



Asamblea General

Distr. general
17 de octubre de 2018
Español
Original: inglés

Septuagésimo tercer período de sesiones

Tema 74 b) del programa

**Promoción y protección de los derechos humanos:
Cuestiones de derechos humanos, incluidos otros
medios de mejorar el goce efectivo de los derechos
humanos y las libertades fundamentales**

El derecho a la privacidad*

Nota del Secretario General

El Secretario General tiene el honor de transmitir a la Asamblea General el informe preparado por el Relator Especial sobre el derecho a la privacidad, Joseph A. Cannataci, presentado de conformidad con la resolución 28/16 del Consejo de Derechos Humanos.

* El informe se presentó después del plazo establecido con el propósito de incluir información sobre los acontecimientos más recientes.



Informe del Relator Especial sobre el derecho a la privacidad

Resumen

El presente informe se divide en dos partes: un resumen de las actividades realizadas durante el período 2017-2018, y el informe final sobre la labor del equipo de tareas sobre macrodatos y datos abiertos establecido por el Relator Especial.

I. Reseña de las actividades realizadas por el Relator Especial sobre el derecho a la privacidad

1. El período comprendido entre octubre de 2017 y octubre de 2018, que ha sido sumamente productivo para el Relator Especial sobre el derecho a la privacidad, se ha caracterizado por la colaboración con la sociedad civil, los gobiernos, los organismos encargados de hacer cumplir la ley, los servicios de inteligencia, las autoridades de protección de datos, las autoridades de supervisión de los servicios de inteligencia, los círculos académicos, las empresas y otros interesados.

2. En marzo de 2018, el Relator Especial presentó al Consejo de Derechos Humanos un examen amplio de su primer mandato de tres años como titular inaugural del mandato creado por el Consejo en marzo de 2015.¹ En ese informe dio cuenta de sus actividades en cada una de las esferas temáticas del mandato. El Relator Especial desea manifestar que es un gran honor que su mandato haya sido prorrogado hasta 2021 y poder seguir adelante con la importante labor encomendada en el mandato.

3. El plan de trabajo del Relator Especial se vio interrumpido cuando hubo de someterse a una intervención quirúrgica en abril de 2018. Agradece a la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (ACNUDH) el apoyo y la asistencia que le prestó durante ese período. El Relator Especial se recuperó plenamente y reanudó sus funciones en junio de 2018.

A. Labor del equipo de tareas sobre la privacidad de los datos sanitarios

4. El equipo de tareas sobre la privacidad de los datos sanitarios examinó diversas cuestiones bajo la dirección de Steve Steffensen de la Dell Medical School de la Universidad de Texas (Estados Unidos de América). Aunque se había comenzado a trabajar en un proyecto de informe, surgieron imprevistos que obligaron a aplazar hasta 2019 la consulta prevista para 2018. El Vicepresidente, Nikolaus Forgo, ha aceptado asumir las responsabilidades de la Presidencia.

B. Labor del equipo de tareas sobre el uso de datos personales por parte de las empresas

5. El derecho a la privacidad nunca ha estado tan en primer plano de la atención política, judicial o personal como en la actualidad, cuando las tensiones entre la seguridad, los modelos empresariales y la privacidad ocupan un lugar cada vez más prominente.

6. En respuesta a sucesos que tuvieron lugar el año pasado, como la vulneración de las normas de protección de datos por parte de la empresa Cambridge Analytica, la introducción de legislación como la Ley de aclaración del uso lícito de datos en el extranjero, en los Estados Unidos, el proyecto de ley sobre telecomunicaciones de 2018 y otras enmiendas legislativas en Australia, y el caso *Estados Unidos c. Microsoft Corp.* ante el Tribunal Supremo de los Estados Unidos, el Relator Especial adelantó la puesta en marcha del equipo de tareas sobre el uso de datos personales por parte de las empresas.

7. El equipo de tareas se reunió por primera vez en Malta en septiembre de 2018. Sus miembros provienen de grandes empresas líderes en la era digital y de entidades fundamentales que promueven la protección del derecho a la privacidad en el mundo

¹ [A/HRC/37/62](#).

de la tecnología. Asesorará al Relator Especial en relación con los nuevos desafíos y las oportunidades para la promoción del derecho a la privacidad, incluidas las consecuencias relativas al género que tienen esas cuestiones.

C. Labor del equipo de tareas para un mejor conocimiento de la privacidad

8. El equipo de tareas para un mejor conocimiento de la privacidad explora el reconocimiento por parte del Consejo de Derechos Humanos del derecho a la privacidad como factor que favorece el desarrollo de la persona, así como los obstáculos que se oponen a ese proceso. Colaborará con iniciativas de todo el mundo, como el estudio de la Comisión de Derechos Humanos de Australia sobre las repercusiones de la era digital en los derechos humanos².

9. Aunque todas las personas tienen derecho a gozar de la protección que ofrece el derecho internacional de los derechos humanos, en ocasiones se ha denunciado que el disfrute del derecho a la privacidad no es ni igual ni universal. El género es uno de los ámbitos donde los efectos protectores y facilitadores de la privacidad y las vulneraciones y lesiones del derecho a la privacidad pueden ser experimentados de manera diferente.

10. A ese respecto, el Tribunal Supremo de la India derogó el artículo 377 del Código Penal de la India, que tipificaba como delito la actividad sexual consentida entre adultos, en un fallo en el que se reconocían los derechos de la comunidad lesbiana, gay, bisexual, transgénero, indecisa (“questioning”) e intersexual de la India. Esa sentencia tendrá considerables repercusiones en el discurso sobre el género y la privacidad en la India, y se deriva de la sentencia de 2017 sobre el derecho a la privacidad en el caso Puttaswamy³.

11. El Relator Especial ha puesto en marcha una consulta en línea sobre las perspectivas de género del derecho a la privacidad en la era digital; en ella se solicita información sobre cuestiones como las siguientes:

a) ¿Qué cuestiones de género surgen en la era digital? ¿Qué desafíos es necesario afrontar y qué experiencias positivas pueden promoverse de manera más amplia?

b) ¿La era digital ha dado lugar a experiencias de privacidad nuevas o apreciablemente diferentes según el género (comprendidas aquellas experiencias relacionadas con la orientación sexual, la identidad de género, la expresión de género y las características sexuales)? En caso afirmativo, ¿cuáles?

c) ¿Cuáles son las repercusiones relacionadas con el género que tienen las invasiones de la privacidad en mujeres y hombres, y en personas de diversas orientaciones sexuales e identidades de género, expresiones de género y características sexuales, que surgen de violaciones del derecho a la privacidad en el ámbito de la salud, la discriminación en el empleo u otros?

d) ¿Cuáles son las buenas prácticas en la legislación y en los modelos de prestación de servicios que tienen en cuenta las diferencias por razón de género en el disfrute del derecho a la privacidad?

² Comisión de Derechos Humanos de Australia, “Major project to focus on human rights and technology”, 22 de mayo de 2018. Puede consultarse en www.humanrights.gov.au/news/stories/major-project-focus-human-rights-and-technology.

³ Comunicación de Smitha Krishna Prasad, Universidad Nacional de Derecho, Delhi (India), 24 de septiembre de 2018.

12. Se pidió que las respuestas se presentaran a más tardar el 30 de septiembre de 2018 para informar al Consejo de Derechos Humanos en 2019. El Relator Especial aceptará con agrado la información que presenten los Estados Miembros después de ese plazo, hasta el 30 de noviembre de 2018.

13. Esta iniciativa sigue a las consultas celebradas en todo el mundo sobre el tema “Privacidad, personalidad y flujos de información” de julio de 2016, mayo de 2017 y septiembre de 2017. El cuarto evento, sobre aspectos de género, cuya celebración se había previsto en mayo de 2018 en América Latina, se aplazó debido a la incapacidad del Relator Especial para viajar y se celebrará a mediados de 2019.

D. Labor del equipo de tareas sobre seguridad y vigilancia

14. Después de que Edward Snowden revelara detalles de los programas de vigilancia e intercambio de información de los servicios de inteligencia de los Estados Unidos y el Reino Unido de Gran Bretaña e Irlanda del Norte, se presentaron solicitudes ante el Tribunal Europeo de Derechos Humanos en relación con la interceptación masiva de comunicaciones, el intercambio de información de inteligencia con gobiernos extranjeros y la obtención de datos de comunicaciones de los proveedores de servicios de comunicaciones con arreglo a la Ley de Regulación de las Facultades de Investigación del Reino Unido de 2000.

15. El Tribunal concluyó recientemente que el régimen de interceptación masiva del Reino Unido había infringido el artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales (Convenio Europeo de Derechos Humanos), relativo al derecho al respeto de la vida privada y familiar y de las comunicaciones, debido a la insuficiente supervisión de la selección de los proveedores de Internet para la interceptación y del filtrado, la búsqueda y la selección de las comunicaciones interceptadas para someterlas a examen, y la falta de salvaguardias adecuadas en la selección de “datos relacionados con las comunicaciones” para someterlos a examen.

16. El Tribunal sostuvo que el régimen para la obtención de datos relativos a las comunicaciones de los proveedores de servicios de comunicaciones había vulnerado el artículo 8, y que los regímenes de interceptación masiva y de obtención de datos relativos a las comunicaciones de los proveedores de servicios de comunicaciones habían vulnerado el artículo 10 de la Convención al no existir suficientes salvaguardias para el material periodístico de carácter confidencial. Además determinó que el régimen de divulgación de información de inteligencia con gobiernos extranjeros no había infringido ni el artículo 8 ni el artículo 10⁴.

17. Aunque esa sentencia se refería al anterior marco legal de vigilancia del Reino Unido, sus conclusiones tienen importantes repercusiones y se señalan a la atención de los Estados Miembros con el fin de que revisen sus prácticas y marcos.

