Naciones Unidas A/HRC/40/63

Asamblea General

Distr. general
16 de octubre de 2019
Español
Original: inglés

Consejo de Derechos Humanos
40º período de sesiones
25 de febrero a 22 de marzo de 2019
Tema 3 de la agenda
Promoción y protección de todos los derechos humanos, civiles, políticos, económicos, sociales y culturales, incluido el derecho al desarrollo

Derecho a la privacidad

Informe del Relator Especial sobre el derecho a la privacidad*

Resumen

En su informe, preparado de conformidad con las resoluciones 28/16 y 37/2 del Consejo de Derechos Humanos, el Relator Especial sobre el derecho a la privacidad se centra en cuestiones relacionadas con la supervisión de los servicios de inteligencia y hace referencia al primer informe sobre la labor en materia de privacidad y género del Equipo de Tareas sobre la Privacidad y la Personalidad y al informe del Equipo de Tareas sobre Datos Sanitarios.

* Este informe se presenta con retraso para poder incluir en él la información más reciente.

GE.19-17878 (S) 021219 031219
1917878

Índice

I. Resumen de las actividades

1. Desde marzo de 2018, el Relator Especial sobre el derecho a la privacidad ha avanzado en la ejecución de su mandato, para lo cual ha examinado la información pertinente, incluidos los desafíos que plantean las nuevas tecnologías, realizado visitas oficiales y "oficiosas" a distintos países, promovido la protección del derecho a la privacidad, abogado por los principios de la privacidad, contribuido a eventos internacionales con el objetivo de promover un enfoque coherente del derecho a la privacidad, sensibilizado sobre el derecho a la privacidad y los recursos efectivos, y denunciado las presuntas vulneraciones de ese derecho.

2. En octubre de 2018, el Relator Especial presentó un informe a la Asamblea General que trataba sobre los macrodatos y los datos abiertos (A/73/438).

3. Desde la presentación de su informe anual de 2018 ante el Consejo de Derechos Humanos (A/HRC/37/62), el Relator Especial ha llevado a cabo, entre otras, las siguientes actividades:

a) Colaboración con los presidentes de los cinco equipos de tareas encargados de las líneas de acción temáticas (los macrodatos y los datos abiertos, los datos sanitarios, la privacidad y la personalidad, la seguridad y la vigilancia, y la utilización de datos personales por las empresas) con el fin de hacer avanzar la labor de los equipos de tareas;

b) Envío de un total de 24 comunicaciones a los Estados Miembros en las que planteaba cuestiones relacionadas con el derecho a la privacidad, y publicación de 14 comunicados de prensa y declaraciones[1];

c) Visitas oficiales al Reino Unido de Gran Bretaña e Irlanda del Norte (junio de 2018) y a Alemania (noviembre de 2018);

d) Participación en eventos internacionales como orador principal o ponente[2];

e) Celebración de consultas con diversos órganos, por ejemplo el Irish Council for Civil Liberties, la Japan Civil Liberties Union, la Japan Federation of Bar Associations, Privacy International y la Comisión de Derechos Humanos de Irlanda del Norte, y participación en múltiples actividades del Foro para la Gobernanza de Internet y de RightsCon, entre muchos otros eventos;

f) Intercambio de información con gobiernos (a nivel nacional y subnacional); autoridades encargadas de la protección de datos y la privacidad; la Presidenta del Grupo de Trabajo del Artículo 29 sobre la Protección de Datos de la Unión Europea; la Presidenta del Comité Consultivo del Convenio del Consejo de Europa para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal (Convenio 108); organizaciones de normalización, como la Unión Internacional de Telecomunicaciones; el Instituto de Ingenieros Electricistas y Electrónicos; organizaciones de la sociedad civil; las misiones permanentes ante la Oficina de las Naciones Unidas en Ginebra; los titulares de mandatos de los procedimientos especiales; la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos; investigadores; representantes del mundo académico; y órganos profesionales.

II. La privacidad en contexto

4. El derecho a la privacidad puede facilitar el ejercicio de otros derechos humanos. Del mismo modo, la vulneración de ese derecho limita el disfrute de otros derechos humanos.

[1] En total, envió 18 cartas y publicó 6 comunicados de prensa conjuntamente con otros Relatores Especiales.

[2] Véase www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2019_HRC_Annex1_Keynotes.pdf.

5. Existen en la historia varios ejemplos de Estados Miembros que ratificaron instrumentos internacionales de derechos humanos sin tener una voluntad real de adoptar las medidas necesarias para aplicarlos. Uno de ellos es la República Democrática Alemana, que, aunque al ratificar el Pacto Internacional de Derechos Civiles y Políticos, el 8 de noviembre de 1973, asumió la obligación de respetar, entre otros, el derecho a la privacidad (art. 17), mantuvo un régimen de vigilancia conocido por vulnerar de manera generalizada y sistemática la privacidad de muchos de sus ciudadanos.

6. Lamentablemente, el Relator Especial observa a menudo contradicciones similares en la actualidad: si bien la mayoría de los Estados Miembros se comprometen inequívocamente a proteger el derecho a la privacidad, muchos actúan de maneras que lo hacen peligrar cada vez más, utilizando nuevas tecnologías que son incompatibles con ese derecho, como los macrodatos y los datos sanitarios, atentando contra la dignidad de sus ciudadanos por motivos de género o de identidad o expresión de género y vigilando de manera arbitraria a su propia población.

7. El derecho a la libre determinación, consagrado en el artículo 1, párrafo 1, del Pacto Internacional de Derechos Civiles y Políticos, permite a todos los pueblos establecer su condición política y proveer libremente a su desarrollo. Del mismo modo, todas las libertades fundamentales enunciadas en el Pacto, como el derecho a la libertad de circulación (art. 12), el derecho a la libertad de asociación (art. 22), el derecho a la libertad de religión (art. 18), el derecho a la libertad de expresión (art. 19) o el derecho a la privacidad (art. 17), protegen el derecho de todas las personas a la autonomía personal. El derecho de los ciudadanos a elegir qué ser, cuándo, dónde y con quién estar y qué pensar y decir forma parte de los derechos inalienables que los países han acordado proteger en virtud del Pacto.

8. El derecho a la privacidad es indisociable de los debates sobre la autonomía personal. Ya en 1976, Paul Sieghart identificó los siguientes vínculos entre la privacidad, los flujos de información, la autonomía y el poder:

> En una sociedad en la que las tecnologías modernas de la información avanzan rápidamente, surge la posibilidad de que muchas más personas lleguen a conocer nuestra manera de actuar. Y eso, a su vez, puede limitar nuestra libertad para comportarnos como queramos, ya que una vez que los demás descubren nuestra forma de actuar, pueden considerar que es más conveniente para ellos, para la sociedad o incluso para nosotros mismos disuadirnos, desanimarnos o incluso impedirnos hacer lo que queramos, y podrían intentar manipularnos para que hagamos lo que ellos quieren [cita traducida][3].

9. El Relator Especial estableció el siguiente vínculo entre esas observaciones y la privacidad:

> Desprovistas del manto protector que les confiere la privacidad, las personas se vuelven transparentes y, por lo tanto, manipulables. Una persona manipulable está a merced de quienes controlan la información sobre ella, y su libertad, que suele ser relativa como mucho, se reduce de manera directamente proporcional a la cantidad y el tipo de opciones y alternativas que dejan a su disposición quienes poseen el control de su información [cita traducida][4].

10. De ahí que exista una relación tan estrecha entre la privacidad y la verdadera autonomía personal. A menudo, la vulneración de la privacidad se enmarca en un sistema que pone en riesgo otras libertades. Y aunque con frecuencia estas vulneraciones las cometen agentes estatales con el objetivo de hacerse con el poder y conservarlo, a veces los responsables son instancias no estatales, como personas y empresas, que desean seguir ejerciendo control sobre otras personas. Por eso, en muchos casos, el Relator Especial debe estudiar la relación que existe entre las vulneraciones del derecho a la privacidad y la violación de otros derechos.

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

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

La privacidad como derecho relativo y el criterio de necesidad en una sociedad democrática

11. El derecho a la privacidad no es un derecho absoluto, sino relativo. Puede restringirse, pero siempre de una manera cuidadosamente delimitada. De conformidad con lo estipulado en el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos, las injerencias en el derecho a la privacidad son permisibles en virtud del derecho internacional de los derechos humanos siempre y cuando no sean arbitrarias ni ilegales. El Comité de Derechos Humanos explicó en su observación general núm. 16 (1988), sobre el derecho a la intimidad, que el término "ilegales" significa que las injerencias deben estar previstas por la ley, que a su vez debe conformarse a las disposiciones, propósitos y objetivos del Pacto. El concepto de arbitrariedad, según el Comité, garantiza que incluso las injerencias previstas en la ley estén en consonancia con las disposiciones, los propósitos y los objetivos del Pacto y sean, en todo caso, razonables en las circunstancias particulares del caso.

12. En su observación general núm. 31 (2004), sobre la índole de la obligación jurídica general impuesta a los Estados partes en el Pacto, el Comité de Derechos Humanos estipula que los Estados partes deben abstenerse de violar los derechos reconocidos por el Pacto, y que cualesquiera restricciones a cualquiera de esos derechos debe ser permisible de conformidad con las disposiciones pertinentes del Pacto. Cuando se introducen restricciones, los Estados deben demostrar su necesidad y adoptar únicamente las medidas que resulten proporcionales a la consecución de los legítimos objetivos para lograr una protección constante y eficaz de los derechos del Pacto. El Comité subraya además que en ningún caso se deben aplicar las restricciones o invocarse de una manera que menoscabe la esencia de un derecho del Pacto.

13. La expresión "necesario en una sociedad democrática" figura como tal en dos artículos del Pacto Internacional de Derechos Civiles y Políticos, a saber, el artículo 21 (derecho de reunión pacífica) y el artículo 22 (libertad de asociación), pero no en el artículo 17.

