ELECTRONIC FRONTIER FOUNDATION eff.org

Anonimato y cifrado

Comentarios enviados a la Relatoría Especial de la Comisión de Derechos Humanos sobre la promoción y protección del derecho a la libertad de opinión y de expresión

10 de febrero de 2015

Contacto:

Katitza Rodríguez, Directora Internacional de Derechos de la EFF
katitza@eff.org

Gracias por brindarle a la Electronic Frontier Foundation (EFF) la oportunidad de añadir nuestra presentación a la consulta acerca del uso de cifrado y anonimato en las comunicaciones digitales. EFF es una organización civil internacional no gubernamental con más de 26,000 donantes a nivel mundial, dedicada a la protección de las libertades fundamentales en línea de las personas. EFF se involucra en litigios estratégicos en los Estados Unidos y trabaja en una serie de áreas de políticas nacionales e internacionales para proteger las libertades civiles, fomentar la innovación, y empoderar a los consumidores. EFF está ubicado en San Francisco, California y cuenta con miembros en 90 países en todo el mundo.

Traducido por J. Andrés Delgado.

I. Anonimato

¿Qué es el anonimato?

El anonimato se puede definir como actuar o comunicarse sin usar o presentar el nombre o identidad propios; o como actuar o comunicarse en una manera que protege la determinación del nombre o identidad propios, o usando un nombre asumido o inventado que no puede necesariamente asociarse con la identidad legal o habitual de uno.[1]

El anonimato puede ser concebido como un espectro, de fuerte a débil. El anonimato es fuerte cuando existen protecciones técnicas y legales que hacen que sea muy difícil desenmascarar la identidad de una persona anónima. El anonimato es débil cuando una persona anónima puede ser desenmascarada mediante métodos sencillos, tales como solicitudes gubernamentales al proveedor de servicio o buscando el nombre asumido en una base de datos existente.

Podemos evaluar el grado de anonimato que una persona puede lograr en línea al considerar cuestiones tales como: ¿Puede la gente abstenerse de firmar lo que escribe? ¿Puede elegir el modo de firmar (o no firmar) sus comunicaciones? ¿Puede acceder a servicios sin registrarse, o sin registrarse con su identidad legal? ¿Los proveedores de servicio requieren que una cuenta esté vinculada a un documento de identidad emitido por el gobierno, o a otros sistemas que están vinculados a la identidad legal, como es el caso de los sistemas de pago? ¿Los proveedores de servicio retienen datos, tales como registros de acceso, que podrían ser usados para identificar a sus usuarios en el futuro? ¿Cuentan los usuarios con herramientas técnicas para ocultar su identidad, tales como tecnologías que mejoran la privacidad y hacen difícil su identificación? ¿Los usuarios confían en que su identidad no será asociada con sus actividades contra su voluntad? Con

[1] Algunas fuentes distinguen entre *anonimato* (no usar nombre alguno) y *seudonimato* (usar un nombre asumido), pero para el propósito de esta presentación no hacemos distinción alguna. En la práctica, los seudónimos digitales requieren de un anonimato fuerte o débil como parte del proceso de separar el nombre asumido de los detalles de la identidad de la persona.

el fin de despojar a una persona del anonimato que eligió, ¿qué esfuerzo debe ser llevado a cabo por otras partes? ¿Pueden terceros determinar la identidad de un individuo sin tener que recurrir a los tribunales, o se debe seguir un proceso legal?

¿Quién necesita anonimato?

Todo aquel que no quiera que las cosas que dice estén conectadas a su identidad permanente tiene interés en el anonimato. Puede que estén preocupados por retribuciones políticas o económicas, acoso, o incluso amenazas a sus vidas, o pueden usar el anonimato como parte de su expresión o desarrollo personal. Algunos necesitan encubrir su identidad de la investigación informal de sus colegas. Otros necesitan protecciones más fuertes contra adversarios más determinados y bien financiados. Habrá quienes requerirán protección contra sus propios gobiernos.[2]

Los padres tratan de crear una forma segura de que los niños exploren en línea.[3] Los adolescentes que exploran su propia identidad son, a menudo, acosados en línea y en sus propias comunidades, y puede que escojan el anonimato en línea para protegerse.[4]

Conforme maduran los individuos, puede que con el tiempo cambien sus nombres como una expresión de su religión, creencias, o como parte del desarrollo completo de su personalidad. Puede que busquen hacer esto para evitar discriminación, o para establecer un nombre que es más fácil de pronunciar o deletrear en una cultura dada.[5]

---

[2] Electronic Frontier Foundation (2013). Speech: anonymity. Obtenido el 6 de febrero de 2015, de https://ilt.eff.org/index.php/Speech:_Anonymity.

[3] Patti M. Valkenburg et al. (2005). 'Adolescents' identity experiments on the Internet". *New Media & Society, vol. 7 no. 3:*383-402. Obtenido el 6 de febrero de 2015, de http://nms.sagepub.com/content/7/3/383

[4] Livescience (2010), *Cyberbullying Rampant for Lesbian and Gay Teens*. Obtenido el 6 de febrero de 2015, de http://www.livescience.com/6199-cyberbullying-rampant-lesbian-gay-teens.html

[5] Sobre la variedad cultural de las convenciones de nombres y la incapacidad de los sistemas de computación para lidiar con ello de manera adecuada, léase Patrick McKenzie (2010), *Falsehoods Programmers Believe About Names*. Kalzumeus. Obtenido el 8 de febrero de 2015, de http://www.kalzumeus.com/

Otros necesitarán reconstruir sus vidas resguardados de opresión previa. Los sobrevivientes de abuso doméstico que necesitan protección de sus abusadores deben asegurarse de no dejar un rastro digital.[6] Los individuos cuyos cónyuges o parejas trabajan para el gobierno o son muy bien conocidos podrían desear esconder aspectos de su propia vida, y a menudo se sienten más cómodos usando herramientas de anonimato. Los programas de protección de testigos y víctimas necesitan anonimato para operar de forma segura.

Las profesiones que hacen posible la libertad de expresión usan el anonimato para proteger a sus clientes. Los bibliotecarios creen que los usuarios de las bibliotecas deben tener el derecho de leer de forma anónima —un requisito esencial para la libertad intelectual y la privacidad.[7] Los editores han luchado para preservar el anonimato de sus clientes por considerar que ser conocido como lector de obras controvertidas puede crear un efecto inhibidor.[8]

El anonimato les permite a las fuentes de periodistas atreverse y hablar sin temor a represalias; los denunciantes reportan noticias que corporaciones y gobiernos preferirían suprimir.[9] El anonimato también es esencial en el contexto de los derechos humanos. Los trabajadores de derechos humanos lo usan en su contienda contra las violaciones de

---

[6] Léase Meghan Neal (2014). *Tor Is Being Used as a Safe Haven for Victims of Cyberstalking*, MotherBoard. Obtenido el 8 de febrero de 2015, de http://motherboard.vice.com/

[7] The International Federation of Library Associations and Institutions (1999). *Statement on Libraries and Intellectual Freedom*. Obtenido el 6 de febrero de 2015, de http://www.ifla.org/publications/ifla-statement-on-libraries-and-intellectual-freedom

[8] Por ejemplo, en la jurisprudencia EE.UU., en Rumley, 345 U.S. 41, un vendedor de libros no pudo ser condenado por negarse a proporcionar una lista de las personas a las que él había hecho ventas al por mayor de libros políticos para su posterior distribución. Para más ejemplos, véase *Privacy Authors and Publishers' Objection to Proposed Settlement*, Authors Guild v. Google, Inc., No. 05CV8136DC. Obtenido el 9 de febrero de 2015, de https://www.eff.org/files/filenode/authorsguild_v_google/file_stamped_brf.pdf

[9] Por ejemplo, varios activistas medioambientales que protestaban por el perjuicio a la Amazonía causado por las actividades de extracción de petróleo de Chevron usan seudónimos por miedo a represalias por parte de la empresa. Obtenido el 6 de febrero de 2015, de https://www.eff.org/files/filenode/effmotionquash.pdf

derechos humanos;[10] funciona como un escudo para aquellos que buscan desafiar poderes centralizados arraigados, o una mayoría intolerante.[11]

Anonimato y Sociedad

El anonimato es vital para una sociedad abierta y libre. Nos importa el anonimato en línea y fuera de línea porque permite a los individuos expresar opiniones impopulares, observaciones honestas y quejas que, de lo contrario, no serían escuchadas. Permite evitar represalias potencialmente violentas de aquellos que puedan sentirse ofendidos, y desempeña un papel central en la lucha para exponer los crímenes y abusos de poder.

Nos importa el anonimato porque queremos una sociedad donde la gente pueda hablar honestamente. El anonimato permite que las voces sean escuchadas —y las ideas juzgadas— en función de su contenido, no de su origen. El anonimato puede ayudar a proteger a un orador de la falacia lógica de los ataques *ad hominem* (responder a los argumentos atacando el carácter de una persona, en lugar del contenido de sus argumentos).

Nuestra sociedad actual no nos obliga a mostrar nuestros documentos de identidad o firmar nuestros nombres antes expresarnos. Los valores que hemos desarrollado a lo largo de muchas décadas se construyeron en el debate franco y de amplio alcance que dicha libertad ofrece. Esos valores, incluyendo el anonimato en sí, deben mantenerse en la era digital.

---

[10] EFF demandó al gobierno etíope en nombre de un activista pro-democracia etíope que vive en el área de Washington DC que está trabajando bajo el seudónimo de "Kidane", debido a preocupaciones por su seguridad y la de su familia. Obtenido el 6 de febrero de 2015, de http://phys.org/news66401288.html o https://www.eff.org/cases/kidane-v-ethiopia

[11] El conocido bloguero y activista ambiental Nguyen Van Hai escribió en su blog bajo el seudónimo de "Dieu Cay." Las autoridades descubrieron su identidad y lo encarcelaron desde 2010 hasta 2014. Obtenido el 6 de febrero de 2015, de https://eff.org/https://eff.org/civilrightsdefenders-anonymity

Anonimato y estándares internacionales de Derechos Humanos

Los derechos a la libre expresión y a la privacidad fueron reconocidos por la Declaración Universal de Derechos Humanos ("DUDH") el 10 de diciembre de 1948.[12] Desde entonces, estos derechos han sido afirmados por los tratados internacionales de derechos humanos subsecuentes de las Naciones Unidas, así como por varios tratados internacionales y otros instrumentos de derechos humanos. Si bien los tratados e instrumentos más recientes adoptaron un lenguaje diferente al empleado por la DUDH al enunciar el derecho a la privacidad y el derecho a la libertad de expresión, un análisis comparativo muestra que ha surgido un consenso coherente sobre las protecciones específicas otorgadas a las personas así como las obligaciones impuestas a los Estados Partes.

Libertad de expresión

La libertad de expresión es reforzada cuando uno puede hacerlo anonimamente. Existen muchas circunstancias donde una persona no hablará por temor a represalias, un desequilibrio de poder inherente, u otra razón, o una asociación de individuos no hablará a menos que esté segura de proteger la identidad de sus miembros. La Relatoría Especial de Libertad de Expresión de la Comisión Interamericana de Derechos Humanos (CIDH) dejó claro que "en todos los casos, los usuarios deben tener derecho a permanecer bajo anonimato y cualquier disputa sobre este punto debe ser resuelta exclusivamente en sede judicial".[13]

El derecho a buscar y recibir información

La capacidad de leer y acceder a información anónimamente es también crucial para el ejercicio de la libre expresión. El artículo 19 de la Declaración Universal de Derechos Humanos, que consagra el derecho a la libertad de opinión y de expresión, incluye el derecho a buscar, recibir e impartir información e ideas a través de cualquier medio. Esta inclusión es necesaria porque no puede haber una protección significativa de

[12] DUDH. Art. 12 (privacidad), Art. 19 (expresión).

[13] CIDH (2013). *Informe de la relatoría especial para la libertad de expresión*. Capítulo IV (Libertad de expresión e Internet). OEA /Serv.L/V/II.149. 31 de diciembre de 2013. Para. 109. Obtenido el 6 de febrero de 2015, de http://www.oas.org/es/cidh/docs/anual/2013/informes/LE2013-esp.pdf

la libertad de expresión de los ciudadanos si los individuos carecen del derecho a leer y comunicarse anónimamente. Los académicos han dejado claro que "la interdependencia cercana entre la recepción y expresión de información y entre la lectura y la libertad de pensamiento hacen del reconocimiento de ese derecho [el derecho a leer anónimamente] una buena política constitucional.[14]

En otras palabras, el derecho a buscar y recibir información es inhibido cuando los gobiernos u otros disponen de acceso irrestricto a los registros que documentan los hábitos de vista o lectura de los individuos:

> "Una vez que los gobiernos pueden demandar de un editor los nombres de los compradores de sus publicaciones, la prensa libre como la conocemos desaparece. Entonces el espectro de una agencia de gobierno mirará sobre los hombres de cualquiera que lee··· El miedo a la crítica acompaña a cada persona en las estanterías de libros··· Algunos temerán leer lo que es impopular, lo que les disgusta a los poderes establecidos··· El miedo toma el lugar de libertad en las bibliotecas, librerías y hogares del país. A través del hostigamiento a las audiencias, investigaciones, informes y citaciones; el gobierno tendrá un palo sobre la expresión y sobre la prensa".[15]

Incluso la existencia de estos registros basta para un efecto inhibitorio, especialmente considerando que muchos lectores no sólo temen el rastreo gubernamental de sus hábitos de lectura, sino también el descubrimiento por parte de los miembros de su familia u otros colaboradores cercanos.

