Módulo 4

PRIVACIDAD DIGITAL Y PROTECCIÓN DE DATOS

Serie de módulos sobre la defensa de la libertad de expresión

MEDIA DEFENCE

Publicado por Media Defence: www.mediadefence.org

Este módulo ha sido preparado con la ayuda de Fundación para la Libertad de Prensa: https://www.flip.org.co/index.php/es/

Tabla de contenidos

PRIVACIDAD DIGITAL Y PROTECCIÓN DE DATOS 1
INTRODUCCIÓN 4
EL DERECHO A LA PRIVACIDAD 4
PROTECCIÓN DE DATOS 6
EL "DERECHO AL OLVIDO" 8
Ámbito internacional 8
Ámbito latinoamericano 10
Límites del derecho al olvido. 12
CIFRADO Y ANONIMATO EN INTERNET 13
VIGILANCIA ESTATAL CON MEDIOS DIGITALES 14
CONCLUSIÓN 17

MÓDULO 4
PRIVACIDAD DIGITAL Y PROTECCIÓN DE DATOS

- El derecho a la privacidad está cobrando importancia con el aumento del flujo de datos y la necesidad concomitante de proteger la información personal.
- En el contexto americano, existen diferentes instrumentos que rigen la protección de datos, tales como la Convención Americana sobre Derechos Humanos y la Declaración Americana de los Derechos y Deberes del Hombre.
- Es importante que los Estados se aseguren de que su legislación nacional detalle los principios para el procesamiento legal de información personal y que se mantenga al día con los desarrollos de protección de datos.
- Junto a la protección de datos están los conceptos de "derecho al olvido", encriptación y vigilancia estatal.
- En particular, la divulgación de fuentes periodísticas como resultado de la vigilancia Estatal tiene un impacto negativo en la libertad de expresión y la libertad periodística.

INTRODUCCIÓN

El derecho a la privacidad y el requisito concomitante de proteger la información personal ha atraído una atención significativa con la era de la información. Si bien en Internet el intercambio de información en línea y la recopilación de datos aumentan de manera exponencial, los desarrollos legislativos no han logrado mantener este ritmo ni proteger adecuadamente la información personal. Sin embargo, con el tiempo, los Estados americanos y los organismos regionales y continentales han comenzado a adoptar instrumentos y reglamentos relacionados con la protección de datos en un intento por remediar y reivindicar el derecho a la privacidad de sus ciudadanos.

Este módulo se centra en la protección de datos en América y los conceptos relacionados del derecho al olvido, el cifrado y la vigilancia.

EL DERECHO A LA PRIVACIDAD

Hay un reconocimiento cada vez mayor de que el derecho a la privacidad juega un papel vital para la facilitación del derecho a la libertad de expresión. Por ejemplo, la confianza en el derecho a la privacidad permite a las personas compartir opiniones de forma anónima en circunstancias en las que pueden

temer ser censurados por esas opiniones, permite a los denunciantes hacer divulgaciones protegidas y permite a los miembros de los medios de comunicación y activistas comunicarse de forma segura sin el alcance de la interceptación gubernamental ilegal.

El derecho a la intimidad fue reconocido por primera vez en el plano internacional en la Declaración Universal de Derechos Humanos. En su artículo 12, se dispone que "toda persona debe ser protegida contra injerencias arbitrarias en su vida privada, familia, domicilio o correspondencia, así como de ataques contra su honra y reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques". Posteriormente, este derecho fue reproducido por otros instrumentos tales como el Pacto Internacional de Derechos Civiles y Políticos[1], la Declaración Americana de Derechos y Deberes del Hombre[2] y la Convención Americana sobre Derechos Humanos[3], entre otros.

El derecho a la intimidad también ha sido reconocido en otros instrumentos regionales y nacionales en el contexto de la protección de datos, que se analizará más adelante. Además, casi todos los Estados americanos garantizan este derecho en sus constituciones nacionales.

En el caso *Fontevecchia y D'Amico vs. Argentina*, la Corte IDH recordó que la Convención Americana prohíbe las invasiones o ataques abusivos o arbitrarios por parte de terceros o por parte de autoridades públicas. La Corte indicó que existen dos criterios relevantes a tener en cuenta cuando se difunde información potencialmente privada: "(a) el diferente umbral de protección para los funcionarios públicos, especialmente los de elección popular, para las figuras públicas y los particulares, y (b) el interés público en las acciones emprendidas"[4]. El diferente umbral de protección respecto a funcionarios públicos se debe al carácter voluntario de su exposición al escrutinio social, lo cual implica que hay mayor probabilidad de lesión con respecto a la privacidad de los funcionarios públicos. En cuanto al interés público, la Corte manifestó que hay una mayor posibilidad de intromisión respecto a la privacidad frente a asuntos en los cuales la sociedad tiene un interés legítimo de estar informada.

