**El derecho a la privacidad en la era digital**

**Resolución aprobada 34/7, Consejo de Derechos Humanos**

**Abril de 2018**

## Introducción

La Red Internacional de Organizaciones de Libertades Civiles (INCLO) desea agradecer a la Oficina del Alto Comisionado para los Derechos Humanos por la oportunidad de aportar su visión acerca de los desafíos que la privacidad en la era digital plantea a los derechos humanos.

En esta presentación explicamos brevemente los problemas y retos relacionados con el cifrado y el anonimato (cuestión n° 3), con la dependencia de la tecnología basada en datos (cuestión n° 4), con los problemas de privacidad de las poblaciones vulnerables (cuestión n° 5) y con la vigilancia e interceptación de comunicaciones digitales (cuestión n° 6).

Al abordar estos desafíos recomendamos una vez más que el Comité de Derechos Humanos emita una nueva Observación general sobre el derecho a la privacidad en virtud del artículo 17 del Pacto Internacional de Derechos Civiles y Políticos (PIDCP). Como el derecho a la privacidad digital ha cobrado una enorme importancia desde que el Comité publicó la Observación general 16 en 1988, esta revisión se necesita con urgencia para ofrecer una guía sobre las obligaciones del Estado en virtud del Pacto Internacional de Derechos Civiles y Políticos.

## I. Cifrado y anonimato

El cifrado y la capacidad de permanecer anónimos en línea son fundamentales para nuestro derecho a la privacidad y a la libertad de expresión y de opinión. Estos derechos están consagrados en leyes

internacionales de derechos humanos[1] y se ha reconocido que merecen fuertes protecciones a través de protocolos de encriptación[2]. Algunos de los desafíos planteados por el cifrado y los derechos al anonimato son:

Acceso restringido a la encriptación para grupos vulnerables y la prensa

El acceso a y la disponibilidad de tecnologías cifradas afectan sobre todo a las poblaciones vulnerables. Esto es así sobre todo en las regiones donde el Estado de derecho es débil y los derechos humanos de grupos demográficos específicos y de poblaciones minoritarias se ven amenazados[3]. Las comunicaciones anónimas que posibilitan las tecnologías de encriptación ofrecen ventajas a las poblaciones discriminadas al brindarles foros seguros para congregarse, organizarse, movilizarse y construir comunidad[4]. Actualmente, esas protecciones tienden a ser atacadas en ciertos Estados que intentan bloquear el acceso o interceptar los protocolos de cifrado[5].

Un desafío adicional es la ausencia de cifrado y derechos al anonimato para la prensa y sus fuentes. A pesar de que se reconoce que la libertad de prensa es una piedra angular de las sociedades democráticas[6], los gobiernos y las agencias de inteligencia han intentado violar este derecho[7]. La falta de respeto por los derechos a la comunicación anónima ayuda a los gobiernos a justificar el acceso al contenido y a los datos de las comunicaciones de los periodistas con el fin de revelar sus fuentes[8].

Restricciones o amenazas a proveedores privados de servicios de cifrado

Las entidades privadas promueven cada vez más el anonimato en línea mediante la implementación de protocolos de cifrado y el desarrollo de aplicaciones de comunicación cifradas. Si bien esto crea una