Como señala el autor Michael Chabon "si no hay privacidad de pensamiento —que incluye implícitamente el derecho a leer lo que uno quiere, sin la aprobación, consentimiento o conocimiento de otros— entonces no hay privacidad, punto".[16]

---

[14] Julie Cohen (1996). *A Right to Read Anonymously: A Closer Look at "Copyright Management" In Cyberspace,* 28 CONN. L. REV. 981.

[15] Véase United States v. Rumely, 345 U.S. 41, 57 (1953) (Douglas, J., concurring). Obtenido el 6 de febrero de 2015, de https://supreme.justia.com/cases/federal/us/345/41/

[16] EFF. *Google Book Search Settlement and Reader Privacy.* Obtenido el 6 de febrero de 2015, de https://www.eff.org/pages/google-book-search-s

Libertad de prensa y protección de las fuentes

Un corolario bien establecido del derecho a la libre expresión es la importancia de una prensa funcional y libre. Para tal fin, el principio básico de que los periodistas tienen derecho a proteger sus fuentes está muy bien establecido en la ley internacional.[17] En particular la CIDH dejó claro que:[18]

> "Una de las bases primarias del derecho a la reserva se constituye sobre la base de que el periodista, en su labor de brindar información a las personas y satisfacer el derecho de las mismas a recibir información, rinde un servicio público importante al reunir y difundir información que de otra forma, sin guardar el secreto de las fuentes, no podría conocerse. Asimismo, el secreto profesional consiste en "guardar discreción sobre la identidad de la fuente para asegurar el derecho a la información; se trata de dar garantías jurídicas que aseguren su anonimato y evitar las posibles represalias que pueda derivar después de haber revelado una información".[19]

Por otra parte, la CIDH ha señalado que el "derecho a la reserva de sus fuentes de información, apuntes y archivos personales y profesionales", se extiende a todo comunicador social incluyendo a los periodistas.[20]

Fuentes como los denunciantes dentro del gobierno necesitan las protecciones más fuertes en contra de ser expuestos, incluso por actores armados con todo el poder del Estado. En la era de Internet, cualquier persona puede ser una fuente así, y cualquier persona puede tener la responsabilidad de proteger las fuentes, ya que realizan el papel de un periodista o comunicador social.

---

[17] Así lo han reconocido el Parlamento Europeo, el Comité de Ministros del Consejo Europeo y la Comisión Interamericana de Derechos Humanos.

[18] CIDH. *Antecedentes e Interpretación de la Declaración de Principios sobre la Libertad de Expresión*. Obtenido el 6 de febrero de 2015, de http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=132&lID=2

[19] Véase Marc Carrillo (1993). La clausura de conciencia y el secreto profesional de los periodistas. Civitas y Centro de Investigación, Barcelona. p. 170

[20] Véase también CIDH. Principio 8 de la *Declaración de Principios sobre Libertad de Expresión*: "Todo comunicador social tiene derecho a la reserva de sus fuentes de información, apuntes y archivos personales y profesionales". Obtenido el 6 de febrero de 2015, de http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=26&lID=2

Privacidad y Libertad de expresión

La cuestión del anonimato en línea también incorpora necesariamente preocupaciones respecto a la expresión y la privacidad, y el cuidadoso análisis de la interacción entre ambos derechos. Como se indica en el Informe de 2011 de la Relatoría Especial de la ONU sobre la promoción y protección del derecho a la libertad de opinión y de expresión, "El derecho a la privacidad es esencial para que las personas se expresen libremente".[21]

Basándose en esto, el Relator Especial de la CIDH sobre Libertad de Expresión señaló que en vista de esta estrecha relación entre la libertad de expresión y la privacidad:

> "Tanto el derecho a la libertad de pensamiento y expresión como el derecho a la vida privada protegen al discurso anónimo frente a restricciones estatales. La participación del debate público sin revelar la identidad del emisor es una práctica usual en las democracias modernas. La protección del discurso anónimo favorece la participación de la personas en el debate público ya que –al no revelar su identidad— pueden evitar ser objeto de represalias injustas por el ejercicio de un derecho fundamental. En efecto, quienes ejercen el derecho a la libertad de pensamiento y de expresión participan del debate público y de la vida política de una comunidad. Ello no supone –solamente— escribir notas de opinión o participar en foros de debate: también supone la posibilidad de llamar a movilizaciones sociales, de convocar a otros ciudadanos a manifestarse, de organizarse políticamente o de cuestionar a las autoridades, aun en situaciones de riesgo".[22]

[21] Véase p. ej., *Informe del Relator Especial sobre la promoción y la protección del derecho a la libertad de opinión y de expresión*, Frank La Rue (2011). Consejo de Derechos Humanos, O.N.U. Doc. A/HRC/17/27 pág. 15

[22] CIDH (2013). *Informe de la relatoría especial para la libertad de expresión*. Capítulo IV (Libertad de expresión e internet). OEA /Serv.L/V/II.149. Par. 134. Obtenido el 6 de febrero de 2015, de http://www.oas.org/es/cidh/expresion/docs/informes/2014_04_22_IA_2013_ESP_FINAL_WEB.pdf

La Declaración de Ministros del Comité Europeo sobre la libertad de comunicación en Internet también ha observado:

> "Con el fin de garantizar la protección contra la vigilancia en línea y de promover la libre expresión de la información y las ideas, los Estados miembros deben respetar la voluntad de los usuarios de Internet de no revelar su identidad".[23]

Un anonimato lo suficientemente fuerte para los Derechos Humanos

El derecho al anonimato se basa en estos derechos humanos fundamentales. El anonimato es una condición previa esencial para el ejercicio de los derechos a la intimidad y la libertad de expresión y debe ser garantizado por el Estado.

El anonimato no debe ser restringido *a priori*. La divulgación forzada sólo debe ocurrir una vez que se haya cometido un delito tipificado legalmente. Los derechos al debido proceso de un interlocutor deben ser respetados antes de identificar a esa persona en respuesta a una solicitud de hacerlo. Los regímenes legales deben garantizar un examen riguroso de los derechos de libre expresión y privacidad del interlocutor antes de forzar identificación alguna.

En muchas de las funciones sociales centrales del anonimato, los interlocutores están defendiendo su identidad de grupos o individuos que pueden esgrimir poderes estatales o institucionales aliados. Por lo tanto, un anonimato fuerte —donde no se mantienen registros y donde las herramientas que protegen la privacidad ocultan la identidad de un individuo— debe estar siempre disponible.

[23] Council of Europe (2003). *Declaration on freedom of communication on the Internet* (Adoptado por el Consejo de Ministros en la 840va reunión de Delegados de Ministros). Artículo 7 sobre Anonimato. Obtenido el 6 de febrero de 2015, de https://wcd.coe.int/ViewDoc.jsp?id=37031

Problemas con el anonimato digital

El anonimato es necesario para la privacidad digital

El anonimato involucra más que esconder el nombre de uno. Más bien, implica la capacidad de mantener la confidencialidad de una amplia variedad de actividades propias en línea, incluyendo la ubicación, la frecuencia de las comunicaciones, y tantos otros detalles. El anonimato en línea debe entenderse no sólo como el estado de no ser identificado por terceros, sino también como la cualidad de ser *incognoscible* para terceros.

La conceptualización del derecho al anonimato en línea como el derecho a participar libremente en cualquier actividad en línea sin revelar el nombre de uno a cualquiera es incompleta. De hecho, la relatora de la CIDH (2013) explicó que la protección a la vida privada implica al menos dos políticas específicas relacionadas con el ejercicio de la libertad de pensamiento y de expresión: "la protección del discurso anónimo y la protección de datos personales".

El *anonimato en línea* también incluye una amplia gama de cuestiones de protección de datos, y la capacidad de ser imposible de encontrar en un medio que graba, por defecto estructural, todo lo que una persona hace —potencialmente hasta las teclas que uno presiona. Cada transacción en línea, ya sea enviando un simple correo electrónico o visualizando un sitio web popular, puede generar metadatos de comunicación, es decir información asociada a una transacción en línea que no es parte del contenido de un mensaje en sí. Por ejemplo, un correo electrónico de la Persona A a la Persona B a través de un proveedor de correo electrónico como Google o Yahoo revela que estas personas están en contacto la una con la otra, y contiene información adicional relacionada con dónde estuvo la Persona A cuando envió el correo electrónico, la hora en ese lugar cuando se envió el correo electrónico, el software que la Persona A utilizó para

componer el correo electrónico y, con frecuencia, la línea de asunto del correo electrónico.[24]

De manera similar, si una Persona A visita un sitio web popular como bing.com, el sitio web conocerá la ubicación física de la Persona A, la hora a la que lo visitó y si previamente ha utilizado el mismo dispositivo para visitar el sitio web. Durante el proceso de enviar un correo electrónico o visitar un sitio web, la Persona A ha dado esta información a su proveedor de servicio de internet, como también a, potencialmente, un motor de búsqueda y muchos otros terceros que proporcionan servicios que permiten nuestro uso diario de Internet.

De hecho, este entendimiento de que el derecho de una persona a la intimidad no se limita al contenido de las comunicaciones, sino también al hecho de la comunicación y a la información sobre la comunicación (es decir, el punto de origen, duración, destinatario, etc.) no es nueva ni se limita a los medios de comunicación en línea.

Por otra parte, a pesar de que la información contenida en un solo correo electrónico, por ejemplo, podría no identificar al usuario, los metadatos de las comunicaciones pueden agregarse para crear perfiles detallados de individuos que contienen el nombre de la Persona A, sus hábitos de compra, intereses personales, afiliaciones religiosas, inclinaciones políticas, amigos, compañeros de trabajo, carrera, ambiciones, y otros aspectos íntimos de la identidad de la Persona A. Tal agregación no sólo es cada vez más común dado que la capacidad de procesamiento y almacenamiento de datos se vuelve más barata, sino que además se ha generado una industria centrada en esta agregación, análisis y reventa de datos.[25]

---

[24] Para una buena explicación sobre esto, http://whatismyipaddress.com/emailheader. Obtenido el 6 de febrero de 2015.

[25] Véase *Caso Escher y otros vs. Brasil* ¶ 114 (“Artículo 11 [el derecho a la privacidad] se aplica a las conversaciones telefónicas independientemente de su contenido e incluso, puede comprender tanto las operaciones técnicas dirigidas a registrar ese contenido, mediante su grabación y escucha, como cualquier otro elemento del proceso comunicativo mismo, por ejemplo, el destino de las llamadas que salen o el origen de las que ingresan, la identidad de los interlocutores, la frecuencia, hora y duración de las llamadas, aspectos que pueden ser

Puede que el anonimato débil sea fácil, pero el anonimato fuerte no lo es

Internet permite fácilmente un anonimato *superficial* —tal como el uso de un alias para comentarios o de correos electrónicos. En la década de 1990, los comentaristas a menudo veían al uso de seudónimos en línea como una razón por la que las comunicaciones por Internet eran altamente anónimas. En 1993, una tira cómica de Peter Steiner ampliamente distribuida mostraba un perro usando una computadora que le decía a otro: "en internet nadie sabe que eres un perro".[26]

Pero una preservación real del anonimato requiere más esfuerzo. Una gran cantidad de información sobre las comunicaciones en línea se graba rutinariamente. Dado que esta información puede ser recolectada, revelada o solicitada judicialmente, cualquier discusión sobre el anonimato en línea debe abordar qué información es revelada, a quién y bajo qué restricciones (si es que existe alguna).[27] A menudo la gente (o los perros) que no han revelado deliberadamente sus identidades legales en sus comunicaciones en línea han revelado a otros, no obstante, una amplia gama de datos que los identifican y potencialmente los identifican —a veces en formas que no son especialmente visibles o evidentes para los usuarios menos sofisticados.