14. En el artículo 8, párrafo 2, del Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales (Convenio Europeo de Derechos Humanos) se explicita la naturaleza de dicha expresión:

> No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás.

15. En la Declaración Universal de Derechos Humanos de 1948, en cuyo artículo 29 aparecía el concepto de "bienestar general en una sociedad democrática", se establecía que la democracia era parte del contexto esencial para el disfrute de los derechos humanos. La interacción entre los autores y los signatarios del Convenio Europeo de Derechos Humanos, aprobado en 1950, y los autores del Pacto Internacional de Derechos Civiles y Políticos continuó durante casi 15 años, hasta la aprobación de este último en 1966. El concepto de "necesario en una sociedad democrática" figura en al menos seis artículos del Convenio Europeo, entre ellos el citado artículo 8, y luego se incorporó en el Pacto, siendo el mejor ejemplo el artículo 22, párrafo 1:

> El ejercicio de tal derecho sólo podrá estar sujeto a las restricciones previstas por la ley que sean necesarias en una sociedad democrática, en interés de la seguridad nacional, de la seguridad pública o del orden público, o para proteger la salud o la moral públicas o los derechos y libertades de los demás.

16. El artículo 22, sin embargo, versa sobre la libertad de reunión y no sobre el derecho a la privacidad. Corresponde a los historiadores que estudien el proceso de elaboración de la Declaración Universal de Derechos Humanos y del Pacto Internacional de Derechos Civiles y Políticos explicar por qué la expresión "necesario en una sociedad democrática" se menciona explícitamente en los artículos 21 y 22 y no en el artículo 17. No obstante, resulta razonable que el Relator Especial aplique el mismo criterio, es decir, que el derecho

solo puede ser restringido mediante las medidas previstas por la ley (art. 17, párr. 2) y que, de acuerdo con su interpretación de la expresión “injerencias arbitrarias o ilegales”, esas medidas deben ser necesarias en una sociedad democrática, por analogía con los artículos 14, 21 y 22 del Pacto.

17. Esa interpretación está en consonancia con el párrafo 2 de la resolución 34/7 del Consejo de Derechos Humanos, en el que se reafirma que los Estados deben velar por que toda injerencia en el derecho a la privacidad se ajuste a los principios de legalidad, necesidad y proporcionalidad, reflejando los términos empleados en la jurisprudencia del Comité de Derechos Humanos (CCPR/C/USA/CO/4, párr. 22).

18. Por lo tanto, hay cuatro criterios esenciales que toda vulneración de la privacidad debe cumplir para ser legítima, a saber: a) no debe ser arbitraria y debe estar prevista por la ley; b) debe perseguir un objetivo necesario en una sociedad democrática; c) debe ir únicamente en interés “de la seguridad nacional, de la seguridad pública o del orden público, o para proteger la salud o la moral públicas o los derechos y libertades de los demás”; y d) debe ser proporcional a la amenaza o riesgo en cuestión.

19. Los criterios de “necesidad” y “necesidad en una sociedad democrática” son fundamentales para evaluar toda medida adoptada por un Estado Miembro que pueda considerarse contraria a la privacidad. También deben tenerse en cuenta al examinar las conculcaciones de otros derechos cuyo ejercicio depende del derecho a la privacidad.

20. El contexto de la privacidad y los vínculos entre la autonomía, la privacidad y las medidas necesarias en un Estado democrático explican por qué el Relator Especial se centra prioritariamente en Estados con instituciones y salvaguardias democráticas sólidas, pues es en esos contextos en los que su intervención tiene más visos de influir positivamente en el disfrute del derecho a la privacidad. Por lo que respecta a los países en los que las garantías democráticas son más débiles, el Relator está tratando de encontrar oportunidades para intervenir con efectos positivos.

21. En 2019 y 2020, el Relator Especial prestará mayor atención a África, Asia y América del Sur, y tiene previsto realizar una visita a cada una de esas regiones. No obstante, seguirá observando la situación en otros países con la ayuda de la sociedad civil, entre otros actores. Esto no quiere decir que no le interese la manera en que se experimenta el derecho a la privacidad en otras regiones del mundo. El Relator Especial no puede investigar esas experiencias con la minuciosidad y de la manera que desearía a causa de tres factores: tiempo, recursos y oportunidades para llevar a cabo una auténtica investigación sobre el terreno. Por lo tanto, el Relator Especial seguirá sometiendo a seguimiento a los Estados en los que, en lugar de imperar el estado de derecho, la ley se convierte en un instrumento de control y opresión del régimen. En la región de Oriente Medio y África del Norte, el Relator Especial examinará la promulgación de legislación sobre ciberdelincuencia, que podría poner en peligro el disfrute del derecho a la privacidad[5].

La privacidad, la tecnología y otros derechos humanos desde una perspectiva de género

22. En el presente informe se exponen los primeros resultados de las actividades en curso del Relator Especial en la esfera de la privacidad y el género. El Equipo de Tareas sobre la Privacidad y la Personalidad proseguirá su labor relativa al vínculo entre la privacidad y la igualdad entre los géneros independientemente de la forma o expresión. Además de celebrar consultas sobre el informe[6], el Relator Especial tiene previsto dedicar una mayor atención en los próximos tres años a esta cuestión, en particular a los vínculos entre la privacidad, la autonomía y el sistema de tutela masculina presente en distintos grados en varios países.

23. Los Estados Miembros que deseen participar en las consultas sobre la privacidad y el género habrán de manifestar su interés antes del 31 de marzo de 2019.

[5] Wafa Ben-Hassine y Dima Samaro, “Restricting cybersecurity, violating human rights: cybercrime laws in MENA region”, Open Global Rights, 10 de enero de 2019.

[6] Véase www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2019_HRC_Annex2_GenderReport.pdf.

Privacidad y datos sanitarios

24. En el presente informe se proporcionan también detalles sobre la labor en curso del Relator Especial en la esfera de la privacidad y los datos sanitarios. Como en el caso del género, en este ámbito hay cuestiones emergentes de gran calado, como la genética, las investigaciones sobre el genoma y los biobancos. Una de las cuestiones que tiene ante sí el Relator Especial es determinar si constituye una medida necesaria y proporcionada obtener los datos de ADN de toda la población de un país. El Relator Especial tendrá el mandato de establecer un diálogo sobre estos asuntos con los Estados que apliquen medidas de ese tipo.

25. El Equipo de Tareas sobre Datos Sanitarios ha detectado problemas que abarcan, entre otras, cuestiones relacionadas con la soberanía de los pueblos indígenas sobre sus datos, la población penitenciaria, las bases de datos forenses, los implantes sanitarios "inteligentes" y los dispositivos o prótesis que transmiten de manera continua datos de la vida real a las empresas y, de este modo, cimentan la visión del cuerpo humano como fuente de datos que pueden ser utilizados en actuaciones judiciales y en aplicaciones de inteligencia artificial, aprendizaje automático o procesamiento automático de datos. Estos asuntos se examinarán en las consultas previstas para 2019.

III. Seguridad y actividades de vigilancia

26. El mandato del Relator Especial surgió a partir de la indignación internacional provocada por las revelaciones de Edward Snowden sobre las actividades de los servicios de inteligencia, especialmente en el ámbito de la protección de la seguridad nacional.

27. Para que se reforzasen las garantías de privacidad en el contexto de las actividades de los servicios de inteligencia, el Relator Especial estableció el Foro Internacional de Supervisión de los Servicios de Inteligencia, que ha celebrado conferencias en Bucarest en 2016, en Bruselas en 2017 y en La Valetta en 2018. A raíz de la conferencia de 2018, el Relator Especial indicó lo siguiente:

a) Las iniciativas regionales recientes, como el Reglamento General de Protección de Datos[7] (que entró en vigor el 25 de mayo de 2018) y la Directiva sobre la Policía[8] (que entró en vigor el 6 de mayo de 2018) de la Unión Europea, aun siendo importantes, no bastan para garantizar que la protección de la privacidad se extienda también al ámbito de la seguridad nacional, lo que incluiría la supervisión de las actividades que los servicios de inteligencia llevan a cabo con fines de seguridad nacional[9].

b) La modernización del Convenio 108[10], una iniciativa mundial reciente que se puso en marcha oficialmente el 10 de octubre de 2018 y en la que han participado 70 de los 193 Estados Miembros de las Naciones Unidas, es digna de elogio por su artículo 11, en el que se estipula un conjunto de principios y salvaguardias de alto nivel que, a diferencia del Reglamento General de Protección de Datos, también se aplican a las actividades realizadas con fines de seguridad nacional.

28. En su informe de 2018 a la Asamblea General (A/73/438), el Relator Especial recomendó que se alentara a todos los Estados Miembros a ratificar la versión modernizada del Convenio (Convenio 108+). Por lo que respecta a la supervisión de los servicios de inteligencia y de las actividades de seguridad nacional que podrían invadir la privacidad, conviene que los Estados Miembros de las Naciones Unidas apliquen de manera inmediata las normas y salvaguardias estipuladas en el artículo 11 del Convenio 108+ para proteger el derecho fundamental a la privacidad.

[7] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016.

[8] Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo de 27 de abril de 2016.

[9] La Unión Europea carece de competencias en el ámbito de la seguridad nacional, por lo que no puede extender debidamente la protección de la privacidad a las actividades que se llevan a cabo en esta esfera, lo que incluye la vigilancia de las actividades que los servicios de inteligencia realizan con fines de seguridad nacional.

[10] Convenio del Consejo de Europa para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal.

29. Esas salvaguardias y normas fundamentales, en particular las relativas a la proporcionalidad y la necesidad, sirvieron de base para dos sentencias emblemáticas dictadas por el Tribunal Europeo de Derechos Humanos en 2018, ambas íntimamente relacionadas con las actividades de los servicios de inteligencia, a saber: *Centrum för Rättvisa c. Suecia* (19 de junio de 2018) y *Big Brother Watch y otros c. el Reino Unido* (13 de septiembre de 2018).

