Naciones Unidas A/72/540

Asamblea General

Distr. general
19 de octubre de 2017
Español
Original: inglés

Septuagésimo segundo período de sesiones
Tema 72 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 del Relator Especial del Consejo de Derechos Humanos sobre el derecho a la privacidad, Joseph A. Cannataci, presentado de conformidad con la resolución 28/16 del Consejo de Derechos Humanos.

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

17-18460 (S) 301017 021117

Informe del Relator Especial del Consejo de Derechos Humanos sobre el derecho a la privacidad

Resumen

El presente informe se divide en dos partes: la primera contiene un resumen de las actividades realizadas durante 2016 y 2017, la segunda contiene el informe provisional sobre la labor del Equipo de Tareas sobre Macrodatos y Datos Abiertos establecido por el Relator Especial del Consejo de Derechos Humanos sobre el derecho a la privacidad.

Índice

Página

I. Reseña de las actividades realizadas por el Relator Especial sobre el derecho a la privacidad en 2016-2017

1. El período 2016-2017 ha sido particularmente intenso para el mandato del Relator Especial en lo que respecta a la colaboración con la sociedad civil, los Gobiernos, las fuerzas del orden, 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 durante el cual tuvieron lugar 26 eventos en 15 países y cuatro continentes. Para cumplir estos compromisos el Relator Especial visitó más de 30 ciudades, algunas de ellas en Asia, África Septentrional y América Central, el 25% de las actividades se realizaron en los Estados Unidos de América y más del 50% en Europa.

A. Proyecto de instrumento jurídico internacional sobre la vigilancia y la privacidad

2. La seguridad y la vigilancia son cuestiones importantes y por ello en 2015 el Consejo de Derechos Humanos estableció el mandato del Relator Especial sobre el derecho a la privacidad.

3. El mandato del Relator Especial sobre el derecho a la privacidad, enunciado en la resolución 28/16 del Consejo de Derechos Humanos, estipula con claridad el deber de "Determinar posibles obstáculos a la promoción y protección del derecho a la privacidad, determinar, intercambiar y promover principios y mejores prácticas a nivel nacional, regional e internacional, y presentar propuestas y recomendaciones al Consejo a ese respecto, entre otras cosas en relación con retos concretos de la era digital"[1].

4. La laguna existente en el derecho internacional con respecto a la vigilancia y la privacidad en el ciberespacio, la esencia misma de las revelaciones de Snowden, son consideradas por el Relator Especial como un obstáculo grave para la privacidad y este asunto es actualmente su principal preocupación. El Relator Especial considera no solo que la falta de normas sustantivas constituye un obstáculo para la promoción y la protección de la privacidad, sino también la inexistencia de mecanismos adecuados[2].

5. Conforme a su mandato, el Relator Especial recomendaría encarecidamente que el Consejo de Derechos Humanos apoye la discusión y la adopción, en el seno de las Naciones Unidas, de un instrumento jurídico para lograr dos finalidades principales:

a) Proporcionar a los Estados Miembros una serie de principios y disposiciones modelo que puedan integrarse en su legislación nacional y que representen y sustenten los más elevados principios de derechos humanos y, en particular, la privacidad en lo que respecta a la vigilancia;

b) Proporcionar a los Estados Miembros una serie de opciones para ayudar a subsanar las deficiencias y colmar la laguna existente en el derecho internacional y en particular las relacionadas con la privacidad y la vigilancia en el ciberespacio.

[1] A/70/53, secc. III. parte A, resolución 28/16, párr. 4 c).

[2] Informe del Relator Especial sobre el derecho a la privacidad al Consejo de Derechos Humanos, marzo de 2017 (la versión no editada anticipada está disponible en línea, véase A/HRC/34/60).

6. Si bien la necesidad de ese instrumento jurídico es evidente, aún deben definirse su alcance exacto y su forma. Si bien se está perfilando la substancia de su contenido en las investigaciones en curso y las consultas con los interesados, el mejor vehículo para lograr esos objetivos todavía no ha sido determinado.

7. Desde hace tiempo se reconoce que una de las pocas esferas en que el derecho a la privacidad no puede ser absoluto es el de la detección, la prevención, la investigación y el enjuiciamiento del delito, así como en la seguridad nacional. No obstante, la preservación de las democracias exige controles y contrapesos para asegurar que cualquier actividad de vigilancia sirva para proteger una sociedad libre. La autorización previa de la vigilancia y la posterior supervisión de las actividades de vigilancia es una parte fundamental de las normas, las salvaguardias y los recursos que necesita una sociedad democrática a fin de preservar las libertades que la definen.

8. El informe del Relator Especial al Consejo de Derechos Humanos de marzo de 2017 contenía conclusiones provisionales para un instrumento jurídico que regule la vigilancia en el ciberespacio y complemente la legislación cibernética vigente, como la Convención sobre la Ciberdelincuencia (la Convención de Budapest) aprobada por el Comité de Ministros del Consejo de Europa en 2001. En el marco de una iniciativa anterior, el proyecto MAPPING (Managing Alternatives for Privacy, Property and Internet Governance), que cuenta con el apoyo de la Unión Europea, se están estudiando opciones para un instrumento jurídico que regule la vigilancia en el ciberespacio. Entidades de la sociedad civil y empresas internacionales están debatiendo un proyecto de texto que será dado a conocer antes de la primavera de 2018.

9. El proceso se describe más detalladamente en el justificante V[3].

B. Cartas de denuncia

10. Algunas de las cartas de denuncia enviadas por el Relator Especial a los Gobiernos en relación con la vigilancia serán publicadas por la Oficina del Alto Comisionado para los Derechos Humanos (ACNUDH) conforme a los informes sobre las comunicaciones de los titulares de mandatos de procedimientos especiales.

C. Otras cartas: dominio público; Japón

11. El 18 de mayo de 2017, el Relator Especial publicó una carta al Gobierno del Japón (véase el justificante III)[4]. En esta carta, el Relator Especial expresó su preocupación por las deficiencias de los proyectos de legislación que permitían la vigilancia sin las salvaguardias necesarias, ostensiblemente para permitir que el Japón ratifique la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional de 2000. Las iniciativas de cooperación acerca de esta cuestión continúan y serán reseñadas en el informe del Relator Especial al Consejo de Derechos Humanos de marzo de 2018.

[3] Véase www.ohchr.org/Documents/Issues/Privacy/A-72-Slot-43103.docx.
[4] Véase www.ohchr.org/Documents/Issues/Privacy/A-72-Slot-43103.docx.

D. Otras iniciativas en curso relativas a la vigilancia

12. Hay otras iniciativas en estudio para su inclusión en el mandato respecto de la vigilancia, la seguridad y la privacidad. Si procede, más adelante se darán a conocer los detalles.

E. Una mejor comprensión de la privacidad

13. El Relator Especial está analizando la privacidad, entre otras cosas, como un derecho esencial que facilita el ejercicio de un derecho fundamental y abarcador al desarrollo libre y sin trabas de la propia personalidad. La Presidenta del Equipo de Tareas sobre la Privacidad y la Personalidad, Elizabeth Coombs, excomisionada para la privacidad de Nueva Gales del Sur (Australia), ha tenido la amabilidad de acceder a cumplir esta labor y hará especial hincapié en el género y la privacidad.

14. El justificante IV contiene más información sobre las actividades llevadas a cabo por el Equipo de Tareas[5].

F. Equipo de Tareas sobre la Privacidad de los Datos relativos a la Salud

15. El Equipo de Tareas del Relator Especial sobre la Privacidad de los Datos relativos a la Salud ha comenzado su labor bajo la dirección del Dr. Steve Steffensen, de los Estados Unidos de América. Se prevé la celebración de consultas en la primavera y el verano de 2018.

G. Utilización de datos personales por las empresas

16. El Relator Especial ha seguido trabajando sobre los modelos institucionales y la privacidad en el uso de datos personales por las empresas, tanto de manera independiente como en el marco del proyecto MAPPING, en preparación para la puesta en marcha del equipo de tareas del Relator Especial sobre el tema con los plazos anunciados en el sitio web del Relator Especial (http://www.ohchr.org/EN/Issues/Privacy/SR/Pages/ThematicReports.aspx).

H. Visitas oficiales a los países

17. Se han realizado o previsto las siguientes visitas a los países: Estados Unidos de América (19 a 28 de junio de 2017), Francia (fechas confirmadas: 13 a 17 de noviembre de 2017);[6] Reino Unido de Gran Bretaña e Irlanda del Norte (fechas confirmadas: 11 a 17 de diciembre de 2017); Alemania (fechas confirmadas: 29 de enero a 2 de febrero de 2018); y la República de Corea (fechas confirmadas: 3 a 15 de julio de 2018).

[5] Véase www.ohchr.org/Documents/Issues/Privacy/A-72-Slot-43103.docx.

[6] Se prevé que el informe final sobre la visita oficial a los Estados Unidos de América se publicará en la primavera de 2018. La declaración de final de la misión puede consultarse en http://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/VisitUSA_EndStatementJune2017.docx.

I. Asignación de recursos

18. Solo la visita oficial a los Estados Unidos y el viaje del Relator Especial y otros oradores a Hong Kong (China) para asistir la Conferencia Internacional de Comisionados para la Protección de Datos y la Privacidad y sus deliberaciones sobre la personalidad y los flujos de información en Asia fueron financiados con cargo al presupuesto para el mandato de Relator Especial administrado por el ACNUDH. Las otras visitas recibieron financiación extrapresupuestaria procedente en gran parte de los anfitriones de los eventos respectivos.