Incluso cuando una plataforma le permite a la gente leer y escribir sin adjuntar sus nombres legales a estas actividades, el operador de la plataforma bien puede conocer quienes son sus usuarios con precisión, así como las ubicaciones particulares desde las cuales se han conectado, mediante el análisis de información como las direcciones del Protocolo de Internet (IP) de los usuarios. Así que la no utilización, conspicua o deliberada, de un nombre en línea de ninguna manera implica que una amplia gama de

---

constatados sin necesidad de registrar el contenido de la llamada mediante la grabación de las conversaciones"). Obtenido el 6 de febrero de 2015, de http://www.corteidh.or.cr/cf/jurisprudencia/ficha.cfm?nId_Ficha=277&lang=es. *Véase también* Análisis Jurídico Internacional de Apoyo y Antecendentes de los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones. Obtenido el 6 de febrero de 2015, de https://es.necessaryandproportionate.org/content/informaci%C3%B3n-protegida

[26] Wikipedia (2015). On the Internet, Nobody Knows You're a Dog. Obtenido el 6 de febrero de 2015, de https://en.wikipedia.org/wiki/On_the_Internet,_nobody_knows_you%27re_a_dog

[27] Por supuesto, existe una gran cantidad de herramientas de seguridad para proteger bits específicos de datos de comunicación.

entidades no sepan (o no puedan deducir) el nombre, historial en línea, y paradero de uno, al examinar los datos que los sistemas de comunicaciones han puesto a su disposición.

La diversidad de formas en las que el anonimato en línea se protege varía desde decisiones de los individuos de no usar sus nombres legales, pasando por las políticas y prácticas de algunos intermediarios (proveedores de servicios de telecomunicaciones, proveedores de correo electrónico y chat, foros en línea, entre otros) para evitar requerir el registro o uso de un nombre legal, a través de las políticas de retención de datos de los intermediarios, hasta el desarrollo y uso de herramientas de software que son diseñadas específicamente para tratar de asegurar el anonimato. Este último grupo comprende una porción de herramientas de software a menudo conocidas como Tecnologías de Mejora de la Privacidad (o PETS por sus siglas en inglés), pero muchas de las herramientas en esta categoría no tienen por objetivo proporcionar *anonimato*, sólo otras propiedades como secreto o confidencialidad de las comunicaciones.

Por ejemplo, un sobre o sello de cera pueden proveer protecciones más fuertes del secreto de una carta que una persona envía a otra, pero si la oficina postal o el mensajero tienen éxito al exigir que las cartas tengan información exacta sobre la dirección de sus remitentes y destinatarios, los patrones de quién está en contacto con quién todavía serían evidentes para aquellos que envían las cartas —no serán anónimos en ese sentido, incluso si los carteros nunca abren o intentar abrir clandestinamente nada de la correspondencia. En el entorno digital, la protección del anonimato es técnicamente más difícil de proporcionar respecto a otros tipos de protección de la privacidad.

Sólo unas pocas herramientas y sistemas de software, tales como el proyecto Internet invisible (I2P),[28] el proyecto TOR,[29] Jondo,[30] o SecureDrop[31] buscan proporcionar

[28] Wikipedia. I2P. Obtenido el 6 de febrero de 2015, de https://es.wikipedia.org/wiki/I2P
[29] The Tor Project. Obtenido el 6 de febrero de 2015, de https://www.torproject.org/
[30] JonDoNym, JonDo – the IP Changer. Obtenido el 6 de febrero de 2015, de https://anonymousproxyservers.net/en/jondo.html
[31] Freedom of the Press Foundation, SecureDrop. Obtenido el 6 de febrero de 2015, de https://freedom.press/securedrop

fuertes garantías técnicas al anonimato de sus usuarios incluso frente a un intento sofisticado de revelar la identidad de un usuario. Estos sistemas van más allá de la simple noción de no solicitar que la gente declare sus nombres; tratan de evitar la creación de un registro significativo que revelaría la identidad de un usuario.

Típicamente estas herramientas trabajan para ofuscar el vínculo entre el remitente y el destinatario de la información al enviar la información repetidamente a través de intermediarios que deliberadamente evitar grabar información sobre cómo fue enviada. Cuando múltiples partes independientes proveen eslabones en la cadena, ninguna entidad puede saber lo suficiente para asociar al remitente original con el destinatario final. Sin embargo, las investigaciones han mostrado que el anonimato así obtenido, todavía podría ser frágil, por ejemplo cuando un interceptor observa que el volumen de datos enviados por una parte coincide con el volumen de datos obtenidos por otra parte más o menos al mismo tiempo.[32]

Dados los medios técnicos para intercambiar mensajes anónimos, los desarrolladores de software pueden tratar de construir aplicaciones sobre estas plataformas, como en el caso de SecureDrop, que permite a las fuentes periodísticas contactar a organizaciones de prensa de forma anónima, y remitirles documentos anónimamente y, a cambio, recibir preguntas y respuestas.

Incluso los sistemas fuertes de anonimato más sofisticados tienen puntos débiles. Si, por ejemplo, un gobierno sospechara que probablemente un disidente tratará de expresarse anónimamente, podría colocar malware en el ordenador del disidente, grabando cada pulsación en el teclado. Mientras funcione el malware, la fortaleza del sistema de anonimato sería irrelevante porque el gobierno vigilaría las actividades y los contactos de la disidentes directamente.

[32] Véase *Selected Papers in Anonymity*, para investigación académica sobre las técnicas para lograr anonimato mediante métodos técnicos y sus limitaciones, desde 1977. Obtenido el 6 de febrero de 2015, de http://www.freehaven.net/anonbib/

Levantando el velo: Divulgación de identidad y el rol de los intermediarios

Todo individuo debe tener la confianza de que los proveedores de servicios que almacenan sus discusiones protegerán su privacidad y expresión. Los intermediarios de internet y proveedores de servicio ocupan una posición clave en las comunicaciones en línea. A diferencia de otros usuarios de internet, los intermediarios de internet y proveedores de servicio, a menudo saben la identidad de la persona que crea un sitio web o publica material en una plataforma.

Para proteger los derechos de los individuos a la expresión anónima, las leyes deben permitir y fomentar que los intermediarios de internet respeten los derechos al debido proceso de un interlocutor en línea antes de identificar a dicho individuo en respuesta a un pedido de hacerlo. La revelación obligada sólo debe ocurrir una vez que un delito tipificado en la ley ha sido cometido. E incluso en esos casos, todos los derechos de un interlocutor en línea deben ser considerados antes de la identificación de esa persona en respuesta a una solicitud de hacerlo.

Como bien señaló la Comisión Interamericana de Derechos Humanos:

> "[La protección del anonimato] no significa, sin embargo, que el anonimato resguarde a cualquier tipo de información. Por ejemplo, el anonimato del emisor de ninguna manera protegería a quien difunda pornografía infantil, a quien hiciera propaganda a favor de la guerra o apología del odio que constituya incitación a la violencia o incitare pública y directamente al genocidio. Estos discursos no están protegidos por la Convención Americana y el anonimato no puede resguardar a los emisores de las consecuencias jurídicas que cada ordenamiento interno establezca —de conformidad con el derecho internacional de los derechos humanos— respecto de cada uno de esos casos. Lo mismo ocurriría en el caso de que el ejercicio del derecho a la libertad de pensamiento y expresión fuera objeto de responsabilidades ulteriores del tipo que autoriza la Convención Americana. En todos esos casos, las autoridades judiciales estarían autorizadas para tomar medidas razonables tendientes a descubrir la identidad del emisor de conductas

prohibidas para aplicar la respuesta proporcionada que prevé el ordenamiento jurídico".[33]

Los sistemas judiciales, no los procesos de toma de decisiones extrajudiciales, son los más adecuados para equilibrar el derecho de los ciudadanos a la expresión anónima con la necesidad de proporcionar un mecanismo para corregir errores.[34] Por lo tanto, es imperativo que la ley no requiera o permita a los intermediarios de Internet revelar la identidad de los usuarios sin una decisión judicial. Pero los sistemas judiciales sólo pueden funcionar cuando una corte ha tenido la oportunidad de revisar las circunstancias antes de que la identidad haya sido revelada. Por tanto, para proteger los derechos fundamentales de los ciudadanos a la libre expresión y privacidad, los intermediarios de Internet sólo deben revelar la identidad de un usuario de su plataforma anónimo o seudónimo tras recibir una orden judicial, concedida después de un proceso de revisión judicial.

Cuando un individuo publica contenido en Internet, puede que terceras personas quieran demandar al individuo por publicar contenido supuestamente difamatorio o ilegal. Para hacerlo, el demandante deberá identificar al interlocutor en línea.

Como mejores prácticas, esas terceras personas deberán:

- Realizar esfuerzos razonables para notificar a la persona cuya identidad está siendo demandada;

---

[33] CIDH (2013). *Informe de la relatoría especial para la libertad de expresión*. Capítulo IV (Libertad de expresión e internet). OEA /Serv.L/V/II.149. Par. 135. Obtenido el 6 de febrero de 2015, de http://www.oas.org/es/cidh/expresion/docs/informes/2014_04_22_IA_2013_ESP_FINAL_WEB.pdf

[34] En los Estados Unidos, antes de que un proveedor de servicios pueda ser obligado a entregar la identidad de alguien que ha publicado de forma anónima, muchos tribunales aplican una prueba muy exigente y únicamente ordena la divulgación de las identidades sólo cuando "es apropiado en el caso excepcional de que la necesidad imperiosa para el develamiento solicitado supera" los derechos de libre expresión de la persona que desea permanecer en el anonimato. Véase, por ejemplo, *Doe v. 2theMart.com*, 140 F. Supp. 2d 1088, 1095 (W.D. Wash. 2001).

- Si es posible, acordar a un calendario para la divulgación de la información a la parte solicitante que ofrezca una oportunidad razonable para que el usuario de Internet presente una reclamación ante un tribunal antes de la divulgación;
- Remitir las declaraciones exactas y materiales proporcionados por la persona que solicita la identidad, incluyendo información sobre la causa de la acción alegada en la demanda y las pruebas aportadas por la parte demandante a la corte cuando se han facilitado al proveedor de servicios.[35]

A los usuarios se les debe proveer una cantidad de tiempo razonable para responder, antes que el proveedor de servicio produzca la información requerida. Esto brindará al usuario una oportunidad para hacer objeciones a la divulgación de su identidad.[36]

Si bien los intermediarios son vistos a menudo como una fuente clave de información que puede levantar el velo del anonimato en línea, no son para nada la única fuente. Como hemos visto, la fragilidad de ocultar la identidad de frente al sofisticado análisis de datos y a la detección y almacenamiento de datos en todas las formas de comportamiento cotidiano (desde caminar por una calle con circuitos cerrados de televisión hasta adquirir bienes electrónicamente) significa que la identidad de los sospechosos puede ser comprobada mediante el trabajo policial determinado y específico.[37] Por tanto, no se les debe requerir a los intermediarios rastrear a todos sus

[35] Esta prueba refleja la ley de EE.UU. sobre el tema. Véase EFF, *Test for Unmasking Anonymous Speech*, Internet Law Treatise. Obtenido el 6 de febrero 2015, de http://ilt.eff.org/index.php/Speech:_Anonymity#Tests_for_Unmasking_Anonymous_Speakers

[36] Véase EFF, Best Practices for Online Service Providers. Obtenido el 6 de febrero de 2015, de http://www.eff.org/wp/osp. Las cortes canadienses también han desarrollado una prueba para determinar si se debe ordenar o no a un tercero, tal como un ISP, la divulgación de la identidad de un acusado anónimo en escenarios donde existe una expectativa razonable de privacidad o donde están implicadas preocupaciones por la libertad de expresión. Si bien existen variantes, la prueba busca asegurar que la orden sea necesaria, que el litigante tiene la intención de perseguir la reclamación y que la indemnización sea legalmente válida. Véase Canadian Internet Policy and Public Interest Clinic, *Online Anonymity & John/Jane Doe lawsuits*. Obtenido el 6 de febrero de 2015, de https://cippic.ca/index.php?q=onlineanonymityanddoelawsuits

[37] Véase, por ejemplo, *How Informants, Undercover Agents And Old-Fashioned Police Work*

usuarios (eliminando de este modo el anonimato fuerte para todos los usuarios). Tampoco se les debería hacer responsables de las acciones de los usuarios que no son identificables como resultado de las acciones o inacción del intermediario.

En algunos casos excepcionales, puede ser difícil, sino imposible, identificar a un interlocutor después del hecho. Por ejemplo, si alguien realizar una única publicación en un foro en línea desde el Wi-Fi de un "cafenet" popular que no tiene registros de sus clientes o cámaras en los sectores aledaños. Esto no es nada nuevo de la era de Internet; por siglos la gente ha podido escribir grafitis en la oscuridad de la noche, comunicándose anónimamente. De hecho, es mucho más difícil en la era moderna comunicarse exitosamente sin dejar huellas delatoras. Si bien puede haber un interés legítimo en desenmascarar a interlocutores que han violado una ley, requerir que siempre sea posible desenmascarar a alguien es un precio demasiado alto.

