sur le plan technologique[58].

93. Le Règlement général sur la protection des données limite le recours à une prise de décision automatisée à certaines circonstances, et exige que soient fournies à la personne concernée des informations relatives à l'existence d'une prise de décision automatisée, à la logique sous-jacente ainsi qu'à l'importance et aux conséquences prévues du traitement des données en question pour la personne concernée[59]. Le Règlement pose une interdiction globale des décisions fondées exclusivement sur un traitement automatisé et produisant des effets juridiques pour la personne concernée ou l'affectant de manière significative, à l'exception de quelques circonstances bien circonscrites.

94. Le Règlement définit le profilage comme le traitement automatisé de données destiné à analyser ou à prédire des éléments concernant une personne physique et pose l'obligation de veiller à la protection des données dès la conception et par défaut. Il sera obligatoire de procéder à des études d'impact sur la confidentialité des données dans le cas de nombreuses applications d'intelligence artificielle et d'apprentissage automatique susceptibles de porter atteinte à la vie privée et tombant sous le coup de la législation relative à la protection des données, et dont l'utilisation laisse entrevoir des risques potentiels importants, s'agissant par exemple du traitement de données sensibles. Dans le cas de l'intelligence artificielle, une telle étude d'impact pourrait – devrait peut-être – permettre aux entités de modéliser les effets de leurs algorithmes à peu près de la même façon que les climatologues modélisent les changements climatiques ou les phénomènes météorologiques[60].

95. L'Agence des droits fondamentaux de l'Union européenne a suggéré qu'un moyen de garantir l'application effective du principe de responsabilité pourrait être de créer des organes spéciaux qui se consacreraient exclusivement à la supervision des technologies fondées sur les mégadonnées et dont la mission se rapprocherait du rôle des autorités chargées de la protection des données[61].

96. Les moyens doivent encore être déterminés, mais il est utile de rappeler que tout au long du XX^{e} siècle l'essor des nouvelles technologies a rendu nécessaire le renforcement du droit international humanitaire[62].

G. Principes relatifs aux mégadonnées et aux données ouvertes

97. Dans son rapport d'octobre 2017, le Rapporteur spécial a évoqué l'élaboration de principes visant à réglementer l'utilisation des mégadonnées et des données ouvertes. Il est ressorti des consultations qu'une telle entreprise devrait, autant que

---

[57] Lee Rainie et Janna Anderson, *Code-Dependant: Pros and Cons of the Algorithm Age*, Pew Research Center, 2017.

[58] Walsh, *2062: The World that AI Made*.

[59] Règlement de l'Union européenne 2016/679 du 27 avril 2016 (règlement général sur la protection des données), art. 13, 14 et 22.

[60] Andrew Smith, « Franken-algorithms: the deadly consequences of unpredictable code », *The Guardian*, 30 août 2018. Texte disponible en anglais à l'adresse https://www.theguardian.com/technology/2018/aug/29/coding-algorithms-frankenalgos-program-danger ; l'auteur cite Neil F. Johnson et al., « Population polarization dynamics and next-generation social media algorithms », 16 décembre 2017. Texte disponible en anglais à l'adresse https://arxiv.org/pdf/1712.06009.pdf.

[61] Agence des droits fondamentaux de l'Union européenne.

[62] Walsh, *2062: The World that AI Made*.

possible, se fonder sur les accords internationaux sur la protection des données considérés comme représentant les « meilleures pratiques ». À l'heure actuelle, les accords en question sont le Règlement général sur la protection des données et la Convention 108 modernisée ; celle-ci émane à l'origine du Conseil de l'Europe, mais tous les États du monde ayant mis en œuvre des principes conformes à ses dispositions peuvent y accéder[63].

98. L'influence du Règlement général sur la protection des données ne s'exerce pas seulement par l'intermédiaire de textes législatifs locaux ou dans le cadre de son application extraterritoriale. Des entreprises non européennes – Microsoft étant l'exemple le plus remarquable – choisissent volontairement de respecter le Règlement dans le cadre de l'ensemble de leurs opérations commerciales, indépendamment de toute obligation juridique de le faire. Ce type d'adoption volontaire est peut-être tout aussi important que l'adoption rendue obligatoire par la loi[64].