30. Esas sentencias podrían tener repercusiones en todo el mundo, habida cuenta del elevado número de miembros del Consejo de Europa (47 Estados) y del alcance mundial que tienen los servicios de inteligencia de la región.

31. El Relator Especial es partidario de que, a modo de referente con repercusiones mundiales, los criterios de proporcionalidad y de necesidad en una sociedad democrática se apliquen de manera rigurosa. Los servicios de inteligencia de otras regiones podrían verse influidos por las normas cada vez más estrictas que se aplican en Europa. Los análisis de los organismos de inteligencia que contienen información personal y otros datos personales y que se transfieren entre Europa y otros Estados deben estar sujetos a una escrupulosa supervisión a fin de garantizar que en Europa se cumplan esas normas de respeto de la privacidad, que podrían servir de buena práctica y modelo en todo el mundo.

32. Es importante señalar que la expresión “una sociedad democrática” es una parte fundamental de los criterios que se aplican al evaluar la protección jurídica que se otorga en los Estados Miembros de las Naciones Unidas. Hay una serie de nuevas tecnologías, en particular Internet, los teléfonos inteligentes, los análisis de macrodatos, los dispositivos ponibles, los sistemas de energía inteligentes y las ciudades inteligentes, que aumentan la vulnerabilidad de las personas y las comunidades a la vigilancia que los Gobiernos nacionales llevan a cabo sobre las empresas de sus países, así como a la ejercida por los servicios de inteligencia de Estados extranjeros y por las empresas.

33. La posibilidad de que los Estados utilicen las nuevas tecnologías de esta forma constituye un importante riesgo para la privacidad y otros derechos humanos, como la libertad de expresión, la libertad de asociación y la libertad de religión o de creencias. Los efectos individuales y acumulativos de esas tecnologías otorgan a los Estados una capacidad sin precedentes de caracterizar y someter a estrecho seguimiento, mediante métodos nuevos, el comportamiento de las personas.

34. Esas tecnologías podrían utilizarse para socavar los derechos humanos y la democracia. Puede que la democracia sea un mecanismo imperfecto, pero, históricamente, ha ofrecido el mejor ecosistema posible para la promoción de los derechos humanos. Por lo tanto, los efectos que tienen en la democracia las medidas que invaden la privacidad constituyen un parámetro básico esencial con el que evaluarlas.

35. El Relator Especial seguirá cooperando con todos los Estados Miembros en la ejecución de su mandato de alcance mundial, si bien es consciente de que hay más probabilidades de que esa cooperación sea fructífera, y en última instancia contribuya al respeto del derecho a la privacidad, en aquellos países que cuentan con instituciones y salvaguardias democráticas sólidas.

36. Durante 2018, uno de los principales motivos de preocupación era la cuestión de qué ocurre con los análisis de los servicios de inteligencia que contienen datos personales una vez que esos servicios o las fuerzas del orden de un país transmiten esa información a otro Estado. ¿Gozan los datos y, por consiguiente, la privacidad de las personas en cuestión del mismo nivel de protección en el Estado de destino que en el Estado de origen? La importancia de esta cuestión hace necesaria la adopción de las medidas que se recomiendan.

37. El 14 de noviembre de 2018, cinco órganos de supervisión de Bélgica, Dinamarca, Noruega, los Países Bajos y Suiza, todos ellos partes en el Convenio 108 y, por lo tanto, obligados por las disposiciones que imponen restricciones al uso de los datos personales con fines de seguridad nacional, emitieron una declaración conjunta en la que planteaban la existencia de un posible vacío en lo referente a la supervisión y proponían maneras de mitigar ese riesgo al supervisar los intercambios de datos entre los servicios de inteligencia

y seguridad de distintos países[11]. Esto constituye un avance importante y positivo que se señaló a la atención de la comunidad internacional.

38. Los participantes en el Foro Internacional de Supervisión de los Servicios de Inteligencia de 2018 consideraron que esa iniciativa era un importante avance paralelo al establecimiento del Consejo de Examen y Supervisión de los Servicios de Inteligencia de los Cinco Ojos, formado por los organismos responsables de la supervisión de los servicios de inteligencia de los miembros de la alianza de los Cinco Ojos, a saber: Australia, el Canadá, los Estados Unidos, Nueva Zelandia y el Reino Unido. El Relator Especial celebra la creación del Consejo y sus actividades, sobre todo habida cuenta de la ubicación y el alcance mundial de los cinco Estados que forman la alianza. Desde 2013, cada uno de ellos ha llevado a cabo reformas legislativas para reforzar las salvaguardias en materia de supervisión y privacidad en el contexto de las actividades de los servicios de inteligencia en el sector de la seguridad nacional y otras esferas. Las reformas no son igual de exhaustivas en todos los Estados; por ejemplo, el titular del mandato ha calificado de motivo de preocupación desde el punto de vista de la protección de la privacidad las medidas legislativas más recientes de Australia[12].

39. La Oficina del Comisionado Encargado de la Supervisión de los Órganos Investigación del Reino Unido emitió un comunicado[13] en el que celebraba la declaración de los organismos de supervisión de Bélgica, Dinamarca, Noruega, los Países Bajos y Suiza. La Oficina tiene la posibilidad, y tal vez incluso la responsabilidad especial, inherente a su ubicación geográfica, de tender un puente entre los organismos de supervisión de la Europa continental y los que integran el Consejo.

40. El Relator Especial facilitará y apoyará esta y otras iniciativas en la medida en que contribuyan a afianzar las normas y salvaguardias internacionales de derechos humanos relativas al intercambio de información personal entre los servicios de inteligencia y las fuerzas del orden de distintos países.

41. La supervisión de las actividades de los servicios de inteligencia fue el eje central de las aportaciones que hizo el Relator Especial durante el examen realizado por el Comité Europeo de Protección de Datos para determinar si la legislación nacional y las salvaguardias del Japón eran adecuadas. Durante las deliberaciones se examinaron la información y las pruebas presentadas por el Relator Especial, y el 5 de diciembre de 2018 se rechazó[14], por un período determinado, la constatación de adecuación relativa al Japón.

42. En septiembre de 2018, el Tribunal Europeo de Derechos Humanos determinó que el régimen de intercepción masiva de comunicaciones del Reino Unido vulneraba el artículo 8 del Convenio Europeo de Derechos Humanos (derecho al respeto a la vida privada y familiar y a la correspondencia) porque no existía una supervisión adecuada del proceso de selección de los canales de transmisión por Internet que serían interceptados ni de los criterios que se aplicaban para filtrar, buscar y seleccionar las comunicaciones que se someterían a examen, y porque no se aplicaban salvaguardias adecuadas para la selección de "datos asociados a las comunicaciones" que se analizarían[15]:

a) El Tribunal dictaminó que el régimen para obtener de los proveedores de servicios de comunicaciones datos relativos a las comunicaciones vulneraba el artículo 8, y que los regímenes para la interceptación masiva de comunicaciones y para obtener de los proveedores de servicios de comunicaciones datos relativos a las comunicaciones vulneraban el artículo 10 debido a la falta de salvaguardias suficientes para proteger el material periodístico confidencial;

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

[12] Comunicación del Relator Especial a la Comisión Parlamentaria Mixta de Inteligencia y Seguridad, núm. 81. 2018, disponible en www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/TelcoAmendmentBill2018/Report_1/section?id=committees%2freportjnt%2f024247%2f26914.

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

[14] Véase https://edpb.europa.eu/news/news_en.

[15] Tribunal Europeo de Derechos Humanos, Sección Primera, *Big Brother Watch and Others v. the United Kingdom*, demandas 58170/13, 62322/14 y 24960/15, sentencia de 13 de septiembre de 2018.

b) Determinó también que el régimen para el intercambio de inteligencia con Gobiernos extranjeros no vulneraba ni el artículo 8 ni el 10.

43. Aunque esta sentencia se refería al anterior marco normativo de vigilancia vigente en el Reino Unido, sus conclusiones tienen gran trascendencia, por lo que se señalan a la atención de los Estados Miembros en interés del examen de sus prácticas y marcos.

44. Esta decisión pone de relieve la importancia de establecer salvaguardias detalladas y efectivas (tanto jurídicas como procesales) en el derecho interno y en las prácticas de los servicios de inteligencia y de los autoridades que los supervisan.

45. Durante la visita oficial del Relator Especial a Alemania en noviembre de 2018, se debatió acerca de las buenas prácticas en el ejercicio de la facultad de reunir datos en masa, y a este respecto se recomienda a los Estados que examinen el compendio de buenas prácticas publicado por la asociación Stiftung Neue Verantwortung[16] (noviembre de 2018).

Recomendaciones

46. El Relator Especial recomienda:

a) Que los Estados Miembros incorporen en sus sistemas jurídicos nacionales las normas y salvaguardias estipuladas en el Convenio 108+, artículo 11, para proteger el derecho fundamental a la privacidad, en particular mediante:

i) La creación de seguridad jurídica, cerciorándose para ello de que todas las medidas que invadan la privacidad, incluso las que se apliquen con fines de seguridad nacional, defensa y seguridad pública o para prevenir, investigar o enjuiciar un delito, estén previstas por leyes que hayan sido sometidas a una consulta pública adecuada y al debido examen parlamentario;

ii) El establecimiento del criterio básico de “medida necesaria y proporcionada en una sociedad democrática” como parámetro esencial que las dependencias de cumplimiento interno de los servicios de inteligencia y de las fuerzas de seguridad deberán aplicar a las medidas que invadan la privacidad, y en el que se basarán las autoridades independientes de supervisión y los tribunales competentes para evaluar las acciones de esos organismos y exigirles responsabilidades;

iii) El establecimiento de uno o varios organismos de supervisión facultados por ley y dotados de los recursos suficientes por el Estado para examinar de manera efectiva todas las actividades de los servicios de inteligencia y las fuerzas del orden que invadan la privacidad;

b) Que se aplique el principio de “si es intercambiable, es supervisable”[17] a toda información personal que intercambien los servicios de inteligencia y las fuerzas del orden tanto a nivel nacional como internacional:

i) Todos los Estados Miembros deberían modificar sus leyes para que las autoridades independientes encargadas de supervisar las actividades de inteligencia estén específica y expresamente facultadas para controlar toda la información

[16] Véase www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2019_HRC_Annex5_CompendiumBulkSurveillance.pdf.