Políticas de anonimato de actores no gubernamentales

Una forma para que un interlocutor proteja su anonimato es no revelar su identidad a los intermediarios. Estos intermediarios pueden ser obligados a revelar esa información al gobierno o a litigantes particulares. Muchos intermediarios emplean procedimientos de autenticación que requieren la divulgación y registro de identidad y otros datos personales, creando así bases de datos individualmente identificables de la actividad del usuario. El uso de tales herramientas no siempre es irracional, pero tales procedimientos deben utilizarse con moderación y en proporción a la preocupación que el intermediario está tratando de resolver. Como lo señaló la Relatoría de Libertad de Expresión de la CIDH:

> "Los requerimientos de identificación y autenticación en línea deben ser utilizados exclusivamente en transacciones e interacciones sensibles y riesgosas, y no de manera generalizada para todos los servicios y aplicaciones. Los requerimientos de autenticación deben seguir el principio de proporcionalidad, que en este caso indica que si el riesgo es alto se

Brought Down The Silk Road. Obtenido el 6 de febrero de 2015, de http://www.ibtimes.com/how-informants-undercover-agents-old-fashioned-police-work-brought-down-silk-road-1807130

> justifica recoger información adicional del usuario. Sin embargo, si el riesgo es bajo, no habrá razón para hacerlo. Este balance permite, entre otros, favorecer plataformas y servicios anónimos en Internet, los cuales posibilitan la libertad de expresión en contextos represivos o de autocensura. Asimismo, el principio de diversidad indica que deben favorecerse múltiples esquemas de identificación para los usuarios en línea, de manera que no existan identificadores únicos o concentrados, que propicien abusos de seguridad e intrusiones a la privacidad."[38]

Como se indica en el Informe Anual de 2013 de la Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos (Párr. 23): "se debe promover la existencia de espacios en línea libres de observación o documentación de la actividad e identidad de los ciudadanos. Esto incluye, por ejemplo, la preservación de plataformas anónimas para el intercambio de contenidos y el uso de servicios de autenticación proporcionales".

Por ejemplo, los términos de servicio de Facebook requieren que sus usuarios proporcionen sus nombres e información reales.[39] Esta práctica crea serios riesgos particularmente para los disidentes y activistas de derechos humanos que usan sus nombres en Facebook en regímenes autoritarios. La transmisión de dichos identificadores, si se cosechan en masa, también se puede utilizar para identificar otra actividad anónima de navegación en línea.

Esto crea un efecto negativo: si se violan los términos de servicio de Facebook, Facebook puede desactivar la cuenta de un individuo. Dada la ubicuidad actual de

---

[38] CIDH (2013). *Informe de la relatoría especial para la libertad de expresión*. Capítulo IV (Libertad de expresión e internet). OEA /Serv.L/V/II.149. Par. 136. Obtenido el 6 de febrero de 2015, de http://www.oas.org/es/cidh/expresion/docs/informes/2014_04_22_IA_2013_ESP_FINAL_WEB.pdf

[39] Facebook, *Statement of Rights and Responsibilities*. Obtenido el 6 de febrero de 2015, de https://www.facebook.com/terms.php

Facebook, se corre el riesgo de apagar una vía clave para el discurso político.[40] La forma en que se aplican estas políticas contra el anonimato, somete a las poblaciones más vulnerables —es decir, las personas con enemigos u opiniones impopulares— a mayores riesgos debido a la facilidad con la que otro usuario puede informar sobre ellos y, por lo tanto, suspender su cuenta. Por ejemplo, cuando un usuario reporta el uso de un nombre "falso", Facebook le pedirá al usuario presentar su identificación oficial. Para los usuarios con seudónimo, esto es imposible; esto también implica otros riesgos para la privacidad.

La regulación del anonimato

Políticas positivas para la regulación del anonimato

Estados Unidos

En Estados Unidos, la Corte Suprema ha dictaminado que el derecho a hablar anónimamente está protegido por la Primera Enmienda. La Corte Suprema ha sostenido que: "El anonimato es un escudo frente a la tiranía de la mayoría [que] ejemplifica el propósito [de la Primera Enmienda] para proteger a los individuos impopulares de represalias (...) a manos de una sociedad intolerante".[41] La Corte Suprema también ha dicho que la "identificación [forzada] y el miedo a las represalias podría disuadir discusiones perfectamente pacíficas sobre asuntos públicos importantes".[42]

La Corte Suprema de EE.UU. ha señalado, además, que los tribunales deben "estar vigilantes [y] protegerse contra obstáculos indebidos a las conversaciones políticas y el intercambio de ideas".[43] Esta revisión vigilante "debe ser llevada a cabo y analizada sobre la base de cada caso (...) donde el principio guía [de la corte] es un resultado basado en un

---

[40] Eva Galperin, *EFF Calls for Immediate Action to Defend Tunisian Activists Against Government Cyberattacks*, EFF, enero 2011. Obtenido el 6 de febrero de 2015, de https://www.eff.org/deeplinks/2011/01/eff-calls-immediate-action-defend-tunisian

[41] *McIntyre v. Ohio Elections Comm'n,* 514 U.S. 334. Obtenido el 6 de febrero de 2015, de http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=us&vol=514&invol=334

[42] *Talley v. California*, 362 U.S. 60 65 (1960). Obtenido el 6 de febrero de 2015, de http://caselaw.lp.findlaw.com/scripts/getcase.pl?navby=case&court=us&vol=362&invol=60

[43] *Buckley*, 525 U.S. at 192. Obtenido el 6 de febrero de 2015, de http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=us&vol=525&invol=182

análisis significativo y un equilibrio adecuado de los derechos de participación en litigio".[44] Esa revisión debe llevarse a cabo independientemente de si el discurso en cuestión toma la forma de panfletos políticos o publicaciones en Internet o cualquier otra cosa.[45]

Como resultado, las cortes estadounidenses se han protegido fuertemente en contra de la divulgación obligada de identidades en una variedad de situaciones: los derechos de las organizaciones a mantener la identidad de sus miembros como confidencial,[46] y los derechos de los usuarios en línea para asegurarse que los intermediarios no se vean obligados a divulgar sus identidades a menos que tal revelación sea realmente necesaria. Como explicó una corte tratando este último tema:

> "A la gente se les permite interactuar mediante seudónimos y de forma anónima entre sí, siempre que estos actos no estén en violación de la ley. Esta capacidad de expresar los pensamientos propios sin la carga de que la otra parte conoce todos los hechos acerca de la identidad de uno puede promover la comunicación abierta y robustecer el debate".[47]

Otras decisiones judiciales en los Estados Unidos han apoyado el derecho de leer de forma anónima en Internet al negar la ejecución de órdenes judiciales que hubieran obligado a un editor a divulgar la identidad de los suscriptores a sus materiales.[48]

Canadá

Otras jurisdicciones también han reconocido la importancia del anonimato como un elemento integrante del derecho a la intimidad. La Corte Suprema de Canadá, en

---

[44] *Dendrite Int'l, Inc. v. Doe.* Obtenido el 6 de febrero de 2015, de http://www.dmlp.org/threats/dendrite-international-v-does

[45] *Reno v. ACLU*, 521 U.S. 844

[46] Véase, por ejemplo, *NAACP v Alabama*, 357 U.S. 449 (1958), *Perry v Schwarzenegger*, 591 F.3d 1126 (9th Cir. 2009)； *Britt v. Superior Court*, 20 Cal. 3d 824 (1978).

[47] *Columbia Insurance Co. v. Seescandy.com*, 185 F.R.D. 573, 578 (N.D. Cal. 1999). Obtenido el 6 de febrero de 2015, de http://archive.today/hsK6

[48] L*ubin v. Agora, Inc* ., 389 Md. 1, 22, 882 A.2d 833, 846 (2005). Obtenido el 6 de febrero de 2015, de http://caselaw.findlaw.com/md-court-of-appeals/1237646.html. Véase también *Tattered Cover v. The City of Thornton*, 2002 Colo. LEXIS 269 (2002). Obtenido el 6 de febrero de 2015, de https://scholar.google.com/scholar_case?case=8628043461770653869, sobre el derecho de las librerías de mantener los registros de compra de libros de sus clientes como confidenciales.

particular, ha publicado recientemente una declaración para la protección del anonimato de las personas en línea —en el momento de la divulgación— cuando dictaminaron que la adquisición de una identidad de usuario por parte de la policía, sin orden judicial, es inconstitucional, declarando:

> "Es de particular importancia, en el contexto del uso de Internet, la comprensión de la privacidad como anonimato. Debe reconocerse que el uso de Internet, vinculado a la identidad de una persona, se acompaña de un interés que va más allá de la intimidad inherente al nombre de la persona, dirección y número de teléfono que se encuentra en la información de los suscriptores. La información de abonado, que tiende a vincular determinados tipos de información a personas identificables, puede poner en riesgo intereses de privacidad relacionados con la identidad de un individuo como la fuente, poseedor o usuario de dicha información. Cierto grado de anonimato es una característica de gran parte de la actividad de Internet y en función de la totalidad de las circunstancias, el anonimato puede ser la base de un interés privado que involucra la protección constitucional contra registros e incautaciones irrazonables. En este caso, la solicitud de la policía para vincular una dirección IP a la información del suscriptor era en efecto una solicitud para vincular una persona específica a actividades específicas en línea. Este tipo de petición involucra el aspecto del anonimato de interés sobre la privacidad de la información al tratar de vincular al sospechoso con las actividades en línea realizadas de forma anónima, actividades que —como ha sido reconocido en otras circunstancias— involucran intereses por una privacidad significativa… La divulgación de esta información a menudo equivale a la identificación de un usuario con actividades íntimas o sensibles que se están llevando a cabo en línea, por lo general en el entendido de que estas actividades serían anónimas. Una petición por parte de un oficial de policía para que un ISP revele voluntariamente dicha información equivale a una búsqueda".[49]

Corea del Sur

En 2007, el poder legislativo surcoreano aprobó el artículo 44-5 de la Ley de Red, Información y Comunicación ("ICNA", en adelante), que obliga a todos los intermediarios de Internet que reciben más de 100.000 usuarios diarios promedio a aceptar envíos únicamente por parte de aquellos usuarios que verifiquen su identidad. El propósito

[49] *R. v. Spencer*, 2014 SCC 43, 13 de junio de 2014

legislativo de esta disposición era hacer la identidad de los usuarios que publicaban '"rastreable" y con ello impedir las actividades ilegales en línea. Sin embargo, no hubo evidencia de que las actividades ilegales disminuyeran con el tiempo según lo revelado por seis estudios empíricos, entre ellos uno encargado por el propio gobierno.[50] Cinco años más tarde, el Tribunal Constitucional de Corea del Sur revocó la disposición ICNA y tomó la decisión como una oportunidad para hacer probablemente la declaración más refinada sobre la relación entre el discurso anónimo en línea y la democracia de la siguiente manera:[51]

> "El discurso anónimo en Internet, al propagarse rápida y recíprocamente, permite a las personas a superar la jerarquía económica o política fuera de línea y, por lo tanto, permite formar la opinión pública libre de la clase, estatus social, edad y distinciones de género, y hace que la gobernabilidad se semeje más a un reflejo de la opiniones de personas de diversas clases y, por lo tanto, promueve la democracia. Por lo tanto, el discurso anónimo en Internet, aunque plagado de efectos secundarios nocivos, debe ser fuertemente protegido en vista de sus valores constitucionales".

Asimismo, el Tribunal razonó claramente sobre por qué la identificación obligatoria de usuarios es casi siempre desproporcionada de la siguiente manera:

> "Aquí la regla exige la verificación de identidad, independientemente del contenido de la publicación de casi todos los usuarios en todos los sitios web principales. Muchos futuros usuarios que publican, no del todo seguros de lo que es una publicación prohibida, probablemente renunciarán totalmente a publicar por temor a la disciplina o el enjuiciamiento, este riesgo se deriva de la exposición de los nombres y los números de registro de residente. Tal resultado de la supresión de publicaciones legales de una gran mayoría habida cuenta de la existencia de una minoría de personas que abusan de Internet es una restricción excesiva a la libertad de expresión

[50] Para una discusión sobre estos seis artículos, véase PARK Kyung Sin, *Freedom of Speech and Communications – Theories and Practices* (표현 통신의 자유), publicado por NonHyung(논형) en 2013, pp. 433-435

[51] Decisión del Tribunal Constitucional de 2010 Hunma 47, 252 (consolidado) anunciado el 28 de agosto 2012

> en el anonimato (⋯) trata a todos como potenciales criminales en favor de la conveniencia de investigación".