[1] Véase Artículo 17 y Artículo 19 de la Asamblea General de la ONU, Pacto Internacional de Derechos Civiles y Políticos, 16 de diciembre de 1966, Naciones Unidas, Treaty Series, vol. 999.
[2] Véase Consejo de Derechos Humanos de la ONU, Informe del Relator Especial sobre la Promoción y Protección del Derecho a la Libertad de Opinión y de Expresión: Informe al Consejo de Derechos Humanos, David Kaye A/HRC/29/32 (22 de mayo de 2016), quien en la página 1 escribió que "el cifrado y el anonimato permiten a los individuos ejercer sus derechos a la libertad de opinión y de expresión en la era digital y, por lo tanto, merecen una protección sólida".
[3] Véase el caso de Egipto, donde las comunidades LGBTQ son crecientemente atacadas por el gobierno y los organismos de aplicación de la ley. En el otoño de 2017, un proyecto de ley firmado por 67 miembros del parlamento amenazó con penalizar explícitamente la actividad sexual entre personas del mismo sexo. Esto siguió al aparente arresto de miembros del público en un concierto donde la gente ondeó banderas arcoiris; Jo Schietti, "Egypt's 'Morality police' get Grinder to trap LGBT community ahead of new homophobic law", *The New Arab*, 27 de noviembre de 2017. Disponible en https://www.alaraby.co.uk/english/indepth/2017/11/27/egypts-morality-police-get-on-grindr
[4] La comunidad LGBTQ de Egipto depende cada vez más de la comunicación cifrada, como la que ofrece Signal; ibid: https://www.alaraby.co.uk/english/indepth/2017/11/27/egypts-morality-police-get-on-grindr
[5] Véase el bloqueo del gobierno egipcio de aplicaciones encriptadas como Signal; Jessica Conditt, "Encrypted Chat App Signal Circumvents Government Censorship", *Engadget,* 21 de diciembre de 2016. Disponible en https://www.engadget.com/2016/12/21/signal-egypt-uae-censorship-block-domain-fronting/
[6] Véase Goodwin v. Reino Unido 22 EHRR 123, 27 de marzo de 1996, párrafo 39 "La protección de las fuentes periodísticas es una de las condiciones básicas de la libertad de prensa... Sin tal protección, las fuentes pueden ser disuadidas de ayudar a la prensa a informar al público en asuntos de interés público."
[7] Véase Elizabeth Farries, "Ireland Not Immune to the Threat of Surveillance Against Journalists" *The Journal,* 9 de noviembre de 2017. Disponible en http://www.thejournal.ie/author/elizabeth-farries/5547/.
[8] En Irlanda, por ejemplo, la Ley de retención de datos y comunicaciones de 2011 permite el acceso a los datos de comunicación de los periodistas en contravención a la legislación de la UE. Disponible en https://www.iccl.ie/wp-content/uploads/2017/12/DRI-ICCL-DR-submission-13.11.17_Website_EF-edit.pdf

ventaja competitiva en el mercado a medida que la gente busca mejores métodos para comunicarse de manera privada, el sector también enfrenta problemas en distintos países. Las agencias de inteligencia, en particular, intentan forzar a las organizaciones privadas a proporcionar herramientas de cifrado o a abrir "puertas traseras" en circunstancias específicas[9], o a entregar claves de cifrado[10], a veces mediante ingenuos malentendidos sobre cómo funciona el cifrado[11]. Las aplicaciones encriptadas son bloqueadas o corren el riesgo de ser bloqueadas en ciertos países[12].

Necesidades del Estado

Las instituciones y los funcionarios de los Estados, en lugar de intentar restringir el cifrado, podrían dar el ejemplo comprendiendo, respaldando y adoptando fuertes protocolos de encriptación. La adquisición ilícita de importantes correos electrónicos de funcionarios[13] y de agencias gubernamentales que guardan información personal de los ciudadanos[14] pone de relieve esta necesidad. El argumento de que los derechos de cifrado deberían limitarse ya que podrían ser utilizados por terroristas, por agencias de inteligencia extranjeras o para cometer actividades delictivas no tiene sentido, ya que son precisamente esos actores contra los que los gobiernos y los ciudadanos deberían protegerse[15].

---

[9] En los Estados Unidos, el FBI intentó obligar a Apple a abrir una "puerta trasera" encriptada en un teléfono inteligente. Véase Eric Lichtblau y Katie Benner, "Apple Fights Order to unlock San Bernardino Gunman's iPhone", *The New York Times,* 17 de febrero de 2016. Disponible en https://www.nytimes.com/2016/02/18/technology/apple-timothy-cook-fbi-san-bernardino.html?rref=collection%2Fnewseventcollection%2Fapple-fbi-case&action=click&contentCollection=technology&region=stream&module=stream_unit&version=latest&contentPlacement=4&pgtype=collection