[17] Los servicios de inteligencia de distintos Estados intercambian datos personales con regularidad, pero no siempre están sometidos al control de organismos de supervisión independientes, ya sea en el Estado de origen o en el de destino. Además, la legislación de algunos países impide de manera efectiva ese tipo de control e imposibilita incluso que los organismos de supervisión independientes de los Estados de origen y destino mantengan consultas al respecto. Se alienta a los Estados a que modifiquen sus leyes para que los organismos independientes de supervisión de su territorio estén facultados para consultar con sus homólogos en otros Estados y a que hagan un seguimiento de todos los casos en los que se hayan intercambiado datos con otro Estado, incluidos tanto los datos personales brutos sin procesar como los datos personales que figuran en los análisis, clasificados por producto de inteligencia, independientemente de si esos datos se encuentran en el Estado de origen o en el de destino. Ambos tipos de datos personales son objeto de intercambio entre servicios de inteligencia y fuerzas del orden, y ambos deben ser sometidos a un control independiente tanto en el Estado de origen como en el de destino.

personal que intercambien los servicios de inteligencia de los países de los que son responsables;

ii) Siempre que sea posible y apropiado, las autoridades independientes de supervisión de los Estados de origen y de destino deben tener acceso inmediato y automático a los datos personales que intercambien los servicios de inteligencia o las fuerzas del orden de sus respectivos países;

iii) Todos los Estados Miembros deberían modificar su legislación para otorgar expresamente a las autoridades nacionales y estatales encargadas de la supervisión de los servicios de inteligencia la autoridad jurídica para compartir información, celebrar consultas y estudiar las mejores prácticas de supervisión con las autoridades de supervisión de los Estados con los que los servicios de inteligencia de sus respectivos países hayan estado en contacto para transmitir o intercambiar de cualquier otra forma datos personales;

iv) Cuando un servicio de inteligencia transmita a un tercer Estado o grupo de Estados análisis de inteligencia recibidos de otro Estado que contengan información personal u otro tipo de datos personales, este intercambio habrá de estar sometido al control de los organismos de supervisión de dichos Estados.

47. Al contemplar la posibilidad de hacer uso de la facultad para la vigilancia en masa, las autoridades competentes de los Estados Miembros deben, en primer lugar, examinar, y después priorizar y adoptar, en la mayor medida posible, las medidas necesarias para instaurar las buenas prácticas recomendadas en el compendio elaborado por la Stiftung Neue Verantwortung[18], además de aplicar los criterios para la puesta en práctica y las salvaguardias estipuladas por el Tribunal Europeo de Derechos Humanos en la sentencia del asunto *Big Brother Watch y otros*, de septiembre de 2018.

IV. Derecho a la privacidad: una perspectiva de género

48. El Consejo de Derechos Humanos, en su resolución 34/7, y la Asamblea General, en su resolución 71/199, exhortaron a los Estados a que "sigan elaborando o manteniendo, a ese respecto, medidas preventivas y procedimientos de recurso para las violaciones y transgresiones del derecho a la privacidad en la era digital, que pueden afectar a todas las personas, incluidas, con repercusiones particulares, las mujeres, así como los niños y las personas en situaciones vulnerables o los grupos marginados".

49. En 1994, el Comité de Derechos Humanos determinó, en el caso *Toonen c. Australia*, que tipificar como delito las relaciones sexuales consentidas entre adultos del mismo sexo suponía una vulneración del derecho a la privacidad. En 2017, el Comité reiteró que el derecho a la privacidad abarca la identidad de género (CCPR/C/119/D/2172/2012, párr. 7.2).

50. Si bien no es absoluto, el derecho a la privacidad es esencial para el libre desarrollo de la personalidad y la identidad de las personas. Es un derecho que se deriva de la dignidad innata de la persona y, al mismo tiempo, la condiciona, además de facilitar el ejercicio y el disfrute de otros derechos humanos[19]. Se trata de un derecho que no se limita a la esfera pública.

51. El derecho a la privacidad, en cuanto que condición previa necesaria para la protección de valores fundamentales como la libertad, la dignidad, la igualdad y el derecho a no ser objeto de intrusión por parte de los Gobiernos, es un ingrediente fundamental para

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

[19] La Asamblea General, el Alto Comisionado de las Naciones Unidas para los Derechos Humanos y varios titulares de mandatos de los procedimientos especiales han reconocido que la privacidad es un elemento necesario para el disfrute de otros derechos; véanse la resolución 68/167 de la Asamblea General, el documento A/HRC/13/37 y la resolución 20/8 del Consejo de Derechos Humanos.

las sociedades democráticas, por lo que requiere una protección firme[20]. El Consejo de Derechos Humanos ha aprobado resoluciones en las que pone de relieve la relación de interdependencia y refuerzo mutuo entre la democracia y los derechos humanos[21].

52. El Relator Especial integra una perspectiva de género en todas las actividades de su mandato[22]. A raíz del éxito de las tres consultas regionales sobre la privacidad, la personalidad y los flujos de información, llevó a cabo una consulta en línea titulada "Las cuestiones de género que plantea la era digital y el efecto que tienen en las mujeres, los hombres y las personas con orientaciones sexuales, identidades de género, expresiones de género y características sexuales diversas".

53. El primer informe completo de la línea de acción temática sobre la privacidad y la personalidad forma parte de una recopilación de las comunicaciones[23] recibidas por el Relator Especial y de investigaciones secundarias. A excepción de las recomendaciones, la recopilación no refleja necesariamente las opiniones de su autora principal, Elizabeth Coombs, presidenta del Equipo de Tareas sobre la Privacidad y la Personalidad, ni las del Relator Especial.

Línea de acción temática sobre la privacidad y la personalidad

54. Las comunicaciones al respecto que recibió el Relator Especial abogaban por hacer un análisis interseccional de las fuerzas económicas, la clase, la religión, la raza y el género para identificar esferas de interés distintas de las cuestiones más dominantes[24] y por reconocer la interdependencia entre el derecho a la privacidad y la democracia[25].

55. Se señaló que la experiencia de cada persona en lo referente a las tecnologías digitales y la privacidad variaba en función de su género y de otros factores, como su origen étnico, cultura, raza, edad, extracción social, situación financiera, autonomía económica y educación, así como de los marcos jurídicos y políticos[26]. Se consideró que el derecho a la privacidad era especialmente importante entre quienes eran objeto de desigualdad, discriminación o marginación por motivos de género, orientación sexual, identidad de género, características sexuales o expresión de género. Gracias a su alcance y al relativo anonimato que ofrece, Internet ha abierto nuevas vías para que las personas lesbianas, gais, bisexuales, transgénero, *queer* e intersexuales (LGBTQI) puedan interactuar y apoyarse mutuamente.

56. En las comunicaciones, se reconoció que las tecnologías digitales afectaban considerablemente a la privacidad, puesto que amplificaban las experiencias del mundo no digital. Se indicó que no todas las personas podían disfrutar en la misma medida de las ventajas que ofrecían las tecnologías digitales a causa de la inequidad estructural y de unas normas de género discriminatorias que afectaban especialmente a las mujeres, las personas de género no binario y no cisnormativas, los pobres y las comunidades religiosas o culturales minoritarias. La cibermisoginia[27] y el ciberacoso en general contra las personas

[20] Daniel Therrien, Comisario de Protección de Datos Personales del Canadá, informe presentado para las consultas nacionales sobre las tecnologías digitales y los datos organizadas por el Ministerio de Innovación, Ciencia y Desarrollo Económico del Canadá, 23 de noviembre de 2018.
[21] Resoluciones 19/36 y 28/14 sobre los derechos humanos, la democracia y el estado de derecho.
[22] Véase www.ohchr.org/SP/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx.
[23] Véase www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2019_HRC_Annex2_GenderReport.pdf.
[24] Por ejemplo, comunicación de la Asociación para el Progreso de las Comunicaciones, 2018.
[25] Por ejemplo, comunicación del Comisario de Protección de Datos Personales del Canadá, 2018.
[26] Phoenix Strategic Perspectives, "2016 survey of Canadians on privacy", informe final preparado para la Oficina del Comisario de Protección de Datos Personales del Canadá, diciembre de 2016.
[27] West Coast Women's Legal Education and Action Fund (LEAF), *#CyberMisogyny: Using and Strengthening Canadian Legal Responses to Gendered Hate and Harassment Online* (Vancouver, 2014).

de género no binario son fenómenos propiciados por las nuevas tecnologías[28], y su alcance, durabilidad e impacto son infinitamente mayores que en el pasado.

57. En las comunicaciones se expresó con rotundidad la opinión de que las cosas no tenían por qué ser así, y que las tecnologías digitales podían facilitar el disfrute en pie de igualdad del derecho a la privacidad.

58. En las comunicaciones se reconocieron las ventajas de los dispositivos inteligentes, las aplicaciones móviles, los buscadores y las plataformas de medios sociales, pero también su capacidad para vulnerar la privacidad de los usuarios en función de su género. Los jóvenes LGBTQI, por ejemplo, utilizan Internet para participar en medios y redes sociales con mayor frecuencia que los demás jóvenes, y tienen más probabilidades que estos de sufrir acoso u hostigamiento en línea (un 42 % frente a un 15 %)[29].

59. Pese a las ventajas de las tecnologías digitales[30], se estimó que las personas que corrían un mayor riesgo eran las mujeres, las niñas, los niños y las personas y comunidades LGBTQI[31], en particular las personas transgénero, los activistas, los docentes homosexuales, los defensores de los derechos humanos, los trabajadores sexuales y las periodistas.

60. Las personas LGBTQI también se exponen a riesgos específicos, por ejemplo a ser "sacadas del armario", y a insultos directamente relacionados con su identidad de género[32].