II. Equipo de Tareas sobre Macrodatos y Datos Abiertos

19. El Equipo de Tareas sobre Macrodatos y Datos Abiertos establecido por el Relator Especial es dirigido por David Watts[7]. Los autores principales del presente informe son David Watts y Vanessa Teague[8]. Entre los miembros del Equipo de Tareas, muchos de los cuales también han contribuido a este informe, figuran Christian d'Cunha (Supervisor Europeo de Protección de Datos), Alex Hubbard (de la oficina del Comisionado de Información del Reino Unido), el Profesor Wolfgang Nejdl (Universidad de Hannover, Alemania), Marty Abrams (Information Accountability Foundation, Estados Unidos) y Marie Georges (Francia). Sean McLaughlan, Elizabeth Coombs y Joe Cannataci también han hecho aportes al informe.

20. Puede obtenerse más información sobre el proceso de redacción del informe sobre macrodatos y datos abiertos en el justificante VII[9].

A. Contexto de las cuestiones

21. Uno de los retos más importantes que afrontan las sociedades de la información del siglo XXI es la tarea de conciliar los beneficios sociales que ofrecen las nuevas tecnologías de la información y las comunicaciones con la protección de los derechos fundamentales, como el derecho a la privacidad . Estas nuevas tecnologías pueden servir para que los Estados respeten, protejan y cumplan sus obligaciones en materia de derechos humanos, pero también encierran el riesgo de socavar algunos derechos humanos, en particular el derecho a la privacidad.

22. Los nuevos métodos de reunión y análisis de datos —el fenómeno de los macrodatos— y la creciente disposición de los Gobiernos de todo el mundo a publicar la información personal que poseen, aunque sea sin identificar a alguien concretamente, a fin de promover el crecimiento económico y estimular la investigación científica —el fenómeno de los datos abiertos— ponen en tela de juicio muchos de los supuestos en que se basan nuestras ideas sobre lo que significa la privacidad, lo que ella entraña y la mejor manera de protegerla.

23. Con el reconocimiento por el Consejo de Derechos Humanos de que la privacidad es un derecho habilitante esencial para el derecho a la dignidad y el desarrollo libre y sin trabas de la propia personalidad (véase la resolución 34/7 del Consejo de Derechos Humanos, de 23 de marzo de 2017), se amplía el desafío que plantean los macrodatos y los datos abiertos.

[7] David Watts es profesor adjunto de derecho en Latrobe University y Deakin University. Hasta el 31 de agosto de 2017 fue Comisionado para la Privacidad y la Protección de Datos del Estado de Victoria (Australia).

[8] Vanessa Teague es profesora titular del Departamento de Informática y Sistemas de Información en la Universidad de Melbourne (Australia).

[9] Véase www.ohchr.org/Documents/Issues/Privacy/A-72-Slot-43103.docx.

24. Algunas afirmaciones acerca de los macrodatos y los datos abiertos han sido calificadas de “utópicas”[10]. Ellas sostienen que los macrodatos ofrecen los medios de adquirir nuevas perspectivas respecto de cuestiones de política pública insolubles, como el cambio climático, la amenaza del terrorismo y la salud pública. En el otro extremo del espectro se encuentran quienes adoptan un punto de vista distópico a causa de la preocupación por la vigilancia cada vez mayor de los agentes estatales y no estatales, la intrusión injustificada en el ámbito privado y el desmoronamiento de la protección de la privacidad.

25. Uno de los principales escollos para la elaboración de este informe ha sido el de examinar y evaluar las afirmaciones de los diversos interesados que intervienen en los debates complejos acerca de los macrodatos y datos abiertos. Aunque ambas cuestiones han generado abundantes comentarios y estudios, aún no se ha llegado a tener un conocimiento cabal de las tecnologías y sus consecuencias futuras; paradójicamente, esa carencia impide que comprendamos los posibles beneficios y daños de los macrodatos y los datos abiertos.

B. Datos

26. Cada día nuestras actividades digitales generan datos que suman 2,5 trillones de octetos[11]. Ello significa 2,5 seguido de 18 ceros[12]. Para ponerlo en perspectiva: una novela corriente de 300 páginas contiene alrededor de 300.000 octetos. El 90% de todos los datos existentes en el mundo fue creado en los dos últimos años y la rapidez con que se están generando sigue creciendo[13].

27. En el mundo conectado en que vivimos, los datos son dominantes y omnipresentes. Cuando utilizamos una computadora, un teléfono inteligente o incluso dispositivos habituales, como sensores capaces de registrar información, se generan datos como subproducto. Este subproducto adopta la forma de caracteres o símbolos que en última instancia son transformados por los dispositivos informáticos en un código binario que es posteriormente procesado, almacenado y transmitido como señales electrónicas.

28. Las fuentes de los datos utilizados para los macrodatos son tan variadas como las actividades que se llevan a cabo utilizando la Internet:

> “Los datos provienen de muchas fuentes distintas, entre ellas, instrumentos científicos, dispositivos médicos, telescopios, microscopios, satélites; medios digitales, incluidos textos, vídeos, grabaciones sonoras, correo electrónico, blogs, mensajes de Twitter, colecciones de imágenes, clics y transacciones financieras; sensores dinámicos, redes sociales y de otra índole; simulaciones científicas, modelos y encuestas; o análisis computacionales de datos procedentes de observación. Los datos pueden ser temporales, espaciales, o dinámicos; estructurados o no estructurados; la información y los conocimientos derivados de los datos pueden diferir en la representación, la complejidad, la granularidad, el contexto, la procedencia, la respetabilidad, la fiabilidad y el

[10] Danah Boyd y Kate Crawford, Critical questions for Big Data, Information, Provocations for a cultural, technological, and scholarly phenomenon”, Communication and Society, Vol. 15, núm. 5.

[11] Véase www-01.ibm.com/software/data/bigdata/what-is-big-data.html.

[12] Esa es la medida utilizada en los Estados Unidos de América. En el Reino Unido, un “quintillion” es 1 seguido por 30 ceros.

[13] Véase www-01.ibm.com/software/data/bigdata/what-is-big-data.html.

alcance. Los datos también pueden diferir en cuanto a la rapidez con que son generados y se accede a ellos”[14].

29. Algunos de los datos creados no guardan relación con personas. Son los datos derivados de otras actividades, como el análisis de las tendencias meteorológicas, la exploración del espacio, los ensayos científicos de materiales y diseños o de los riesgos vinculados al comercio de valores en los mercados financieros. Sin embargo, hay una gran proporción de datos que creamos nosotros mismos o que se generan acerca de nosotros. El presente informe se centra en esta categoría de datos, la información personal, ya sea esta proporcionada, observada, derivada o inferida[15].

30. La información personal capta nuestra individualidad como seres humanos. Esta capacidad de identificar a cada persona hace que la información personal sea tan valiosa.

31. Al crear nuestros propios datos nos convertimos en agentes. Esos datos comprenden nuestros mensajes de correo electrónico y mensajes de texto, así como las imágenes y los vídeos que creamos y compartimos. Otros datos sobre nosotros son creados por terceros, pero en circunstancias en las que hemos participado, al menos en cierta medida, en su creación, por ejemplo, los registros electrónicos sobre salud o las operaciones de comercio electrónico.

32. Otros datos sobre nosotros son generados en formas que no resultan evidentes, ya que se producen entre bastidores, en circunstancias poco claras y en gran medida desconocidas y que tampoco podemos llegar a conocer. Son las “migajas digitales”, artefactos electrónicos y otras huellas electrónicas que dejamos como resultado de nuestras actividades tanto virtuales como presenciales[16]. Estos datos pueden abarcar la hora y el lugar en que nuestros dispositivos móviles se conectan con las torres de telefonía móvil o los satélites del sistema de posicionamiento global (GPS), los registros de los sitios web que visitamos o las imágenes captadas por los sistemas de circuito cerrado de televisión. Estas “migajas digitales que dejamos, y que probablemente quedarán a perpetuidad en los servidores, son indicios acerca de quiénes somos, qué hacemos y qué queremos. Por ello los datos personales —los datos sobre las personas— son inmensamente valiosos, tanto para el bien público como para las empresas privadas”[17].

33. Un mundo inmerso en datos, procesos informáticos y comunicaciones digitales instantáneas plantea interrogantes acerca de la manera en que los derechos a la privacidad pueden coexistir con las nuevas tecnologías que permiten reunir datos personales, procesarlos y analizarlos en formas que no podrían haberse imaginado cuando se redactó la Declaración Universal de Derechos Humanos de 1948 y el Pacto Internacional de Derechos Civiles y Políticos de 1966.

34. De resultas de la ubicuidad de la mediación informática, casi todos los aspectos del mundo se plasman en una nueva dimensión simbólica en forma de eventos, objetos y procesos y las personas se tornan visibles y es posible conocerlas

[14] Fundación Nacional para la Ciencia de los Estados Unidos, Critical Techniques and Technologies for Advancing Big Data Science & Engineering (BIGDATA), licitación NSF 14-543. Véase www.nsf.gov/pubs/ 2014 /nsf 14543 /nsf 14543.pdf en pág. 3.

[15] Martin Abrams, “The origins of personal data and its implications for governance”, en http://informationaccountability.org/wp-content/uploads/Data-Origins-Abrams.pdf.

[16] Evan Schwartz, Finding our way with digital bread crumbs, MIT Technology Review, 18 de agosto de 2010. En www.technologyreview.com/s/ 420277/finding-our-way-with-digital-bread-crumbs/.

[17] Julie Lane y otros (eds.), *Big Data, and the Public Good: Frameworks for Engagement*, (New York, Cambridge University Press, 2014.

y compartirlas de una manera novedosa. El mundo renace en forma de datos y el texto electrónico alcanza una magnitud y un alcance universales[18].

35. La manera en que las tecnologías de la información y las comunicaciones permiten conocer a las personas mediante el análisis de sus datos implica "observar el carácter de una persona como si estuviera constituido por la información acerca de ella". El fenómeno que lo facilita son los llamados macrodatos[19].

C. Macrodatos

36. El término "macrodatos" se utiliza comúnmente para describir el volumen de datos enorme y creciente y las técnicas analíticas avanzadas que se emplean para buscar, cotejar, analizar y extraer conclusiones de ellos.