[10] En Rusia, dos periodistas prominentes intentaron demandar a la agencia de seguridad federal sin éxito porque esta ha intentado obligar a las aplicaciones de mensajería cifradas a entregar claves de cifrado, lo que compromete directamente la confidencialidad de las fuentes periodísticas. Véase Anon: "Journalists are Challenging Russia's 'anti-terrorist' Demands on Instant Messengers', *Meduza,* 25 de octubre de 2017. Disponible en https://meduza.io/en/news/2017/10/25/journalists-are-challenging-russia-s-anti-terrorist-demands-on-instant-messengers

[11] Ochenta y tres organizaciones y expertos expresaron en una declaración conjunta a la alianza de los Cinco Ojos que "los intentos de diseñar 'puertas traseras' u otras debilidades deliberadas en softwares de encriptación comerciales, exigir que las empresas conserven la capacidad de descifrar datos de los usuarios o forzar a los proveedores de servicios a diseñar herramientas de comunicación que permitan la interceptación del gobierno son miopes y contraproducentes". Disponible en la Asociación Canadiense de Libertades Civiles: https://ccla.org/83-organizations-experts-5-nations-demand-five-eyes-respect-strong-encryption/

[12] Telegram se ha negado a entregar claves de cifrado al Servicio Federal de Seguridad y las autoridades ahora tienen un terreno formal para bloquear la aplicación en Rusia. Véase Tom Spring, "Telegram ordered to hand over encryption keys to Russian authorities", *Threat Post,* 20 de marzo de 2018. Disponible en https://threatpost.com/telegram-ordered-to-hand-over-encryption-keys-to-russian-authorities/130581/
El regulador de Telecom en Rusia solicitó permiso a la corte para bloquear Telegram, con éxito. Se envió una orden el 13 de abril de 2018 con implementación inmediata. En Egipto, la aplicación de código abierto Signal ha esquivado los intentos del gobierno egipcio de bloquearla. Véase Jessica Conditt, "Encrypted chat app Signal circumvents governmental censorship", *Engadget,* 21 de diciembre de 2016. Disponible en https://www.engadget.com/2016/12/21/signal-egypt-uae-censorship-block-domain-fronting/.sinead

[13] Véase, por ejemplo, la adquisición de correos electrónicos pertenecientes a Hillary Clinton y Theresa May.

[14] Véase, por ejemplo, el ataque global de ransomware que paralizó al National Health Service y el hackeo a la base de datos Aadhaar de la India.

[15] Apoyamos las conclusiones de 2016 del informe del gobierno de los Países Bajos, que señalan que "no es apropiado adoptar medidas legales restrictivas contra el desarrollo, la disponibilidad y el uso del cifrado". Brief Van De Ministers Van Veiligheid En Justitie En Van Economische Zaken, 4 de enero de 2016. Disponible en https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2016Z00009&did=2016D00015

Abordar estos desafíos

Si bien los derechos a la privacidad y a la libertad de expresión no son absolutos, deben salvaguardarse rigurosamente. Las medidas de protección aplicadas a las comunicaciones privadas offline también deben ser aplicadas en espacios digitales y online. El cifrado es, por lo tanto, una medida tecnológica ideal para proteger las comunicaciones anónimas. Las alternativas de apoyo pueden incluir:

- Educar a miembros de agencias gubernamentales, policiales y de inteligencia en el significado y los mecanismos de encriptación, y en la ayuda que estos protocolos brindan a nuestros derechos fundamentales;
- respaldar a y colaborar con tecnologías de código abierto que ofrezcan protocolos de encriptación fuertes para poblaciones vulnerables; y
- brindar apoyo legal a compañías bajo ataque gubernamental a través de litigios y apoyos amicus curiae.

**II. Dependencia de la tecnología basada en datos**

Cómo las nuevas tecnologías ayudan a promover y proteger el derecho a la privacidad

Al momento de desarrollar nuevas tecnologías, la privacidad debería ser un elemento central por diseño y por defecto. El escándalo de Cambridge Analytica muestra cuánto daño pueden hacer las tecnologías a la privacidad cuando su diseño se centra únicamente en los beneficios o la usabilidad[16]. Identificar posibles riesgos a la privacidad antes y durante el proceso de desarrollo es la mejor manera de que una nueva tecnología ayude a protegerla. Por ejemplo, una red eléctrica inteligente está diseñada para recolectar datos sobre el consumo de electricidad de los usuarios finales, pero puede revelar información sensible y privada, como en qué momento un usuario final se encuentra en su casa. Identificar ese riesgo de antemano y diseñar la tecnología en función de él puede reforzar notablemente la protección del derecho a la privacidad en el producto final[17].