99. Par ailleurs, les pays qui se sont dotés de lois relatives à la localisation des données de grande portée sont en train d'établir de nouvelles normes en matière de confidentialité applicables aux données collectées dans leur zone de juridiction. En Chine, la loi sur la cybersécurité introduit des restrictions applicables aux transferts transfrontières de données qui diffèrent des dispositions des régimes internationaux de protection de la vie privée, tels que le Règlement général sur la protection des données et les règles de confidentialité applicables, à titre volontaire, aux opérations transfrontières (*Cross-Border Privacy Rules*) promulguées par l'Association de coopération économique Asie-Pacifique[65]. Bien que le Règlement et la loi chinoise semblent prévoir des tests similaires concernant les transferts transfrontières, la seconde ne permet aucune dérogation, au contraire du premier[66]. En outre, la loi chinoise ne prévoit pas l'établissement de certains mécanismes prévus par le Règlement, tels que la mise en place de règles contraignantes ou de clauses standard de protection des données pour permettre à des entreprises d'obtenir une autorisation.

100. Bien qu'elles aient été élaborées indépendamment du Règlement général sur la protection des données et de la Convention 108 modernisée, les recommandations préliminaires formulées par le Rapporteur spécial dans son rapport d'octobre 2017 à l'Assemblée générale sont en adéquation avec ces instruments (voir tableau)[67]. C'est un élément qui a son importance compte tenu du contexte international au sens large : la portée de la Convention 108 modernisée ne cesse de s'étendre à l'échelle mondiale, et cet instrument comprend un grand nombre des nouveaux éléments figurant dans le Règlement[68]. Il est probable qu'au cours des cinq à dix prochaines années les effets extraterritoriaux du Règlement, combinés à l'augmentation constante du nombre des États parties à la Convention, auront une incidence importante sur le renforcement de

---

[63] Contribution de Graham Greenleaf, Université de Nouvelle-Galles du Sud, Sydney, août 2018.

[64] Graham Greenleaf, « Global convergence of data privacy standards and laws: speaking notes for the European Commission events on the launch of the General Data Protection Regulation in Brussels and New Delhi », Université de Nouvelle-Galles du Sud, Law Research Series, nº 56, 25 mai 2018. Texte disponible en anglais à l'adresse www.austlii.edu.au/au/journals/UNSWLRS/2018/56.html.

[65] Samm Sacks, Paul Triolo et Graham Webster, « Beyond the worst-case assumptions on China's cybersecurity law », billet publié sur un blog, New America, 13 octobre 2017 ; et contribution du Allens Hub for Technology, Law and Innovation, 14 août 2018.

[66] Xiaoyan Zhang, « Cross-border data transfers: CSL vs. GDPR », *The Recorder*, 2 janvier 2018 ; et contribution du Allens Hub for Technology, Law and Innovation, 14 août 2018.

[67] Contribution de Graham Greenleaf, août 2018.

[68] Depuis 2011, la portée de la Convention 108 s'est étendue : en plus des 47 États Parties qui sont également membres du Conseil de l'Europe, des demandes d'adhésion ont été reçues des pays suivants : Argentine, Burkina Faso, Cabo Verde, Maroc, Maurice, Mexique, Sénégal, Tunisie et Uruguay. Onze autres pays, ou leurs autorités chargées de la protection des données, sont des observateurs au Comité consultatif instauré par le mécanisme de la Convention.

la culture de la protection de la vie privée à l'échelle mondiale. La nature précise de cette évolution n'est pas encore connue, de même qu'on ne sait pas encore dans quelle mesure cette évolution rendra nécessaire la prise de nouvelles mesures, comme l'élaboration de principes autonomes concernant les mégadonnées et les données ouvertes.

101. Si l'établissement d'un cadre international réglementant de manière cohérente l'utilisation des mégadonnées et des données ouvertes est nécessaire, il serait prématuré d'entamer des travaux sur la formulation de principes portant spécifiquement sur ces types de données avant que suffisamment de temps se soit écoulé pour que l'on puisse s'assurer de la solidité et de l'incidence au niveau international du Règlement général sur la protection des données et de la Convention 108 modernisée.

102. Par conséquent, les recommandations relatives aux mégadonnées et aux données ouvertes doivent être lues à la lumière des principes de protection de la vie privée et des données existants, et non pas comme de nouvelles règles spécifiques.