Al igual que con el derecho a la libertad de expresión, una limitación del derecho a la intimidad debe cumplir con un test de proporcionalidad y necesidad. De acuerdo con la Corte Interamericana, en el caso *Tristán Donoso vs. Panamá*:

---

[1] El artículo 17 del Pacto Internacional de Derechos Civiles y Políticos establece lo siguiente respecto al derecho a la privacidad: Nadie podrá ser objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.

[2] El artículo 5 de la Declaración Americana de los Derechos y Deberes del Hombre dispone lo siguiente respecto al derecho a la privacidad: "Toda persona tiene derecho a la protección de la Ley contra los ataques abusivos a su honra, a su reputación y a su vida privada y familiar. Además de esta disposición, el artículo 9 se refiere a la inviolabilidad del domicilio y el artículo 10 hace referencia a la inviolabilidad y circulación de la correspondencia.

[3] El artículo 11 de la Convención Americana sobre Derechos Humanos establece lo siguiente: "Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques".

[4] Corte Interamericana de Derechos Humanos. *Fontevecchia D'Amico v. Argentina*. Sentencia de 29 de noviembre de 2011. Serie C No. 238, párr. 159.

> "El derecho a la privacidad no es un derecho absoluto y, por tanto, puede ser restringido por los Estados. Esto, siempre que las injerencias no sean abusivas o arbitrarias. Por lo cual, el límite a esas restricciones debe ser: (i) estar previstas en ley; (ii) perseguir un fin legítimo y (iii) cumplir con los requisitos de idoneidad, necesidad y proporcionalidad, es decir, deben ser necesarias para una sociedad democrática"[5].

De manera particular, en el caso *Escher y otros vs. Brasil* , la Corte se refirió al uso de tecnología y la tensión con la privacidad, advirtiendo que:

> "La fluidez informativa que existe hoy en día coloca al derecho a la vida privada de las personas en una situación de mayor riesgo debido a las nuevas herramientas tecnológicas y su utilización cada vez más frecuente. Este progreso, en especial cuando se trata de interceptaciones y grabaciones telefónicas, no significa que las personas deban quedar en una situación de vulnerabilidad frente al Estado o a los particulares. De allí que el Estado debe asumir un compromiso, aún mayor, con el fin de adecuar a los tiempos actuales las fórmulas tradicionales de protección del derecho a la vida privada."[6]

A continuación, consideramos aspectos específicos del derecho a la intimidad y el impacto que ha tenido Internet en el disfrute de este derecho.

PROTECCIÓN DE DATOS

Las leyes de protección de datos tienen como objetivo proteger y salvaguardar el tratamiento de la información personal. Esto hace referencia a cualquier información relativa a una persona identificada o identificable. El sujeto de los datos puede ser identificado por uno o más factores específicos de su identidad física, fisiológica, mental, económica, cultural o social. El responsable del tratamiento, que normalmente puede ser un organismo público o privado, se refiere a la persona o entidad responsable del tratamiento de la información personal del interesado.

La protección de datos es una de las principales medidas a través de las cuales se hace efectivo el derecho a la intimidad. Ya son varios los Estados americanos que han promulgado leyes de protección de datos, y otros más que están en proceso de hacerlo. Igualmente, a marzo de 2022, tres países de la región eran signatarios del Convenio 108 del Consejo de Europa de 28 de enero de 1981 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal. Además de hacer efectivo el derecho a la privacidad, la legislación de protección de datos también desempeña un papel fundamental a la hora de facilitar el comercio entre Estados, ya que muchas leyes de protección de datos restringen las transferencias transfronterizas de datos en circunstancias en las que el Estado que recibe la información no proporciona un nivel adecuado de protección.

En relación con la protección de la información personal, la Observación General No. 16 del Comité de Derechos Humanos de Naciones Unidas sobre el artículo 17 del PIDCP establece lo siguiente:

> "La recopilación y el registro de información personal en computadoras, bancos de datos y otros dispositivos, tanto por las autoridades públicas como por las particulares o entidades

[5] Corte Interamericana de Derechos Humanos. *Tristán Donoso v. Panamá*. Sentencia de 27 de enero de 2009. Serie C No. 193.
[6] Corte Interamericana de Derechos Humanos. *Escher y otros vs. Brasil*. Sentencia de 6 de julio de 2009.

privadas, deben estar reglamentados por la ley. Los Estados deben adoptar medidas eficaces para velar por que la información relativa a la vida privada de una persona no caiga en manos de personas no autorizadas por ley para recibirla, elaborarla y emplearla y para que nunca se la utilice para fines incompatibles con el Pacto. Para que la protección de la vida privada sea lo más eficaz posible, toda persona debe tener el derecho de verificar si hay datos personales suyos almacenados en archivos automáticos de datos y, en caso afirmativo, de obtener información inteligible sobre cuáles son esos datos y con qué fin se han almacenado. Asimismo, toda persona debe poder verificar qué autoridades públicas o qué particulares u organismos privados controlan o pueden controlar esos archivos. Si esos archivos contienen datos personales incorrectos o se han compilado o elaborado en contravención de las disposiciones legales, toda persona debe tener derecho a pedir su rectificación o eliminación"[7].