Si bien construir privacidad dentro de la propia tecnología es una solución integral, las soluciones tecnológicas intermedias también pueden ayudar a quienes dependen de programas e infraestructuras que invaden la privacidad. Estas incluyen herramientas de cifrado fáciles de usar, "espías de smart data" y el uso de Inteligencia Artificial para que las personas controlen sus propios conjuntos de datos personales[18], entre otros. Los actores del sector privado son clave, y deben explorarse estrategias para alentarlos a que tomen debidamente en cuenta la privacidad, lo que podría incluir desarrollar pautas que establezcan estándares para el desarrollo de una tecnología ética.

---

[16] Véase Nicole Ozer y Chris Conley, "After Facebook Privacy Debacle, It's Time for Clear Steps to Protect Users", *American Civil Liberties Union,* 23 de marzo de 2018. Disponible en https://www.aclu.org/blog/privacy-technology/internet-privacy/after-facebook-privacy-debacle-its-time-clear-steps-protect

[17] Shaohua Li y otros, "PPMA: Privacy-Preserving Multisubset Data Aggregation in Smart Grid", *IEEE Transactions on Industrial Informatics*, vol. 14 (2 de febrero de 2018).

[18] Ann Cavoukian, "Privacy controls must be placed back into the hands of the individual" Globe and Mail, 27 de marzo de 2018. Disponible en https://www.theglobeandmail.com/opinion/article-privacy-controls-must-be-placed-back-into-the-hands-of-the-individual/

Los principales desafíos en relación al impacto sobre el derecho a la privacidad y otros derechos humanos

La proliferación de datos biométricos y otras recolecciones de datos de la vida cotidiana –para acceder a servicios bancarios, servicios esenciales, edificios, teléfonos celulares, etc.– puede tener un efecto corrosivo en la privacidad debido a la sensibilidad de los datos recopilados sin un control o supervisión adecuados[19]. Un ejemplo del peligro que suponen los controles insuficientes al recolectar y procesar datos biométricos se da en Sudáfrica: los proveedores de servicios privados pueden acceder y monetizar legalmente la información almacenada en el registro biométrico del Departamento de Asuntos Internos con el objeto de comercializar tecnologías de verificación biométrica[20].

Alternativas para abordar los desafíos a la privacidad de la tecnología basada en datos

Contar con un conocimiento técnico adecuado es clave para regular la tecnología. Sin esa comprensión por parte de quienes toman las decisiones relevantes, es casi imposible crear una regulación adecuada. Esto se aplica a los órganos multilaterales y nacionales encargados de regular la recolección de datos biométricos y la recolección y análisis de grandes volúmenes de datos para garantizar que la privacidad y otras consideraciones relacionadas con los derechos humanos sean fundamentales en el desarrollo e implementación de nuevas soluciones tecnológicas. También creemos que confiar solamente en los mecanismos legales no garantizará la privacidad a menos que ofrezcamos una guía clara a quienes construyen tecnologías basadas en datos.

Bajo esta perspectiva, los principios estandarizados para recolectar, usar y retener datos biométricos deben incluir controles reguladores en general, más allá de las condiciones del contrato. Y estos controles deben, como mínimo, reflejar los requisitos del Reglamento General de Protección de Datos (GDPR por sus siglas en inglés) (UE) 2016/679. Conforme al GDPR, los datos biométricos son una de las "categorías especiales" de datos personales, a las que otorga protecciones en su Artículo 9. Respaldamos como mínimo los requisitos impuestos por esta regulación en relación a la portabilidad, consentimiento, aviso y transparencia algorítmica y centrada en el usuario[21].