18. En relación con el fallo del Tribunal de Justicia de la Unión Europea de diciembre de 2016 sobre la retención de datos relativos a las comunicaciones y la consulta del Gobierno del Reino Unido acerca de su proyecto de respuesta, el Relator Especial hizo aportaciones a principios de 2018, que podrán consultarse en la página web del ACNUDH dedicada al titular del mandato⁵.

⁴ Tribunal Europeo de Derechos Humanos, Sección Primera, *Big Brother Watch y otros c. el Reino Unido*, Solicitudes núms. 58170/13, 62322/14 y 24960/15, Nota informativa sobre la sentencia de 13 de septiembre de 2018. Se puede consultar en [https://hudoc.echr.coe.int/eng#{"itemid":\["002-12080"\]}](https://hudoc.echr.coe.int/eng#{).

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

19. En septiembre de 2018, el Gobierno de Australia presentó el proyecto de ley de telecomunicaciones y otras enmiendas legislativas, que tiene profundas repercusiones para los derechos humanos y la ciberseguridad en los planos tanto internacional como nacional.

20. El proyecto de ley tiene graves defectos. Se trata de una medida de seguridad nacional mal concebida con muchas probabilidades de poner en peligro la seguridad; es dudoso desde el punto de vista tecnológico que pueda alcanzar sus objetivos y evitar la introducción de vulnerabilidades en la ciberseguridad de todos los dispositivos, sean teléfonos móviles, tabletas, relojes inteligentes, vehículos o redes de televisión de circuito cerrado, y socava indebidamente los derechos humanos, entre ellos el derecho a la privacidad. Las garantías de que no se trata de una “puerta trasera” para las comunicaciones cifradas no son de fiar ya que, en realidad, tiene la capacidad de generar no solo nuevas llaves para la “puerta delantera”, sino también más puertas delanteras.

21. El proyecto de ley prevé un nivel excesivamente alto de discrecionalidad en el uso de poderes excepcionales. La rendición de cuentas no incumbe al Parlamento, sino a ciertos organismos y al Fiscal General del Estado. Carece de mecanismos de supervisión judicial o de vigilancia independiente, hay una falta de transparencia sumamente preocupante, y la capacidad propuesta de introducir programas informáticos en los dispositivos, entre otras acciones, parece una inquietante modalidad de piratería informática por parte del gobierno. El proyecto se presentó al Parlamento tras un período de consultas insuficiente y a pesar de haber recibido al parecer más de 14.000 alegaciones, apenas dos semanas después de concluidas las consultas.⁶

22. Las preocupaciones del Relator Especial aumentan ante la posición del Gobierno de Australia en cuanto a las vías de recurso en caso de graves invasiones de la privacidad y los limitados mecanismos de protección de los derechos humanos y la privacidad en el país, en particular la falta de protección constitucional de la privacidad; la ausencia de una carta de derechos que consagre la privacidad; la inexistencia del delito de vulneración de la privacidad; y, a diferencia de su vecina Nueva Zelanda, una Ley de Protección de la Privacidad que no ha superado la evaluación europea de la idoneidad.

23. Se necesita un nuevo enfoque para hacer frente a los desafíos que supone el cifrado para la aplicación de la ley y la seguridad nacional. Aunque la tecnología plantea problemas a las fuerzas del orden y a los servicios de inteligencia, y aunque es importante combatir el abuso sexual de niños en línea y desactivar las amenazas terroristas, la protección de los derechos humanos de los ciudadanos también es legítima y necesaria en una sociedad democrática. Las mismas tecnologías que permiten a los delincuentes y terroristas eludir la detección o lanzar ataques malintencionados proporcionan enormes beneficios en los ámbitos de la ciberseguridad, la privacidad y la economía⁷. Debilitar la tecnología de cifrado pone en peligro la seguridad de la economía de la información moderna⁸.

⁶ Justin Hendry, “Decryption laws enter parliament”, IT News, 20 de septiembre de 2018. Puede consultarse en 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 y William A. Carter, *The Effect of Encryption on Lawful Access to Communications and Data* (Washington D.C., Centro de Estudios Estratégicos e Internacionales, 2017). Puede consultarse en 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

24. Para hacer frente a las complicaciones que trae consigo el cifrado para las investigaciones de las fuerzas del orden y la recopilación de información de inteligencia se necesita un enfoque que evite debilitar el cifrado y con ello la seguridad nacional de otros países.

25. Recomiendo a los Estados Miembros el enfoque adoptado por el Gobierno de los Países Bajos, que ha reconocido que las medidas nacionales no pueden considerarse separadamente de su contexto internacional y sin tener en cuenta la falta de opciones para debilitar los productos de cifrado sin comprometer la seguridad de los sistemas digitales que utilizan el cifrado⁹.

26. El Foro Internacional de Supervisión de los Servicios de Inteligencia organizado por el Relator Especial se reunirá en Malta a finales de noviembre de 2018. El interés por esta cuestión es tal que se han cubierto todas las inscripciones en el foro y hay lista de espera.

E. Comunicaciones

27. El Relator Especial ha presentado 17 comunicaciones desde el 22 de septiembre de 2017, entre ellas 8 “cartas de denuncia”, 7 “cartas de otro tipo” y 2 “llamamientos urgentes”. De las 17 comunicaciones, 15 fueron presentadas conjuntamente con otros titulares de mandatos de procedimientos especiales; las otras 2 fueron presentadas solo por el Relator Especial.

F. Promoción del derecho a la privacidad

28. El Relator Especial cooperó con otros titulares de mandatos de procedimientos especiales por medio de comunicados de prensa y declaraciones conjuntas, así como intercambiando asesoramiento e información. El Relator Especial agradece las constructivas consultas mantenidas con la Relatora Especial sobre la violencia contra la mujer, sus causas y consecuencias.

29. El Relator Especial ha publicado 11 comunicados y declaraciones de prensa. De ellas, dos fueron publicadas conjuntamente con otros titulares de mandatos: una trataba sobre los derechos de los activistas ambientales en el próximo 24^o período de sesiones de la Conferencia de las Partes en la Convención Marco de las Naciones Unidas sobre el Cambio Climático¹⁰, y la otra sobre el proyecto de ley de seguridad de México¹¹.

30. Los días 19 y 20 de febrero de 2018, el Relator Especial hizo una exposición sobre la función del derecho a la privacidad en el marco de los derechos humanos y la protección del espacio cívico, y moderó una sesión sobre tendencias nuevas y

backdoors”, comunicado de prensa, 10 de septiembre de 2018; Michelle Mosey y Adam Henschke, “Defining thresholds in law – sophisticated decryption and law enforcement”, National Security College Policy Options Paper, núm. 8 (Universidad Nacional de Australia, abril de 2018).

⁹ G.A. Van der Steur, Ministro de Seguridad y Justicia, y H.G.J. Kamp, Ministro de Asuntos Económicos, Países Bajos, “Cabinet’s view on encryption”, carta de posición enviada al Presidente de la Cámara de Representantes de los Estados Generales, 4 de enero de 2016.

¹⁰ Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (ACNUDH), “UN experts urge Poland to ensure free and full participation at climate talks”, 7 de mayo de 2018. Puede consultarse en www.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=23042&LangID=E.

¹¹ ACNUDH, “Mexico draft security law threatens rights and should be rejected, UN rights experts warn”, 14 de diciembre de 2017. Puede consultarse en www.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=22535&LangID=E.

emergentes en el taller de expertos sobre el derecho a la privacidad en la era digital, organizado en Ginebra por el ACNUDH.

G. Visitas a países

31. En junio de 2018, el Relator Especial visitó el Reino Unido. En su declaración de fin de misión formuló observaciones preliminares¹². El informe definitivo al respecto será presentado al Consejo de Derechos Humanos en su 40º período de sesiones.

32. En 2015, el Relator Especial criticó las propuestas legislativas que habían incrementado las facultades de vigilancia del Gobierno del Reino Unido. Desde entonces se habían introducido importantes mejoras en el régimen de supervisión de los servicios de inteligencia, entre ellas el establecimiento de una Oficina del Comisionado de Facultades de Investigación mejor dotada de recursos y un sistema de doble cerrojo, en el que el equivalente a cinco comisionados judiciales a tiempo completo examinan las decisiones de autorización más sensibles que firman altos funcionarios del Gobierno, como el Secretario del Interior y el Secretario de Relaciones Exteriores. Un aspecto positivo es que esas salvaguardias contra la vigilancia arbitraria o ilícita se aplican por igual a todas las personas sometidas a vigilancia por las autoridades del Reino Unido en su territorio, sin distinción alguna por motivos de nacionalidad o de residencia.

33. El Relator Especial sigue preocupado por las posibles deficiencias de la nueva Ley de Poderes de Investigación de 2016, incluido el requisito de que la Oficina del Comisionado de Poderes de Investigación realice la doble tarea de autorizar la vigilancia y supervisar esa misma vigilancia. Esto puede comprometer la independencia de la supervisión *a posteriori*.

34. El Relator Especial señaló la necesidad de contar con directrices claras y sólidas y de supervisar todo acuerdo de intercambio de datos para el Servicio Nacional de Salud, y recomendó encarecidamente que esas directrices se hicieran públicas a la mayor brevedad posible. Las conversaciones con el Custodio Nacional de los Datos sugieren que esto podría suceder durante los próximos 12 a 24 meses. El Relator Especial recomendó que la función del Custodio de los Datos estuviese regulada por ley lo antes posible.

35. Entre otras cuestiones incluidas en su declaración de fin de misión cabe citar las medidas antirradicalización y el programa “Prevenir” y su impacto en los musulmanes; las propuestas de penalizar el acceso a material extremista; y cuestiones planteadas por organizaciones de la sociedad civil.

Visitas previstas a los países

36. La próxima visita oficial será a Alemania, del 29 de octubre al 9 de noviembre de 2018, e irá precedida de una solicitud de contribuciones de las partes interesadas en la página web del ACNUDH dedicada al titular del mandato.