37. No hay una definición aceptada de los macrodatos. El Instituto Nacional de Ciencia y Tecnología de los Estados Unidos los describe como la incapacidad de las estructuras de datos tradicionales para manejar con eficiencia los nuevos conjuntos de datos. Las características de los macrodatos que obligan a adoptar nuevas estructuras son las siguientes:

a) Volumen (es decir, el tamaño del conjunto de datos);

b) Variedad (es decir, datos de múltiples repositorios, dominios o tipos);

c) Velocidad (es decir, la rapidez con que circulan); y

d) Variabilidad (es decir, los cambios de características).

38. Estas características —volumen, variedad, velocidad y variabilidad— son conocidas coloquialmente como las "Uves" de los macrodatos[20].

39. La descripción citada del Instituto Nacional, así como muchas otras iniciativas para perfilar el fenómeno de los macrodatos, como la definición de la Unión Europea que dice que "los macrodatos se refieren a grandes cantidades de datos producidos muy rápidamente por un número elevado de fuentes diversas", apuntan a las tecnologías que de consuno hacen que la recopilación, el procesamiento y el análisis de grandes cantidades de datos se convierta en un hecho corriente[21]. Sin embargo, el alto grado de generalización de estas descripciones y su enfoque predominante en las tecnologías no son suficientes para explicar el fenómeno de los macrodatos.

40. Diversos expertos han tratado de formular una descripción más exhaustiva de los macrodatos que abarque mucho más que las cuatro "Uves". Una descripción útil y más detallada de los macrodatos es la siguiente:

a) Un volumen enorme formado por teraoctetos o petaoctetos de datos;

b) Alta velocidad por lo que se crean en tiempo real o poco menos;

c) Diversa variedad, pueden ser estructurados o no estructurados;

d) Alcance exhaustivo, pues tratan de abarcar poblaciones o sistemas en su totalidad;

[18] Shoshana Zuboff, "Big Other: Surveillance capitalism and the prospects of an information civilization" *Journal of Information Technology*, vol. 30 núm. 1 (marzo de 2015).

[19] Luciano Floridi, "Four challenges for a theory of informational privacy", *Ethics and Information Technology*, vol. 8, núm. 3 (julio de 2006).

[20] Se les atribuyen otras "Uves" pero estas cuatro son las principales. Véase http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP. 1500-1.pdf.

[21] Véase https://ec.europa.eu/digital-single-market/en/policies/big-data.

e) Alta resolución, ya que pueden ser identificados e indexados con singularidad;

f) Carácter relacional, gracias a campos comunes que permiten amalgamar conjuntos de datos diferentes;

g) Flexibles, pues añaden nuevos campos con facilidad y pueden aumentar su tamaño con rapidez[22].

41. Un caso particular de macrodatos no encierra necesariamente todas y cada una de estas características.

42. Otros enfoques consideran que los macrodatos son algo más que un fenómeno tecnológico:

> "Definimos a los macrodatos como un fenómeno cultural, tecnológico y académico que radica en la interacción de:
>
> a) La tecnología para maximizar el poder de computación y la exactitud algorítmica para reunir, analizar, vincular y comparar grandes conjuntos de datos;
>
> b) El análisis: servirse de grandes conjuntos de datos para determinar pautas a fin de formular principios económicos, sociales, técnicos y jurídicos;
>
> c) Mitología: la creencia generalizada de que los grandes conjuntos de datos ofrecen una forma superior de inteligencia y conocimientos que pueden servir para hacer descubrimientos que eran anteriormente imposibles, con un halo de verdad, objetividad y exactitud"[23].

43. El argumento principal que aducen los partidarios de los macrodatos es que pueden ofrecer una solución para las limitaciones de que adolecen las investigaciones a causa de la falta de pruebas empíricas, es decir, una falta de datos, y nos proporcionan la verdad objetiva sobre las circunstancias o los fenómenos. Estas afirmaciones epistemológicas, que tienden a elevar a los macrodatos a una nueva forma de método científico, motivan la inquietud que muchos han expresado acerca de las limitaciones y los riesgos que plantean los macrodatos.

44. Hay un consenso amplio en que los macrodatos pueden generar beneficios sociales, incluidos servicios personalizados, un mayor acceso a los servicios, mejores resultados en materia de salud, adelantos tecnológicos y mejoras en la accesibilidad.[24] La Comisión Europea señala que "la necesidad de comprender los macrodatos está dando lugar a innovaciones tecnológicas, al desarrollo de nuevas herramientas y nuevas aptitudes"[25].

---

[22] Rob Kitchin, Big Data, new epistemologies and paradigm shifts, Big Data and Society, vol. 1 núm. 1 (abril-junio de 2014).

[23] Boyd y Crawford, "Critical questions for big data".

[24] También hay opiniones muy contrarias. Por ejemplo, véase la declaración de la Unión Europea, Grupo de Trabajo de la Unión Europea sobre Protección de Datos conforme al Artículo 29 acerca de los efectos del desarrollo de macrodatos para la protección de las personas, en relación con el procesamiento de sus datos personales, Unión Europea, 16 de septiembre de 2014: "Se esperan muchos beneficios individuales y colectivos del desarrollo de los macrodatos, a pesar de que aún no se ha probado el valor real de los macrodatos. El Grupo de Trabajo apoyaría sin duda las iniciativas serias que se emprendan en la Unión Europea o a nivel nacional con miras a obtener beneficios reales para las personas en la UE, ya sea a título individual o colectivo". Véase http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp221=en.pdf.

[25] Véase https://ec.europa.eu/digital-single-market/en/making-big-data-work-europe.

45. La Comisión Europea considera que la información es un bien económico, tan importante para la sociedad como la mano de obra y el capital[26]. Es significativo que este mercado esté dominado por un pequeño número de grandes empresas de tecnología cuya cuota de mercado depende del uso de datos.

D. Análisis avanzado

46. El cambio fundamental es la enorme utilización de datos para informar al algoritmo cuyo comportamiento ulterior depende de los datos a que tiene acceso.

> "La expresión aprendizaje automático se refiere a la detección automatizada de pautas significativas en los datos. En dos decenios, se ha convertido en un instrumento común de casi cualquier tarea que exija extraer información de grandes conjuntos de datos.
>
> Una característica común de todas estas aplicaciones es que, a diferencia de los usos más tradicionales de las computadoras, en estos casos, debido a la complejidad de las pautas que hay que detectar, un programador humano no puede proporcionar una especificación explícita y muy detallada de la manera en que deberían ejecutarse tales tareas ... Las herramientas de aprendizaje automático tienen por objeto dotar a los programas de la capacidad de aprender y adaptarse"[27].

47. La diferencia fundamental entre "ahora" y "entonces" es el carácter autónomo y semiautónomo de las nuevas técnicas.

48. Una de las técnicas de análisis de uso más común es la llamada "manejo de datos". Es un proceso por el cual se extraen los datos de conjuntos voluminosos de datos y se los analiza posteriormente para determinar si existen pautas o correlaciones El manejo de datos facilita la simplificación y el resumen de cantidades ingentes de datos brutos y la inferencia de conocimientos a partir de las pautas que aparecen[28].

49. El mecanismo que impulsa estas técnicas e instrumentos es el algoritmo.

E. Algoritmos

50. Los algoritmos no son algo nuevo. "Han existido desde el comienzo de los tiempos y existían mucho antes de que se acuñara una palabra especial para denominarlos"[29].

51. Los algoritmos no se limitan a las matemáticas. Los babilonios los utilizaban para decidir cuestiones de derecho, los maestros de latín los utilizaban para evitar errores de gramática y se los ha empleado en todas las culturas para predecir el futuro, para decidir un tratamiento médico o para la preparación de alimentos. Actualmente todo el mundo usa algoritmos de algún tipo, a menudo sin saberlo, al seguir una receta o una plantilla para tejido o al emplear un electrodoméstico[30].

---

[26] *Ibid.*

[27] Shai Shalev-Shwartz y Shai Ben-David, *Understanding Machine Learning* (Nueva York, Cambridge University Press, 2014).

[28] Datos que solo se refieren a una persona.

[29] Jean-Luc Chabert (ed), *A History of Algorithms: from the Pebble to the Microchip*, Berlín, Springer-Verlag, Berlin, Heidelberg, 1999.

[30] *Ibid.*

52. Al igual que para otros elementos de macrodatos, “es muy difícil dar una caracterización precisa de lo que es un algoritmo”. A los efectos del presente informe, una definición práctica es la siguiente:[31]

> “un conjunto de instrucciones específicas para realizar un procedimiento o resolver un problema, por lo general con el requisito de que el procedimiento termine en algún momento. A veces los algoritmos específicos son denominados método, procedimiento o técnica. El proceso de aplicar un algoritmo a un aporte para obtener un producto se denomina cálculo”[32].

53. Lo que diferencia a un algoritmo utilizado para hornear una torta de un algoritmo que evalúa la capacidad crediticia de una persona es el grado de automatización del proceso, su carácter autónomo y no lineal y la cantidad de datos procesados.

54. Cada vez más, la manera en que nos entendemos y nuestra relación con el mundo tienen lugar desde la perspectiva de los algoritmos. Los algoritmos son ahora una parte fundamental de las sociedades de la información, cada vez más gobiernan las “operaciones, decisiones y elecciones que antes quedaban en manos de los seres humanos”[33]33, recomiendan parejas en sitios de citas[34]34, determinan el mejor camino para viajar[35]35 y evalúan nuestro riesgo de crédito36[36]. Se utilizan para elaborar perfiles, es decir para determinar las características personales y las pautas de comportamiento a fin de hacer predicciones personalizadas, por ejemplo respecto de los bienes o servicios que nos interesaría comprar. Determinan la manera en que deberían interpretarse los datos y qué medidas deberían adoptarse en consecuencia. Sirven de “mediadores en los procesos sociales, en las transacciones comerciales, en las decisiones gubernamentales y en la manera en que percibimos y entendemos nuestro medio ambiente e interactuamos entre nosotros y con él”[37].