**III. Interferencias indebidas al derecho a la privacidad digital de grupos vulnerables**

Las acciones de vigilancia, tanto por parte de los Estados como de organismos del sector privado, a menudo apuntan desproporcionadamente a las poblaciones marginadas y vulnerables. Esto ha sido así desde hace mucho tiempo en el espacio físico, y puede intensificarse en el espacio digital. Mujeres y niñas, minorías religiosas, personas que viven en la pobreza, grupos raciales y étnicos así como miembros de comunidades indígenas, personas de diferentes géneros y de todas las edades pueden

[19] Yue Liu, "Privacy Regulations on Biometrics in Australia", *Computer Law & Security Review,* vol. 2, No. 6 (2010).
[20] Un ejemplo son los servicios de verificación de identidad ofrecidos por IDEMIA. Disponible en http://www.idemia.com.
[21] También apoyamos la evidencia presentada en el Informe avanzado de SPR sobre privacidad en la 72.a sesión de la Asamblea General; Bart Custers y otros "A Comparison of Data Protection Legislation and Policies Across the EU" *Computer Law & Security Review*, vol. 34 (2018), junto con las recomendaciones del "Centre for Information Policy Leadership, Recommendations for Implementing Transparency, Consent and Legitimate Interest under the GDPR - Centre for Information Policy Leadership GDPR Implementation Project" (19 de mayo de 2017).

experimentar golpes desproporcionados a su privacidad. La interferencia indebida de los sistemas digitales en los derechos a la privacidad de grupos marginados ha sido bien documentada[22]. A continuación, presentamos una muestra no exhaustiva de este problema[23].

Algoritmos y decisiones basadas en algoritmos

Está claro que los grupos vulnerables que ya sufren un escrutinio gubernamental desproporcionado se verán aun más agobiados por estas tecnologías algorítmicas[24]. La toma de decisiones basada en algoritmos suele presentarse como objetiva, pero escribir algoritmos imparciales es difícil y los programadores pueden, por error o incluso por diseño, incorporar desinformación, racismo, sesgos y prejuicios "que tienden a castigar a los pobres y oprimidos[25]". Este potencial discriminador se ve agravado por la opacidad de los programas, muchos de los cuales son exclusivos y patentados, y por una tendencia social a asumir que una decisión tomada por una máquina tiene más chances de ser objetiva. Si bien ha habido un importante trabajo académico y orientado hacia políticas concretas que busca soluciones para crear algoritmos "justos", no existen estándares internacionales firmes que impulsen el control o la transparencia[26].

Sesgo sistémico en conjuntos históricos de datos

Los algoritmos detectan patrones en conjuntos grandes de datos. Sin embargo, muchos conjuntos históricos de datos contienen sesgos debido a años de prácticas de recolección problemáticas[27]. Por ejemplo, existe la preocupación de que técnicas de vigilancia sesgadas contribuyan a datos policiales sesgados. En Canadá, un análisis de 10 años de datos sobre arrestos y cargos por posesión de marihuana, adquiridos de los Servicios Policiales de Toronto, reveló que las personas negras sin antecedentes penales tenían tres veces más probabilidades de ser arrestadas que las personas blancas con antecedentes similares[28]. También se han recopilado e interpretado datos sobre comunidades

---

22 Virginia Eubanks, *Automating Inequality: How High-Tech Tools Profile, Police and Punish the Poor* (New York, NY; St. Martin's Press, 2018); Safiya, U. Noble, *Algorithms of Oppression: How Search Engines Reinforce Racism* (New York, NY; New York University Press, 2018); Cathy O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy* (New York, NY; Broadway Books, 2017); Joshua R. Scannell, "Broken Windows, Broken Code", *Reallifemag,* 29 de agosto de 2016. Disponible en http://reallifemag.com/broken-windows-broken-code/

23 Unión Americana de Libertades Civiles, "Will Artificial Intelligence Make Us Less Free? Experts Consider How the Growing Use of AI Will Impact Civil Liberties". Disponible en https://www.aclu.org/issues/privacy-technology/will-artificial-intelligence-make-us-less-free