La mayoría de las leyes de protección de datos suelen contemplar los siguientes principios[8]:

- La información personal debe ser tratada de forma justa y legal, y no debe ser utilizada a menos que se cumplan las condiciones estipuladas.
- La información personal debe obtenerse para un propósito específico y no debe ser utilizada de ninguna manera incompatible con ese propósito.
- Los datos personales deben ser adecuados, pertinentes y no excesivos en relación con la finalidad (o finalidades) para la que se tratan.
- Los datos personales deben mantenerse actualizados.
- La información personal no debe conservarse durante más tiempo del necesario para la finalidad de su recolección.
- La información personal debe tratarse de acuerdo con los derechos de los interesados previstos en las respectivas leyes de protección de datos.
- Deben adoptarse medidas técnicas y organizativas adecuadas contra el tratamiento no autorizado o ilegal de los datos personales y contra la pérdida o destrucción accidental de los datos personales, así como contra su deterioro.
- Los datos personales no deben transferirse a otro país que no garantice un nivel adecuado de protección de los derechos y libertades de los interesados en relación con el tratamiento de la información personal.

Además de esto, hay algunos instrumentos regionales americanos que tratan la protección de datos personales:

- Principios de Privacidad y Protección de Datos Personales en las Américas[9]: En marzo de 2012, la Organización de Estados Americanos (OEA) adoptó la propuesta de principios elaborada por el Comité Jurídico Interamericano (CJI), para orientar a los Estados Miembros a

[7] Human Rights Committee, General Comment 16, (Twenty-third session, 1988), Compilation of General Comments and General Recommendations Adopted by Human Rights Treaty Bodies, U.N. Doc. HRI/GEN/1/Rev.1 at 21 (1994). Para 10.

[8] Information Commissioner's Office. Principios de la Protección de Datos. Obtenido en: https://ico.org.uk/for-organisations/guide-to-data-protection/data-protection-principles

[9] Organización de Estados Americanos (2012). *Propuesta de declaración de principios de privacidad y protección de datos personales en las Américas*. CJI/RES. 186 (LXX-O/12). Periodo ordinario de sesiones. Obtenido de: http://www.oas.org/es/sla/cji/docs/CJI-RES_186_LXXX-O-12.pdf

adoptar medidas respecto a la privacidad y los datos personales, para que estos Estados adoptaran leyes congruentes con lo allí establecido. En abril de 2021, el CJI aprobó la actualización de los principios sobre la privacidad y protección de datos personales, con anotaciones.

- Estándares de Protección de los Estados Iberoamericanos[10]: Estos estándares incluyen temas relacionados con el ejercicio de la privacidad, el derecho a la desindexación, el uso de tecnologías de vigilancia y el uso de big data.

- Guía Legislativa sobre la Privacidad y la Protección de Datos Personales en las Américas[11]: En el año 2013, la Asamblea General de la OEA solicitó al Comité Jurídico Interamericano (CJI) formular propuestas sobre las diferentes formas de regular la protección de datos personales. Así, en el 2015 se adoptó una guía legislativa que amplía y explica los principios adoptados en el 2012, la cual sirve como hoja de ruta para apoyar los esfuerzos de los Estados Miembros al momento de implementar o actualizar su normatividad sobre la materia.

Además de hacer efectivo el derecho a la intimidad, las leyes de protección de datos también suelen facilitar el derecho de acceso a la información. A este respecto, la mayoría de las leyes de protección de datos prevén que los interesados soliciten y tengan acceso a la información que el responsable del tratamiento tiene sobre ellos. Este mecanismo puede permitir a los interesados comprobar si su información personal se está procesando de acuerdo con las leyes de protección de datos aplicables y si se están respetando sus derechos.