Visitas oficiosas y eventos internacionales

37. Durante su visita a Australia para la consulta sobre macrodatos y datos abiertos, el Relator Especial visitó tres estados y se reunió con organizaciones de la sociedad civil, un ministro del Gobierno y el Fiscal General de la Oposición, funcionarios del Gobierno, representantes de empresas y asociaciones profesionales, miembros del mundo académico y otras personas. También se reunió con el Comisionado de

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

Derechos Humanos de Australia y Presidente de la Comisión y dio varias conferencias públicas en la Universidad de Nueva Gales del Sur en Sídney, la Universidad de Melbourne, la Universidad de La Trobe y la Universidad Edith Cowan. El centro de seguridad cibernética de la Universidad Optus Macquarie organizó una reunión informativa entre el Relator Especial y las principales empresas cotizadas. La sección de Australia y Nueva Zelandia de la Asociación Internacional de Profesionales de la Privacidad organizó reuniones con profesionales dedicados a cuestiones relacionadas con este asunto.

38. El Relator Especial también participó en la 16ª Conferencia Internacional sobre el Ciberespacio, celebrada en Chequia en noviembre de 2017; la 11ª Conferencia Internacional sobre Informática, Privacidad y Protección de Datos, celebrada en Bruselas en enero de 2018; un taller de expertos sobre el derecho a la privacidad en la era digital, celebrado en Ginebra en febrero de 2018; la Conferencia Mundial sobre Internet y Jurisdicción, celebrada en Ottawa en febrero de 2018; y la Conferencia MAPPING, celebrada en Malta en febrero de 2018.

H. Novedades en la cuestión del derecho a la privacidad

Capacidad para obtener reparación

39. El Relator Especial siguió señalando a la atención de los Estados Miembros pertinentes las denuncias de violaciones del derecho a la privacidad y, en su informe de 2018, informó al Consejo de Derechos Humanos sobre las violaciones del artículo 12 de la Declaración Universal de Derechos Humanos y del artículo 17 del Pacto Internacional de Derechos Civiles y Políticos.

40. El Relator Especial sigue convencido de que un elemento clave en la reparación del daño causado por las vulneraciones de la privacidad es la confianza en que se dispondrá de un juicio imparcial y un posible remedio jurídico. La capacidad de tener acceso a vías de recurso es fundamental para la protección de los derechos humanos y sigue siendo una de las grandes prioridades del Relator Especial.

Inteligencia artificial

41. Habida cuenta de que cada vez más decisiones que afectan a la vida de todas las personas se adoptan recurriendo a algoritmos y al aprendizaje automático, el impacto de esas decisiones en los derechos humanos debe ser evaluado de forma cuidadosa y constante.

42. Estas tecnologías están tan generalizadas que incluso se utilizan como prueba en los procedimientos judiciales. A pesar de ello, se desconoce en gran medida la forma en que funcionan los algoritmos complejos, así como su progresión de desarrollo en el caso del aprendizaje automático. Es necesario examinar esta cuestión desde la perspectiva de los derechos humanos en conjunto antes de adoptar políticas que fomenten y permitan el desarrollo y la implantación de productos basados en la inteligencia artificial, o en conjunción con ellas¹³. Para proteger los derechos humanos afectados es imprescindible contar con un marco jurídico y ético sólido.

¹³ Priyanar Bhunia, "Taskforce recommends establishment of national mission for coordinating AI-related activities across India", Open Gov, 9 de abril de 2018.

Introducción de la legislación sobre privacidad y protección de datos en todo el mundo

43. Ha aumentado considerablemente el número de países que han adoptado leyes de privacidad o protección de datos¹⁴; a este respecto, 2018 ha sido un año particularmente activo en todo el mundo.

44. Cabe destacar en particular el proyecto de ley de la India tras la decisión del Tribunal Supremo en el caso *Puttaswamy*¹⁵. El proyecto de ley, publicado a mediados de 2018, tiene muchas características positivas que también aparecen en el Reglamento General de Protección de Datos de la Unión Europea (Reglamento 2016/679), como las evaluaciones del impacto en la protección de datos, el derecho al olvido y las sanciones de aplicación adecuadas. Pero también hay aspectos preocupantes, como las restricciones a la investigación sobre la posible reidentificación de personas incluidas en conjuntos de datos supuestamente anonimizados. Además, mientras que el uso de datos personales por parte de las fuerzas de seguridad ha de ser “necesario y proporcionado”, la divulgación de datos en los procedimientos judiciales goza de amplias exenciones¹⁶. El Relator Especial insta al Gobierno de la India a colaborar con los expertos, los investigadores y las organizaciones de la sociedad civil que plantean esas cuestiones.

45. En un fallo de fecha 26 de septiembre de 2018, el Tribunal Supremo de la India confirmó la constitucionalidad de la Ley Aadhaar, pero revocó: a) el artículo 57, en virtud del cual las empresas privadas podían pedir detalles a los consumidores utilizando el programa Aadhaar con fines de identificación; b) el artículo 33, párrafo 2, sobre el intercambio de datos con organismos de seguridad por motivos de seguridad nacional; y c) el artículo 47, en virtud del cual solo el Gobierno puede presentar una denuncia en caso de robo de datos de Aadhaar¹⁷. El Tribunal exigió al Gobierno que introdujera una legislación firme en materia de protección de datos.

46. En la Unión Europea se han introducido importantes reformas. El Reglamento General de Protección de Datos entró en vigor el 25 de mayo de 2018, y a partir del 6 de mayo de 2018 entró en vigor una directiva específica sobre protección de datos en los ámbitos policial y judicial. La Directiva 2002/58/CE sobre la privacidad y las comunicaciones electrónicas va a ser sustituida por el nuevo Reglamento sobre la privacidad electrónica¹⁸. El Reglamento (CE) 45/2001 establece las normas de protección de datos en las instituciones de la Unión Europea y las funciones del Supervisor Europeo de Protección de Datos. El 10 de enero de 2017, la Comisión

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, núm. 45 (2017).

¹⁵ Tribunal Supremo de la India, Jurisdicción Civil Original, *Justice K. S. Puttaswamy (Retired), and Another v. Union of India and Others*, Petición Escrita (Civil) núm. 494 de 2012, Fallo, 24 de agosto de 2017. Puede consultarse en [http://supremecourtindia.nic.in/pdf/jud/ALL%20WP\(C\)%20No.494%20of%202012%20Right%20to%20Privacy.pdf](http://supremecourtindia.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 de julio de 2018. Puede consultarse en www.theregister.co.uk/2018/07/31/india_privacy_boffin_ban/.

¹⁷ Tribunal Supremo de la India, Jurisdicción Civil Original, *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 de septiembre de 2018. Puede consultarse en http://economictimes.indiatimes.com/articleshow/65961697.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst.

¹⁸ Véase Comisión Europea, “Proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and protection of personal data in electronic communications repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)”, 10 de enero de 2017.

Europea adoptó una propuesta por la que se derogaba dicho Reglamento y lo adaptaba al Reglamento General de Protección de Datos; está previsto que ambas medidas se apliquen a partir de finales de 2018. Con esta reforma, la Unión Europea completará la primera gran modernización de su marco para la protección de la privacidad y la protección de datos en más de 20 años.¹⁹

47. Estas importantes medidas de consolidación dentro de la Unión Europea se aplican a todos los sectores, excepto a la privacidad y a la “seguridad nacional”, cuestión excluida de la competencia de la Unión Europea en virtud del artículo 4.2 del Tratado de la Unión Europea. La vigilancia dentro del ámbito de la seguridad nacional, y no de la aplicación de la ley, está regulada de manera mucho más desigual dentro de la Unión Europea a raíz de las iniciativas de países como Bélgica, Francia, los Países Bajos y el Reino Unido para actualizar su legislación.

48. A escala regional, es alentador observar que el Convenio modernizado para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (también denominado “Convenio 108 modernizado”) se ultimó en junio de 2018, y que su instrumento jurídico habilitante (Protocolo CETS 223) se abrió a la firma el 10 de octubre de 2018. Se trata de un hito importante ya que, a diferencia del Reglamento General de Protección de Datos, el Convenio también abarca la seguridad nacional y ha sido ratificado por más de 55 Estados Miembros de las Naciones Unidas, entre ellos un número cada vez mayor de Estados no europeos.

49. En el Brasil, el Senado aprobó una ley general de protección de datos que entrará en vigor en febrero de 2020. Entre los elementos clave cabe citar los siguientes²⁰: jurisdicción transfronteriza; principios de privacidad y un enfoque basado en el riesgo; nuevos derechos para los particulares; más bases jurídicas para el tratamiento de datos personales; evaluaciones de impacto de la asignación de datos y la protección de datos; notificación obligatoria de las infracciones y designación de un funcionario responsable de la protección de datos; y restricciones a la transferencia transfronteriza de datos de carácter personal.

50. Las multas por incumplimiento pueden alcanzar el 2% de la facturación de la empresa o el grupo de empresas, o una suma máxima, por infracción, de aproximadamente 12,9 millones de dólares.

Pueblos indígenas y datos

51. El Relator Especial ha estudiado la cultura de la privacidad de los aborígenes australianos durante muchos años. Dado que esa cultura es una de las expresiones de privacidad más complejas e interiorizadas a nivel individual, familiar y colectivo, que se materializa por medio de conductas, ritos y prácticas, en espacios privados y comunales, el Relator Especial expresó su satisfacción por el hecho de que en la consulta sobre macrodatos y datos abiertos se explorara la soberanía de los datos indígenas, aunque fuera de manera modesta.

52. El Relator Especial alienta a los gobiernos y a las empresas a que reconozcan la soberanía inherente de los pueblos indígenas con respecto a los datos que les conciernen o que se recaben de ellos, y que guarden relación con sus sistemas de conocimientos, sus costumbres o sus territorios.