55. Desde una perspectiva individual, las recomendaciones y decisiones resultantes de los procesos algorítmicos parecen surgir de una caja negra inescrutable y misteriosa, una suerte de oráculo délfico del siglo XXI que al parecer hace pronunciamientos incontrovertibles y autorizados ajenos a la acción humana. La tarea de desentrañar los mecanismos de procesamiento algorítmico y, de ese modo evaluar los riesgos que plantean, es compleja y exige examinar múltiples cuestiones. Estas complicaciones obstaculizan nuestra capacidad para entender cómo funcionan los algoritmos y la manera en que afectan a nuestras vidas.

56. Hay cada vez más estudios que ponen de relieve los problemas que pueden causar y que aconsejan actuar con cautela antes de precipitarnos hacia un futuro algorítmico sin reflexionar sobre las salvaguardias que necesitamos para gestionar los riesgos.

---

[31] Felicitas Kraemer, Kees van Overveld y Martin Peterson, “Is there an ethics of algorithms?” Ethics and Information Technology, vol. 13, núm. 3 (septiembre de 2011).

[32] Véase http://mathworld.wolfram.com/Algorithm.html.

[33] Brent Mittelstadt y otros, The ethics of algorithms: mapping the debate, Big Data and Society, vol. 3 núm. 2 (Julio-diciembre de 2016).

[34] Véase, por ejemplo, Rebecca Harrington, “Dating services tinker with the algorithms of love”, Scientific American, 13 de febrero de 2015, en https://www.scientificamerican.com/article/dating-services-tinker-with-the-algorithms-of-love/.

[35] Véase https://motherboard.vice.com/en us/article/4x3pp 9 /the-simple-elegant-algorithm-that-makes-google-maps-possible.

[36] Véase Michael Byrne, “The simple, elegant algorithm that makes Google Maps possible”, 22 de marzo de 2015, en http://mitsloan.mit.edu/media/Lo_ConsumerCreditRiskModels.pdf.

[37] Brent Mittelstadt y otros, “The ethics of algorithms”.

1. Los algoritmos conllevan valores

57. Contrariamente a su estructura aritmética que les da una apariencia de objetividad, los algoritmos "inevitablemente conllevan valores". Los valores que encarnan suelen reflejar los supuestos culturales o de otra índole de los ingenieros informáticos que los diseñan y les implantan dentro de su estructura lógica a modo de opiniones tácitas[38].

58. Por ejemplo, un algoritmo de calificación crediticia podría estar diseñado para determinar el lugar de nacimiento de una persona, el lugar en que concurrió a la escuela y en que reside y su situación laboral. La elección de esos datos implica un juicio de valor dado que las respuestas a esas preguntas son pertinentes para determinar si se debe otorgar el crédito y, en tal caso, en qué condiciones. En cualquier caso, el solicitante de crédito muy a menudo no tiene forma de conocer el motivo de una decisión crediticia y no puede determinar los juicios de valor que se han aplicado.

59. Aunque estos datos indirectos podrían ser pertinentes para las evaluaciones crediticias en algunas sociedades, en el mejor de los casos serán distracciones inútiles, y en el peor de los casos resultarán perjudiciales. Por ejemplo, su utilización en algunos países en desarrollo, donde buena parte de la población tal vez carece de domicilio fijo, tiene escasa educación formal y trabaja por cuenta propia, serviría para denegar a perpetuidad el acceso al crédito.

60. Por otra parte, los algoritmos que analizan las formas no tradicionales de datos podrían demostrar que una persona que carece de antecedentes crediticios convencionales podría ser no obstante un buen riesgo, con lo cual se facilitaría el desarrollo humano[39].

2. El problema de los datos imperfectos

61. La materia prima que alimenta los algoritmos son los datos, pero no todos los datos son precisos, suficientemente amplios, actuales ni fiables[40]. La procedencia de algunos datos, por ejemplo, los registros tributarios por lo general pueden obtenerse fácilmente, pero su exactitud puede variar de un organismo tributario a otro dentro de un mismo Estado y entre Estados. Otras fuentes de datos pueden haber sido extraídas de bases de datos anticuadas que nunca fueron depuradas debidamente o de fuentes no seguras o en las que no se han registrado los datos como es debido ni se han respetado las normas correspondientes.

62. La función de los algoritmos es procesar datos, y "por lo tanto están sujetos a una limitación compartida por todos los tipos de procesamiento de datos, a saber, que el producto nunca puede superar la información aportada"[41]. Se aplica el principio de que "si entra basura, saldrá basura".

3. La elección de los datos

63. Este riesgo respecto a la elección de datos es análogo al que se señala en el párrafo 62. Así como los datos deficientes producen resultados deficientes, la

[38] *Ibid.*

[39] Comisión Federal de Comercio de los Estados Unidos, "Big data: a tool for inclusion or exclusión, understanding the issues" (2016), en www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf.

[40] Por ejemplo, los intereses de grupos minoritarios que no están bien representados en un determinado conjunto de datos pueden ser afectados por las decisiones y predicciones adoptadas sobre la base de esa información.

[41] Mittelstadt y otros, "The ethics of algorithms".

selección de datos inadecuados o irrelevantes también produce resultados que pueden ser poco fiables y engañosos.

64. Gran parte del procesamiento algorítmico entraña un razonamiento inductivo y la determinación de correlaciones entre elementos de datos aparentemente dispares. Si se utilizan datos erróneos, las recomendaciones o decisiones no tendrán valor.

4. El sesgo, la discriminación y la incorporación de desventajas

65. Aunque algunos expertos establecen distinciones entre el sesgo y la discriminación, los riesgos que plantean en el contexto de los macrodatos son lo suficientemente similares como para justificar un examen conjunto[42].

66. Los algoritmos pueden utilizarse para la elaboración de perfiles, es decir, para "identificar correlaciones y hacer predicciones sobre el comportamiento a nivel grupal, aún con grupos (o perfiles) que están en constante evolución y son redefinidos por el algoritmo" utilizando el aprendizaje automático:

> "Ya sea dinámica o estática, la persona es interpretada en función de las conexiones con otras personas identificadas por el algoritmo, en lugar de su verdadero comportamiento. Las opciones que eligen las personas se estructuran según la información sobre el grupo. La utilización de perfiles puede crear sin quererlo una base empírica que conduce a la discriminación"[43].

67. Algunos comentaristas han argumentado que las técnicas de análisis avanzadas, como la elaboración de perfiles, intensifican las desventajas. Un ejemplo de ello es la policía de predicción, que se basa en la utilización de estadísticas sobre delincuencia y análisis algorítmicos para predecir los focos críticos de delincuencia y convertirlos en prioridades de los organismos de represión[44]. Dado que esos focos son más vigilados por la policía y a menudo se encuentran en zonas socialmente desfavorecidas, y no en los lugares en que hay delincuencia de cuello blanco, la mayor vigilancia tiende a concentrar las detenciones y condenas en determinados lugares. Esto conduce a un ciclo vicioso en que se repite e intensifica la identificación de los mismos focos críticos, con lo cual se expone a la gente desfavorecida a un mayor riesgo de detención y castigo con arreglo al derecho penal.

68. La posible utilización de esos instrumentos por los gobiernos para controlar, atacar o infligir algún otro daño a determinadas comunidades también ha suscitado preocupación[45].

5. Responsabilidad y rendición de cuentas

69. Los daños causados por el procesamiento algorítmico son mayormente atribuibles a las dificultades relacionadas con el procesamiento de grandes volúmenes de conjuntos de datos dispares y la formulación y aplicación de los algoritmos utilizados para el procesamiento. Dado que hay muchísimas variables, es difícil determinar quién es el responsable de los daños causados. A menudo, el análisis de macrodatos se basa en el descubrimiento y la exploración, a diferencia del ensayo de una hipótesis, por lo que es difícil predecir (y, en el caso de las personas, articular) al comienzo cuál será el objetivo último de la utilización de los datos.

---

[42] Se considera que el sesgo es la expresión coherente o reiterada de una determinada preferencia, valor o creencia a la hora de adoptar decisiones. La discriminación es la consecuencia negativa y desproporcionada que puede derivarse de la adopción de decisiones algorítmicas.

[43] Brent Mittelstadt y otros, "The ethics of algorithms".

[44] Véase, por ejemplo, www.predpol.com/how-predictive-policing-works.

[45] Lee Rainie y Janna Anderson, "Code-dependent: pros and cons of the algorithm age", Pew Research Center, 8 de febrero de 2017. En www.pewinternet.org/2017/02/08/code-dependent-pros-and-cons-of-the-algorithm-age/ .

70. La opacidad de los algoritmos no es necesariamente un hecho inamovible; técnicamente es posible conservar los datos empleados y el resultado de la aplicación del algoritmo en todas las etapas de su procesamiento.

6. Desafíos a la privacidad

71. La Organización de Cooperación y Desarrollo Económicos (OCDE) publicó sus Orientaciones sobre la Protección de la Vida Privada y las Corrientes Transfronterizas de Datos Personales en 1980[46]. Los ocho principios enunciados en las Orientaciones de la OCDE, junto con principios similares formulados en el Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (Convenio para la protección de datos), adoptado por el Consejo de Europa en 1981, y en los Principios Rectores sobre la Utilización de Ficheros Informatizados de Datos Personales de 1990, aprobados por la Asamblea General en su resolución 45/95 de 14 de diciembre de 1990, han servido para promulgar leyes sobre la privacidad de la información en todo el mundo.