México

El anonimato ha sido protegido como una condición previa para el ejercicio de la confidencialidad de las fuentes y el derecho al secreto profesional periodístico. La Suprema Corte de Justicia ha manifestado, por ejemplo, que:

> "El periodista tiene el derecho de mantener la identidad secreta de las fuentes que le han dado información en condición reservada, expresa o implícita. Por lo tanto, (...) el reportero llamado a declarar en los procesos civiles, podrá invocar su derecho al secreto y rehusarse a identificar sus fuentes y negarse a dar respuestas que podrían revelar la identidad de las mismas".

La legislación mexicana Federal y del Distrito Federal también reconoce este derecho. Por ejemplo, el Código Federal de Procedimientos Civiles reconoce el secreto profesional, que se opone a la obligación de presentar documentos y proporcionar todo tipo de asistencia a los tribunales en sus investigaciones.[52] Asimismo, el Código Federal de Procedimientos Penales reconoce que los periodistas no están obligados a declarar sobre la información que reciban, conozcan o tengan en su poder

> "Los periodistas, respecto de los nombres o las grabaciones, registros telefónicos, apuntes, archivos documentales y digitales y todo aquello que de manera directa o indirecta pudiera llevar a la identificación de las personas que, con motivo del ejercicio de su actividad, les proporcionen como información de carácter reservada, en la cual sustenten cualquier publicación o comunicado".[53]

El nuevo Código de Procedimiento Penal, que entrará en vigor gradualmente en todo el país de México, también reconoce este derecho.[54] Por último, la Ley Del Secreto Profesional Del Periodista En El Distrito Federal otorga una amplia protección a

---

[52] Artículo 90 del Código Federal de Procedimientos Civiles de México.

[53] Artículo 243 Bis del Código Federal de Procedimientos Penales de México.

[54] Véase Artículos 244 y 362. Nuevo *Código Nacional de Procedimientos Penales*. Obtenido el 6 de febrero de 2015, de http://dof.gob.mx/nota_detalle.php?codigo=5334903

periodistas y medios de comunicación asociados.[55] Estas protecciones incluyen el derecho a la reserva de la identidad de sus fuentes; el derecho a no ser obligados a reportar datos o hechos difundidos que son parte del periodismo de investigación; el derecho a no ser objeto de inspección por parte de cualquier autoridad que desea tener acceso a las notas de los periodistas, equipos de grabación, computadoras, directorios, registros telefónicos y cualquier documento que pueda conducir a la identificación de las fuentes de la grabación, el derecho a no ser sometido a la inspección de sus datos personales, entre otros.

Estas decisiones establecen una política y principios fuertes para la protección del anonimato.

Políticas que socavan el derecho al anonimato

Corea del Sur

En general, las prácticas de Corea del Sur no pueden ser consideradas únicamente como las mejores prácticas, porque incluso con la histórica decisión de su Corte Constitucional, otros tres requisitos de verificación de identidad siguen vigentes: [1] Los artículos 82-6 (1) y 82-6 (5) de la Ley de Elección de Funcionarios Públicos, requieren que prácticamente todos los intermediarios de Internet importantes acepten publicaciones creadas por los usuarios para apoyar u oponerse públicamente a un candidato durante un período de campaña electoral (por lo general 23 semanas) sólo cuando los usuarios verifiquen su identidad;[56] [2] El artículo 16 (4) de la Ley de Protección de Menores, que requiere que todos los intermediarios de Internet que ponen a disposición material para adultos verifique de antemano la identidad de los usuarios de ese material;[57] [3] El artículo 12 (3) Párrafo 1 Ítem 1 de la Ley de Promoción de la Industria de Juegos, que

[55] *Ley Del Secreto Profesional Del Periodista En El Distrito Federal*. Obtenido el 6 de febrero de 2015, de http://www.aldf.gob.mx/archivo-86d0c120a3269ea2302bc5179d543a1f.pdf

[56] *Public Officials Election Act*. Obtenido el 6 de febrero de 2015, de http://elaw.klri.re.kr/kor_service/lawView.do?hseq=25035&lang=ENG

[57] *Juveniles Protection Act*. Obtenido el 6 de febrero de 2015, de http://elaw.klri.re.kr/kor_service/lawView.do?hseq=27676&lang=ENG

requiere que todos los proveedores de "juegos de Internet" verifiquen de antemano la edad y, por lo tanto, la identidad de los jugadores.[58]

Las deficiencias más evidentes en la protección del anonimato en línea son las leyes que requieren o permiten a los intermediarios de Internet revelar la identidad de los usuarios sin una orden judicial o cualquier otra aprobación judicial. Estados Unidos,[59] Reino Unido,[60] Alemania[61] y Francia;[62] todos fallan en este sentido, pero las políticas de Corea del Sur han llevado a la divulgación masiva de identidades de usuario por parte de los intermediarios de Internet a la policía sin orden judicial, llegando hasta un 20% de toda la población del país en algunos años.[63] En un intento por frenar esta práctica, un tribunal de apelación intermedio de Corea en octubre de 2012 declaró a un importante sitio web responsable de la divulgación de la identidad de un blogger a la policía que investigaba un caso de difamación contra un político que se produjo sin orden judicial. La decisión dio lugar a que los proveedores de contenidos y aplicaciones de Internet detengan por completo el suministro de datos sin una orden judicial. Las empresas de telecomunicaciones coreanas mantienen la práctica.

Brasil

En Brasil, la Constitución prohíbe el discurso anónimo.[64] La intención detrás de esta prohibición es mantener la posibilidad de identificar a cualquiera que exprese sus opiniones, creencias o comentarios, tanto en línea como en el mundo fuera de línea. Como hemos expresado previamente en este documento, el anonimato es un prerrequisito para la libertad de expresión y la privacidad, las cuales hacen posible que los ciudadanos se expresen libremente y sin miedo a represalias. Al no permitir que los ciudadanos brasileños participen del discurso anónimo, la Constitución impone obstáculos

[58] *Game Industry Promotion Act*. Obtenido el 6 de febrero de 2015, de http://elaw.klri.re.kr/kor_service/lawView.do?hseq=28802&lang=ENG
[59] 18 U.S. Code, Secciones 2703(c)(1)(E), (2)
[60] UK Regulation of Investigatory Powers Act 2000, Artículo 23
[61] Federal Electronic Communications Act, Artículo 113 (1)
[62] Code des Postes et Communications Électroniques, Artículos L34-1 al L34-6
[63] Park Kyung Sin, *Communications Surveillance in Korea*. Obtenido el 6 de febrero de 2015, de https://eff.org/r.internetsurveillanceprivacy987
[64] Constitución de la República Federativa de Brasil de 1988, artículo 5, IV: "la expresión del pensamiento es libre, quedando prohibido el anonimato".

significativos a su capacidad de reportar abusos de poder o expresar opiniones impopulares.No obstante, esta prohibición no se extiende a la protección de la privacidad.

A pesar de que el uso de seudónimos no está prohibido explícitamente por la Constitución brasileña, la prohibición de discurso anónimo se ha utilizado como base legal para la revelación de las solicitudes de identidad, que a menudo son concedidos por los tribunales brasileños. Esta práctica ha estado liderando la consolidación de la jurisprudencia que toma una postura firme en contra del uso de perfiles no reales.[65]

El Marco brasileño de Derechos Civiles para Internet ("*Marco Civil da Internet*"), promulgado en 2014, enfatiza que la libertad de expresión es un principio fundamental para los usuarios de Internet en Brasil.[66] Sin embargo, esto tiene que ser interpretado bajo las limitaciones impuestas por la Constitución, dejando muy poco espacio para interpretaciones que podrían permitir el anonimato para los propósitos de la libre expresión.[67]

El Marco de los Derechos Civiles para Internet de Brasil también establece que la legislación brasileña debe ser aplicable a cualquiera de los productos o servicios utilizados por los individuos ubicados en Brasil.[68] Esta disposición ha permitido a los fiscales y

[65] Las investigaciones sugieren que en más del 48% de los casos, los jueces emitieron medidas cautelares que exigen la divulgación de información de identificación por parte de los intermediarios, como registros de aplicaciones y direcciones IP.

[66] Art. 2: "La disciplina de la utilización de Internet en Brasil se basa en el respeto a la libertad de expresión, así como (⋯)"

[67] Art. 3: "La disciplina de la utilización de Internet en Brasil cuenta con los siguientes principios: I – garantía de la libertad de expresión, la comunicación y la manifestación del pensamiento, según la Constitución; (⋯)".

[68] Art. 11: "En cualquier operación de recolección, almacenamiento, protección o tratamiento de registros, datos personales o de comunicaciones por proveedores de conexión y de aplicaciones de internet en las que por lo menos uno de estos actos ocurra en territorio nacional, deberá ser obligatoriamente respetada la legislación brasilera, los derechos a la privacidad y a la protección de los datos personales y al secreto de las comunicaciones privadas y de los registros. §1º Lo dispuesto en el artículo se aplica a los datos recolectados en territorio nacional y al contenido de las comunicaciones en las cuales por lo menos uno de los dos está localizado en Brasil. §2º Lo dispuesto en este artículo se aplica también aunque las actividades sean llevadas a cabo por personas jurídicas domiciliadas en el exterior, siempre que oferten servicios al público brasileño o que al menos una integrante del mismo

oficiales encargados de hacer cumplir la ley reclamar que la prohibición constitucional sobre el discurso anónimo debe impedir el uso de aplicaciones de Internet que permiten la expresión anónima.

Un ejemplo reciente de esta restricción es la prohibición impuesta a "Secret", una aplicación de Internet que se promociona como un "lugar seguro para decir lo que está en su mente de forma anónima." Invocando la prohibición de la Constitución del Brasil, la Fiscalía presentó una demanda en contra del servicio, que rápidamente se había popularizado en Brasil. Aunque más tarde fue revocada, se concedió una medida cautelar para prohibir "Secret" en las tiendas de aplicaciones en línea (Google y Apple) en Brasil y retirarla de forma remota de dispositivos donde ya había sido instalada.

Este caso de alto perfil señala un peligro potencial de ampliar el alcance de la prohibición de la Constitución y su aplicación para evitar el uso de tecnologías que mejoran la privacidad, lo que también traería repercusiones indeseables a los derechos de lectura y navegación anónima.

Vietnam

En 2013, el gobierno de Vietnam aprobó el decreto 72 sobre "Gestión, Suministro, Uso de los Servicios de Internet y la Información de Contenidos en Línea" que prohibió el uso de seudónimos, obligando a las personas con blogs personales a listar públicamente su nombre y domicilio reales. El principal objetivo del decreto era privatizar la censura poniendo el peso de la tarea en las empresas de tecnología, y silenciar las voces disidentes que no están en línea con el Partido Comunista de Vietnam.

---

grupo económico posea un establecimiento en Brasil. §3º Los proveedores de conexión y de aplicaciones de internet deberán presentar, en línea con la reglamentación, información que permita la verificación del cumplimiento de la legislación brasilera en lo referente a la recolección, protección, almacenamiento o tratamiento de datos, así como en lo que respecta a la privacidad y al secreto de las comunicaciones. §4º Un decreto reglamentará el procedimiento de determinación de infracciones a lo dispuesto en este artículo".

Rusia

Rusia también ha tomado medidas enérgicas contra los blogueros anónimos y seudónimos, que una vez formaron una sociedad civil activa en la RuNet. En abril de 2014, la Duma rusa aprobó una ley que requiere a los blogueros declarar su apellido, iniciales y dirección de correo electrónico. Cualquier autor que escribe principalmente en ruso (incluidos los situados fuera de Rusia), cuya página o red social web tiene 3.000 visitantes al día o más, deben registrarse en una lista especial y cumplir con las restricciones aplicables a los medios de comunicación.

Europa

Las fuertes regulaciones de protección de datos de Europa establecen límites a la divulgación y almacenamiento de información de identificación personal. La legislación alemana establece que los proveedores de servicios en línea "deben permitir que el uso de telemedia y el pago por este servicio se produzca de forma anónima o a través de un seudónimo cuando sea técnicamente posible y razonable".[69] Sin embargo, los reguladores alemanes han encontrado dificultades al hacer cumplir dichas disposiciones a proveedores como Facebook, cuyos términos de servicio prohíben los seudónimos.[70]

Otro desafío a la protección del anonimato en Europa es una reciente decisión de la Sala Constitucional del Tribunal Europeo de Derechos Humanos, la cual determinó que "la elección de una empresa [intermediaria] de permitir comentarios de usuarios no registrados" indica que el intermediario debe ser responsable por el carácter difamatorio de los comentarios alojados.[71] Si bien la decisión se encuentra en apelación ante la Gran Sala del mismo Tribunal, el efecto de la ampliación de la responsabilidad en los casos de

---

[69] Ley de Telemedia 2007 Sección 13 (6). "Telemedia" aquí se refiere a todos los servicios de comunicaciones electrónicas, excepto a radiodifusión y servicios de telecomunicación puros (transmisión de la señal).