¹⁹ Véase https://edps.europa.eu/data-protection/data-protection/legislation_en.

²⁰ Véase www.onetrust.com/what-is-the-brazil-general-data-protection-law-igpd/.

II. Consulta sobre el anterior informe del Relator Especial a la Asamblea General

53. En su informe de octubre de 2017 a la Asamblea General (A/72/540), el Relator Especial examinó las dificultades para garantizar el derecho humano a la privacidad en el contexto de una de las características que definen la era digital: los macrodatos y los datos abiertos. Desde entonces, se introdujo el Reglamento General de Protección de Datos y se conoció lo sucedido en relación con Facebook y Cambridge Analytica.

54. Los días 26 y 27 de julio de 2018 se celebraron en Australia consultas con funcionarios gubernamentales, organizaciones de la sociedad civil, empresas y particulares sobre ese informe. Antes de las consultas hubo una invitación a presentar comunicaciones que concluyó el 28 de abril de 2018; las comunicaciones presentadas fueron resumidas para la consulta. También se recibieron aportaciones en reuniones con entidades de la sociedad civil organizadas por la Fundación Australiana para la Protección de la Vida Privada, así como de comunicaciones llegadas después de la consulta.

A. Resumen de los comentarios recibidos

55. En la consulta pública se examinaron los orígenes y usos de los macrodatos y los datos abiertos; los posibles beneficios y perjuicios de cada uno de ellos; las repercusiones del uso de datos personales en otros derechos humanos; la idoneidad de las técnicas de desidentificación; las buenas prácticas en el uso de datos de carácter personal; la importancia de los derechos humanos y la ética en las tecnologías automatizadas de adopción de decisiones; la soberanía de los datos indígenas; cuestiones relativas al consumo y al género; y perspectivas de países no europeos.²¹ Gran parte de los debates se centraron en los datos abiertos y en las consecuencias que tiene su interacción con los macrodatos para la privacidad.

B. Datos abiertos

56. Los análisis de macrodatos y las técnicas computacionales basadas en la inteligencia artificial proporcionan beneficios al tiempo que aumentan los riesgos potenciales para la privacidad de las personas y las comunidades, así como para el propio entramado de las sociedades democráticas. La divulgación de información en poder de los gobiernos, en particular la publicación iterativa de conjuntos de datos que contienen información de carácter personal, requiere un examen más matizado y detallado²².

57. En la consulta se examinó la afirmación de que la analítica de macrodatos tiene la capacidad de identificar a personas individuales a pesar de que se haya procedido a la desidentificación²³. Se afirmó que determinar si los datos o los resultados de un proyecto de análisis de datos contienen información de carácter personal depende de las circunstancias del uso o la divulgación, y que eso puede cambiar atendiendo a otros factores. Por consiguiente, es preferible describir la reidentificación en términos

²¹ Amanda Lo, “The right to privacy in the age of big data and open data”, The Allens Hub for Technology, Law and Innovation, Universidad de Nueva Gales del Sur, 21 de agosto de 2018.

²² Comunicación de M. Paterson, Universidad Monash, agosto de 2018.

²³ Véase Oficina del Comisionado de Información de Victoria, “Protecting unit-record level personal information: the limitations of de-identification and the implications for the Privacy and Data Protection Act 2014”, mayo de 2018. Puede consultarse en <https://ovic.vic.gov.au/resource/protecting-unit-record-level-personal-information/>.

de niveles de riesgo que en términos absolutos. Los niveles de riesgo dependen de quién tiene acceso a los datos, qué grado de granularidad tienen los datos (el tamaño del grupo más pequeño de los datos), qué otros conjuntos de datos pueden vincularse con precisión a los datos y el contexto externo asociado.

58. La “información de carácter personal” incluida en los datos abarca un amplio campo y las descripciones varían de una jurisdicción a otra. Lo que la mayoría de las definiciones tienen en común es que el alcance de la información personal puede ser amplio y se refiere a la capacidad de identificar a un individuo concreto, y no solo a si los datos en sí mismos identifican al individuo.

59. Dos aspectos clave para determinar los datos que contienen información de carácter personal son: a) los datos propiamente dichos deben identificar a una persona; o b) debe ser razonablemente posible identificar a una persona.

60. Cada uno de los tres mecanismos principales para el intercambio de datos — explícito, derivado e inferido— va acompañado de consideraciones sobre el grado de información personal contenida y las obligaciones de la organización que obtiene, utiliza y almacena esos datos.

61. Los datos sobre la navegación y las compras en línea pueden utilizarse para personalizar cada vez más los servicios sin conocer la identidad del usuario. Sin embargo, se han planteado dudas sobre si ciertos identificadores anónimos altamente selectivos constituyen información personal. Los datos de la red de telefonía móvil se han utilizado con fines que van más allá de la optimización de la red, lo que ha permitido anticipar la pérdida de clientes e incluso conocer las relaciones con otros usuarios de móviles sin conocer la identidad de las personas interesadas²⁴.

62. Un desafío fundamental en el intercambio de datos es que actualmente no hay manera de determinar de manera inequívoca si existe información de carácter personal en los datos agregados, o si los datos desagregados pueden volver a agregarse. El riesgo de reidentificación depende del acceso a los conjuntos de datos relacionados (y de la capacidad de vincularlos), de las técnicas utilizadas para desidentificar y del grado de agregación o perturbación de los datos. Por consiguiente, en las distintas organizaciones se utilizan diferentes técnicas y niveles de agregación de datos, en función del riesgo percibido que se asocie a los datos compartidos.

63. La elaboración de normas para determinar qué se entiende por datos “desidentificados” ayudaría a afrontar los retos que plantea el tratamiento de la privacidad. A escala internacional, actualmente sólo existen orientaciones de muy alto nivel, y ciertamente ninguna orientación cuantitativa, sobre lo que significa “desidentificado”, por lo que muchas organizaciones han de determinar lo que significa para ellas caso por caso, basándose en diferentes conjuntos de datos y en cómo pueden ser razonablemente utilizados o combinados con otros datos.

64. En 2017, la Sociedad de Informática de Australia publicó un libro blanco técnico en el que exploraba los problemas que surgen en relación con el intercambio de datos y destacaba que un reto fundamental para la creación de servicios inteligentes es la cuestión de si un conjunto de conjuntos de datos contiene información personal. Responder a esa pregunta es un gran desafío, ya que el hecho mismo de combinar conjuntos de datos genera información. El documento proponía además una versión modificada del marco de “cinco cajas fuertes” para el intercambio de datos con el fin de cuantificar diferentes umbrales de “caja fuerte”. Esa labor continúa con el apoyo de Standards Australia y se propone iniciar los trabajos necesarios para elaborar normas internacionales sobre la preservación de la privacidad y el intercambio de

²⁴ Comunicación de Ian Opperman, Centro de Análisis de Datos, Gobierno de Nueva Gales del Sur, Australia, 31 de agosto de 2018.

datos. Se ha previsto un segundo libro blanco en octubre de 2018, que se espera constituya la base de las actividades internacionales de normalización con el objetivo de definir en última instancia marcos sólidos para la preservación de la privacidad y el intercambio de datos²⁵.

65. Un ejemplo de las limitaciones que tiene la desidentificación a la hora de proteger los registros de nivel unitario fue la publicación en línea, en agosto de 2016, de un gran conjunto de datos longitudinales respecto de una muestra del 10% de australianos que habían solicitado prestaciones de Medicare desde 1984, o prestaciones farmacéuticas desde 2003²⁶. Esto afectó a los datos médicos de unos 2,9 millones de australianos, en cuanto a recetas, episodios quirúrgicos, pruebas (excluidos los resultados) y visitas a médicos generales y especialistas (excluidas las notas de los médicos)²⁷. El conjunto de datos se había descargado 1.500 veces antes de que fuera retirado de la red a raíz de denuncias según las cuales las identificaciones de los médicos eran fáciles de descifrar²⁸ y, más tarde, que era posible identificar a los pacientes²⁹. La publicación de los datos por el Departamento de Salud de Australia tenía como propósito facilitar la investigación médica.

66. Entre las cuestiones importantes que plantean esos ejemplos figuran la de si los conjuntos de datos de información personal que obran en poder de las administraciones deben divulgarse al exterior, cuando existe un riesgo cada vez mayor de que se produzcan vulneraciones de la privacidad en gran escala por medio de la reidentificación, debido en parte a la disponibilidad de otra información divulgada públicamente y a las insuficientes capacidades tecnológicas a nivel institucional; y cuál sería la respuesta adecuada para evitar que ese tipo de incidentes se repitan.

67. De la información recopilada en la consulta se desprende claramente que la divulgación de información en poder de las administraciones requiere medidas adecuadas de protección de la privacidad y respuestas reglamentarias. Se expresó la firme opinión de que el acceso sin restricciones a los datos del nivel de registro unitario, así como a otros datos de carácter personal que no pueden divulgarse de forma segura en forma agregada, es incompatible con el derecho a la privacidad. Los comentarios recibidos no respaldaban las respuestas normativas basadas en

²⁵ *Ibid.*, inclusive Sociedad Australiana de Informática, *Data Sharing Frameworks*, Technical White Paper (Sydney, 2017). Puede consultarse en www.acs.org.au/content/dam/acs/acs-publications/ACS_Data-Sharing-Frameworks_FINAL_FA_SINGLE_LR.pdf.

²⁶ Comunicación de Vanessa Teague al Relator Especial durante las consultas sobre macrodatos y datos abiertos, 26 y 27 de julio de 2018, Universidad de Nueva Gales del Sur, Sídney (Australia). Véase también Oficina del Comisionado de Información de Australia, “Publication of MBS/PBS data”, informe de investigación iniciado a instancias del Comisionado, 20 de marzo de 2018, págs. 7 a 9. Puede consultarse en www.oaic.gov.au/resources/privacy-law/commissioner-initiated-investigation-reports/publication-of-mbs-pbs-data.pdf.