72. El principio rector enunciado en las Orientaciones de la OCDE y el Convenio para la protección de datos, el principio de "limitación de la recogida de datos", es que solo puede recogerse información personal en forma lícita y equitativa y, cuando proceda, con el conocimiento y el consentimiento de la persona interesada[47]. El "principio de especificación de la finalidad" exige que la finalidad de la recopilación de datos personales sea especificado en el momento en que se recogen y que la utilización ulterior de la información debería limitarse a los fines de la recopilación o a un propósito compatible y que estos deben ser especificados cada vez que haya un cambio de finalidad[48]. El "principio de limitación del uso" restringe la divulgación de información personal para fines incompatibles, salvo con el consentimiento de la persona o mediante autorización legal[49]. El "principio de calidad de los datos" se ve contrariado por la recopilación de enormes cantidades de datos y el requisito de que solo se procese información personal apropiada y pertinente y no una cantidad excesiva. Los Principios Rectores de las Naciones Unidas aprobados en 1990 establecen el principio de la proporcionalidad en la recopilación de datos con miras al procesamiento de la información.

73. Los macrodatos plantean dificultades respecto de esos principios pues surgen cuestiones éticas y dilemas sociales derivados del uso desaprensivo de los algoritmos. En lugar de resolver problemas de política pública, existe el riesgo de provocar consecuencias imprevistas que socavan los derechos humanos, como la protección contra todas las formas de discriminación, incluida la discriminación contra las mujeres, las personas con discapacidad y otras personas.

74. Al mismo tiempo, hay indicios de un cambio de criterio para el diseño de los algoritmos que llevaría a la adopción de soluciones algorítmicas mejores en relación con los macrodatos, que se observa por ejemplo en la iniciativa de la Standards Association del Instituto de Ingenieros Electricistas y Electrónicos acerca del diseño conforme a normas éticas[50].

---

[46] Organización de Cooperación y Desarrollo Económicos (OCDE), Orientaciones sobre la Protección de la Vida Privada y las Corrientes Transfronterizas de Datos Personales. En www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

[47] Véase OCDE, Orientaciones sobre la Protección de la Vida Privada, en http://oecdprivacy.org/.

[48] *Ibid.*

[49] *Ibid.*

[50] Institute of Electrical and Electronics Engineers (Instituto de Ingenieros Electricistas y Electrónicos (IEEE)), IEEE Global Initiative for Ethical Considerations in Artificial Intelligence and Autonomous Systems, *Ethically Aligned Design: A Vision for Prioritizing Wellbeing with*

75. En cuanto a la privacidad, los instrumentos internacionales pertinentes amplían el significado del derecho a la privacidad a fin de rebasar el alcance de los derechos a la privacidad de la información enunciados en las Orientaciones de la OCDE y el Convenio sobre la protección de los datos. Habida cuenta del reconocimiento de la privacidad como un derecho habilitante que tiene importancia para el disfrute de otros derechos humanos, y siendo que es un derecho estrechamente vinculado con los conceptos de dignidad humana y desarrollo libre e irrestricto de la personalidad (véase la resolución 34/7 del Consejo de Derechos Humanos), los escollos que plantean los macrodatos para la privacidad se extienden a otros diversos derechos humanos. La tendencia de los macrodatos a inmiscuirse en la vida de la gente mediante la divulgación pormenorizada de sus actividades informáticas entre quienes recogen y analizan sus huellas virtuales es totalmente incompatible con el derecho a la privacidad y los principios dirigidos a proteger ese derecho.

76. Las repercusiones reglamentarias son tan profundas como los cambios que se observan en las prácticas industriales y gubernamentales.

F. Datos abiertos

77. El concepto de datos abiertos se ha popularizado en forma paralela al desarrollo de análisis avanzados. Tiene por objeto alentar a los sectores privado y público a que divulguen datos para fomentar la transparencia y la apertura, en particular en el gobierno.

78. Los datos abiertos son definidos como:

> "… datos que pueden ser utilizados, reutilizados y redistribuidos libremente por cualquiera, con la única limitación de que deben ser atribuidos y compartidos por igual"[51].

79. Los datos abiertos pueden abarcar cualquier categoría de datos. La Open Knowledge Foundation los resume de la siguiente manera:

a) Cultura: datos sobre obras y artefactos culturales, por ejemplo títulos y autores, reunidos y conservados generalmente por galerías, bibliotecas, archivos y museos;

b) Ciencia: datos producidos como parte de investigaciones científicas, desde la astronomía a la zoología;

c) Finanzas: datos diversos, como cuentas del Gobierno (gastos e ingresos) e información sobre mercados financieros (títulos, acciones, bonos, etc.);

d) Estadísticas: datos producidos por las oficinas de estadística, como censos e indicadores socioeconómicos esenciales;

e) Tiempo: los numerosos tipos de información que se utilizan para comprender y predecir el tiempo y el clima;

f) Medio ambiente: información relacionada con el medio ambiente natural, como la presencia y el nivel de contaminantes, la calidad y los ríos y mares[52].

80. A fin de satisfacer los requisitos de la definición de datos abiertos, estos suelen ser publicados con arreglo a licencias de Creative Commons. La licencia CCBY4.0

Artificial Intelligence and Autonomous Systems, ver. 1 (IEEE Press, 2016). Disponible en http://standards.ieee.org/develop/indconn/ec/ead_v1.pdf.

[51] Véase http://opendatahandbook.org/guide/en/what-is-open-data/.

[52] Véase https://okfn.org/opendata/.

de Creative Commons permite la copia, redistribución y adaptación sin restricciones (incluso con fines comerciales) del material facilitado con la condición de que se declare la procedencia[53].

81. Los datos que posea un gobierno acerca de los ciudadanos no se encuadran en ninguna de estas categorías. Los datos abiertos y el Gobierno abierto tenían por objeto dar acceso a los datos relativos al propio gobierno y al mundo en que vivimos. No tenían por finalidad incluir los datos que los gobiernos reúnen acerca de los ciudadanos. Al reconocer este hecho, algunas jurisdicciones excluyen expresamente de los datos abiertos los datos "personales" y otras categorías de información, como la información comercial o la información relativa a un gabinete gubernamental[54]. No debemos perder de vista en medio de toda la terminología, como "intercambio" y "conexión", que se ha producido un retroceso pues en lugar de divulgar datos acerca de la manera en que funciona el gobierno, que el público puede utilizar para que este rinda cuentas de sus actos, los gobiernos están divulgando datos acerca de sus ciudadanos.

G. Gobierno abierto

82. Una de las primeras medidas del Gobierno de Obama fue emitir un decreto para alentar la divulgación de la información que posee el Gobierno para fomentar la confianza del público y promover la transparencia, la participación y la colaboración[55].

83. A raíz de ello se creó la Alianza para el Gobierno Abierto, la que publicó una Declaración sobre el Gobierno Abierto en septiembre de 2011[56]. La Declaración se centra en proporcionar a la gente más información sobre las actividades del Gobierno y hacen hincapié en la necesidad de una mayor participación ciudadana y una mayor transparencia por parte del Gobierno, en luchar contra la corrupción, empoderar a los ciudadanos y aprovechar el poder de las nuevas tecnologías para que el gobierno sea más eficaz y responsable.

84. La Declaración sobre el Gobierno Abierto compromete a sus miembros, con carácter voluntario y no vinculante. a que:

a) Aumenten la disponibilidad de información sobre las actividades del Gobierno;

b) Apoyen la participación cívica;

c) Apliquen las normas más rigurosas de integridad profesional en toda la administración;

d) Aumenten el acceso a las nuevas tecnologías en aras de la apertura y la rendición de cuentas[57],

85. Al primer decreto del gobierno de Obama siguió otro decreto, emitido el 9 de mayo de 2013 cuyo objeto era que toda la información del Gobierno de los Estados Unidos fuera pública y susceptible de lectura mecánica por defecto[58]. Con ello se

[53] Véase https://creativecommons.org/licenses/by/4.0/.

[54] Australia, Gobierno de Nueva Gales del Sur, Open Data Policy, Departamento de Finanzas y Servicios, 2013.

[55] Presidente Obama, "Transparency and Open Government", 21 de enero de 2009, memorando para los Jefes de Departamentos Ejecutivos y Organismos. Disponible en https://obamawhitehouse.archives.gov/the-press-office/transparency-and-open-government.

[56] Véase https://www.opengovpartnership.org/open-government-declaration

[57] https://www.opengovpartnership.org/open-government-declaration.

[58] Presidente Obama, decreto de 9 de mayo de 2013, "Making open and machine readable the new

modificó el propósito del decreto de 2009. El decreto expresaba que los datos gubernamentales abiertos “promueven la prestación de servicios eficientes y eficaces a la población y contribuyen al crecimiento económico. Como uno de los beneficios esenciales del gobierno abierto, la facilitación del acceso a recursos de información valiosos puede impulsar iniciativas empresariales, innovaciones y descubrimientos científicos que sirvan para mejorar las vidas de los estadounidenses y contribuyan de manera significativa a la creación de empleo”[59].

86. En años sucesivos, el concepto de datos abiertos ha seguido evolucionando y en 2017 abarca mucho más que la divulgación pública de datos no personales ni derivados de información personal y comprende también la divulgación de información personal no identificativa. Los partidarios de este enfoque afirman que las bases de datos gubernamentales u otros depósitos de información encierran elementos muy valiosos y que poner esa información a disposición del público alentará la investigación y estimulará el crecimiento de la economía de la información.

87. Así pues, los datos abiertos que se derivan de información personal dependen por completo de la eficacia de los procesos de “despersonalización” para impedir una nueva identificación y, en consecuencia, su vinculación a la persona de que se obtuvieron. Los debates acerca de si la eliminación de elementos identificativos ofrece o no protección de la privacidad y al mismo tiempo datos útiles para la investigación han sido sumamente polémicos.

H. La complejidad de los macrodatos

88. En 2015, el periodista australiano Will Ockenden publicó en línea sus metadatos de telecomunicaciones y preguntó a la gente qué podían inferir sobre su vida. Los metadatos incluían la hora exacta de todas las llamadas telefónicas y los mensajes de texto, junto con la indicación de la torre de telefonía más cercana. Aunque sustituyó los números de teléfono por seudónimos, fue posible contestar fácil y correctamente a diversas preguntas, como “¿Dónde vive mi madre?” únicamente sobre la base de las pautas de comunicación y lugar. No fue complicado, la gente adivinó (con acierto) que su madre vivía en el lugar que visitó el día de Navidad.