61. En el Canadá se ha observado que, pese a que los medios sociales permiten a las mujeres y a las niñas cultivar sus relaciones sociales, también amplifican las normas sociales, pues intensifican la vigilancia con fines comerciales, refuerzan las normas sociales y aumentan la vigilancia por parte de familiares y compañeros[33].

62. Se denunció que tanto agentes estatales como no estatales utilizaban cuentas falsas en aplicaciones de citas de la comunidad LGBTI para tender trampas a los hombres homosexuales con el objetivo de detenerlos, someterlos a tratos crueles o degradantes o chantajearlos[34].

63. Según la información recibida, había medios de comunicación, algunos de ellos pertenecientes a los nuevos medios de comunicación, que publicaban información personal de personas LGBTQI y de defensores de los derechos humanos, poniendo así en peligro su seguridad[35].

64. Internet no solo permite crear historias contemporáneas, sino también perpetuar las originadas en la era predigital, con las correspondientes vulneraciones de la privacidad[36].

---

[28] Comunicación de la Eastern European Coalition for LGBT+ Equality, "Gender perspectives on privacy in Eastern partnership countries and Russia", 2018; véase también www.ucl.ac.uk/steapp/research/themes/digital-policy-laboratory/gender-and-iot.

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

[30] Comunicación (nombre omitido), 2018, en la que se cita a Valerie Horres, "Online and enabled: ways the Internet benefits and empowers women", *Interface: The Journal of Education, Community and Values*, vol. 10, núm. 4 (2010).

[31] Comunicaciones de 2018: Kazakhstan Feminist Initiative "Feminita"; Oficina de Defensa de Derechos e Interseccionalidad; Grupo LGTB "Stimul" y Transgender Legal Defense Project (Rusia); Richard Lusimbo; MPact Global Action for Gay Men's Health and Rights; Transgender Europe; Federatie van Nederlandse Verenigingen tot Integratie Van Homoseksualiteit; y Asociación Internacional de Lesbianas, Gais, Bisexuales, Trans e Intersex.

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

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

[34] Kazakhstan Feminist Initiative "Feminita", comunicación, 2018.

[35] *Ibid.*

[36] Facultad de Derecho de Osgoode, comunicación confidencial, diciembre de 2018.

65. Algunas comunicaciones trataban sobre el reconocimiento de la identidad de género, de la autonomía y de la integridad física y sobre la expresión de estas, y en ellas se manifestaba preocupación por la gestión inadecuada de la privacidad en el contexto de los cambios de nombre y de género en los documentos de identidad[37]. Numerosas actividades comunes del día a día para las que se requieren documentos de identidad, como los viajes, los trámites bancarios o las citas médicas, a menudo imponen invasiones de la privacidad profundamente embarazosas y angustiosas para las personas transgénero, algo que no experimentan las personas de género binario.

66. El Tribunal Europeo de Derechos Humanos ha determinado que los Estados con procedimientos de reconocimiento del género que vulneran el derecho a la privacidad de las personas transgénero infringen el artículo 8 del Convenio Europeo de Derechos Humanos[38].

67. La disponibilidad en Internet de documentos públicos, notificaciones judiciales y decisiones relativas a la identidad de género constituía un problema de privacidad, en particular en combinación con los macrodatos y la capacidad de los buscadores[39].

68. Para las personas intersexuales, las invasiones de la privacidad pueden comenzar literalmente al nacer, con la realización de cirugías de cambio de sexo y la administración de tratamientos hormonales destinados a atribuir al niño un determinado sexo. La "normalización" de las intervenciones quirúrgicas en lactantes intersexuales puede tener repercusiones desde el punto de vista de los derechos humanos, entre ellos el derecho a la privacidad, pues infringe los derechos a la autonomía personal y a la libre determinación en relación con el tratamiento médico. Se indicó que la respuesta de los países a este fenómeno era diversa[40].

69. En las comunicaciones, también en la presentada por la Relatora Especial sobre la violencia contra la mujer, sus causas y consecuencias, se hacía referencia al creciente número de investigaciones internacionales, regionales y nacionales sobre la violencia de género digital.

70. Las tecnologías digitales y los dispositivos inteligentes ofrecen medios casi ilimitados para acosar y controlar a los demás[41]. En la violencia facilitada por las tecnologías se combinan las cuestiones relativas a la desigualdad de género, la violencia sexual, la regulación de Internet, el anonimato de la red y la privacidad (véase A/HRC/38/47).

71. El fenómeno de los abusos a través de las imágenes o la "pornovenganza", que consiste en difundir imágenes y grabaciones íntimas de contenido sexual sin el consentimiento de la persona afectada con el objetivo causar daño, es una forma muy conocida de abuso en línea. Según unas investigaciones realizadas en Australia, los hombres y las mujeres corren el mismo riesgo de sufrir abusos a través de las imágenes, mientras que las personas que se identifican como lesbianas, gais o bisexuales tienen más probabilidades de ser víctimas de esos actos (36 %) que los heterosexuales (21 %)[42].

72. Cada vez es más frecuente que la violencia doméstica entrañe el uso de dispositivos domésticos inteligentes contra las mujeres y las personas dependientes[43] pues tales dispositivos ofrecen nuevas posibilidades de invasión de la privacidad y de restricción de la

[37] Comunicación de la Eastern European Coalition for LGBT+ Equality, 2018.

[38] Tribunal Europeo de Derechos Humanos, Sección Segunda, *L. v. Lithuania*, demanda 27527/03, sentencia definitiva de 31 de marzo de 2008; Tribunal Europeo de Derechos Humanos, Sección Quinta, *A. P., Garçon and Nicot v. France*, demandas 79885/12, 52471/13 y 52596/13, sentencia de 6 de abril de 2017.

[39] Comunicación de Kazakhstan Feminist Initiative "Feminita", 2018.

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

[41] Comunicación de Dejusticia, septiembre de 2018.

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

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

autonomía y la libre determinación en el hogar[44] y en las comunicaciones[45]. En ocasiones, la protección jurídica que se ofrece es inadecuada[46] o la policía no interviene en caso de infracción[47].

73. La cibermisoginia es un fenómeno surgido en las plataformas digitales[48]. Según la información recibida, Twitter era la principal plataforma para la promoción de campañas de odio contra las mujeres y la difusión de contenidos sexuales, mientras que Facebook era donde se producían la mayoría de los ataques contra mujeres por defender sus derechos[49].

74. Las intromisiones en la vida privada y la violencia en línea afectan con mayor frecuencia a los hombres que no se ajustan a los estereotipos masculinos convencionales y a las personas lesbianas, gais y bisexuales[50].

75. Las diferencias en la forma en que se vive la privacidad en función del género afectan también al disfrute de otros derechos, por ejemplo en el caso de las mujeres que también son víctimas de la censura y el recurso a los estereotipos en línea en campañas dirigidas contra mujeres activistas y periodistas[51].

Línea de acción temática sobre seguridad y vigilancia

76. La vigilancia, a menos que se lleve a cabo de manera legal y proporcionada y responda a una necesidad legítima, constituye una vulneración del derecho humano a la privacidad. El género, la raza, la clase, el origen social, la religión y las opiniones y su expresión pueden influir a la hora de decidir quién debe ser vigilado en la sociedad, lo cual puede hacer que determinadas personas estén más expuestas a la violación de su derecho a la privacidad[52].

77. Son numerosos los países donde la existencia de prejuicios de género se evidencia en el mayor grado de vigilancia que se ejerce sobre quienes se identifican como miembros de grupos LGBTQI[53]. En algunos países, la legislación ha facilitado el control estatal de la comunidad LGBTQI. Uno de los ejemplos mencionados es la Ley contra la Ciberdelincuencia aprobada en Egipto en 2018[54].

78. Aunque por lo común se dice que las actividades de vigilancia de los Estados se centran principalmente en los hombres[55], según la información recibida las medidas antiterroristas afectan de manera desproporcionada a las mujeres y las personas transgénero solicitantes de asilo, refugiadas o inmigrantes[56].

79. Las mujeres pueden contar con que casi todos los detalles de su vida íntima estarán sometidos a múltiples formas de vigilancia, tanto por el Estado como por agentes privados,

[44] Bowles, “Thermostats, locks and lights”.
[45] Corinne Lysandra Mason y Shoshana Magnet, “Surveillance studies and violence against women”, *Surveillance and Society*, vol. 10, núm. 2 (2012); comunicación de la Asociación para el Progreso de las Comunicaciones, 2018.
[46] Bowles, “Thermostats, locks and lights”.
[47] Al-Alosi Hadeel, “Cyber-violence: digital abuse in the context of domestic violence”, *University of South Wales Law Journal*, vol. 40, núm. 4 (2017).
[48] West Coast LEAF, *#CyberMisogyny*.
[49] Comunicaciones del Instituto de las Mujeres de la Ciudad de México y la Asociación para el Progreso de las Comunicaciones, 2018.
[50] Irish Council for Civil Liberties.
[51] Comunicación de Dejusticia, 2018.
[52] Mary Anne Franks, “Democratic surveillance”, *Harvard Journal of Law and Technology*, vol. 30, núm. 2 (primavera de 2017).
[53] Comunicación de la Asociación para el Progreso de las Comunicaciones, 2018.
[54] Comunicación internacional conjunta, 2018; véase también George Sadek, “Egypt: President ratifies Anti-Cybercrime Law”, Global Legal Monitor, 5 de octubre de 2018.
[55] Privacy International 2017.
[56] Informe del Relator Especial sobre la promoción y la protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo (A/64/211).

lo que va desde la violencia doméstica hasta la cosificación sexual, pasando por cuestiones relacionadas con la reproducción[57].

80. En la actualidad, los principales proveedores de plataformas ofrecen funciones de gestión de la identidad mediante la autenticación de la identidad en línea. Hay sitios web, aplicaciones móviles y servicios en línea que requieren claves de acceso y dan por auténticas las credenciales proporcionadas al iniciar sesión con una cuenta de Facebook o de Google[58]. Facebook acapara el 60 % de este mercado de "inicio de sesión social"[59], que facilita el acceso a enormes cantidades de información para la elaboración de perfiles, lo cual permite extraer conclusiones, en las que el género es una variable, acerca del comportamiento de las personas, las familias, los grupos y las comunidades.