²⁷ Vanessa Teague, Chris Culnane y Ben Rubinstein, “The simple process of re-identifying patients in public health records”, Universidad de Melbourne, Pursuit, 18 de diciembre de 2017. Puede consultarse en <https://pursuit.unimelb.edu.au/articles/the-simple-process-of-re-identifying-patients-in-public-health-records>.

²⁸ Chris Culnane, Benjamin Rubinstein y Vanessa Teague, “Health data in an open world”, informe sobre la reidentificación de pacientes en el conjunto de datos MBS/PBS y sus repercusiones en futuras publicaciones de datos por el Gobierno de Australia, Universidad de Melbourne, 18 de diciembre de 2017. Puede consultarse en <https://arxiv.org/ftp/arxiv/papers/1712/1712.05627.pdf>.

²⁹ La Oficina del Comisionado de Información de Australia encontró que era posible identificar a los médicos, y que los pacientes también podían ser identificados, si bien no eran “razonablemente identificables” a tenor de lo dispuesto en la Ley de Privacidad de Australia. Se entiende que las personas afectadas no han sido informadas al respecto.

criminalizar la reidentificación realizada para someter a prueba la seguridad de los conjuntos de datos publicados³⁰.

68. Los participantes describieron mecanismos ya existentes que permiten el uso de datos personales identificables con fines de investigación³¹ y señalaron que era posible ampliarlos, cuando proceda, para otros usos de interés público³².

69. La cuestión, al parecer, sería la de si dispondríamos de prácticas más sostenibles si los datos útiles se entendieran como un recurso limitado, en lugar de como un recurso ilimitado por explotar³³.

70. Las prácticas actuales que alienan al sujeto de los datos han sido descritas metafóricamente como “matar a la gallina de los huevos de oro”, dado que la desconfianza hacia la capacidad de la administración o de los agentes privados para gestionar debidamente la información de carácter personal hace que las personas no utilicen los servicios —lo que a su vez puede tener impactos sociales adversos, por ejemplo, en las esferas relacionadas con la salud pública—, o proporcionen información incompleta o inexacta³⁴. Estas acciones también socavan la calidad de los datos y, en última instancia, la precisión de los algoritmos de aprendizaje automático.

71. La opinión mayoritaria en la consulta fue la de que la sostenibilidad de las prácticas relacionadas con los datos aumenta si los sujetos de los datos son socios de pleno derecho en las operaciones de datos³⁵. Se afirmó que esto resulta particularmente evidente e importante en el caso de los pueblos indígenas.

C. Soberanía de los datos indígenas

72. Los datos son un recurso cultural, estratégico y económico para los pueblos indígenas. Sin embargo, los pueblos indígenas siguen en gran medida siendo apartados de la recopilación, la utilización y aplicación de datos acerca de ellos mismos, sus tierras y sus culturas³⁶. Los datos y la infraestructura de datos existentes no reconocen ni dan prioridad a los conocimientos y las cosmovisiones indígenas, ni satisfacen las necesidades actuales y futuras de los pueblos indígenas en materia de datos. Las prácticas actuales en torno a los macrodatos y los datos abiertos, bajo los auspicios sea de los gobiernos sea de las empresas, probablemente alejarán aún más los intereses de los pueblos indígenas de los centros donde se adoptan las decisiones que tienen que ver con sus datos.

³⁰ Comunicaciones de, entre otros, M. Paterson.

³¹ Esos mecanismos suelen estar sometidos a la supervisión de comités de ética, y el acceso está restringido a investigadores sujetos a obligaciones en materia de confidencialidad.

³² Por ejemplo, sobre la base de mecanismos como el Marco de las Cinco Cajas Fuertes: véase Oficina de Estadística de Australia, “Managing the risk of disclosure: the five safes framework”, Confidentiality Series, parte 3, agosto de 2017. Puede consultarse en www.abs.gov.au/ausstats/abs@.nsf/Latestproducts/1160.0Main%20Features4Aug%202017?opendocument&tabname=S.

³³ Presentación de Theresa Dirndorfer Anderson, Universidad de Tecnología, Sídney (Australia).

³⁴ Oficina del Comisionado de Información de Australia, *Australian community attitudes to privacy survey, 2017* (Canberra, 2017). Puede consultarse en www.oaic.gov.au/engage-with-us/community-attitudes/australian-community-attitudes-to-privacy-survey-2017. Australia, Oficina del Comisionado de Información de Australia, *Community Attitudes to Privacy Survey: Research Report 2013* (Canberra, 2013). Puede consultarse en www.oaic.gov.au/images/documents/privacy/privacy-resources/privacy-reports/2013-community-attitudes-to-privacy-survey-report.pdf.

³⁵ Comunicación de Theresa Dirndorfer Anderson.

³⁶ Tahu Kukutai y Maggie Walter, “Recognition and indigenizing official statistics: reflections from Aotearoa New Zealand and Australia”, *Statistical Journal of the IAOS*, vol. 31, núm. 2 (2015).

73. La soberanía de los datos indígenas es un movimiento mundial que se ocupa de los derechos que tienen los pueblos indígenas a poseer, controlar, tener acceso y poseer datos obtenidos de ellos y que se refieren a sus miembros, sistemas de conocimiento, costumbres o territorios³⁷. Está respaldada por los derechos de los pueblos indígenas a la libre determinación y la gobernanza de sus tierras, recursos y cultura, tal como se describen en la Declaración de las Naciones Unidas sobre los Derechos de los Pueblos Indígenas. En la soberanía de los datos indígenas está implícito el deseo de que los datos se utilicen de maneras que apoyen y mejoren el bienestar colectivo de las poblaciones indígenas.

74. La soberanía de los datos indígenas tiene un importante papel como principio fundamental en los acuerdos de gobernanza relacionados con los macrodatos y los datos abiertos. Se practica por medio de una gobernanza de los datos indígenas que abarca principios, estructuras, mecanismos de rendición de cuentas, políticas relativas a la gobernanza de los datos, la privacidad y la seguridad, e instrumentos jurídicos. Los marcos de soberanía de los datos indígenas se aplican tanto a los datos nacionales o tribales propios y controlados internamente, como a los datos que se almacenan o gestionan en el nivel externo. Las redes de soberanía de datos indígenas de Australia y Nueva Zelanda están elaborando protocolos en torno a la gobernanza de esos datos³⁸.

75. La soberanía de los datos indígenas ilustra que las buenas prácticas relativas a los macrodatos y los datos abiertos requieren tener presentes los datos que faltan, están subrepresentados o indebidamente representados³⁹, y de los intereses a los que sirven, o no, dichas prácticas.

D. Cuestiones de género

76. En la consulta se afirmó que la privacidad puede ser experimentada de manera diferente por personas de diferente género o identidad de género.

77. La cuestión de la privacidad preocupa cada vez más a las personas lesbianas, gais, bisexuales, transgénero, indecisas e intersexuales, por ejemplo, y también puede ser esencial para la seguridad de las personas, generalmente mujeres, que huyen de la violencia doméstica, familiar o religiosa.

78. Mientras que las prácticas inclusivas de recolección de datos transmiten aceptación y respeto, una recolección intrusiva puede ser una barrera importante a la hora de obtener acceso a los servicios, dado que las comunidades de lesbianas, gais, bisexuales, transexuales, indecisos e intersexuales y otros tienen inquietudes justificadas acerca de la privacidad después de haber sufrido experiencias de discriminación, estigmatización y violencia específica.

79. El grupo de trabajo sobre la privacidad y la personalidad estudiará esta cuestión con mayor detenimiento. Sin embargo, en relación con los macrodatos y los datos abiertos, las buenas prácticas requieren la revisión de la forma en que se recopilan los datos, teniendo presentes las repercusiones que pueden tener unas prácticas

³⁷ Tahu Kukutai y John Taylor, "Data sovereignty for indigenous peoples: current practice and future needs" y C. Matthew Snipp, "What does data sovereignty imply: what does it look like?", en Kukutai y en Taylor (eds.), *Indigenous Data Sovereignty: Towards an Agenda*, Research Monograph, 2016/38 (Canberra, Australian University Press, 2016). Puede consultarse en <https://press.anu.edu.au/publications/series/centre-aboriginal-economic-policy-research-caepr/indigenous-data-sovereignty>.

³⁸ Comunicación de Maggie Walter, Universidad de Tasmania, Australia.

³⁹ Comunicación de Theresa Dirndorfer Anderson.

deficientes en materia de privacidad y las diferentes consecuencias para las personas de diferente género o identidad de género.

E. Derechos del consumidor y recogida y uso de datos de carácter personal

80. En los mercados de consumo basados en datos, el uso creciente de datos para desarrollar, vender y promocionar productos de consumo ha hecho que muchas cuestiones relacionadas con la protección de datos se hayan convertido también en cuestiones de consumo, y viceversa. La distinción entre el derecho de los consumidores y el derecho de protección de datos ya no es tan nítida como antes⁴⁰.

81. El uso de los datos personales de los consumidores por parte de los servicios financieros y otros sectores ha suscitado preocupación tanto a nivel de políticas públicas como a nivel individual⁴¹. El tratamiento correcto de los datos personales forma parte cada vez más de las expectativas razonables de los consumidores con respecto a los servicios y productos que utilizan⁴².

82. En la consulta se compararon los enfoques de la legislación en materia de consumo y de protección de la privacidad y los datos, y se tomó nota de que algunos países están introduciendo iniciativas de protección de la privacidad de los consumidores.