89. Este es un tema fundamental de las investigaciones sobre la privacidad: que las pautas que se observan en los datos, sin los nombres, números de teléfono ni otros identificadores evidentes, pueden utilizarse para identificar a una persona y, por consiguiente, obtener más información acerca de ella a partir de los datos. Esto adquiere una importancia particular cuando esas pautas pueden utilizarse para relacionar muchos conjuntos de datos distintos a fin de construir un retrato complejo de una persona.

90. Inevitablemente algunos datos deben ser revelados. Las compañías telefónicas conocen los números que marca cada cliente y los médicos conocen los resultados de los análisis de sus pacientes. Por consiguiente, se plantean controversias sobre la divulgación de esos datos a otras entidades, como empresas o investigadores, y sobre las formas en que los gobiernos pueden utilizar la información e interferir en el ejercicio de los derechos humanos de sus ciudadanos.

default for Government information”. En https://obamawhitehouse.archives.gov/the-press-office/ 2013/05/09 /executive-order-making-open-and-machine-readable-new-default-government-.

[59] *Ibid.*

91. Otros datos son recogidos en forma deliberada, a menudo sin el conocimiento ni el consentimiento de la persona. Los investigadores de la Fundación de la Frontera Electrónica publicaron los resultados del "Panopticlick", un experimento que demostró que era posible identificar con certeza el navegador de una persona en función de características simples, como los "plugins" y la tipografía[60]. Advirtieron que corría peligro la privacidad al navegar por Internet si no se ponía límites al almacenamiento de huellas de navegación y sus vínculos con el historial del navegador. No se hicieron cambios sustantivos en las políticas. Hoy, en 2017, la privacidad de la navegación por Internet ha desaparecido. Muchas empresas, en forma habitual y deliberada, rastrean a la gente, por lo general con fines comerciales. El rastreo en la Web es casi generalizado y solo es posible eludirlo con gran esfuerzo.

92. Gran parte de la economía de la Internet actual depende de la captación de datos complejos sobre posibles clientes con el fin de venderles cosas, una práctica conocida como el "capitalismo de la vigilancia"[61]. Sin embargo, la vigilancia no parece más justificable para la eficiencia impulsada por datos que el trabajo infantil para una economía industrial. Es solo el medio más conveniente y fácil de explotar la información. No es ni de lejos un derecho fundamental, como es el derecho a la privacidad. De hecho, la economía impulsada por datos podría sobrevivir y prosperar si hubiera normas mínimas y mejores tecnologías que hicieran que las empresas y los gobiernos tuvieran que desenvolverse en un mundo en que la gente común tenga mucho más control sobre sus propios datos[62].

93. Los gobiernos también podrían innovar con mayor legitimidad. El grado de confianza de la comunidad en el gobierno determina en gran medida su opinión acerca de los posibles efectos de las iniciativas sobre datos abiertos y gobierno abierto. Quienes confían en el gobierno son los que más probablemente pensarán que los datos abiertos aportan beneficios[63]. Las investigaciones demuestran que en su mayoría la gente aprueba que su gobierno proporcione datos en línea sobre sus comunidades, aunque manifiestan cierta alarma cuando los datos se refieren a ellas. La confianza de los ciudadanos difiere según el ámbito de recolección de datos de que se trate[64].

94. La mayoría de las leyes sobre privacidad de la información regulan la recopilación y el procesamiento de datos personales; no hay leyes que regulen el procesamiento de datos que no sean personales. Muchas de esas leyes reconocen que los datos personales pueden ser despersonalizados para que puedan ser utilizados o procesados para otros fines, como las investigaciones de interés público, de una manera que no vulnere los derechos a la privacidad de la información de las personas. Los gobiernos y otras entidades han tratado de mantener la confianza de las personas sobre las que reúnen datos dándoles garantías de despersonalización.

---

[60] Peter Eckersley, "How unique is your web browser?" en *Privacy Enhancing Technologies*, Mikhail Atallah y Nicholas Hopper, eds. (Berlin, Springer-Verlag, 2010).

[61] Shoshana Zuboff, "Big other: surveillance capitalism and the prospects of an information civilization", *Journal of Information Technology*, vol. 30, núm. 1 (marzo de 2015).

[62] No es necesario obligar a las empresas y los gobiernos a que ofrezcan medidas de protección de la privacidad. Para ejemplos de enfoques éticos adoptados por empresas véase Information Commissioner's Office, "Big data, artificial intelligence, machine learning and data protection", ver. 2.2 (2017). En https://ico.org.uk/media/for-organisations/documents/ 2013559 /big-data-ai-ml-and-data-protection.pdf

[63] John Horrigan y Lee Rainie, "Americans' views on open Government data", Pew Research Center, 21 de abril de 2015.

[64] *Ibid.*

95. Esto lleva a considerar un aspecto importante: ¿los procesos de despersonalización proporcionan datos que no vulneran los derechos a la privacidad de la información de las personas?

96. Los tipos de datos sencillos, como las estadísticas globales, son susceptibles de un tratamiento que preserve verdaderamente la privacidad, como el trato diferencial de la privacidad. Los algoritmos diferenciales de la privacidad dan mejores resultados a grandes escalas y se están incorporando en el análisis de datos comerciales. Los algoritmos aleatorios que logran una privacidad diferencial son un instrumento valioso para la protección de la privacidad, pero no permiten despersonalizar en forma generalizada conjuntos de datos muy complejos que contienen información personal de carácter individual[65]. Un ejemplo de la manera en que se utiliza la privacidad diferencial a gran escala lo dio la empresa Apple en 2016[66].

97. Los datos de nivel unitario de dimensiones altas no pueden ser despersonalizados en forma segura sin reducir sustancialmente su utilidad. Este es el tipo de datos producidos por un rastro longitudinal de los datos de una persona referidos, entre otras cosas, a cuestiones de salud, movilidad y búsquedas en la Web. El justificante I[67] contiene un resumen de los instrumentos y controversias sobre despersonalización.

Datos gubernamentales abiertos

98. Hay numerosos ejemplos de éxito en volver a identificar a personas en los datos publicados por los gobiernos[68]. Esta “re-identificación pública” es pública en dos sentidos: los resultados se hacen públicos y para la re-identificación solo se utiliza información pública auxiliar.

99. Cuanto más información auxiliar haya, tanto más fácil será volver a identificar a más personas. A medida que se vincula un mayor número de conjuntos de datos, se reduce la información auxiliar necesaria para volver a identificar a las personas. La divulgación pública y la vinculación de conjuntos de datos permite recoger una cantidad enorme de información sobre personas en el mismo lugar, lo que facilita mucho la reidentificación de los datos relacionados con ellas.

100. La posibilidad de volver a identificar datos abiertos es un pequeño indicio de un problema mucho mayor; la reidentificación de conjuntos de datos comerciales “despersonalizados” que en forma habitual se venden, intercambian y comercializan.

---

[65] Fue en el caso de una sola persona.

[66] Andy Greenberg, “Apple’s ‘differential privacy’ is about collecting your data — but not your data”, 13 de junio de 2016. En https://www.wired.com/2016/06/apples-differential-privacy-collecting-data/https://techcrunch.com/2016/06/14/differential-privacy/ https://arxiv.org/abs/1709.02753.

[67] Véase www.ohchr.org/Documents/Issues/Privacy/A-72-Slot-43103.docx.

[68] En su testimonio ante el Comité Asesor sobe Privacidad e Integridad del Departamento de Seguridad Interior, el 15 de junio de 2005, Sweeney declaró que en 1997 “pudo demostrar cómo se podía volver a personalizar la historia clínica de William Weld, a la sazón Gobernador de Massachusetts, utilizando solamente su fecha de nacimiento, género y código postal. De hecho, el 87% de la población de los Estados Unidos está identificada en forma precisa por la fecha de nacimiento, por ejemplo, mes, día y año, género y sus códigos postales de 5 dígitos. La cuestión es que los datos que pueden parecer anónimos no lo son necesariamente”. Véase www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_06-2005_testimony_sweeney.pdf; véase también Latanya Sweeney, “Matching known patients to health records in Washington state data”, Universidad de Harvard, 2012. En http://dataprivacylab.org/projects/wa/1089-1.pdf y http://dataprivacylab.org/index.html; Latanya Sweeney, “Achieving k-anonymity privacy protection using generalization and suppression”, *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, vol. 10, núm. 5 (2002).

101. Hay fuerzas poderosas que se oponen al derecho a la privacidad en la era de los macrodatos y los datos abiertos. Quienes trabajan con datos, ya sea con fines comerciales o de otra índole, probablemente preferirán desde el punto de vista financiero que la despersonalización se haga en la forma más tenue posible, y los gobiernos son objeto de presión no solo en lo que respecta a permitir el acceso a los datos de personas, sino también en cuanto a la regulación de este acceso.

102. Las organizaciones no gubernamentales han expresado su preocupación por el aumento de los macrodatos sin que se tengan debidamente en cuenta la participación de las personas, las cuestiones éticas y jurídicas derivadas de la gestión inapropiada de la información personal de la gente ni la adopción de una reglamentación adecuada[69]. Esas organizaciones seguirán bregando por la debida protección y por la adopción de medidas apropiadas.

I. Considerando el presente: los metadatos comerciales y la privacidad

103. El aumento exponencial de la recopilación de datos y el apresuramiento por conectar aparentemente todo objeto a la Internet, sin considerar lo suficiente la seguridad de los datos, ha creado riesgos para las personas y los grupos. Con objeto de dar seguridades a los consumidores y a la gente respecto de la seguridad de la información que los identifica, se han hecho públicas algunas ideas. Por ejemplo, una industria que se beneficia de la sensación equivocada de anonimato que perciben los usuarios, promueve la idea de que hay datos "anonimizados" de gran complejidad[70].