Recommandations formulées par le Rapporteur spécial dans son rapport d'octobre 2017 et correspondance de celles-ci avec le Règlement général sur la protection des données et la Convention 108 modernisée

Paragraphe du rapport d'octobre 2017 du Rapporteur spécial (A/72/540)	*Section du Règlement général sur la protection des données de l'Union européenne*	*Article de la Convention 108 modernisée*
131 a), sur la responsabilité	Art. 5, par.2 « Responsabilité »	10, par. 1
131 b), sur la transparence	Art. 12 « Transparence » ; art. 22, par. 3 « Décision automatisée » et transparence	5, par. 4 ; 8, par. 1
131 c), sur la qualité	Art. 5, par. 1 c) « Minimisation des données » et d) « exactitude »	5, par. 1
131 d), sur la prévisibilité des résultats en cas d'apprentissage automatisé	Art. 22 « Décision automatisée »	8, par. 1 et 2
131 e), sur la sécurité	Art. 32 à 34 « Sécurité » (y compris notification des violations)	7, par. 1
131 f), sur les outils permettant de détecter et d'atténuer les risques	Art. 35 « Analyse d'impact relative à la protection des données » ; art. 36 « Consultation préalable »	10, par. 2
131 g), sur la formation des employés	Art. 37 à 39 « Délégué à la protection des données »	–
131 h), sur l'établissement d'un mandat clair des autorités chargées de faire respecter la vie privée	52 « Indépendance » de l'autorité de contrôle	15, par. 5
131 i), sur les pouvoirs de réglementation qui doivent être à la hauteur des mégadonnées	Art. 57 « Missions » et art. 58 « Pouvoirs » de l'autorité de contrôle	12 et 15
131 j), sur les lois sur la protection de la vie privée qui doivent être adaptées aux avancées technologiques	Art. 4, par. 1 « Données à caractère personnel » ; art. 4, par. 4 « Profilage » ; art. 4, par. 5 « Pseudonymisation » ; art. 22 « Décision automatisée » ; art. 25 « Protection des données dès la conception et protection des données par défaut »	8, par. 1 et 2 ; 10, par. 3

Paragraphe du rapport d'octobre 2017 du Rapporteur spécial (A/72/540)	*Section du Règlement général sur la protection des données de l'Union européenne*	*Article de la Convention 108 modernisée*
131 k), sur des mécanismes de consultation formels	Art. 36 « Consultation préalable » ; art. 57 b), c), d) et g) « Missions » de l'autorité de contrôle	–
131 l) sur les consultations concernant les pratiques risquées	Art. 36 « Consultation préalable »	–
131 m), sur les techniques nouvelles	Art. 57 i) « Missions » de l'autorité de contrôle – suivre les évolutions des technologies ; art. 25 « Protection des données dès la conception et protection des données par défaut »	10, par. 3
131 n) sur la sensibilisation des citoyens	Art. 12 « Transparence » ; art. 13 à 15 « Informations à fournir aux personnes concernées » ; art. 57 b), c), e) « Missions » de l'autorité de contrôle	15, par. 2 e)
126, sur l'obligation contraignante de garantir la fiabilité des procédés de désidentification destinés à permettre la publication sous forme de données ouvertes et de prévoir des mécanismes d'application solides	Art. 25 « Protection des données dès la conception et protection des données par défaut » ; art. 4, par. 1 « Données à caractère personnel » ; art. 4, par. 5 « Pseudonymisation »	10, par. 3
127, sur la conduite d'évaluations rigoureuses de l'incidence sur le respect de la vie privée de l'utilisation de données unitaires dans des données ouvertes	Art. 35 « Analyse d'impact relative à la protection des données »	10, par. 2
128, sur l'interdiction de publier en ligne ou d'échanger des données unitaires en l'absence de procédés rigoureux de désidentification	Art.4, par. 1 « Données à caractère personnel » ; art.4, par. 5 « Pseudonymisation »	2 d)
129, sur la nécessité de veiller à la mise en place de mesures de protection supplémentaires pour les données sensibles	9 « Catégories particulières »	6

Source : Graham Greenleaf, contribution soumise après les consultations, 7 août 2018.

H. Conclusions

103. **Les données sont et resteront une ressource économique clef, au même titre que le capital et le travail. Ces données étant par nature dépendantes d'informations à caractère personnel, leur traitement nécessite des accommodements avec les législations relatives au respect de la vie privée et à la protection des données.**

104. **Le droit international des droits de l'homme exige que toute atteinte au droit à la vie privée soit légitime, nécessaire et proportionnée. Il arrive que l'atteinte au droit à la vie privée soit licite, mais une autre question se pose, celle de savoir si elle est conforme à l'éthique. Il n'est pas certain que certains des exemples examinés ici soient conformes à l'éthique, licites, nécessaires et proportionnés. Les cas de mauvaise gestion de données personnelles par des**

organismes privés et publics constatés récemment doivent entraîner des sanctions fermes afin de prévenir la survenue d'autres affaires du même type.