83. Tras el escándalo de Cambridge Analytica, en junio de 2018 el estado de California en los Estados Unidos promulgó la Ley de Privacidad del Consumidor, que entrará en vigor en enero de 2020 para proteger la privacidad de los datos de los usuarios de tecnología y otros mediante la imposición de nuevas normas a las empresas que recopilan, utilizan y comparten datos personales⁴³. La Ley crea cuatro derechos básicos para las personas: el derecho a saber qué información de carácter personal tiene una empresa sobre ellas y de dónde procede o se recibió esa información personal; el derecho a eliminar la información personal que una empresa haya recopilado sobre ellas; el derecho a optar por no consentir que se venda información personal sobre ellas; y el derecho a recibir el mismo servicio y precio de una empresa aunque ejerzan sus derechos de privacidad al amparo de la ley⁴⁴. La Ley también crea un derecho limitado para que los consumidores demanden a las empresas por violaciones de la seguridad de los datos, sobre la base de la ley de notificación de violaciones de datos existente en California.

84. Sin embargo, se ha informado de que es necesario reforzar los derechos consagrados en la ley, por las razones que se exponen a continuación:

⁴⁰ Natali Helberger, Frederik Zuiderveen Borgesius y Agustín Reyna, “The perfect match? A closer look at the relationship between EU consumer law and data protection law”, *Common Market Law Review*, vol. 54 (2017).

⁴¹ Lee Rainie y Maeve Duggan, “Privacy and information sharing”, 14 de enero de 2016 (el grado de comodidad de las personas depende de la percepción de confianza, de lo que ocurre después de la recogida y del tiempo de retención). Phuong Nguyen y Lauren Solomon, *Consumer Data and the Digital Economy – Emerging Issues in Data Collection, Use and Sharing* (Consumer Policy Research Centre, 2018) (observaron que los consumidores querían disponer de más opciones sobre qué datos se recopilan y cómo se usan, y que el gobierno participe en la mejora del control por el consumidor de los datos y la protección contra el uso indebido de estos).

⁴² Helberger, Zuiderveen Borgesius y Reyna, “The perfect match?”.

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

⁴⁴ Adam Schwartz, Lee Tien y Corynne McSherry, “How to improve the California Consumer Privacy Act of 2018”, Electronic Frontier Foundation, 8 de agosto de 2018.

a) El término “empresa” se define de forma restrictiva⁴⁵. En la era digital, los pequeños agentes tecnológicos y los particulares también pueden socavar la privacidad de multitud de maneras por no disponer de los conocimientos, las competencias o los recursos necesarios para aplicar una protección de datos adecuada⁴⁶;

b) Las empresas pueden seguir cobrando un precio más alto a los usuarios que ejercen sus derechos de privacidad;

c) Los usuarios no pueden llevar fácilmente a los infractores ante los tribunales debido a las estrictas excepciones;

d) El consentimiento del usuario solo se requiere para la venta de datos, no para su recopilación, y los usuarios han de optar expresamente por no consentir la venta de datos;

e) El “derecho a saber” no especifica fuentes y destinatarios, y el “derecho a la supresión” se refiere a la información que se recopila sobre ellos, y no a la información que se tiene sobre ellos;

f) La responsabilidad de la aplicación de la ley recae principalmente en el Fiscal General de California y no en una entidad independiente.

85. Con arreglo a la legislación de protección de datos de la Unión Europea, algunos aspectos del Reglamento General de Protección de Datos prevén nuevas protecciones para los consumidores dentro de la Unión Europea, entre ellas una transparencia y un control de los datos que las empresas recaban sobre ellas mayores de los que proporcionan las directivas de protección del consumidor de la Unión Europea⁴⁷.

86. Australia está estableciendo un “derecho del consumidor sobre los datos”, un derecho de portabilidad de los datos⁴⁸ que no está a la altura de las protecciones más amplias que ofrecen las leyes de privacidad o de protección de datos a los consumidores australianos cuyos datos son recogidos, compartidos y utilizados a diario⁴⁹. En la consulta se afirmó que este derecho de portabilidad de los datos, en lugar de proteger los datos de los consumidores, podría exponerlos a un mayor uso por parte de terceros⁵⁰.

87. Establecer una fuerte conexión entre el derecho del consumidor y el derecho a la privacidad resulta ventajoso, por ejemplo, en una acción legal coordinada⁵¹. El derecho del consumidor puede ser un instrumento útil para salvaguardar el equilibrio general de la relación comercial entre consumidores y proveedores y puede utilizarse para evaluar la equidad de aquellas situaciones en las que las empresas exigen que los

⁴⁵ *Ibid.*, “la Ley define ‘una empresa’ como una persona jurídica con fines de lucro con: i) ingresos brutos anuales de 25 millones de dólares; ii) la recepción o divulgación anual de información personal correspondiente a 50.000 consumidores, hogares o dispositivos; o iii) la recepción del 50% o más de sus ingresos anuales por la venta de información personal (artículo 140 c))”.

⁴⁶ Comunicación de Roland Wen, Universidad de Nueva Gales del Sur, Sídney, Australia.

⁴⁷ Helberger, Zuiderveen Borgesius y Reyna, “The perfect match?”.

⁴⁸ Australian Competition and Consumer Commission, “Consumers' right to their own data is on its way”, comunicado de prensa, 16 de julio de 2018. Puede consultarse en www.accc.gov.au/media-release/consumers-right-to-their-own-data-is-on-its-way.

⁴⁹ Nguyen y Solomon, *Consumer Data and the Digital Economy*.

⁵⁰ Comunicación de Vanessa Teague al Relator Especial durante las consultas sobre macrodatos y datos abiertos, 26 y 27 de julio de 2018, Universidad de Nueva Gales del Sur, Sídney, Australia.

⁵¹ Grupos de consumidores de los Estados Unidos y de la Unión Europea han pedido conjuntamente a las agencias de consumidores y a las autoridades de protección de datos que examinen las infracciones de la protección de datos y del derecho de los consumidores que se producen en los juguetes conectados. Helberger, Zuiderveen Borgesius y Reyna, “The perfect match?”.

consumidores den su consentimiento al tratamiento de cantidades desproporcionadas de datos o al intercambio de datos con terceros.

88. Entre las observaciones recibidas acerca de las medidas prácticas para ayudar a las entidades a mejorar su relación de confianza con los usuarios, algunas aludieron a la comunicación de las condiciones de uso de los datos por medio de licencias estándar similares a las seis licencias Creative Commons normalizadas. Se consideró que esto podría ser un medio de mitigar algunos de los problemas que plantean las políticas complejas en materia de privacidad, simplificando y normalizando al mismo tiempo la comunicación con los usuarios de distintos países⁵². Los proyectos de tipos de licencia podrían ir respaldados por políticas de privacidad de “condiciones estándar” más detalladas.

89. Indicar los riesgos para la privacidad mediante el uso de etiquetas de calificación de la privacidad podría servir para que las opciones de privacidad fueran más accesibles para los consumidores y para aumentar la transparencia y la información sobre los riesgos para la privacidad por parte de los responsables del tratamiento de los datos⁵³.

F. Inteligencia artificial

90. El aprendizaje automático y la inteligencia artificial utilizan enormes cantidades de datos y, a su vez, generan más datos. La combinación de la disponibilidad de datos, la potencia de cálculo y las capacidades analíticas utilizando algoritmos complejos, unida al aprendizaje automático y la inteligencia artificial, tiene el potencial de revolucionar positivamente las sociedades, pero también de alterar profundamente nuestro mundo y nuestras posibilidades de supervivencia, no necesariamente para mejor⁵⁴.

91. Este último resultado podría darse a raíz del posible impacto negativo de la inteligencia artificial en los derechos humanos, entre ellos el derecho a la privacidad. Los métodos de inteligencia artificial pueden ser y están siendo utilizados para identificar a personas que desean permanecer en el anonimato; para permitir la microselección a fin de orientar los mensajes; para generar información sensible sobre personas a partir de datos no sensibles; para trazar el perfil de personas utilizando datos de escala poblacional; y para adoptar decisiones sirviéndose de esos datos, influyendo profundamente con ello en la vida de las personas⁵⁵.

92. A medida que aumenta el número de acciones y decisiones que se transfieren a las máquinas, es urgente garantizar que los algoritmos y el aprendizaje automático sean transparentes en cuanto a su lógica y sus supuestos. Los algoritmos utilizados en el aprendizaje automático y la inteligencia artificial son cada vez más complejos; la transparencia será difícil de lograr. Con todo, esa complejidad no debe ser un obstáculo para realizar auditorías encaminadas a determinar la legalidad⁵⁶. En la

⁵² Comunicación presentada por el Centro de Tecnología Allens, Law and Innovation, 14 de agosto de 2018.

⁵³ Véase Lorrie Faith Cranor, “Necessary but not sufficient: standardized mechanisms for privacy notice and choice”, *Journal on Telecommunications and High Technology Law*, vol. 10, núm. 2 (verano de 2012).

⁵⁴ Toby Walsh, *2062: The World that AI Made*, (Carlton, Victoria (Australia), La Trobe University Press, 2018).

⁵⁵ Privacy International y Artículo 19, “Privacy and freedom of expression in an age of artificial intelligence”, abril de 2018.

⁵⁶ Agencia de los Derechos Fundamentales de la Unión Europea, *#BigData: Discrimination in Data Supported Decision Making* (Luxemburgo, Oficina de Publicaciones de la Unión Europea, 2018).

actualidad, el uso de tecnologías relacionadas con los macrodatos no está sometido a un escrutinio suficiente en cuanto al cumplimiento del derecho internacional de los derechos humanos, las normas de protección de datos, las normas sectoriales de privacidad, los códigos de ética o las normas de la industria⁵⁷. Se ha argumentado que las máquinas deben cumplir normas éticas más estrictas que los seres humanos y que, si se toman las decisiones correctas, la privacidad no será una anomalía histórica, sino un derecho otorgado tecnológicamente⁵⁸.