[70] Las oficinas europeas de Facebook se basan en Irlanda, y los tribunales alemanes han determinado que la legislación alemana no sería aplicable al tratamiento de datos de la compañía fuera de Alemania. Véase IDG News Service (2013), *Facebook can keep its real name policy, German appellate court decides.* Obtenido el 9 de febrero de 2015, de http://news.idg.no/cw/art.cfm?id=2872E148-CD11-E822-FFF3051EA573B6DD

[71] *Delfi AS v. Estoni*, [2013] ECHR 941, 58 EHRR 29, (2014) 58 EHRR 29. Obtenido el 9 de febrero de 2015, de http://www.bailii.org/eu/cases/ECHR/2013/941.html

que un intermediario ignore las identidades de sus usuarios limitará inevitablemente el apoyo comercial para los usuarios que buscan proteger fuertemente su identidad.

Estados Unidos

El Congreso de Estados Unidos tampoco ha protegido adecuadamente el anonimato. En algunas situaciones, la información que identifica a una Parte ante las compañías de telecomunicaciones se hace accesible sin ninguna orden judicial o incluso antes del hecho de supervisión judicial,[72] permitiendo la mala práctica de los intermediarios, que se describe a continuación, de dar cumplimiento a un enorme número de solicitudes firmadas por simples abogados solicitando la identidad de la usuarios.

En los EE.UU., es muy común que los demandantes en casos civiles emitan citaciones a los intermediarios para obtener la identidad de sus críticos con el fin de intimidarlos y silenciarlos, incluso cuando quienes tratan de hacer la identificación no tienen ninguna intención de perseguir una demanda contra el interlocutor o cuando el contenido publicado es legal. Estas citaciones pueden ser emitidas por abogados sin aprobación judicial previa. En algunas circunstancias raras, como en citaciones emitidas de conformidad con la Digital Millennium Copyright Act, una demanda no necesariamente se presenta primero.[73]

Los EE.UU. también permite al Estado a emitir cartas de seguridad nacional (NSL) que pueden exigir la información de identidad de un interlocutor en línea sin control

[72] 18 U.S. Code, Secciones 2703(c)(1)(E), (2)

[73] La Sección 512 (h) de la Digital Millennium Copyright Act permite a los titulares de derechos de autor solicitar a los proveedores de servicios información sobre la identidad del usuario sin tener que presentar una demanda. Véase, Digital Millennium Copyright Act. Disponible en https://ilt.eff.org/index.php/Copyright:_Digital_Millennium_Copyright_Act. Aunque las cortes estadounidenses han reconocido las limitaciones sobre cuándo se pueden usar dichas solicitudes aceleradas. No se extiende a la obtención de la identidad de aquellos que presuntamente comparten archivos extrajudicialmente. Véase *Recording Industry Association of America, Inc. v. Verizon Internet Services, Inc*., 351 F.3d 1229 (D.C. Cir. 2003); *Recording Industry Association of America, Inc. v. Charter Communications*, Inc., 393 F.3d 771 (8th Cir. 2005)

judicial.[74] Estas NSL casi siempre están acompañadas de una orden de silencio, prohibiendo que el proveedor de servicios revele a nadie que ha recibido una NSL, haciendo imposible que el sujeto se oponga a la demanda en un tribunal. Mientras que un tribunal de Estados Unidos ha declarado que el poder de la NSL es inconstitucional, esa decisión quedó pendiente tras una apelación en curso por parte del gobierno.[75]

Litigaciones masivas de derechos de autor

En los últimos años, unas pocas firmas corporativas en los EE.UU., el Reino Unido y Europa han utilizado litigaciones masivas sobre derechos de autor para extraer la ubicación física de ciertos individuos. Estos grupos de firmas de abogados tratan de incrementar los negocios de demanda a los usuarios de Internet en nombre de los propietarios de derechos de autor.[76] Estas demandas siguen el modelo de aquellas presentadas por miembros de la Asociación de la Industria Discográfica de Estados Unidos en 2003.[77]

Las demandas de Estados Unidos demandaron a miles de "Juan Nadie" anónimos y pidieron a las cortes que emitan solicitudes judiciales a los ISP obligándoles a divulgar la identidad de los presuntos infractores a los propietarios de derechos de autor, para que los propietarios de derechos de autor puedan demandar a las personas identificadas. Una vez que se conoce la identidad del usuario de Internet, la posibilidad de una indemnización de daños y perjuicios legales preestablecidos (de hasta $ 150.000 por la presunta violación intencional del derecho de autor de una obra) frecuentemente presionan a los a un acuerdo. Estas demandas plantean inquietudes sobre el debido

[74] 18 U.S.C. § 2709.

[75] *In re Matter of National Security Letters*, No. 131165 (N.D. Cal. Mar. 14, 2013), https://www.eff.org/document/nsl-ruling-march-14-2013

[76] EFF, *Copyright Trolls*. Obtenido el 6 de febrero de 2015, de https://www.eff.org/issues/copyright-trolls. EFF, *USCG v. The People*. Obtenido el 6 de febrero de 2015, de https://www.eff.org/cases/uscg-v-people

[77] Empezaron demandando a un Juan Nadies desconocido, entonces tratan de solicitar a los proveedores de Internet de los usuarios con el fin de obtener sus identidades, después demandan a los propios individuos.

proceso y la protección del derecho de los ciudadanos a la privacidad.[78] En particular, el potencial para la identificación errónea de los supuestos infractores como ocurrió en campañas masivas de litigio de derechos de autor anteriores plantea serias preocupaciones por las muchas personas inocentes que fueron atrapados en el fuego cruzado.[79]

Vigilancia masiva

Por último, los descontroaldos programas de vigilancia masiva digital de la actualidad, llevada a cabo por los servicios de inteligencia de señales de los países de los Cinco Ojos (Estados Unidos,[80] Canadá,[81] Reino Unido, Australia y Nueva Zelanda[82]), y potencialmente muchos más estados, constituyen un ataque generalizado sobre los derechos de anonimato de aquellos que se comunican digitalmente.

La recopilación y correlación de tantos datos y metadatos de comunicaciones proporcionan a estos servicios de inteligencia una capacidad sin precedentes para despojar del anonimato a millones de usuarios inocentes de los sistemas de telecomunicaciones. En algunos casos, estos programas de interceptación de masas han incluido proyectos específicamente dirigidos a socavar las herramientas de anonimato de propósito general, como la red TOR.[83]

Una crítica completa de estos programas y el daño que representan para la libertad de expresión va más allá del alcance de esta presentación, pero hay que señalar que su

---

[78] *Achte Neunte v. Does*. Obtenido el 6 de febrero de 2015, de http://www.eff.org/cases/achte-neunte-v-does. Véase también EFF, *Anonymity Protection Lawsuits*. Obtenido el 6 de febrero de 2015, de https://www.eff.org/issues/anonymity

[79] EFF, *RIAA v. the People: Five Years Later Report*. Obtenido el 6 de febrero de 2015, de http://www.eff.org/wp/riaa-v-people-years-later

[80] Véase *NSA Spying on Americans*, https://www.eff.org/nsa-spying

[81] Véase *Ottawa Statement on Mass Surveillance in Canada*, https://openmedia.ca/statement

[82] Véase *Eyes Wide Open*, https://www.privacyinternational.org/?q=node/301

[83] Guardian (2013), *NSA and GCHQ Target Tor Network That Protects Anonymity of Web Users*. Obtenido el 9 de febrero de 2015, de http://www.theguardian.com/world/2013/oct/04/nsa-gchq-attack-tor-network-encryption

existencia pone de relieve tanto la fragilidad de proteger el anonimato en línea como la importancia de contar con las garantías legales[84] y técnicas[85] para defenderlo.

II. Cifrado

Cifrado y libre expresión

En el entorno digital, la libertad de utilizar la tecnología de cifrado es a menudo un prerrequisito para el ejercicio de los derechos de privacidad y de expresión.[86] En la ausencia de cifrado, las comunicaciones pueden ser fácilmente interceptadas.[87] Debido a la forma en que Internet se ha desarrollado, los intermediarios de Internet que almacenan y reenvían nuestras comunicaciones están a menudo en condiciones de poseer y leer todas las comunicaciones que pasan a través de sus redes. Con el fin de preservar la seguridad y la privacidad de sus usuarios, los proveedores de servicios deben ser capaces de diseñar sistemas que aseguren la privacidad de extremo a extremo, es decir, sistemas que aseguren que un mensaje puede ser leído por su destinatario y nadie más.

La libertad de expresión tiene varias intersecciones con el derecho a desarrollar y usar tecnología de cifrado. El cifrado protege directamente la expresión impidiendo que los sistemas técnicas automatizados de censura bloqueen el acceso a un contenido en

---

[84] Por ejemplo, los *Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones*. Obtenido el 9 de febrero de 2015, de https://es.necessaryandproportionate.org/text

[85] Por ejemplo, véase e RFC 7258, *Pervasive Monitoring Is an Attack*. Obtenido el 9 de febrero de 2015, de https://tools.ietf.org/html/rfc7258

[86] El cifrado permite a los usuarios tener conversaciones privadas mediante correo electrónico, navegación web, o teléfonos celulares. Para obtener más información: Véase EFF (2014), *Surveillance Self Defense*. Obtenido el 6 de febrero de 2015, de https://ssd.eff.org/.

[87] Véase, por ejemplo *Firesheep* (2010). Obtenido el 6 de febrero de 2015, de http://codebutler.com/firesheep. Véase también John P. Mello Jr. , *Free Tool Offered To Combat Firesheep Hackers*, PCWorld. Obtenido el 6 de febrero de 2015, de http://www.pcworld.com/article/211531/free_tool_offered_to_combat_firesheep_hackers.html. Seth Schoen, Richard Esguerra (2010). *The Message of Firesheep: "Baaaad Websites, Implement Sitewide HTTPS Now!*, EFF. Obtenido el 6 de febrero de 2015, de http://www.eff.org/deeplinks/2010/10/message-firesheep-baaaad-websites-implement. EFF, *Tool Offers New Protection Against 'Firesheep'*, 23 de noviembre de 2010. Obtenido el 6 de febrero de 2015, de https://www.eff.org/press/archives/2010/11/23

particular (o incluso a palabras clave particulares). Protege la expresión indirectamente brindando confianza a los usuarios sobre la confidencialidad de sus comunicaciones polémicas o de sus decisiones controvertidas de lectura, ya que están protegidos por medios técnicos. Los desarrolladores de software de cifrado se dedican a su propia actividad expresiva cuando publican código. Cualquier intento de prohibir el uso de cifrado también iría en contra de la libertad de expresión. Muchos programas robustos de cifrado "extremo a extremo" son software libre, su código está publicado y están disponibles para que cualquier persona los descargue desde un amplia variedad de fuentes. Si un Estado intenta prohibir estos programas, tendría que controlar el acceso a esta información, prohibir la publicación, o instituir la infraestructura necesaria para detectar y penalizar su uso. Todos estos métodos tendría consecuencias graves y negativas para la libertad de expresión.

En 1999, un tribunal de apelación de Estados Unidos estuvo de acuerdo con la EFF en que una amplia gama de derechos individuales fueron comprometidos por los agresivos controles gubernamentales a la publicación del código fuente de la tecnología de cifrado —tanto los derechos de los que buscan publicar el código como de aquellos que, potencialmente, tratan de utilizarlo para proteger su privacidad.