105. **Le droit international des droits de l'homme énonce également l'obligation de faire en sorte que les personnes qui subissent une violation de leur droit à la vie privée aient accès à des voies de recours. Cette obligation est encore plus importante à l'ère des mégadonnées et des données ouvertes.**

106. **L'un des principaux problèmes qui se posent s'agissant de la publication de données ouvertes est qu'il n'existe aucun moyen de déterminer avec certitude si des informations personnelles figurent dans des ensembles de données ou dans des données agrégées censés être désidentifiés.**

107. **Les politiques et pratiques régissant la gestion des données ouvertes sont sous-tendues par des facteurs économiques et politiques. Les modèles de fonctionnement sur lesquels se fondent les économies capitalistes n'incitent guère à protéger les données personnelles en l'absence de sanction économique venant contrebalancer les bénéfices escomptés.**

108. **L'instauration d'un cadre international établissant des protections cohérentes en matière de données et des règles claires régissant l'accès transnational aux données aiderait à mettre en balance les mesures de protection de la vie privée et les intérêts divergents que peuvent avoir les pays en matière d'accès aux données, par exemple d'un point de vue répressif, ou l'intérêt que peuvent avoir les multinationales à gérer en interne leurs flux de données.**

109. **Les initiatives permettant le partage de données sans aucune restriction et celles qui démantèlent les garanties juridiques existantes en matière de protection de la vie privée vont à l'encontre de la protection du droit à la vie privée et doivent cesser.**

110. **L'idée de criminaliser la ré-identification (dans l'intérêt public) d'ensembles de données désidentifiés en guise de garantie de protection des données personnelles n'emporte pas l'adhésion.**

111. **Des données unitaires détaillées (données identifiables) ne devraient pas être divulguées ou publiées en ligne sans le consentement de la personne concernée. Il convient d'utiliser des méthodes physiques et techniques, comme la sécurisation des environnements de recherche, pour restreindre l'accès aux données unitaires sensibles.**

112. **Le droit de la consommation et la législation relative à la protection des données peuvent se compléter utilement. La législation relative à la protection de la vie privée, qui tient compte des droits de l'homme et de l'évolution des sociétés, constitue un point d'ancrage pour le droit de la consommation. Le fait de s'appuyer uniquement sur le droit de la consommation privera les personnes des aspects bénéfiques plus larges découlant de l'interdépendance entre les droits fondamentaux de la personne humaine et les mécanismes de recours associés.**

113. **Les manifestations actuelles et potentielles de l'intelligence artificielle rendent nécessaires l'instauration d'une supervision indépendante assurée par des experts de différents domaines. L'évolution de cette technologie nécessite l'établissement d'un cadre politique et juridique solide axé sur les droits de l'homme. Il s'agit là d'une mesure urgente et cruciale.**

114. **L'application de l'article 22 du Règlement général sur la Protection des données doit faire l'objet d'un suivi attentif s'agissant de sa capacité à traiter les questions liées au traitement automatisé découlant de l'utilisation de l'intelligence artificielle.**

115. **Il est essentiel de remédier au manque des moyens technologiques nécessaires à la mise au point de systèmes, de méthodes et de procédures appropriés et de mettre en place des systèmes, des méthodes et des procédures solides permettant une protection efficace des données personnelles. Les petites entreprises de technologie et les start-up devraient être associées à cette entreprise.**

116. **Lorsque des États Membres envisagent d'adopter une législation promouvant les données ouvertes, il est recommandé de prendre en compte les paramètres suivants**[69] **:**

g) Toutes les lois doivent être strictement alignées sur les obligations en matière de droits de l'homme contractées par chaque État au niveau international ;

h) Les législations relatives à la protection des données reconnues comme constituant des pratiques optimales devraient être étudiées en tant qu'exemples à suivre ;

i) Il faut établir des cadres déontologiques et des mécanismes d'application du principe de responsabilité fondés sur les principes d'équité et de justice pour réglementer les pratiques relatives aux données du secteur public et du secteur privé ;

j) Pour être satisfaisants, les dispositifs réglementaires en matière de protection de la vie privée et des données doivent posséder une indépendance structurelle, disposer de ressources suffisantes et être chapeautés par une autorité de contrôle ayant les moyens d'être indépendante ;

k) Le démantèlement des lois relatives à la protection de la vie privée et des données pour permettre le libre accès aux données est contraire aux tendances mondiales et déraisonnable et contrevient aux obligations qu'impose le droit international des droits de l'homme aux États en matière de droit à la vie privée ;

l) Il faut établir une distinction dans les définitions et les concepts entre partage, utilisation, divulgation et publication de données sous forme de données ouvertes ;

m) Les cadres de conception conjointe doivent recourir à des modèles et des mécanismes participatifs faisant appel à des représentants suffisamment divers pour traiter de questions telles que la souveraineté des peuples autochtones sur les données les concernant.