24 Ibíd.

25 Cathy O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy* (New York, N;: Broadway Books, 2017) en 3.

26 Véase Bruno Lepri y otros, "Fair, Transparent, And Accountable Algorithmic Decision-making Processes: The Premise, the Proposed Solutions, and the Open Challenges" (2017) *Philosophy & Technology* (2017). Disponible en https://doi.org/10.1007/s13347-017-0279-x; Sorelle A. Fiedler & Christo Wilson (eds), "Proceedings of Machine Learning Research", *Conference on Fairness, Accountability and Transparency*, vol 81 (23-24 de febrero de 2018) New York NY, EE.UU. Disponible en http://proceedings.mlr.press/v81/; Nicholas Diakopoulos & Sorelle Friedler, "How to Hold Algorithms Accountable," *MIT Technology Review* (17 de noviembre de 2016). Disponible en https://www.technologyreview.com/s/602933/how-to-hold-algorithms-accountable/

27 Frank Pasquale, *The Black Box Society: The Secret Algorithms that Control Money and Information* (Cambridge, MA; Harvard University Press, 2015).

28 Jim Rankin, Sandro Contenta y Andrew Bailey, "Toronto Marijuana Arrests Reveal 'startling' Racial Divide", *The Star,* 6 de julio de 2017. Disponible en https://www.thestar.com/news/insight/2017/07/06/toronto-marijuana-arrests-reveal-startling-racial-divide.html

indígenas con hincapié en estadísticas que reflejan desventajas y estereotipos negativos[29]. Al mismo tiempo, los crímenes que afectan particularmente a las mujeres, incluidas las agresiones domésticas y sexuales, pueden estar subrepresentados en modelos de vigilancia policial predictiva basados en datos debido a que históricamente no se ha informado lo suficiente sobre ellos.

Los algoritmos y los datos sesgados así como el comportamiento discriminatorio dan como resultado la discriminación por Big Data[30]. La investigación demuestra claramente que las comunidades vulnerables son desproporcionadamente susceptibles a la discriminación por Big Data. De hecho, "las analíticas de Big Data tienen el potencial de eclipsar protecciones a los derechos civiles respecto del uso de información personal sobre vivienda, crédito, empleo, salud, educación y mercado"[31], así como "la inmigración, seguridad pública, vigilancia policial y el sistema de justicia"[32].

Acoso y abusos facilitados por el entorno digital

Incluso si los algoritmos y los conjuntos de datos carecieran de sesgos, el comportamiento discriminatorio de los individuos y las instituciones podría expandirse en la era digital. Un ejemplo es la proliferación de tecnologías de spyware que "se empaquetan y venden para facilitar la violencia doméstica, el acecho y otras formas de acoso y abuso que amenazan la seguridad de las mujeres y las niñas y que son facilitados por esta tecnología"[33].

No se trata solo de las tecnologías que otros pueden usar, sino de las plataformas en las que se desarrolla cada vez más la vida social y que facilitan la violencia, el acoso y el abuso de género. Las mujeres y las niñas son desproporcionadamente propensas a sufrir "hostigamiento, hacking, ataques de denegación de servicio, calumnias basadas en el género, la publicación de información personal privada e identificable ("doxing"), suplantación de identidad, extorsión, violación y amenazas de muerte, tráfico electrónico y explotación sexual o engaño a menores"[34].

---

[29] Open North y la British Columbia First Nations Data Governance Initiative, "Decolonizing data: Indigenous Data Sovereignty Primer" (abril de 2017).

[30] Seeta Gangadharan, Virginia Eubanks y Solon Barocas, "Data and discrimination: Collected essays." (2014). Disponible en https://www.newamerica.org/oti/policy-papers/data-and-discrimination/; Nathan Newman, "How Big Data Enables Economic Harm to Consumers, Especially to Low-Income and Other Vulnerable Sectors of the Population" (2014). Disponible en https://www.ftc.gov/system/files/documents/public_comments/2014/08/00015-92370.pdf; Solon Barocas y Andrew D. Selbst, "Big data's Disparate Impact." *California Law Review,* vol. 104 (2016); Mary Madden, Michele Gilman, Karen Levy y Alice Marwick, "Privacy, Poverty and Big Data: A Matrix of Vulnerabilities for Poor Americans" vol. 95, *Washington University Law Review* (2017).