Línea de acción temática sobre los macrodatos y los datos abiertos

81. El aumento en la recopilación, el almacenamiento y la manipulación de los datos ha incrementado las posibilidades de que se produzcan vulneraciones de la privacidad, cuyas consecuencias pueden variar en función del género.

82. El procesamiento de datos puede enquistar los sesgos relacionados con los roles y las identidades de género, especialmente debido a que el modelado de datos para la intervención social a menudo va más allá de la persona para centrarse en grupos o comunidades[60].

83. Los métodos de análisis de datos que resultan en inferencias acerca de personas o grupos basadas en el género, y que dan lugar a discriminación, son contrarios al derecho de los derechos humanos.

Línea de acción temática sobre los datos sanitarios

84. Un motivo de especial preocupación para las personas LGBTQI es la revelación de datos sanitarios sin el consentimiento del interesado, en particular sobre su estado serológico respecto del VIH[61]. Se descubrió que la aplicación de Grindr, por ejemplo, contenía rastreadores y transmitía a terceros información personal de los usuarios, incluido su estado serológico respecto del VIH[62].

85. Se ha observado que el trato recibido en los entornos sanitarios en materia de privacidad influye en la utilización de los servicios de salud, lo cual tiene consecuencias para la salud personal y pública.

86. El miedo a ser humilladas o discriminadas como consecuencia de la pérdida de privacidad puede llevar a las personas transgénero a utilizar menos o a evitar los servicios de salud[63].

87. Las vulneraciones del derecho a la privacidad durante el parto pueden tener un fuerte efecto disuasorio en las mujeres a la hora de solicitar asistencia sanitaria en posteriores alumbramientos[64].

---

57 Franks, "Democratic surveillance"; Comunicación de la Asociación para el Progreso de las Comunicaciones, 2018.

58 "The Economist essay", *The Economist*, edición de Navidad, 22 de diciembre de 2018.

59 *Ibid.*

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

61 Comunicación de Kazakhstan Feminist Initiative "Feminita", 2018.

62 Comunicación de la Asociación para el Progreso de las Comunicaciones, 2018.

63 "New health care clinic for transgender people in pipeline", *Times of Malta*, 7 de abril de 2018.

64 White Ribbon Alliance for Safe Motherhood, "Respectful maternity care: the Universal Rights of Childbearing Women Charter", 2011; y Meghan A. Bohren y otros, "The mistreatment of women during childbirth in health facilities globally: a mixed-methods systematic review", *PLOS Medicine*, vol. 12, núm. 6 (2015). Comunicaciones de Dejusticia y de la Asociación para el Progreso de las Comunicaciones.

88. Tecnologías como Google Street View pueden afectar a la utilización de los servicios de salud por parte de las mujeres, por el miedo de estas a que se las identifique como usuarias de determinados servicios sanitarios[65].

Línea de acción temática sobre la utilización de datos personales por las empresas

89. Suscita cada vez mayor consenso la idea de que el sector privado tiene obligaciones dimanantes del derecho de los derechos humanos, tal como se indica en el marco para "Proteger, Respetar y Remediar" propuesto por el Representante Especial del Secretario General para la Cuestión de los Derechos Humanos y las Empresas Transnacionales y Otras Empresas, John Ruggie, en 2008 (A/HRC/8/5)[66].

90. Los sistemas de toma de decisiones automatizadas que utilizan las plataformas digitales pueden producir resultados con consecuencias distintas en función del género. Según se informó, había en marcha acciones judiciales contra Facebook por, supuestamente, haber permitido que los propietarios de viviendas y los intermediarios inmobiliarios restringieran la visibilidad de sus anuncios en función del género del usuario[67].

91. Se expresó preocupación ante el aumento del número de páginas y grupos en los medios sociales que se utilizaban para promover la violencia contra las mujeres, el sexismo y los estereotipos de género nocivos y ante la gran presión comunitaria que había sido necesaria para que las plataformas procedieran a eliminar esas páginas.

92. Según se informó, se desconocían los detalles del proceso de toma de decisiones de las plataformas de Internet una vez que recibían denuncias por actos de violencia en línea, los tipos y el número de casos denunciados por país y las medidas adoptadas. Amnistía Internacional ha observado que Twitter no investiga de manera adecuada las denuncias de violencia y abusos que recibe, y ha instado a la empresa en repetidas ocasiones a que publique "información relevante sobre las denuncias por actos de violencia y abuso contra mujeres y otros grupos ocurridos en la plataforma, junto detalles sobre cómo actúa la empresa ante esas denuncias" [cita traducida][68].

93. En una de las comunicaciones se informaba de las medidas positivas que había adoptado Grindr con el objetivo de reducir el uso indebido que se hacía de su aplicación para tender trampas a los hombres homosexuales[69]. No obstante, según la información recibida, la respuesta habitual de las plataformas digitales (Facebook, Twitter, los medios de comunicación, etc.) ante casos de violencia de género en línea eran la impunidad y la opacidad, lo que hacía que las víctimas a menudo se sintieran abandonadas[70].

94. Se indicó que entre los perjuicios causados a las personas a raíz de invasiones de su privacidad motivadas por cuestiones de género y perpetradas por medios tecnológicos figuraban consecuencias graves y bien documentadas, como el fraude, la pérdida del empleo y de oportunidades educativas, las restricciones a la libertad de circulación, de asociación y de vestimenta, la injerencia en las capacidades de crianza, la pérdida de reputación y de confianza en general, la violencia (incluso la muerte) y el encarcelamiento, entre otros[71].

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

[66] Coalición por los Derechos y Principios de Internet, "Carta de Derechos Humanos y Principios para Internet", 2014; comunicación de la Asociación para el Progreso de las Comunicaciones, 2018.

[67] Comunicación del Consumer Policy Research Centre, en la que se cita el artículo titulado "Money", CNN News, marzo de 2018.

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

[69] Comunicación de Kazakhstan Feminist Initiative "Feminita", 2018.

[70] Medios electrónicos citados en la comunicación de Dejusticia, 2018.

[71] Comunicación de la Asociación para el Progreso de las Comunicaciones, 2018; N. Pushkarna y M. M. Ren, comunicación, 2018; Oficina del Comisario de Protección de Datos Personales del Canadá, "Online reputation: what are they saying about me?", enero de 2016; casos recibidos por Transgender

95. No todas las personas viven de la misma manera las invasiones de su privacidad: esas vulneraciones pueden dar lugar al aumento de la violencia doméstica entre las mujeres y de la discriminación entre las personas LGBTQI[72].

96. Las intromisiones en la vida privada constituyen una invasión de la personalidad humana en sí misma y sus repercusiones son de ámbito social. Las formas extremas de los abusos y las invasiones de la privacidad personal y familiar que sufren a través de Internet algunas mujeres prominentes disuaden a las niñas y a las mujeres de desempeñar funciones públicas, lo que socava su derecho a participar en los asuntos públicos y afecta a la representatividad de las instituciones democráticas[73].

97. En las comunicaciones se señalaban las buenas prácticas que protegen la privacidad desde una perspectiva de género, entre las que se encuentran las reformas legislativas, los marcos de políticas neutros en cuanto al género y basados en datos empíricos, las decisiones de los tribunales, la participación de las organizaciones de la sociedad civil y el aprovechamiento de su experiencia, los programas comunitarios en materia de privacidad que tienen en cuenta las cuestiones de género y los recursos educativos.

98. Se consideró que las buenas prácticas para dar respuesta a los problemas de privacidad vinculados a la orientación sexual y la identidad de género estaban consagradas en los Principios Adicionales y Obligaciones de los Estados sobre la Aplicación de la Legislación Internacional de Derechos Humanos en relación con la Orientación Sexual, la Identidad de Género, la Expresión de Género y las Características Sexuales como Complemento a los Principios de Yogyakarta[74].

V. Conclusiones

99. **En la Declaración Universal de Derechos Humanos se exhorta a todas las personas e instituciones a que promuevan y respeten los derechos humanos[75]. Todos los Estados, empresas, órganos religiosos, miembros de la sociedad civil, organizaciones profesionales y personas desempeñan un papel importante.**

100. **También es fundamental para la salud de las sociedades y la democracia que los ciudadanos confíen en que pueden expresar sus ideas y reunirse. La pérdida de la privacidad puede hacer que las personas pierdan esa confianza y la confianza en el gobierno y las instituciones establecidas para representar los intereses públicos, y opten por no participar en la sociedad, lo cual puede afectar negativamente a las democracias representativas y ponerlas en peligro.**

101. **Aunque el derecho a la privacidad tiene su precio y no está exento de riesgos para los Gobiernos, los problemas que plantea se ven compensados por el interés colectivo en la democracia. El derecho a la privacidad es extremadamente importante para las mujeres, los niños y las personas con orientaciones sexuales, identidades de género, expresiones de género y características sexuales diversas por todos los motivos indicados en este documento y señalados en las comunicaciones[76].**

Europe; Agencia de los Derechos Fundamentales de la Unión Europea, *Violence against Women: an EU-Wide Survey – Main Results* (Luxemburgo, Oficina de Publicaciones de la Unión Europea, 2015).

[72] Gay, Lesbian and Straight Education Network, *Out Online: The Experiences of Lesbian, Gay, Bisexual and Transgender Youth on the Internet* (Nueva York, 2013), en la comunicación internacional conjunta, 2018.

[73] Comunicación de la Australian Women Against Violence Alliance, 2018.

[74] Comunicación conjunta de organizaciones de la sociedad civil, 2018; Peter Micek y Denis Nolasco, "The gender of surveillance: how the world can work together for a safer Internet", Access Now, blog, 6 de febrero de 2018.

[75] Resolución 217 A (III) de la Asamblea General, preámbulo.