93. El Reglamento General de Protección de Datos limita el uso de la adopción de decisiones automatizada en determinadas circunstancias y exige que se facilite a las personas información sobre la existencia de la adopción de decisiones automatizada, la lógica asociada y la importancia y las consecuencias que previsiblemente tendrá el tratamiento de esos datos para la persona⁵⁹. Existe una prohibición general, con estrictas excepciones, de la toma de decisiones únicamente mediante procesos automatizados cuando dichas decisiones tienen efectos legales u otros efectos de importancia.

94. El Reglamento define la elaboración de perfiles como el tratamiento automatizado de datos para analizar o formular predicciones sobre las personas y establece la obligación de incorporar la protección de datos desde el diseño y por defecto. Las evaluaciones del impacto sobre la privacidad de los datos serán obligatorias para muchas aplicaciones de inteligencia artificial y de aprendizaje automático que son invasivas de la privacidad y que entran en el ámbito de aplicación de la legislación sobre protección de datos y tienen importantes riesgos previstos, como el tratamiento de datos sensibles. En el caso de la inteligencia artificial, una evaluación del impacto en la privacidad de los datos podría —quizás debería— permitir que las entidades elaborasen modelos de los efectos de sus algoritmos de forma análoga a los científicos del clima cuando elaboran modelos del cambio climático o las pautas meteorológicas⁶⁰.

95. La Agencia de los Derechos Fundamentales de la Unión Europea ha sugerido que una manera de asegurar una rendición de cuentas efectiva podría ser el establecimiento de órganos especiales con un mandato exclusivo para encargarse de la supervisión de las tecnologías relacionadas con los macrodatos, similar al papel de las autoridades encargadas de la protección de datos⁶¹.

96. Aunque todavía no se han determinado los medios, es importante que las nuevas tecnologías hayan requerido el fortalecimiento del derecho internacional humanitario a lo largo del siglo XX⁶².

G. Principios relativos a los macrodatos y los datos abiertos

97. En su informe de octubre de 2017, el Relator Especial planteó la cuestión de la elaboración de principios para regular los macrodatos y los datos abiertos. En la consulta se señaló que, en la medida de lo posible, la elaboración de esos principios

⁵⁷ Lee Rainie y Janna Anderson, *Code-dependent: pros and cons of the algorithm age*, Pew Research Center, 2017.

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

⁵⁹ Reglamento General de Protección de Datos de la Unión Europea 2016/679 de 27 de abril de 2016, artículos 13, 14 y 22.

⁶⁰ Andrew Smith, “Franken-algorithms: the deadly consequences of unpredictable code”, *The Guardian*, 30 de agosto de 2018. Puede consultarse en www.theguardian.com/technology/2018/aug/29/coding-algorithms-frankenalgos-program-danger, donde se cita a Neil F. Johnson y otros, “Population polarization dynamics and next-generation social media algorithms”, 16 de diciembre de 2017. Puede consultarse en <https://arxiv.org/pdf/1712.06009.pdf>.

⁶¹ Agencia de los Derechos Fundamentales de la Unión Europea.

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

debe tener presentes los acuerdos internacionales sobre protección de datos considerados como “mejores prácticas”. En la actualidad, esos acuerdos son el Reglamento General de Protección de Datos y el Convenio 108 modernizado; este tiene su origen en el Consejo de Europa, pero está abierto a la adhesión a escala mundial de los Estados que hayan promulgado principios afines⁶³.

98. El Reglamento General de Protección de Datos no ejerce su influencia únicamente por medio de la promulgación de leyes locales o de su aplicación extraterritorial. Muchas empresas no radicadas en Europa -Microsoft es el ejemplo más destacado- están asumiendo voluntariamente la observancia del Reglamento en todas sus operaciones comerciales, con independencia de que tengan o no la obligación jurídica de hacerlo. Dicha adopción voluntaria puede ser tan importante como la adopción legalmente exigida⁶⁴.

99. Desde otra perspectiva, los países que cuentan con leyes amplias de localización de datos están creando nuevos criterios de privacidad respecto de los datos recopilados dentro de su jurisdicción. En China, la Ley de Ciberseguridad introduce restricciones a las transferencias transfronterizas de datos que difieren de los regímenes internacionales en materia de privacidad, como el Reglamento General de Protección de Datos y las Reglas de Privacidad Transfronteriza, de carácter voluntario, del Foro de Cooperación Económica de Asia y el Pacífico⁶⁵. Aunque el Reglamento y la Ley parecen tener criterios de prueba similares en relación con las transferencias transfronterizas, la segunda no prevé las excepciones que figuran en la primera⁶⁶. La Ley tampoco contiene ciertos mecanismos previstos en el Reglamento, como normas corporativas obligatorias o cláusulas estándar de protección de datos para que las empresas obtengan la aprobación.

100. Las recomendaciones preliminares del Relator Especial en su informe de octubre de 2017 a la Asamblea General se elaboraron de forma independiente del Reglamento General de Protección de Datos y del Convenio 108 modernizado, pero están en consonancia con esos instrumentos (véase el cuadro)⁶⁷. El grado de consonancia que se ha logrado es importante si se tiene en cuenta el contexto internacional más amplio: el Convenio 108 modernizado se está globalizando poco a poco e incluye muchos de los nuevos elementos del Reglamento, aunque no todos⁶⁸. Es probable que, en los próximos 5 a 10 años, los efectos extraterritoriales del Reglamento con el grupo cada vez más amplio de Estados partes en el Convenio tengan un efecto apreciable en la profundización de la cultura mundial de la privacidad. La naturaleza exacta de esa evolución está aún por precisar, al igual que su pertinencia en relación con la necesidad de nuevos avances, por ejemplo principios autónomos relativos a los macrodatos y los datos abiertos.

⁶³ Comunicación de Graham Greenleaf, Universidad de Nueva Gales del Sur, Sídney, agosto de 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”, University of New South Wales Law Research Series, núm. 56, 25 de mayo de 2018. Puede consultarse en www.austlii.edu.au/au/journals/UNSWLRS/2018/56.html.

⁶⁵ Samm Sacks, Paul Triolo y Graham Webster, “Beyond the worst-case assumptions on China’s cybersecurity law”, publicación en blog, *New America*, 13 de octubre de 2017; y comunicación presentada por el Centro de Tecnología Allens, Law and Innovation, 14 de agosto de 2018.

⁶⁶ Xiaoyan Zhang, “Cross-border data transfers: CSL vs. GDPR”, *The Recorder*, 2 de enero de 2018; y comunicación presentada por el Centro de Tecnología Allens, Law and Innovation, 14 de agosto de 2018.

⁶⁷ Comunicación de Graham Greenleaf, agosto de 2018.

⁶⁸ Desde 2011, a las 47 partes del Convenio 108 que son miembros del Consejo de Europa se han sumado las solicitudes de adhesión de la Argentina, Burkina Faso, Cabo Verde, Marruecos, Mauricio, México, el Senegal, Túnez y el Uruguay. Otros 11 países, o sus autoridades de protección de datos, son observadores en su Comité Consultivo.

101. Si bien es necesario disponer de un marco internacional coherente para la regulación de los macrodatos y los datos abiertos, sería prematuro comenzar a trabajar sobre unos principios independientes específicamente relativos a los macrodatos o los datos abiertos antes de haber tenido tiempo suficiente para determinar la solidez y el efecto internacional del Reglamento General de Protección de Datos y del Convenio 108 modernizado.

102. Por consiguiente, las recomendaciones relativas a los macrodatos y los datos abiertos deben entenderse incluidas en el ámbito de los principios de privacidad y protección de datos ya existentes, y no en relación con un conjunto de normas especiales nuevas.

Recomendaciones del Relator Especial en su informe de octubre de 2017 y su correspondencia con el Reglamento General de Protección de Datos y el Convenio 108 Modernizado

<i>Párrafo del informe del Relator Especial de octubre de 2017 (A/72/540)</i>	<i>Artículo del Reglamento General de Protección de Datos de la Unión Europea</i>	<i>Artículo del Convenio 108 Modernizado</i>
131 a), sobre la responsabilidad	5, párr. 2 “Responsabilidad”	10, párr. 1
131 b), sobre la transparencia	12 “Transparencia”; 22, párr. 3 “Decisiones automatizadas” y transparencia	5, párr. 4; 8, párr. 1
131 c), sobre la calidad	5, párr. 1 c) “minimización de datos”, d) “exactitud”	5, párr. 1
131 d), sobre la previsibilidad del aprendizaje automático	22 “Decisiones automatizadas”	8, párrs. 1, 2
131 e), sobre la seguridad	32-34 “Seguridad del tratamiento” (incluida la notificación de violaciones de la seguridad)	7, párr. 1
131 f), sobre los instrumentos de determinación y mitigación de riesgos	35 “Evaluación de impacto relativa a la protección de datos”; 36 “Consulta previa”	10, párr. 2
131 g), sobre la capacitación de los empleados	37-39 “Delegado de protección de datos”	–
131 h), sobre el enfoque inequívoco de la regulación de la privacidad	52 “Independencia” de la autoridad de protección de datos	15, párr. 5
131 i), sobre facultades de regulación suficientes para los “macrodatos”.	57 “Funciones”, 58 “Poderes”	12, 15
131 j), sobre leyes de privacidad adaptadas a los avances tecnológicos	4, párr. 1 “datos personales”; 4, párr. 4 “elaboración de perfiles”; 4, párr. 5 “seudonimización”; 22 “Decisiones automatizadas”; 25 “Protección de datos desde el diseño y por defecto”	8 párrs. 1 y 2; 10, párr. 3
131 k), sobre los mecanismos formales de consulta	36 “Consulta previa” 57 b), c), d) y g) Autoridad de control “Funciones”	–
131 l), sobre las consultas relativas a prácticas peligrosas	36 “Consulta previa”	–

<i>Párrafo del informe del Relator Especial de octubre de 2017 (A/72/540)</i>	<i>Artículo del Reglamento General de Protección de Datos de la Unión Europea</i>	<i>Artículo del Convenio 108 Modernizado</i>
131 m), sobre técnicas nuevas	57 i) autoridad de control “Funciones - “seguimiento de las nuevas tecnologías”; 25 “protección de datos desde el diseño y por defecto”	10, párr. 3
131 n), sobre el grado de conocimiento de los ciudadanos	12 “Transparencia”; 13-15 “Información al interesado “; 57 b), c), e) autoridad de control “Funciones”	15, párr. 2 e)
126, sobre requisitos vinculantes y mecanismos de aplicación rigurosos respecto de los datos abiertos en relación con la desidentificación	25 “Protección de datos desde el diseño y por defecto”; 4, párr. 1 “datos personales”; 4, párr. 5 “seudonimización”	10, párr. 3
127, sobre evaluaciones rigurosas de los efectos sobre la privacidad cuando en los datos abiertos su utilizan datos del nivel de registro unitario	35 “Evaluación de impacto relativa a la protección de datos”	10, párr. 2
128, No habrá datos abiertos o intercambio de datos de nivel unitario sin una desidentificación segura	4, párr. 1 “datos personales”; 4, párr. 5 “seudonimización”	2 d)
129, Garantizar protecciones adicionales para los datos sensibles	9 “Categorías especiales”	6

Fuente: Graham Greenleaf, comunicación posterior a la consulta, 7 de agosto de 2018.