> “Señalamos que los esfuerzos del gobierno para regular y controlar la propagación de los conocimientos relativos a la tecnología de cifrado puede comprometer más derechos que aquellos garantizados mediante la Primera Enmienda a los criptógrafos. En esta era cada vez más electrónica, todos necesitamos en nuestra vida cotidiana depender de la tecnología moderna para comunicarnos unos con otros. Esta dependencia sobre la comunicación electrónica, sin embargo, ha traído consigo una disminución dramática de nuestra capacidad de comunicarnos de forma privada. Los teléfonos celulares son objeto de monitoreo, el correo electrónico es interceptado fácilmente, y las transacciones a través de Internet son a menudo menos que seguras. Algo tan común como el suministro de nuestro número de tarjeta de crédito, número de seguro social, o cuenta bancaria pone a cada uno de nosotros en riesgo. Por otra parte, cuando empleamos métodos electrónicos de comunicación, a menudo dejamos "huellas digitales" electrónicas detrás, huellas digitales que pueden rastrearse nuevamente hacia nosotros. Ya sea que estemos siendo vigilados por nuestro gobierno,

> por criminales, o por nuestros vecinos, es justo decir que nuestra capacidad de proteger a nuestros asuntos de miradas indiscretas nunca ha estado a un nivel tan bajo. La disponibilidad y uso de cifrado seguro pueden ofrecer una oportunidad para recuperar una parte de la privacidad que hemos perdido. Los esfuerzos del gobierno para controlar el cifrado, por tanto, bien pueden comprometer no sólo a los derechos de la Primera Enmienda de los criptógrafos decididos a empujar los límites de su ciencia, sino también los derechos constitucionales de cada uno de nosotros como posibles beneficiarios de la generosidad de la tecnología de cifrado. Visto desde esta perspectiva, los esfuerzos del gobierno para retardar el progreso en la criptografía puede comprometer la Cuarta Enmienda, así como el derecho de hablar en forma anónima [...], el derecho contra el discurso obligado [...], y el derecho a la privacidad de información [...]".[88]

El uso de cifrado en las comunicaciones digitales

El cifrado es el proceso matemático de utilizar códigos y claves para comunicarnos de forma privada. A lo largo de la historia, la gente ha utilizado métodos cada vez más sofisticados de cifrado para enviarse mensajes entre sí con el objetivo de que no puedan ser leídos por cualquier persona además de los destinatarios. Las primeras formas de cifrado a menudo eran operaciones simples que podían realizarse a mano, por ejemplo, el "cifrado César" de la antigua Roma.[89] Hoy en día, las computadoras son capaces de realizar un cifrado mucho más complejo y seguro para nosotros. Los propósitos para los cuales la tecnología criptográfica existe se ha expandido más allá de los mensajes secretos; hoy en día, la criptografía se puede utilizar para otros fines, por ejemplo para verificar la autoría de los mensajes[90] o la integridad de las descargas de software, o para navegar la Web anónimamente con TOR.[91]

La mayoría de tecnologías de cifrado modernas se basa en un concepto conocido como cifrado de llave pública. El cifrado de llave pública se basa en un par de llaves

---

[88] *Bernstein v. U.S. Dept. of Justice*, 176 F.3d 1132, 11451146 (9th Cir. 1999) (citas internas omitidas). La opinión no es precedente.

[89] Chris Savarese & Brian Hart '99, *The Caesar Cipher.* Obtenido el 6 de febrero de 2015, de http://www.cs.trincoll.edu/~crypto/historical/caesar.html

[90] PGPi, "Digital Signatures How PGP Works". *Introduction to Cryptography*. Obtenido el 6 de febrero de 2015, de http://www.pgpi.org/doc/pgpintro/#p12

[91] "Staying Anonymous," *Tor Project Overview*. Obtenido el 6 de febrero de 2015, de https://www.torproject.org/about/overview.html.en#stayinganonymous

coincidentes: una clave privada, que es un archivo mantenido en secreto por el usuario y le permite leer los mensajes que están destinados sólo para él o ella, y una clave pública, que es un archivo que el usuario publica o da a los demás y permite a las personas comunicarse con él o ella en privado. Una clave privada también permite al usuario colocar firmas digitales infalsificables en los mensajes enviados a otras personas para que éstas puedan verificar que los mensajes que supuestamente le pertenecen no hayan sido falsificados o modificados. Las claves privadas y públicas vienen en pares coincidentes, se generan al mismo tiempo por un proceso que crea una relación matemática especial entre la clave pública y la privada. El resultado es que cualquiera puede verificar que un mensaje fue firmado por un usuario con una clave privada particular, mediante el examen de la clave pública de ese usuario. En conjunto, estas características de la criptografía de clave pública permiten a los usuarios de Internet tener comunicaciones confidenciales con sitios y servicios o con otros usuarios, y les permite estar seguros de que el contenido de sus comunicaciones no ha sido manipulado. También pueden utilizar la criptografía de clave pública para garantizar la integridad de los documentos y descargas de software; una herramienta esencial para la prevención de la instalación de aplicaciones de software modificado de forma malintencionada.

El cifrado también es esencial para la protección de datos "en reposo" cuando se almacenan en un disco duro o un dispositivo portátil. Muchos de nosotros llevamos historias enteras de nuestros contactos, nuestras comunicaciones y nuestros documentos actuales en los ordenadores portátiles, o incluso teléfonos móviles. Estos datos pueden incluir información confidencial de decenas, incluso miles, de personas. Un teléfono o portátil pueden ser robados o copiados en cuestión de segundos. Los dispositivos electrónicos en los que confiamos y de los cuales dependemos para almacenar y administrar nuestra información personal, a su vez se basan en una aplicación diferente de tecnología de cifrado para proteger los datos que les confiamos.

La mayoría de las computadoras y los teléfonos inteligentes ofrecen, el cifrado de disco completo como una opción, y algunos fabricantes —especialmente los de dispositivos móviles— actualmente habilitan el cifrado del disco completo de forma

predeterminada. Así es cómo Apple describe su aplicación de cifrado de disco completo, al que llama FileVault 2:

> Con FileVault 2, tus datos están seguros y protegidos - incluso si tu Mac cae en las manos equivocadas. FileVault 2 cifra todo el disco en tu Mac, protegiendo tus datos con cifrado XTS-AES 128 ⋯ ¿Quieres empezar desde cero o darle a tu Mac a otra persona? FileVault 2 hace que sea fácil limpiar los datos de tu Mac. Instant Wipe elimina las claves de cifrado de tu Mac —haciendo que los datos sean completamente inaccesibles— entonces se procede con una minuciosa limpieza de todos los datos del disco.[92]

La descripción de Apple resalta otro uso de la tecnología de cifrado: sin cifrado de disco completo, es muy difícil garantizar que los datos privados desaparezcan por completo de un ordenador o dispositivo de almacenamiento cuando llega el momento de venderlo o disponer de él.[93] Sólo con cifrado pueden los usuarios asegurarse de que sus datos no serán accesibles a la siguiente persona que toma posesión del dispositivo. Sin el cifrado, los datos personales de los antiguos propietarios de los dispositivos desechados o revendidos están en riesgo —de hecho, los datos personales de *todos* lo están cuando las prácticas legales y médicas, escuelas, entidades gubernamentales, y otros descartan dispositivos que contienen archivos personales sin cifrar.[94] El cifrado también es ampliamente reconocido como medida cautelar para prevenir o mitigar los efectos de las violaciones de datos.[95]

---

[92] Apple Inc, *Safety. Built Right In*. Obtenido el 6 de febrero de 2015, de https://www.apple.com/osx/what-is/security/

[93] Los datos cifrados aún podrían estar presentes en forma codificada, pero la siguiente persona que use el dispositivo no podrá leerlos.

[94] Véase Simson L. Garfinkel & Abhi Shelat, *"Remembrance of Data Passed: A Study of Data Sanitization Practices"*, IEEE Privacy and Security, Enero/Febrero 2003 (que describe los resultados de la compra y examinación del contenido de un gran número de discos duros usados, incluyendo cantidades masivas de datos personales sensibles).

[95] Por ejemplo, en los Estados Unidos, las estrictas normas de notificación de violación de datos sobre información de salud, se dejan de lado si los datos comprometidos se encuentran cifrados. Véase *74 Fed. Reg. 19006* (Abr. 27, 2009).

Tecnología de cifrado y el Estado

A pesar de la importancia preponderante del cifrado en todos los aspectos de seguridad de la información, los esfuerzos para ponerlo a disposición del público más fácil y convenientemente a menudo han provocado la ira de los gobernantes. Durante más de dos décadas, el Internet nos ha proporcionado una plataforma de expresión verdaderamente global. Hoy en día, cualquier persona puede escribir un blog de oposición, colocar fotografías de sus gatos, organizar una protesta callejera, contribuir a un proyecto de criptografía de software libre, participar en la búsqueda de vida extraterrestre, o minar Bitcoins. Algunas de las actividades en internet —con o sin razón— han provocado la ira de los gobiernos de todo el mundo. Su reacción ha sido desafortunadamente predecible; no sólo prohíben las actividades que consideran peligrosas, sino que también tratan de establecer normas sobre la forma de funcionamiento del Internet. El hecho de que fracasen repetidamente de alguna manera no los disuade de volver a intentarlo de tanto en tanto.

Muchos Estados han tratado de utilizar la regulación y control de exportaciones e importaciones, la legislación nacional o su reglamento, para limitar el acceso del público a las herramientas de cifrado o para intentar imponer concesiones de debilitamiento de seguridad por parte de los fabricantes y desarrolladores de software.[96] En casos muy sonados, así como mediante negociaciones a puerta cerrada, los gobiernos han presionado directamente a fabricantes individuales con la amenaza de prohibir o bloquear sus productos y servicios. De 2010 a 2013, por ejemplo, el fabricante de teléfonos celulares canadiense BlackBerry participó en enfrentamientos públicos con (al menos) los gobiernos de Arabia Saudita, Emiratos Árabes Unidos y la India, que se opusieron al uso, por parte del BlackBerry, de servicios de cifrado robusto que terminaban en Canadá, y sugirieron que el uso de productos de la empresa podría ser prohibido en

[96] Véase BertJap Koops (2013), *Crypto Law Survey*. Obtenido el 9 de febrero de 2015, de http://cryptolaw.org/ (listando los controles conocidos sobre uso, importación y exportación de tecnologías de cifrado).

sus territorios.[97] El fabricante respondió acordando entregar una solución que otorgaría a los gobiernos acceso para espiar a los usuarios no empresariales.[98]

Los Estados Unidos, en cierta ocasión, requirieron licencias gubernamentales para todas y cada una de las copias de software de cifrado exportado, incluso a través de descargas de Internet a los usuarios fuera de los Estados Unidos (o por medio de publicación abierta en línea en un foro que los extranjeros pudieran acceder). Con base en una tradición de considerar a la tecnología criptográfica como militar en lugar de civil, las regulaciones originales trataban a los dispositivos o software de cifrado con una longitud de clave superior a 40 bits como "munición", y su exportación se controlaba de igual manera que la exportación de armas físicas. El resultado fue absurdo. El software desarrollado en los Estados Unidos se produjo comúnmente en versiones "internacionales" y "Estados Unidos", con la versión Internacional despojada de cifrado robusto. A los usuarios se les presentó una elección: ¿querían una versión de software que soporta sólo 40 bits (rompible en horas o minutos en los ordenadores actuales), o querían la versión con capacidad de 128 bits? La versión "fuerte" sólo estaba disponible si el usuario marcaba una casilla afirmando que vivía en los Estados Unidos o Canadá. La ineficaz restricción fue resultado del hecho de que en el momento no había mecanismos precisos para verificar la ubicación de un usuario de Internet.

Las restricciones de los Estados Unidos sobre la tecnología de cifrado llevaron a resultados ridículos (una casilla de verificación para comprobar si el usuario estaba en los Estados Unidos, por ejemplo —o diferentes normas aplicadas precisamente a la exportación del mismo código de cifrado en un disquete o en un libro impreso), pero fracasaron totalmente en detener la propagación de tecnologías de cifrado fuerte.

---

[97] Véase, por ejemplo, BBC News (2010), *Two Gulf States to Ban Some BlackBerry Functions.* Obtenido el 9 de febrero de 2015, de http://www.bbc.com/news/world-middle-east-10830485.

[98] Véase Wired News (2013), *BlackBerry gives Indian government ability to intercept messages*. Obtenido el 9 de febrero de 2015, de http://www.wired.co.uk/news/archive/2013-07/11/blackberry-india

Los Estados Unidos finalmente revirtieron lo que equivalía a una prohibición generalizada de la exportación de cifrado fuerte —tras una importante oposición por parte de industria y la sociedad civil y una demanda del profesor Daniel J. Bernstein, representado por la Electronic Frontier Foundation.[99] Pero los gobiernos no han dejado de intentar detener la propagación de la información, y las regulaciones de exportación siguen siendo el método preferido.

Actualmente, sin embargo, vemos que el Reino Unido conduce un nuevo esfuerzo, no sólo contra la exportación de cifrado, sino también en contra de su propio desarrollo y uso por parte del público. Cameron, Primer Ministro de Reino Unido —con el apoyo de Obama, presidente de Estados Unidos— por ejemplo, ha pedido que las empresas de tecnología mantengan en su software "puertas delanteras muy claras" mediante las cuales las fuerzas del orden, armadas con procesos jurídicos adecuados, puedan acceder al contenido y mensajes de todos. [100]

Si bien no ha habido ninguna propuesta formal en el Reino Unido o los EE.UU., la declaración del primer ministro Cameron implica que su gobierno cree que los desarrolladores de herramientas de comunicación deberían tener el mandato de asegurar que el contenido de sus mensajes siempre debe ser accesible a terceros (en este caso, las fuerzas del orden). Como se describió anteriormente, sin embargo, la seguridad de la tecnología de cifrado se proporciona específicamente porque evita que terceros tengan acceso al contenido cifrado. Cualquier esquema de cifrado en el que es posible que

[99] Para un relato amplio de la derrota de las políticas contra el de cifrado por parte del gobierno estadounidense en la década de 1990, véase Steven Levy*, Crypto: How the Code Rebels Beat the Government—Saving Privacy in the Digital Age (*New York: Viking Penguin, 2001).