[76] Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, *Nacidos libres e iguales: Orientación sexual e identidad de género en las normas internacionales de derechos humanos* (Nueva York y Ginebra, 2012).

102. Las vulneraciones de la privacidad motivadas por cuestiones de género son una forma sistémica de denegación de los derechos humanos, son discriminatorias por naturaleza y a menudo perpetúan la desigualdad de las estructuras sociales, económicas, culturales y políticas.

103. Para hacer frente a las invasiones de la privacidad motivadas por cuestiones de género, es necesario establecer marcos a nivel internacional, regional y nacional.

104. A fin de prevenir las intrusiones en la vida privada motivadas por cuestiones de género, los Estados deben proteger activamente la privacidad al elaborar políticas, realizar reformas legislativas, prestar servicios, adoptar medidas normativas, brindar apoyo a las organizaciones de la sociedad civil y crear marcos educativos y de empleo, aprovechando para ello las experiencias de las mujeres, los hombres, las mujeres y los hombres transgénero, las personas intersexuales y otras personas que se identifiquen como no binarias o no cisnormativas.

105. La protección de la información personal en línea debe ser una prioridad, para lo cual es necesario que los países que no sean partes en el Reglamento General de Protección de Datos adopten disposiciones que equivalgan o superen a las previstas en este. El género debe ser una consideración fundamental en el proceso de elaboración y aplicación de marcos para la protección de la privacidad.

106. Es necesario que las empresas privadas sean transparentes en cuanto al uso que hacen de los datos personales de los usuarios[77] y a su respuesta ante las denuncias de ciberacoso. También es importante que haya una mayor diversidad de género entre los encargados de dar forma a las experiencias en línea a fin de que los productos y plataformas sean más seguros, asuman mayor responsabilidad social y rindan cuentas.

VI. Resumen de las recomendaciones

107. **Los órganos de las Naciones Unidas, todos los titulares de mandatos competentes de los procedimientos especiales y otros mecanismos del Consejo de Derechos Humanos y de los órganos creados en virtud de tratados de derechos humanos deberían integrar las cuestiones de género y privacidad en la ejecución de sus respectivos mandatos.**

108. **Se recomienda a los Estados Miembros que:**

a) Adopten un enfoque interseccional que tenga en cuenta que las ventajas del derecho a la privacidad, la manera en que este se disfruta y las amenazas que pesan sobre él varían en función del género, y que contemple los principios generales de la privacidad y los derechos humanos;

b) Sometan a evaluación los marcos jurídicos de los que disponen para prevenir y sancionar las vulneraciones de la privacidad motivadas por cuestiones de género, para determinar si se ajustan a las leyes y tratados pertinentes a nivel mundial, regional y nacional;

c) Adopten marcos jurídicos, regulatorios y de políticas que establezcan una protección integral en lo que respecta al uso y el desarrollo de sistemas de comunicación digital seguros;

d) Promuevan el acceso efectivo a Internet y cierren la brecha digital entre los géneros, si la hubiere;

e) Adopten las medidas legislativas, administrativas y de otra índole que sean necesarias para prevenir, investigar y sancionar las vulneraciones de la privacidad perpetradas por motivos de género, orientación sexual o identidad de género.

[77] Comisión de Defensa de la Competencia y del Consumidor de Australia, *Digital Platforms Inquiry: Preliminary Report* (Canberra, Australia, 2018).

109. **Las empresas deberían aplicar los Principios Rectores sobre las Empresas y los Derechos Humanos: Puesta en Práctica del Marco de las Naciones Unidas para "Proteger, Respetar y Remediar" y evitar violar los derechos humanos de las personas afectadas por sus prácticas, tomando en consideración de manera efectiva las repercusiones que sus actividades tienen sobre cada género.**

VII. Protección de los datos sanitarios

110. La salud es lo más importante en la vida de todas las personas. Los cambios en el estado de salud siempre llevan aparejados cambios en la vida, muchos de ellos de carácter permanente. En algún momento de la vida, todos nos convertimos en pacientes. También surgen situaciones en las que nuestro estado de salud tiene una influencia decisiva en nuestra vida. Por lo tanto, es muy legítimo el interés que todos tenemos en proteger nuestra dignidad y autonomía mediante la aplicación de las normas más exigentes en lo que respecta a los datos referidos a nuestra salud.

111. La relación entre el titular de los datos en calidad de paciente y el profesional de la salud es muy delicada: los pacientes están, por definición, en una posición vulnerable. La situación puede ser angustiosa y peligrosa y tener consecuencias de por vida. Por la naturaleza de su trabajo, los profesionales de la salud necesitan información completa y exacta sobre el paciente y contar con procesos que les permitan utilizar esa información de manera estandarizada y transparente.

112. La protección de los pacientes (y de sus parientes consanguíneos) en esos momentos de vulnerabilidad existencial es objeto de consideraciones y normas legales y éticas desde hace milenios. Principios tales como el secreto médico, la obligación de obtener el consentimiento plenamente informado antes de un tratamiento, el registro adecuado del tratamiento administrado y la libertad de elección del médico son el resultado de siglos de reflexión sobre la mejor manera de proteger los derechos de los pacientes.

113. Todas las situaciones médicas generan datos personales. Esos datos son importantes para el tratamiento y deben ser procesados respetando las normas legales y éticas más estrictas. La digitalización genera cada vez más datos médicos, y serán cada vez más los profesionales médicos que deberán intercambiar esa información, conforme aumente su nivel de especialización, y del mismo modo esos profesionales deberán colaborar ateniéndose a las normas de calidad más rigurosas.

114. Los datos procesados con fines médicos también son importantes para muchos otros interesados y para muchos otros fines más allá de la relación potencialmente trascendental entre el profesional de la salud y el paciente. En primer lugar, el paciente tiene un interés legítimo en controlar esos datos y puede dar su consentimiento para que se compartan tanto durante el tratamiento como después de él. En segundo lugar, hay otras personas y entidades que podrían tener interés en acceder a esos datos, como los familiares de los pacientes, las instituciones con las que el paciente tiene una obligación, por ejemplo las instituciones de la seguridad social, las aseguradoras o los empleadores, y otras partes interesadas con una relación menos directa, como los investigadores en medicina y la sociedad en general, que depende de la eficacia y eficiencia del sistema de salud.

115. Las tensiones entre los intereses y las necesidades de las distintas partes plantean problemas legales y éticos muy complejos.

Cuestiones fundamentales

Consentimiento informado

116. Por lo general, el paciente tiene derecho a aceptar un tratamiento tras ser informado de los posibles riesgos, efectos secundarios y alternativas. Los requisitos del procedimiento para la obtención del consentimiento informado para un tratamiento o trabajo de investigación médica están sometidos a normas estrictas, detalladas y controvertidas.

117. Esas normas todavía no están armonizadas con los requisitos relativos a la información que se debe proporcionar a los titulares de los datos ni con los criterios que establecen la validez del consentimiento informado como base jurídica para el procesamiento de los datos. A menudo, los criterios para el consentimiento informado son vagos y contradictorios.

118. Los titulares de los datos pueden sentirse abrumados ante la multiplicidad de procedimientos para la obtención del consentimiento informado en un momento en que la protección de los datos no es su principal motivo de preocupación. Asimismo, no siempre cuentan con la disposición o capacidad para entender plenamente las implicaciones que tienen los distintos tipos de consentimiento informado que dan. Tampoco existe una distinción clara entre los diferentes tipos de consentimiento informado necesarios (para las pruebas, el tratamiento, los trabajos de investigación médica y el procesamiento de datos), los cuales están sujetos a normas distintas y, en ocasiones, contradictorias y sometidos a la supervisión de diferentes autoridades. Esto somete a un elevado nivel de estrés a los pacientes y a sus familiares, lo que menoscaba su capacidad para otorgar su consentimiento libre e informado.

Uso secundario para trabajos de investigación médica

119. La recopilación y el procesamiento de datos personales son necesarios para el tratamiento médico. Una vez recopilados, los datos se almacenan, a veces durante décadas, para dejar constancia del tratamiento administrado. A menudo, esos datos pueden constituir una buena fuente de información para los trabajos de investigación médica. Hay argumentos de peso para defender que existe una justificación (o incluso una necesidad) ética para utilizar esos datos en trabajos de investigación que beneficien a las futuras generaciones de pacientes.

120. La investigación persigue un fin distinto que el tratamiento, por lo que requiere una base jurídica diferente para el procesamiento de los datos. Los requisitos de esta segunda base jurídica son muy diversos y poco claros, ya que muchas de las cuestiones éticas subyacentes no se describen ni analizan con claridad. En particular, se plantea, entre otras, la cuestión de si es necesario volver a obtener el consentimiento informado del paciente o la autorización del comité de ética o las autoridades supervisoras competentes para ese uso secundario. Entre los problemas que surgen se encuentra el de la autonomía personal derivada de la privacidad del cuerpo y el de la responsabilidad con el "bien colectivo".

121. Si se sustituyera el consentimiento informado por otra base jurídica, sería necesario tomar medidas adicionales para proteger los derechos fundamentales del titular de los datos. La falta de legislación internacional al respecto da lugar a situaciones en las que los médicos necesitan —o creen necesitar— que los pacientes afectados firmen otra declaración de consentimiento informado, lo cual, en algunos casos, resulta ya imposible por motivos técnicos o éticos.

Uso secundario para otros fines

122. Los datos médicos también son muy valiosos para otros fines, en particular para la seguridad social, la salud pública, el empleo y las empresas. Las leyes nacionales no suelen contener disposiciones relativas al procesamiento de datos para estos fines, y no está claro si esos propósitos tienen justificación ética y legal ni cuáles de los usos secundarios deben supeditarse al consentimiento informado y cuáles a otra base jurídica legítima. Por lo tanto, a menudo se ignora o vulnera el principio de limitación de la finalidad, según el cual el uso secundario de los datos personales debe ser compatible con los fines iniciales.