104. Se recoge una gran cantidad de datos sobre el común de los usuarios sin su conocimiento ni consentimiento. Estos datos pueden ser vendidos y vinculados con datos de otras fuentes para producir un registro complejo de muchos aspectos de la vida de una persona. Esta información sirve para muchos fines, incluido el control político, como lo ha demostrado un conjunto de datos divulgado involuntariamente por una organización política de los Estados Unidos[71]. Ese conjunto de datos incluía detalles personales acerca de casi 200 millones de votantes de los Estados Unidos, junto con detalles sorprendentes recogidos (o adivinados) en relación con sus convicciones políticas. En China, hay un proyecto de "crédito social" dirigido a calificar no solo la solvencia financiera de los ciudadanos, sino también a hacer un seguimiento de su comportamiento social y posiblemente, político. Se basa en datos de diversas fuentes, principalmente fuentes en línea, registrados en el transcurso del tiempo[72].

105. Los intermediarios de datos —empresas que recogen información personal de los consumidores y la revenden o la comparten con otros— son partícipes importantes en la economía de los macrodatos. Al elaborar sus productos, los intermediarios de datos adquieren una gran variedad de información detallada y concreta sobre consumidores procedente de diversas fuentes, la analizan para hacer

[69] Véase www.privacyinternational.org/node/8.

[70] Aunque estén anonimizados, los principios y consideraciones de privacidad, como el de "consentimiento", no dejan de tener importancia.

[71] Sam Biddle, "Republican data-mining firm exposed personal information for virtually every American voter", *The Intercept*, 19 de junio de 2017, en https://theintercept.com/ 2017/06/19 /republican-data-mining-firm-exposed-personal-information-for-virtually-every-american-voter/.

[72] "China invents the digital totalitarian state", *The Economist*, 17 de diciembre de 2016. En https://www.economist.com/news/briefing/21711902-worrying-implications-its-social-credit-project-china-invents-digital-totalitarian; Lucy Hornby, "China changes tack on 'social credit' scheme plan", *Financial Times*, 4 de julio de 2017. En www.ft.com/content/f772a9ce-60c4-11e7-91a7-502f7ee26895.

inferencias acerca de los consumidores, algunas de las cuales pueden ser delicadas[73]; y comparten la información con clientes de distintas industrias. Todas estas actividades se llevan a cabo a espaldas de los consumidores[74].

106. Si bien los productos de los intermediarios de datos ayudan a prevenir el fraude, sirven para mejorar la oferta de productos y prestar servicios personalizados, muchas de las finalidades para las cuales los intermediarios de datos recogen y utilizan los datos plantean riesgos para los consumidores. Preocupa la falta de transparencia, la recopilación de datos sobre los jóvenes, la conservación indefinida de datos y la utilización de esos datos para la determinación del derecho a recibir prestaciones o para fines de discriminación ilícita[75].

107. El reciente proyecto de informe del Parlamento Europeo sobre la regulación de la privacidad en Europa recomienda que "se ofrezca a los usuarios finales un conjunto de opciones de privacidad, desde la más estricta (por ejemplo, 'nunca aceptar cookies") hasta la menos estricta (por ejemplo, 'siempre aceptar cookies') y niveles intermedios ..."[76].

108. Se están celebrando amplias deliberaciones acerca de la necesidad de aumentar el control de las personas sobre su privacidad en la Internet. La gente utiliza sus propios dispositivos y sus datos para obtener la información que necesita, como mapas y direcciones, y para ver la publicidad que le interesa. Aunque las tecnologías que facilitan el control del usuario final son importantes, en este sentido es indispensable preguntar hasta qué punto la gente puede ejercer un control suficientemente amplio de la protección. La adopción de estas herramientas se contrapone a las fuerzas económicas que actualmente conforman la Internet[77]. ¿Los gobiernos desempeñan alguna función en la elaboración y adopción de estas herramientas?

Tecnologías de control de la recopilación de datos

109. El control (incluido el bloqueo) de la recopilación de datos tiene importancia para los datos que la gente no quiere compartir. Con una tecnología "antigua" no tenía importancia, ya que el usuario inevitablemente tenía control porque la tecnología no permitía otra cosa que no fuera la determinación del usuario: los dispositivos tenían tapas en las cámaras o había conexiones a la Internet solamente por Ethernet que podían anularse en forma manual. Ahora hay Wi-Fi en interiores y cámaras sin tapa. Los televisores tienen micrófonos que no se pueden apagar. Las

[73] Se han dado a conocer numerosos casos de adquisición de datos comerciales en gran escala de dispositivos inteligentes, como televisores, "aparatos íntimos", juguetes para niños, aplicaciones de transporte compartido y "automóviles conectados".

[74] Comité de Comercio, Ciencia y Transporte del Senado de los Estados Unidos, "A review of the data broker industry: collection, use, and sale of consumer data for marketing purposes", informe del personal, 18 de diciembre de 2013. En http://educationnewyork.com/files/rockefeller databroker.pdf.

[75] Comisión Federal de Comercio de los Estados Unidos, "Data brokers: a call for transparency and accountability", mayo de 2014. En www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may- 2014 /140527databrokerreport.pdf.

[76] Marju Lauristin, "Draft report on the proposal for a regulation of the European Parliament and of the European Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC", Comisión de Libertades Civiles, Justicia y Asuntos de Interior del Parlamento Europeo, 2017.

[77] Por ejemplo, AdNauseum obstaculiza el rastreo haciendo clic en forma automática en todos los anuncios presentados a un usuario a fin de ocultar los que el usuario lee en verdad. Google Chrome ha bloqueado esa función. Otros sitios detectan y bloquean a las personas que tienen instalados bloqueadores de avisos. Véase Daniel Howe y Helen Nissenbaum, "Engineering privacy and protest: a case study of AdNauseam". En https://adnauseam.io/.

funciones de desactivación manual han desaparecido, aunque existen tecnologías para obstruir la recopilación de datos[78]. El gran éxito de la campaña denominada "TLS Everywhere" (Seguridad de la capa de transporte) significa que la mayor parte del tráfico de Internet está ahora codificado y hay muchas menos probabilidades de interceptación en tránsito por una entidad desconocida para el usuario. Esas tecnologías tienen beneficios que deben ser estudiados más a fondo y promovidos.

110. La idea de encubrir nuestra identidad y lo que hacemos tampoco es nueva, basta pensar en los conflictos en torno a las políticas de "nombres verdaderos" de algunas redes sociales, a las que se oponen quienes defienden su derecho a registrarse con pseudónimo. El encubrimiento exige herramientas que permitan que los usuarios puedan presentar un perfil "reservado" y separarlo de otros perfiles que deseen presentar.

111. Las investigaciones indican sistemáticamente que si a la gente le preocupan las prácticas relativas a la información personal de las organizaciones con que tratan, hay más probabilidades de que proporcionen información inexacta o incompleta[79]. Dado que la privacidad y la protección de los datos generan confianza, tienen un efecto positivo sobre la calidad de los datos y también sobre su análisis. La confianza de los usuarios en su privacidad es también importante para la estabilidad y la precisión de los algoritmos de aprendizaje automático. El aprendizaje automático ordinario puede ser sumamente susceptible a los aporte de datos que en forma deliberada tratan de provocar la confusión[80]. ¿Qué ocurriría si un gran número de personas adoptaran deliberadamente instrumentos dirigidos a encubrirse por motivos de privacidad?

112. Un enfoque simplista de los macrodatos, datos abiertos que no capten la interacción compleja entre las prácticas institucionales aparentes de gestión de la privacidad, la confianza en el respeto de la privacidad y los comportamientos de las personas, no facilitará "macrodatos" sino que dará lugar a la adopción de decisiones potencialmente inexactas y de mala calidad.

J. Principios para el futuro: controlar la divulgación de datos

113. Las leyes sobre privacidad suelen estar basadas en principios lo suficientemente flexibles como para poder abordar los riesgos en la materia a medida que se plantean. Es útil considerar si se necesitan otros principios que complementen los principios de confidencialidad vigentes a fin de proteger los datos personales contra las injerencias tecnológicas.

114. Se han propuesto los siete principios siguientes para el intercambio de datos[81]:

1. Trasladar el algoritmo a los datos: compartir los resultados y no los datos en forma directa.

[78] El direccionador Tor (red anónima) oculta a quienes se comunican entre sí (es decir, los metadatos de las telecomunicaciones), pero no es muy utilizado. Algunos navegadores (como Firefox y Brave) incluyen una función de "navegación privada" que impide la recopilación de datos. El "Privacy Badger" de la Fundación de la Frontera Electrónica y el "TrackMeNot" de la Universidad de Nueva York son muy eficaces pero no se los utiliza con frecuencia.

[79] Oficina del Comisionado de Información de Australia, Australian community attitudes to privacy survey, 2017 y 2013; Deloitte, "Trust starts from within: Deloitte Australian privacy index 2017", 2017.

[80] Ian Goodfellow, Jonathon Shlens y Christian Szegedy, "Explaining and harnessing adversarial examples", prepublicación de ArXiv, 2014.

[81] Alex Pentland y otros, "Towards an Internet of trusted data: a new framework for identity and data sharing", 2016.

2. Algoritmos abiertas: examen abierto y escrutinio público de todos los algoritmos para el intercambio de datos y la protección de la privacidad, a fin de poder detectar y corregir los errores o las deficiencias.

3. Uso permisible: respeto del permiso (explícito o implícito) para la utilización de los datos o "integridad contextual"[82]. En un contexto médico, se ha puesto en práctica la concesión explícita o el retiro del consentimiento en la interfaz de consentimiento dinámico[83].