H. Conclusiones

103. **Los datos son y seguirán siendo un activo económico fundamental, como el capital o la mano de obra. Su dependencia integral respecto de la información personal exige la observancia de las leyes en materia de privacidad y protección de datos.**

104. **El derecho internacional de los derechos humanos exige que toda injerencia en el derecho a la privacidad sea legal, necesaria y proporcionada. En ocasiones, las vulneraciones de la privacidad pueden ser legales, pero otra cuestión es que sean éticas. Es discutible que algunos de los ejemplos que aquí se examinan sean éticos, legales, necesarios y proporcionados. Los casos recientes de mala gestión de los datos personales por parte de entidades privadas y públicas exigen respuestas contundentes a fin de evitar que se repitan.**

105. **El derecho internacional de los derechos humanos también exige que las personas que sufran una vulneración de su derecho a la privacidad tengan acceso a vías de recurso. Esto cobra aún más importancia en la era de los macrodatos y los datos abiertos.**

106. **Una dificultad fundamental para la divulgación pública de datos en forma de datos abiertos es que no existe una manera de determinar inequívocamente si los conjuntos de datos supuestamente desidentificados o los datos agregados contienen información de carácter personal.**

107. **En las políticas y las prácticas relacionadas con los datos abiertos subyacen factores económicos y políticos. Los modelos de negocio asociados a las economías capitalistas tienen pocos incentivos para proteger los datos personales**

cuando esta protección no da lugar a una desventaja económica que menoscabe los beneficios previstos.

108. Un marco internacional dotado de mecanismos coherentes de protección de datos y reglas claras respecto del acceso transnacional ayudaría a sopesar las protecciones de la privacidad y los intereses contrapuestos que los países pueden tener a la hora de acceder a los datos, por ejemplo en el contexto de la aplicación de la ley, o que las empresas multinacionales pueden tener en la gestión de los flujos de datos a nivel interno.

109. Las iniciativas que permiten el intercambio de datos sin restricciones y las que desmantelan las salvaguardias legales existentes en materia de privacidad son contrarias a la protección del derecho a la privacidad y deben cesar.

110. La criminalización de la reidentificación (en aras del interés público) de conjuntos de datos desidentificados no se considera adecuada como forma de salvaguardar los datos personales.

111. Los datos detallados a nivel de registro unitario (datos identificables) no deben divulgarse ni publicarse en línea sin el consentimiento del interesado. Es apropiado el uso de métodos físicos y técnicos, como entornos de investigación seguros, para restringir el acceso a datos sensibles a nivel de registro unitario.

112. El derecho del consumidor y el derecho de protección de datos pueden complementarse provechosamente entre sí. El derecho en materia de privacidad, con sus dimensiones sociales y de derechos humanos, proporciona un anclaje para el derecho del consumidor. Apoyarse únicamente en el derecho del consumidor priva a las personas de los aspectos habilitantes más amplios que tiene la dependencia entre los derechos humanos fundamentales y sus mecanismos de reparación.

113. Las manifestaciones actuales y potenciales de la inteligencia artificial exigen una supervisión independiente por parte de expertos en diferentes disciplinas. La evolución de esta tecnología necesita un sólido marco jurídico y político que esté anclado en los derechos humanos. Se trata de una cuestión urgente y crítica.

114. La aplicación del artículo 22 del Reglamento General de Protección de Datos debe ser objeto de un estrecho seguimiento en lo que se refiere a su capacidad para abordar los problemas del tratamiento automatizado derivados del uso de la inteligencia artificial.

115. Es fundamental resolver la falta de las capacidades tecnológicas necesarias para diseñar sistemas, métodos y procesos adecuados y para garantizar la solidez de los sistemas, métodos y procesos con miras a una sólida protección de los datos de carácter personal. En este aspecto deben participar las pequeñas empresas y empresas emergentes del campo de la tecnología.

116. En los casos en que los Estados Miembros estén estudiando la posibilidad de adoptar legislación para la promoción de los datos abiertos⁶⁹, se recomiendan los siguientes parámetros:

g) Toda la legislación debe estar firmemente alineada con las obligaciones internacionales de cada Estado en materia de derechos humanos;

⁶⁹ Por ejemplo, véanse las propuestas de Australia en “New Australian Government data sharing and release legislation: issues paper for consultation”, disponible en www.pmc.gov.au/resource-centre/public-data/issues-paper-data-sharing-release-legislation, la comunicación de M. Paterson.

h) La legislación sobre protección de datos que constituya mejores prácticas debe estudiarse y tomarse como ejemplo;

i) Los marcos de ética en relación con los datos y los mecanismos de rendición de cuentas basados en los principios de imparcialidad y justicia son necesarios para las prácticas de los sectores público y privado en la esfera de los datos;

j) Los modelos reguladores adecuados para la protección de la privacidad y de los datos requieren independencia estructural, recursos adecuados y un regulador capaz de trabajar con independencia;

k) Desmantelar las leyes de privacidad y protección de datos para permitir los datos abiertos es contrario a las tendencias mundiales, desacertado y opuesto a las obligaciones internacionales de los Estados en materia de derechos humanos en lo que atañe al derecho a la privacidad;

l) Las definiciones y los conceptos deben distinguir entre intercambio, uso, divulgación y publicación de datos;

m) Los marcos de diseño conjunto deben utilizar modelos y mecanismos participativos con una representación suficientemente diversa para abordar cuestiones como la soberanía de los datos indígenas.

I. Recomendaciones

117. Las recomendaciones iniciales que el Relator Especial formuló en su informe a la Asamblea General de fecha 19 de octubre de 2017 (A/72/540) se han ampliado teniendo en cuenta los resultados de la consulta, como sigue:

a) El intercambio interno de datos personales por parte de los gobiernos debe distinguirse en la legislación, las políticas y las prácticas de la divulgación de datos al público en forma de datos abiertos;

b) A menos y hasta que sea posible determinar de forma inequívoca si existe información personal en los datos agregados o que los datos desagregados no pueden volver a agregarse, los datos abiertos no deben contener datos a nivel de registro unitario;

c) Los trabajos encaminados a elaborar normas internacionales de privacidad que preserven el intercambio de datos y las actividades internacionales de normalización deben proseguir sin demora y recibir el apoyo de los Estados Miembros;

d) La investigación sobre la privacidad diferencial es necesaria y debe utilizarse para estadísticas agregadas y tipos de datos complejos, así como para otras tecnologías dirigidas a preservar la privacidad, como el cifrado homomórfico y la computación multiparte segura;

e) Como respuesta mínima provisional a la aceptación de normas detalladas de protección de la privacidad armonizadas a nivel mundial, se alienta a los Estados Miembros a que ratifiquen el Convenio 108 modernizado por medio de su instrumento jurídico habilitante (Protocolo CETS 223) y a que apliquen sin demora injustificada los principios contenidos en él por conducto de la legislación nacional, prestando especial atención a la aplicación inmediata de las disposiciones que exigen salvaguardias para los datos personales recogidos con fines de vigilancia y otros fines de seguridad nacional;

f) A fin de ajustarse a las mejores prácticas, al revisar y actualizar su legislación nacional como parte de la aplicación del Convenio 108 modernizado,

se alienta a los Estados Miembros no pertenecientes a la Unión Europea a que, siempre que sea posible, incorporen también las salvaguardias y vías de recurso que figuran en el Reglamento General de Protección de Datos, pero que no son obligatorios en virtud del Convenio;

g) Los gobiernos y las empresas deben reconocer la soberanía de los pueblos indígenas respecto de los datos que les conciernen o que se han recopilado sobre ellos y que se refieren a las poblaciones, los sistemas de conocimientos, las costumbres o los territorios indígenas, incluyendo siempre los principios formalizados elaborados por los indígenas, una atención especial al liderazgo indígena y mecanismos de rendición de cuentas;

h) Los Estados Miembros deben examinar la idoneidad de todos los marcos jurídicos y normativos en materia de inteligencia artificial para la protección de la libertad de expresión y el derecho a la privacidad; fomentar una intensa colaboración multidisciplinaria entre estadísticos, juristas, sociólogos, informáticos, matemáticos y expertos en la materia; e idear estrategias para prevenir o afrontar cualquier efecto negativo en el disfrute de los derechos humanos que se derive de la utilización de algoritmos, el tratamiento automatizado, el aprendizaje automático y la inteligencia artificial.

118. El Relator Especial reitera además las recomendaciones que formuló en su informe anterior (véase [A/72/540](#), párrs. 126 a 131).