123. Las diferencias en la legislación sobre este tema llevan a una carrera hacia el mínimo común denominador, pues a los servicios públicos e incluso a las empresas que dependen de información personal relacionada con la salud les resulta más conveniente operar en zonas donde la protección de datos es escasa.

124. La protección de los derechos de los titulares de los datos (en particular, el derecho a la transparencia, lo que incluye la información y el acceso) plantea varios problemas, ya que estos no conocen a los responsables del tratamiento de los datos que llevan a cabo esos usos secundarios y, con frecuencia, ignoran su propósito.

La propiedad de los datos como forma de protección alternativa

125. Una consecuencia de las situaciones descritas anteriormente es que algunos juristas (e incluso algunos legisladores) han empezado a abogar por un derecho a la propiedad de los datos, similar al derecho de propiedad intelectual, que solucionaría los problemas que plantea el intercambio de datos personales y no personales. Estos conceptos no encajan fácilmente con los fundamentos de protección de datos existentes y requieren un razonamiento y justificación claros basados en previsiones empíricas de las consecuencias. De momento, falta una base objetiva y fáctica.

Reparto poco claro de las responsabilidades

126. Los tratamientos y trabajos de investigación médica están sometidos a la supervisión de órganos reguladores, en particular comités de ética, integrados por expertos y representantes de las partes interesadas, muchos de ellos sin formación jurídica, que carecen de conocimientos especializados sobre protección de datos.

127. No obstante, muchos de los requisitos establecidos por estos órganos en lo que se refiere al procesamiento de datos con fines de tratamiento e investigación guardan relación con la protección de datos, como es el caso de los requisitos específicos (y a menudo contradictorios) relativos a los procedimientos para la obtención del consentimiento informado, la información que se debe proporcionar al paciente o al titular de los datos, el derecho del paciente a saber y a no saber, las consecuencias de retirar el consentimiento, etc.

128. Las reglas propuestas por esos órganos pueden entrar en conflicto con las normas de protección de datos, y su labor de supervisión pueden interferir con la de las personas y autoridades encargadas exclusivamente de vigilar el cumplimiento de las disposiciones sobre protección de datos, como los funcionarios y autoridades independientes de protección de datos.

Ámbito de aplicación poco claro: datos personales, seudonimizados y anónimos

129. La premisa básica de que las leyes de protección de datos se aplican solamente cuando los datos son personales, es decir, cuando pertenecen a una persona concreta, es muy difícil de mantener en el contexto médico, ya que los datos sobre la salud rara vez se pueden anonimizar por completo. Por lo tanto, sigue sin quedar claro qué medida de anonimización es lo "bastante buena" para que esa información no esté sujeta a la legislación sobre protección de datos.

130. Este es un problema particularmente complejo que surge al estudiar si los datos médicos deben formar parte de iniciativas de acceso libre o de datos abiertos, para las que es necesario hacer públicos los datos (que no sean personales). Los responsables del tratamiento de datos podrían, por un lado, estar obligados a mantener los datos bajo su control para proteger el anonimato y, por el otro, verse forzados a facilitar el libre acceso a los datos, arriesgándose a su desanonimización. La falta de claridad podría facilitar la protección *de facto* de la propiedad de los datos médicos por parte de los responsables del tratamiento de datos, que, en la práctica, tienen la capacidad para decidir quién obtiene acceso a los datos (anonimizados de alguna forma) y bajo qué condiciones.

131. El Relator Especial señaló de forma inequívoca en su informe de 2018 a la Asamblea General que los datos de registro unitario sensibles y de alta dimensionalidad relativos a particulares no deberían publicarse en Internet ni intercambiarse a menos que se haya demostrado de manera concluyente que han sido sometidos a un proceso de anonimización seguro y no reversible en el futuro.

Falta de portabilidad de los datos y de digitalización

132. A menudo, los datos médicos se siguen recogiendo de manera analógica. Las anamnesis suelen contener información desordenada e incompleta y los diagnósticos se basan a veces en datos de baja calidad.

133. La digitalización de los datos médicos, la estandarización de los formatos y los procesos y el establecimiento de criterios mínimos en lo que respecta a la calidad de los datos pueden ayudar tanto a los pacientes como a los profesionales de la salud a controlar y gestionar de una manera responsable los datos sanitarios.

134. Pese a ello, los Estados tienden a establecer sus propios sistemas informáticos biosanitarios a nivel nacional sin la participación de los ciudadanos ni de los profesionales de la salud y sin estandarización. Esto puede imposibilitar la portabilidad de los datos para los pacientes y reducir la capacidad de estos de controlar sus datos médicos, a falta de un instrumento estándar que permita almacenar y gestionar con seguridad sus datos aplicando las normas que ellos decidan.

Nubes

135. Cada vez se almacena más información médica en la nube (al igual que cualquier otro tipo de datos). Las consecuencias que ello acarrea son numerosas, entre ellas la transferencia de datos personales a través de las fronteras, lo que conlleva posibles conflictos entre jurisdicciones, la falta de control por parte de los pacientes e incidentes de seguridad de gran repercusión que podrían afectar a millones de personas.

136. Los requisitos mínimos para los proveedores de servicios en la nube, sin embargo, no están armonizados, lo que puede dar pie a que operen desde zonas con un bajo nivel de protección de los datos.

Productos relacionados con el bienestar y dispositivos ponibles

137. Los datos relativos a la salud no siempre están relacionados (directamente) con enfermedades, y en la actualidad se recogen con fines distintos del tratamiento o la prevención de patologías. En particular, las aplicaciones y dispositivos relacionados con el bienestar (los “ponibles”) recopilan cantidades considerables de datos sobre la salud, con o sin el consentimiento informado de los titulares de los datos. Estos son cada vez más populares, y, pese a ello, la base jurídica para la recopilación de los datos y los requisitos para su uso no están claramente definidos, no existen normas mínimas de transparencia y el principio de limitación de la finalidad no se tiene lo suficientemente en cuenta.

Seguridad y protección

138. Aunque los datos relacionados con la salud son muy delicados y cualquier error en los dispositivos que procesan esos datos podría poner en peligro la vida del paciente, no existen reglas claras y concretas sobre las normas mínimas que se han de aplicar en materia de seguridad y protección. La consecuencia de esto es una serie de incidentes relacionados con la seguridad y la protección con graves repercusiones para los titulares de los datos afectados.

Notificación de las filtraciones de datos, falta de transparencia

139. Aunque las filtraciones de datos sobre la salud son un hecho frecuente, no hay normas que estipulen cómo y cuándo se debe informar de estos incidentes a las personas afectadas y a la población en general. Esta situación revela una falta de transparencia y el incumplimiento de los requisitos de rendición de cuentas que la población espera.

Acceso a la justicia

140. El incumplimiento de la legislación en materia de protección de datos puede poner en peligro la vida de los titulares de los datos. Pese a ello, la legislación relativa a la protección de datos carece, desde su origen, de instrumentos efectivos para garantizar su cumplimiento. La poca claridad de las normas relativas al reparto de las competencias entre las autoridades de protección de datos, los tribunales, los defensores del pueblo, los funcionarios responsables de la protección de datos y las autoridades del sector médico encargadas de la supervisión, junto con la desigualdad en la difusión de la información y los conocimientos y la complejidad de los marcos regulatorios, hacen que las personas afectadas tengan muchas dificultades para hacer valer sus derechos.

141. Esa falta de medidas para hacer cumplir la legislación da lugar a la pérdida de confianza en el sistema médico y, en particular, al deterioro de la relación entre el paciente y el profesional de la salud, lo que puede tener efectos perjudiciales en todos los pacientes. Por lo tanto, la formulación de normas mínimas por parte de las Naciones Unidas tiene una importancia estratégica máxima.

Etapas siguientes

142. El Relator Especial tiene la intención de ofrecer orientaciones para reglamentar el procesamiento de los datos relacionados con la salud a fin de promover la protección de los datos personales y del derecho a la privacidad, de conformidad con lo estipulado en el artículo 12 de la Declaración Universal de Derechos Humanos y el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos.

143. En el proyecto de orientaciones[78] en el que se establecen los principios rectores para el procesamiento de datos relacionados con la salud, se pone de relieve la importancia de que exista una base legítima para el procesamiento de los datos sanitarios que abarque las cuestiones descritas anteriormente. Los objetivos de las orientaciones son, en primer lugar, servir de base común a nivel internacional para la formulación de normas mínimas nacionales para la protección de los datos sanitarios y, en segundo lugar, ser un punto de referencia para el debate en curso sobre cómo se puede proteger y seguir promoviendo el derecho a la privacidad en la esfera de los datos sanitarios, junto con otros derechos humanos (como la libertad de expresión, el derecho a un juicio imparcial y la protección de la propiedad), en un contexto en el que los datos médicos se procesan y comparten a escala mundial.

144. El proyecto de orientaciones, que actualmente están examinando los expertos del equipo de tareas, se encuentra disponible para consulta pública y abierto para la formulación de observaciones por escrito hasta el 11 de mayo de 2019, tras lo cual las partes interesadas celebrarán una reunión pública en Estrasburgo los días 11 y 12 de junio de 2019. Los Estados Miembros que deseen participar en esa reunión deben manifestar su interés antes del 11 de mayo.

145. El grupo de redacción, basándose en las aportaciones de los interesados, formulará una recomendación final al Relator Especial, que este incorporará en su informe anual de 2019 a la Asamblea General, previsto para finales de 2019.

VIII. Parámetros para evaluar la privacidad

146. El Relator Especial también está celebrando consultas sobre los “parámetros para evaluar la privacidad”[79]. Se invita a la sociedad civil, a los Gobiernos y a los particulares a que envíen sus observaciones y propuestas antes del 30 de junio de 2019. El objetivo sería utilizar esos parámetros como herramienta de investigación estándar durante las visitas a los países, tanto las oficiales como las oficiosas.

[78] Véase www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2019_HRC_Annex3_HealthData.pdf.

[79] Véase www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2019_HRC_Annex4_Metrics_for_Privacy.pdf.