4. Dar siempre "respuestas seguras": privacidad diferencial en la práctica.

5. Datos siempre cifrados: los datos cifrados solo pueden ser leídos por quienes conocen la clave para descifrarlos[84].

6. Entornos de colaboración en red y cadenas de bloques para auditoría y rendición de cuentas.

7. Incentivos económicos y sociales.

115. Estos principios no son necesariamente soluciones completas en sí mismas, ya que a su vez plantean más cuestiones. Por ejemplo, la transparencia resulta particularmente difícil cuando las técnicas utilizadas para proteger la intimidad son tan complejas que solo unas pocas personas pueden comprenderlas. El principio de "algoritmos abiertos" es un primer paso fundamental, pero los propios algoritmos que se utilicen y sus repercusiones seguirán planteando dificultades en la práctica.

116. Se han propuesto otros enfoques de "principio", como los de "agente" y "transparencia"; el primero incluye el derecho de modificar los datos, desfigurarlos o experimentar con los retoques[85]. La dinámica en que se basa todo eso es el empoderamiento de las personas y la introducción de una nivelación del poder entre las empresas/titulares de los datos y los usuarios. Otros plantean los principios de la oportunidad de encubrir, prevenir o renunciar a la recopilación de datos.

117. En general, los principios de la transparencia y el control de los usuarios son importantes para que estos puedan elegir los datos que divulgan sin incurrir en una pérdida excesiva de comodidad o servicios.

118. Sobre todo, los intentos de producir macrodatos, principios de datos abiertos que respetan la intimidad, ofrecen un punto de partida útil para el debate.

---

[82] La privacidad se define como "el requisito de que la información sobre las personas ("información personal") circule en forma apropiada, entendiéndose por ello la conformidad con las normas de información ... Los contextos sociales constituyen el telón de fondo de este enfoque de la privacidad …". Véase Solon Barocas y Helen Nissenbaum, "Big data's end run around anonymity and consent", en *Privacy, Big Data, and the Public Good: Frameworks for Engagement*, Julia Lane y otros, eds. (Cambridge University Press, 2014).

[83] Jane Kaye y otros, "Dynamic consent: a patient interface for twenty-first century research networks", *European Journal of Human Genetics*, vol. 23, Núm. 2 (2014).

[84] Los últimos avances de la criptografía permiten que muchas partes computen conjuntamente una función de sus aportaciones privadas y que posteriormente divulguen únicamente los resultados bien definidos. Existen instrumentos muy generales basados en la computación por partes múltiples (véase, por ejemplo, Ivan Damgård y otros, Multiparty computation from somewhat homomorphic encryption", *Advances in Cryptology* – CRYPTO, vol. 7417 (2012); y cifrado homomórfico, en www.microsoft.com/en-us/research/project/homomorphic-encryption/ #). La mayoría de las herramientas no son lo suficientemente rápidas para conjuntos de datos voluminosos, pero es posible que aparezcan variantes más simples en el futuro. Hay numerosos protocolos específicos que resuelven los problemas particulares de grandes conjuntos de datos. La idea general de la computación de datos cifrados funciona muy bien para hacer cálculos sencillos en un solo conjunto de datos, pero puede no ser viable para cálculos complejos o conjuntos de datos distribuidos en varios lugares.

[85] Andreas Weigend, *Data for the People: How to Make our Post-Privacy Economy Work for You* (Nueva York, Basic Books, 2017).

Independientemente de los principios que se adopten, se debe consultar como es debido a todas las partes interesadas, incluidas las organizaciones de la sociedad civil, a fin de asegurar la idoneidad de esos principios.

119. La aplicación de estos principios plantea cuestiones relativas a la función del gobierno y el tipo de incentivos y reglamentación que facilitarán la protección de la privacidad y otros derechos humanos y la evaluación de sus "efectos comparativos en los valores éticos y políticos, como la equidad, la justicia, la libertad, la autonomía, el bienestar y otros más específicos para el contexto en cuestión"[86].

120. Una economía de la información innovadora probablemente tendría un mayor apoyo de la comunidad si se observara la adhesión de los gobiernos y las empresas a una regulación firme de la adquisición, distribución y control de los datos de las personas.

III. Justificantes

121. Los documentos siguientes que fundamentan el presente informe pueden consultarse en el sitio web del Relator Especial[87]:

I. Understanding history: de-identification tools and controversies;

II. Engagements by the Special Rapporteur in Africa, America, Asia and Europe;

III. Background on the open letter to the Government of Japan;

IV. Activities of the Task Force Privacy and Personality;

V. Description of the process for the draft legal instrument on surveillance;

VI. Acknowledging assistance;

VII. Procedural clarifications on the thematic report on big data and open data.

IV. Conclusión

122. **Las cuestiones señaladas en el presente informe no se limitan a unos pocos países. La disponibilidad de enormes nuevas colecciones de datos permite que los particulares, las empresas y los Estados de todo el mundo adopten decisiones con más y mejores fundamentos, pero la mala gestión de la privacidad pone en riesgo su valor potencial.**

123. **Es preciso comprender bien y mitigar con éxito los riesgos para la privacidad, para otros derechos humanos conexos y para los valores éticos y políticos de la autonomía y la imparcialidad.**

124. **Los datos son y seguirán siendo un activo económico fundamental, como el capital y la mano de obra. La privacidad y la innovación pueden y deben ir juntas. Será difícil comprender la manera de utilizar con eficacia los macrodatos y de compartir sus beneficios con equidad sin socavar la protección de los derechos humanos, pero en última instancia valdrá la pena.**

[86] Solon Barocas y Helen Nissenbaum, "Big data's end run around anonymity and consent", en *Privacy, Big Data, and the Public Good: Frameworks for Engagement*, Julia Lane y otros, eds. (Cambridge University Press, 2014).

[87] Véase www.ohchr.org/EN/Issues/HRAndClimateChange/Pages/HRClimateChangeIndex.aspx; véase también www.ohchr.org/Documents/Issues/Privacy/A-72-Slot-43103.docx.

V. Recomendaciones

125. **En espera de las observaciones que se formulen durante el período de consulta, que se extiende hasta marzo de 2018, y de los resultados de las investigaciones en curso y las cartas de denuncia a los Gobiernos, el Relator Especial está examinando las siguientes recomendaciones que se incluirán en una versión actualizada del presente informe, que se publicará en 2018 o después.**

126. **Las políticas sobre datos abiertos exigen que se estipulen claramente los límites del uso de la información personal, de acuerdo con normas y principios internacionales, incluida una categoría de datos personales exentos con el requisito vinculante de que se asegure la fiabilidad de los procesos de despersonalización a fin de que esa información pueda ser divulgada como datos abiertos, y mecanismos de aplicación rigurosos.**

127. **Toda iniciativa de gobierno abierto relativa a información personal, sea que esta esté despersonalizada o no, exige un análisis riguroso, público y científico de las protecciones para la privacidad de los datos, incluida una evaluación de los efectos sobre la privacidad.**

128. **Los datos de nivel unitario, sensibles y de dimensiones altas acerca de personas no deben ser publicados en línea ni intercambiados a menos que haya pruebas irrefutables de que se ha efectuado una despersonalización segura y que resistirá futuros intentos dirigidos a personalizarlos.**

129. **Deben establecerse marcos de gestión del riesgo de que se faciliten datos sensibles a los investigadores.**

130. **Los gobiernos y las empresas deberían apoyar activamente la creación y el uso de tecnologías de refuerzo de la privacidad.**

131. **Se han de considerar las opciones siguientes a la hora de manejar macrodatos:**

Gobernanza

a) Responsabilidad: determinación de competencias, proceso de adopción de decisiones y, cuando proceda, determinación de los encargados de adoptar decisiones;

b) Transparencia: qué ocurre, cuándo y de qué manera, con los datos personales antes de ser divulgados al público, y su utilización, incluidos los “algoritmos abiertos”;

c) Calidad: garantías mínimas de la calidad de los datos y su procesamiento;

d) Previsibilidad: cuando se trata del aprendizaje automático los resultados deberían ser previsibles;

e) Seguridad: medidas apropiadas para impedir que haya injerencias indebidas en los datos ingresados y los algoritmos;

f) Desarrollo de nuevas herramientas para determinar los riesgos y especificar medidas de mitigación de los riesgos;

g) Apoyo: capacitar (y, cuando proceda, acreditar) a los empleados acerca de los requisitos jurídicos, políticos y administrativos relacionados con la información personal;

Entorno regulador

h) Velar por que existan disposiciones dirigidas a determinar objetivos, responsabilidades y facultades inequívocas para los reguladores encargados de proteger los datos de los ciudadanos;

i) Las facultades de regulación deberían ser proporcionales a los nuevos desafíos que plantean los macrodatos, por ejemplo, la capacidad de los reguladores para poder examinar el proceso analítico y sus resultados;

j) Examen de las leyes de privacidad para velar por su idoneidad en relación con los desafíos derivados de los avances tecnológicos, como la información personal generada en forma automática y los análisis de datos, como la despersonalización;

Inclusión de mecanismos de recepción de comentarios

k) Formalizar mecanismos de consulta, entre ellos, comités de ética, con organismos profesionales, comunitarios y de otra índole, así como con los ciudadanos, para evitar el menoscabo de los derechos y determinar prácticas racionales;

l) Realizar una consulta amplia sobre las recomendaciones y las cuestiones planteadas en el presente informe, por ejemplo el deseo de que se prohíba el suministro de conjuntos de datos gubernamentales;

Investigación

m) Investigación técnica: investigar técnicas relativamente nuevas, como la privacidad diferencial y el cifrado homomórfico, para determinar si ofrecen procesos y productos adecuados en materia de privacidad;

n) Examinar el grado de conocimiento que tienen los ciudadanos acerca de las actividades de los gobiernos y las empresas, la utilización de la información personal, inclusive para la investigación, y los mecanismos tecnológicos para reforzar el control individual de sus datos y aumentar su capacidad de utilizarlos para sus necesidades.