[100] The White House Office of the Press Secretary (2015). *Remarks by President Obama and Prime Minister Cameron of the United Kingdom in Joint Press Conference*. Obtenido el 6 de febrero de 2015, de https://www.whitehouse.gov/the-press-office/2015/01/18/remarks-president-obama-and-prime-minister-cameron-united-kingdom-joint-

alguien que no sea el destinatario previsto acceda al mensaje incluye una debilidad fundamental que tiende, en la práctica, a ayudar a todos los atacantes.[101]

El experto en seguridad informática Steven Bellovin ha explicado algunas de las razones por las cuales las puertas traseras debilitan la seguridad en general. En primer lugar, es difícil asegurar las comunicaciones correctamente incluso entre dos partes. El cifrado con una puerta trasera añade un tercero, lo que requiere un protocolo más complejo, y como Bellovin dice: "Muchos de los intentos anteriores para agregar estas características han dado lugar a nuevos fallos de seguridad fácilmente explotados en lugar de mejorar el acceso al cumplimiento de la ley".[102] Bellovin señala además:

> "La complejidad de los protocolos no es el único problema; los protocolos requieren que los programas informáticos los pongan en práctica, y el código más complejo en general crea errores más explotables. En el incidente más notorio de este tipo, el interruptor de un teléfono celular en Grecia fue hackeado por un desconocido. Los mecanismos de la denominada 'intercepción legal' en el interruptor, es decir, las características diseñadas para permitir a la policía realizar escuchas telefónicas fácilmenete fueron abusadas por el atacante para controlar al menos un centenar de teléfonos celulares, incluyendo al Primer Ministro. Este ataque no habría sido posible si el vendedor no habría escrito el código de intercepción legal".

[101] Para críticas contemporáneas sobre quejas a las demandas de cumplimiento de la ley en Estados Unidos acerca de productos de cifrado, en particular al software de cifrado de disco completo de Apple, véase Jeremy Gillula (2014), *Even a Golden Key Can Be Stolen by Thieves: The Simple Facts of Apple's Encryption Decision*. Obtenido el 9 de febrero de 2015, de https://www.eff.org/deeplinks/2014/10/even-golden-key-can-be-stolen-thieves-simple-facts-apples-encryption-decision. Kevin Poulsen (2014), *Apple's iPhone Encryption is a Godsend, Even if Cops Hate It, Wired*. Obtenido el 9 de febrero de 2015, de http://www.wired.com/2014/10/golden-key/ (cada uno respondiendo a las críticas de seguridad de Apple en el cifrado de disco y destacando los riesgos de seguridad creados por las puertas traseras en los sistemas de cifrado).

[102] Steve Bellovin (2010). *The Worm and the Wiretap, SMBlog*. Obtenido el 6 de febrero de 2015, de https://www.cs.columbia.edu/~smb/blog//2010-10/2010-10-16.html

Más recientemente, la investigadora de seguridad Susan Landau explicó:[103]

"Un investigador de IBM encontró que una arquitectura de escuchas telefónicas de Cisco, diseñada para adaptarse a los requisitos de la ley —un sistema que ya está siendo usado por las compañías más importantes— tenía numerosos agujeros de seguridad en su diseño.[104] Esto habría hecho que sea fácil entrar en la red de comunicaciones y escuchar comunicaciones privadas subrepticiamente".

Lo mismo es cierto para Google, cuyas tecnologías de "cumplimiento" fueron hackeadas por China.[105]

Esto no es sólo un problema para el individuo promedio, o incluso para los millones de empresas que necesitan comunicaciones seguras. Las agencias gubernamentales de todo el mundo utilizan actualmente muchos productos comerciales — de empresas a quienes que quieren forzar a tener puertas traseras. Las fuerzas del orden no serán capaces de garantizar que otros no puedan acceder a las mismas puertas traseras que ellos, a su vez, utilicen.

Por otra parte, los usuarios que quieran un cifrado fuerte podrán conseguirlo - de los muchos lugares en el mundo donde se ofrece tecnología de cifrado a la venta y de forma gratuita. En 1996, el Consejo de Investigación Nacional de los Estados Unidos publicó un estudio titulado "El papel de la criptografía en la seguridad de la sociedad de la

[103] Susan Landau (2010), *Moving Rapidly Backwards on Security*, Huffington Post. Obtenido el 6 de febrero de 2015, de http://www.huffingtonpost.com/susan-landau/moving-rapidly-backwards-_b_760667.html

[104] Tom Cross (2010), *Exploiting Lawful Intercept to Wiretap the Internet*. Obtenido el 6 de febrero de 2015, de https://www.blackhat.com/html/bh-dc-10/bh-dc-10-archives.html#Cross

[105] Bruce Schneier (2010), *U.S. Enables Chinese Hacking of Google*. Obtenido el 6 de febrero de 2015, de http://edition.cnn.com/2010/OPINION/01/23/schneier.google.hacking/index.html

información", apodado CRISIS[106] por sus siglas en inglés. El Consejo Nacional de Investigación observó:

> "Actualmente, los productos que utilizan tecnología de cifrado no comprometida están siendo usados por millones de usuarios, y estos productos están disponibles en muchos sitios de Internet en el extranjero difícil de censurar. Los usuarios podrían 'precifrar' sus datos, utilizando cualquier medio disponible, antes de que sus datos fuesen aceptados por un dispositivo o sistema de cifrado comprometido. Los usuarios podrían almacenar sus datos en equipos remotos, accesibles a través de un clic del ratón, pero de otra manera desconocidos para nadie más que el titular de los datos, tales prácticas pueden ocurrir con toda legalidad, incluso con la prohibición del uso del cifrado no comprometido. El conocimiento de técnicas de cifrado fuerte están disponible en las publicaciones oficiales del Gobierno de Estados Unidos y en otras fuentes en todo el mundo, y los elementos criminales bien podrían generar una alta demanda de expertos que entienden cómo utilizar ese conocimiento".[107]

Nada de eso ha cambiado. Y, por supuesto, hay más tecnología de cifrado más fácilmente disponible en la actualidad que en 1996; es una característica básica de los sistemas operativos, lenguajes de programación, protocolos de red del ordenador, y se enseña de forma rutinaria en los programas universitarios de todo el mundo. Así que a menos que los gobiernos quieran prohibir a los usuarios ejecutar cualquier cosa que no esté aprobado por el gobierno en sus dispositivos, sus esfuerzos para prevenir que actores maliciosos se apoderen de herramientas de cifrado tendrán una eficacia extremadamente cuestionable.

Además, con el fin de asegurarse de que no existe una tecnología "no interceptable", lo que el Primer Ministro Cameron parece proponer equivaldría a un mandato tecnológico y un marco regulatorio draconiano. Las implicaciones de esto para la

---

[106] Kenneth W. Dam and Herbert S. Lin (1996). *Cryptography's Role in Securing The Information Society.* Obtenido el 6 de febrero de http://www.nap.edu/openbook.php?record_id=5131

[107] Informe de "CRISIS". Tecnología de cifrado "comprometida" aquí se refiere a un conjunto de sistemas promovidos por la administración del presidente de Estados Unidos Bill Clinton, en los que alguien que no sea un usuario final —un "agente de custodia"— mantiene una copia de repuesto de las claves de descifrado del usuario u otros datos técnicos que permitirían descifrar los mensajes del usuario.

innovación son nefastas. ¿Podría Mark Zuckerberg han construido Facebook en su dormitorio si hubiera tenido que diseñas las capacidades de vigilancia antes del lanzamiento con el fin de evitar multas del gobierno? ¿Podría el Skype original haber existido si se hubiera visto obligado a incluir un cuello de botella artificial para permitir que el gobierno tenga fácil acceso a todas sus comunicaciones entre pares? Esto tiene implicaciones especialmente graves para la comunidad de software libre y los pequeños innovadores. Algunos desarrolladores de software libre ya han tomado una posición en contra de la construcción de puertas traseras en el software.[108] Y cualquier mandato adicional sobre los proveedores de servicios requeriría que gasten una gran cantidad de dinero para hacer sus tecnologías compatibles con las nuevas reglas. Por supuesto, uno no puede realmente preguntarse quién va a pagar la factura: los proveedores pasarán esos costos a sus clientes.

Defendiendo el derecho a cifrar

A pesar de que existen propuestas similares para prohibir el cifrado seguro de extremo a extremo por lo menos desde 1995,[109] los gobiernos de todo el mundo han fracasado por completo probando que la tecnología de cifrado realmente causa un problema para hacer cumplir la ley. En 2010, el New York Times informó que los funcionarios del gobierno que presionan por esto sólo han llegado con unos pocos ejemplos hipotéticas (y no está claro que todos los ejemplos realmente impliquen tecnología de cifrado) y no hechos reales que permitan confirmación o investigación independiente.[110]

---

[108] Zooko O'Whielacronx (2010), *Statement on Backdoors*. Obtenido el 6 de febrero de 2015, de https://tahoe-lafs.org/pipermail/tahoe-dev/2010-October/005353.html

[109] Cindy Cohn (2014). *EFF Response to FBI Director Comey's Speech on Encryption*, Electronic Frontier Foundation. Obtenido el 6 de febrero de 2015, de https://www.eff.org/deeplinks/2014/10/eff-response-fbi-director-comeys-speech-encryption

[110] Charlie Savage (2010). *U.S. Tries to Make It Easier to Wiretap the Internet*, New York Times. Obtenido el 6 de febrero de 2015, de http://www.nytimes.com/2010/09/27/us/27wiretap.html?pagewanted=all

Tanto los individuos como las agencias gubernamentales dependen de un cifrado seguro en sus actividades diarias.[111] Por otra parte, los activistas de derechos humanos, periodistas, refugiados, bloggers, y los denunciantes (soplones) se basan en fuertes tecnologías de cifrado para proteger sus comunicaciones, los nombres y la ubicación de sus fuentes y/ o testigos, etc. El cifrado impacta la libertad de expresión de dos maneras. En primer lugar, el cifrado permite a las personas hablar confidencialmente con los demás, sin temor a represalias por ideas impopulares. En segundo lugar, cualquier intento de restringir la distribución la tecnología de cifrado impacta los derechos de los creadores de software para expresar su punto de vista a través de código. Además, muchos investigadores de seguridad proporcionan software libre para el cifrado, y dan a conocer los algoritmos de cifrado como parte integral de la examinación de la tecnología de cifrado, en busca de defectos y debilidades. Esto significa que el cifrado se encuentra disponible para el mundo. El secreto de las comunicaciones y la libertad de expresión también incluye el derecho de toda persona de publicar e investigar sobre tecnologías de cifrado.

[111] Véase, por ejemplo *Tor Project*. Obtenido el 6 de febrero de 2015, de https://www.torproject.org/about/torusers.html.en

III. Conclusión

Respetuosamente sugerimos a la Relatoría Especial:

- Reafirmar que toda persona tiene derecho a la libertad de expresión, lo que incluye el derecho a hablar, leer y comunicarse de forma anónima;
- Establecer que el anonimato no debe limitarse a priori (incluidas las prohibiciones legales sobre el discurso anónimo, herramientas de anonimato o empresas y proveedores de servicios que ofrecen servicios anónimos);
- Afirmar que un fuerte anonimato —provisto por la tecnología de protección de privacidad, las mejores prácticas del sector privado, y garantías legales sólidas— es vital para algunos de los principales beneficios sociales base del anonimato, incluyendo situaciones en las que actores poderosos (incluidos los que ejercen el poder del Estado) podrían, de otro modo, determinar la identidad del interlocutor;
- Afirmar que la divulgación obligada de interlocutores anónimos sólo debe ocurrir una vez se haya cometido un delito legalmente tipificado. Y en todos los casos, los derechos de un interlocutor en línea deben ser considerados y respetados mediante proceso judicial antes de identificar a esa persona en respuesta a una solicitud de hacerlo;
- Reconocer la libertad de usar tecnología de cifrado y de publicar y distribuir tecnologías e investigación de cifrado;
- Reiterar los peligros de las prohibiciones de cifrado y la inclusión obligatoria de "puertas traseras" en el software y equipos de seguridad;
- Recomendar que los intermediarios de Internet no deben bloquear o limitar la transmisión de comunicaciones cifradas, y
- Recomendar que se aliente a los proveedores de servicios de Internet a diseñar sistemas de cifrado de extremo a extremo.