[31] The White House 2014, p. 3.

[32] Obar y McPhail 2018.

[33] Ronald J. Deibert, Lex Gill, Tamir Israel, Chelsey Legge, Irene Poetranto y Amitpal Singh, presentación del Citizen Lab (Munk School of Global Affairs, Universidad de Toronto) al Relator Especial de las Naciones Unidas sobre la violencia contra la mujer, sus causas y consecuencias, Sra. Dubravka Šimonović, 2 de noviembre de 2017, p. 15. Disponible en https://citizenlab.ca/wp-content/uploads/2017/11/Final-UNSRVAG-CitizenLab.pdf. La totalidad de este informe es una contribución relevante a la cuestión del impacto de la privacidad de mujeres y niñas en la era digital.

[34] Ibid., P. 2; véase, como se cita en esta fuente, lo siguiente: CE, Instituto Europeo para la Igualdad de Género, "Cyber Violence Against Women and Girls" (2017). Disponible en http://eige.europa.eu/rdc/eige-publications/cyber-violence-against-women-and-girls; Grupo de trabajo de la Comisión de Banda Ancha de la ONU para el Desarrollo Digital sobre Banda Ancha y Género, "Cyber Violence against Women and Girls: A Worldwide Wake-Up Call" (2015). Disponible en http://www.broadbandcommission.org/Documents/reports/bb-wg-gender-discussionpaper2015-executive-summary.pdf; Linda Baker, Marcie Campbell y Elsa Barreto, "Understanding Technology-Related Violence Against

El efecto paralizador de la vigilancia

Los sistemas digitales no solo funcionan de manera discriminatoria, sino que también tienen un mayor impacto en los grupos vulnerables y marginados. Por ejemplo, Jonathan W. Penney examinó los efectos paralizadores de la vigilancia en línea y descubrió que es más probable que los jóvenes y las mujeres se paralicen y menos probable que tomen medidas para resistir las acciones regulatorias y defenderse[35]. Del mismo modo, los estudios han demostrado que una abrumadora mayoría de musulmanes estadounidenses cree que el gobierno de EE.UU. supervisa sus actividades desde el 11 de septiembre de 2001 y, en consecuencia, ha cambiado su manera de utilizar de Internet[36].

Alternativas para proteger a grupos vulnerables y marginados

Abordar estos desafíos podría suponer una combinación de estrategias que incluyen:

- Desarrollar estándares internacionales para auditar y eliminar sesgos en algoritmos y conjuntos de datos;
- modernizar la legislación existente respecto de la privacidad y la protección de datos a nivel estatal para garantizar su efectividad continua;
- promover y regular la responsabilidad de las entidades que crean y usan algoritmos y conjuntos de datos;
- desarrollar y promover la alfabetización tecnológica y la educación sobre privacidad en poblaciones vulnerables; y
- lanzar y apoyar investigaciones que lleven las voces de las mujeres y las niñas a la discusión sobre el diseño de políticas[37], y promover una iniciativa similar centrada en otras poblaciones marginadas y vulnerables.

**IV. Protecciones contra la vigilancia, el procesamiento y la interceptación de comunicaciones digitales**

El derecho a la privacidad solo puede estar limitado por una ley que regule las violaciones a la privacidad. La Resolución de la Asamblea General de las Naciones Unidas sobre el derecho a la privacidad en la era digital reafirma el principio del derecho internacional de que nadie será objeto de injerencias arbitrarias e ilícitas en su derecho a la privacidad[38]. Además, hace un llamado a los Estados para que revisen la legislación y los procedimientos que habilitan la vigilancia legal, así como para

---

Women: Types of Violence and Women's Experiences,", Centro de investigación y educación sobre la violencia contra las mujeres y los niños, Learning Network Brief 6 (2013). Disponible en http://www.learningtoendabuse.ca/sites/default/files/Baker_Campbell_Barreto_Categories_Technology-Related_VAW_.pdf; véanse las cuentas personales detalladas en Bytes for All (B4A), en asociación con la Association for Progressive Communications (APC). Disponible en http://content.bytesforall.pk/sites/default/files/ViolenceAgainstWomenPakistanCountryReport.Pdf

[35] Jonathon W. Penney "Internet Surveillance, Regulation and Chilling Effects Online: a Comparative Case Study" *Journal on Internet Regulation,* vol. 6 (2017).