I. Recommandations

117. **Les recommandations originellement formulées par le Rapporteur spécial dans son rapport à l'Assemblée générale en date du 19 octobre 2017 (A/72/540) ont été étoffées sur la base de ce qu'il est ressorti des consultations, comme suit :**

a) La pratique des autorités publiques consistant à partager en interne des données personnelles doit pouvoir être distinguée, sur le plan de la législation,

[69] Voir par exemple les propositions de l'Australie dans « New Australian Government data sharing and release legislation: issues paper for consultation », document disponible en anglais à l'adresse : www.pmc.gov.au/resource-centre/public-data/issues-paper-data-sharing-release-legislation, dans la contribution de M. Paterson.

des politiques et des pratiques, de la mise à disposition de données au grand public sous la forme de données ouvertes ;

b) Tant qu'il ne sera pas possible de déterminer avec certitude si des informations personnelles sont présentes dans les données agrégées ou que les données désagrégées ne peuvent être ré-agrégées, les données ouvertes ne devraient pas contenir d'informations unitaires ;

c) Les travaux visant à élaborer des normes internationales de protection de la vie privée qui n'empêchent pas le partage de données et les activités de normalisation au niveau international doivent se poursuivre sans retard et être appuyées par les États Membres ;

d) Les travaux de recherche sur la confidentialité différentielle sont nécessaires et devraient être utilisés dans le cadre des statistiques agrégées et les types de données complexes, ainsi que d'autres technologies respectueuses de la vie privée, telles que la cryptographie homomorphe et le calcul multipartite sécurisé ;

e) À titre de mesure minimale visant à harmoniser les règles détaillées de protection de la vie privée au niveau mondial, les États Membres sont invités à ratifier la Convention 108 modernisée par l'intermédiaire de son instrument juridique (le Protocole STCE 223) et à mettre en œuvre sans délai les principes qui y sont formulés en promulguant des lois nationales à cet effet, en s'attachant tout particulièrement à mettre immédiatement en œuvre les dispositions exigeant la mise en place de garanties concernant les données personnelles collectées à des fins relatives à la sécurité nationale, et notamment de surveillance ;

f) Afin de s'aligner sur les meilleures pratiques, les États Membres extérieurs à l'Union européenne sont encouragés, à l'occasion de l'examen et de la mise à jour de leurs législations nationales dans le cadre de la mise en œuvre de la Convention 108 modernisée, à intégrer dans la mesure du possible les garanties et voies de recours prévues dans le Règlement général sur la protection des données qui ne sont pas obligatoires au titre de la Convention ;

g) Les autorités publiques et les entreprises devraient reconnaître la souveraineté des peuples autochtones sur les données les concernant ou collectées auprès d'eux et ayant trait aux peuples autochtones, à leurs systèmes de connaissances, à leurs coutumes ou à leurs territoires, notamment en veillant toujours à inclure des principes élaborés et formalisés par ces peuples et en mettant l'accent sur les dispositifs de direction et de responsabilisation propres à ces peuples ;

h) Les États Membres devraient vérifier que les cadres juridiques et politiques relatifs à l'intelligence artificielle, dans leur ensemble, sont adaptés à l'objectif de protection de la liberté d'expression et du droit à la vie privée ; favoriser une étroite collaboration pluridisciplinaire entre statisticiens, juristes, spécialistes des sciences sociales, informaticiens, mathématiciens et experts de la question ; et concevoir des stratégies visant à prévenir ou à corriger tout effet négatif sur l'exercice des droits de l'homme découlant de l'utilisation d'algorithmes, du traitement automatisé, de l'apprentissage automatique et de l'intelligence artificielle.

118. **Le Rapporteur spécial réitère également les recommandations qu'il a formulées dans son précédent rapport (voir A/72/540, par. 126 à 131).**