[36] Dawinder S. Sidhu, "The Chilling Effect of Government Surveillance Programs on the Use of the Internet by Muslim Americans" *University of Maryland Law Journal,* vol 7 (2007).

[37] Un buen ejemplo canadiense es el proyecto E-girls, dirigido por el equipo de investigación de Jane Bailey, Valerie Steeves, Jacquelyn Burkell, Priscilla Regan, Madelain Saginur y Jane Tallim. Disponible en https://egirlsproject.ca/the-project/what-we-are

[38] El derecho a la privacidad en la era digital A/RES/68/167 en 1.

asegurar la existencia de mecanismos de supervisión independientes y efectivos para promover la transparencia[39].
Los siguientes principios deben ser tenidos en cuenta en los fundamentos mínimos al momento de diseñar legislaciones, regulaciones y políticas gubernamentales:

- Independencia institucional de los órganos de supervisión, incluyendo seguridad en el cargo para el personal ex officio, control presupuestario completo y transparencia administrativa para el ejecutivo, pero no respecto de las decisiones relacionadas con las funciones obligatorias;
- contar con una autorización para vigilar por parte de una autoridad judicial o cuasi judicial, que no sea demasiado próxima a las instituciones que llevan a cabo la vigilancia, y solo cuando haya pruebas claras de una amenaza real y la acción de vigilancia propuesta sea selectiva, estrictamente necesaria y proporcionada; y
- una solución efectiva y accesible a quienes han sido sometidos a la vigilancia ilegal, incluyendo la notificación posterior y la posibilidad de una compensación civil y de una sanción penal.

Si bien la atención se suele poner en la vigilancia conducida por el Estado y la supervisión de la misma, notamos que cada vez cobra más importancia la supervisión y la provisión de soluciones contra el accionar de entidades privadas. El alcance de los datos recolectados por entidades privadas así como la propiedad privada de las infraestructuras de información permiten un amplio margen para la violación del derecho a la privacidad por parte de entidades privadas.

**V. Comentarios finales y próximos pasos**

Los importantes desafíos señalados aquí –el cifrado y el anonimato, la dependencia de la tecnología impulsada por datos y la privacidad digital de grupos vulnerables– podrían abordarse a través de una mayor elaboración e interpretación autorizada de las obligaciones legales existentes que protegen el derecho a la privacidad consagradas en el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos.

Hasta la fecha, el Comité de Derechos Humanos es el único organismo relevante de derechos humanos de Naciones Unidas que no ha tomado medidas para abordar los derechos de privacidad digital (y las obligaciones del Estado para protegerlos) de manera sistemática y exhaustiva. La palabra del Comité sobre la privacidad de la información es indispensable en este momento crítico. A través del proceso de revisión de la Observación general 16, el Comité tendrá la oportunidad de abordar los asuntos urgentes descritos en este informe. El Comité también tendrá la oportunidad de restablecerse como un organismo líder en la protección de la privacidad, reconocida hoy como uno de los derechos humanos que más se violan en el mundo y de una vulnerabilidad crítica en la era digital.

En contraste, ante la ausencia de aportes del Comité, los Estados continuarán confiando en las normas anticuadas tanto al informar al Comité sobre el cumplimiento del Pacto Internacional de Derechos Civiles y Políticos como al defender las peticiones individuales, socavando así el correcto desarrollo del derecho internacional. El proceso general de revisión de comentarios –y los comentarios resultantes–

[39] El derecho a la privacidad en la era digital A/RES/68/167 en 2.

también ayudará a otros organismos regionales y de los EE.UU., así como a las legislaturas y tribunales nacionales, al formular leyes, políticas y prácticas que adopten los estándares de privacidad del PIDCP.

*INCLO es una red de 13 organizaciones nacionales independientes de derechos humanos del sur y el norte global. Trabajamos juntos para promover los derechos y libertades fundamentales.*