Dado que el periodismo consiste en la recolección, transformación, almacenamiento y difusión de información de personas, es una actividad que puede entrar en conflicto con la protección de datos personales. Por esta razón, algunas legislaciones establecen excepciones sobre la aplicación de estas normas sobre bases de datos y archivos periodísticos o que sean necesarios para el ejercicio de la libertad de expresión.[12]

EL "DERECHO AL OLVIDO"

Ámbito internacional

El llamado "derecho al olvido" —que tal vez se describe mejor como "derecho a la supresión"— hace referencia al derecho a solicitar que los motores de búsqueda comerciales u otros sitios web que recopilan información personal con fines lucrativos, como Google, eliminen los enlaces a información privada cuando se les solicita en atención a criterios específicos. El derecho al olvido se deriva del derecho de los interesados que figura en muchas leyes de protección de datos, según el cual la información personal que se tiene sobre una persona debe borrarse en circunstancias en las que sea

[10] Red Iberoamericana de Protección de Datos (2017). *Estándares de protección de datos personales para los Estados Iberoamericanos*. Obtenido de: https://www.redipd.org/sites/default/files/inline-files/Estandares_Esp_Con_logo_RIPD.pdf

[11] Organización de Estados Americanos (2015). *Guía Legislativa del CJI*. Obtenido de: https://www.oas.org/es/sla/ddi/proteccion_datos_personales_Guia_Legislativa_CJI_2015.asp

[12] Algunos ejemplos en la región son la Ley N° 25.326, 2000, art 1 en Argentina, la Ley N° 1581, 2012, art 2.d en Colombia y la Ley N° 8968, 2011, art 1en Costa Rica. En el mismo sentido se puede ver el artículo 9.2.b del Convenio 108 del Consejo de Europa.

inadecuada, irrelevante o ya no sea pertinente, o excesiva en relación con los fines para los que se recogió.

En 2014, el Tribunal de Justicia de la Unión Europea dictó una importante sentencia en el caso de Google España v. González[13]. El señor González, de nacionalidad española, presentó una queja en 2010 ante el regulador español de la información. El motivo de la queja era que, cuando un usuario de Internet introducía su nombre en el motor de búsqueda de Google, el usuario obtenía enlaces a páginas del periódico español de 1998 que hacían referencia a procedimientos de embargo contra él para el cobro de determinadas deudas. El Sr. González solicitó que se eliminaran u ocultaran los datos personales relativos a su persona, ya que el procedimiento contra él se había resuelto por completo y, por tanto, la referencia a su persona era ya totalmente irrelevante.

La Audiencia Nacional española conoció del caso a nivel español y, previamente a decidir, sometió una petición prejudicial al TJUE con respecto a la aplicación de la ley de protección de datos de la Unión Europea vigente en ese momento en el caso concreto. El Tribunal señaló que la visualización de información personal en una página de resultados de búsqueda constituye un tratamiento de dicha información, por lo cual no había ninguna razón por la que un motor de búsqueda no debiera estar sujeto a las obligaciones y garantías establecidas en la ley. Además, se señaló que el tratamiento de información personal realizado por un motor de búsqueda puede afectar significativamente los derechos fundamentales a la intimidad y a la protección de datos personales cuando se realiza una búsqueda del nombre de una persona, ya que permite a cualquier usuario de Internet obtener una visión estructurada de la información relativa a esa persona y establecer un perfil de la misma. Según el TJUE, el efecto de la injerencia "se acentúa teniendo en cuenta el importante papel que desempeñan Internet y los motores de búsqueda en la sociedad moderna, que hacen que la información contenida en esa lista de resultados sea omnipresente"[14].

En lo relativo a la desindexación en los motores de búsqueda, el TJUE sostuvo que la eliminación de enlaces en la lista de resultados de los buscadores podría, dependiendo de la información en cuestión, tener efectos sobre los usuarios de Internet potencialmente interesados en tener acceso a esa información[15]. Esto requeriría un justo equilibrio entre ese interés y los derechos fundamentales del interesado, teniendo en cuenta la naturaleza de la información, su sensibilidad para la vida privada del interesado, y el interés del público en disponer de esa información, que puede variar según el papel desempeñado por el interesado en la vida pública.

El TJUE también declaró que un interesado puede solicitar que la información sobre él deje de estar disponible para el público en general mediante su inclusión en una lista de resultados de búsqueda cuando, teniendo en cuenta todas las circunstancias, la información parezca inadecuada, irrelevante o ya no pertinente, o excesiva en relación con los fines del tratamiento llevado a cabo por el operador del motor de búsqueda. En tales circunstancias, la información y los enlaces en cuestión en la lista de resultados deben ser borrados[16].

[13] Google España SL y otro v. Agencia Española de Protección de Datos (AEPD). Asunto núm. C-131/12, 13 de mayo de 2014. Obtenido en: https://eur-lex.europa.eu/
[14] *Ibídem*.
[15] *Ibídem*.
[16] *Ibídem.*

Ámbito latinoamericano

En el informe Estándares para una Internet libre, abierta e incluyente, la Relatoría Especial para la Libertad de Expresión (RELE) menciona que con base en las normas de protección de datos personales en América Latina, se han registrado en la región varias solicitudes de remoción y desindexación de contenidos a administradores de motores de búsqueda. Sin embargo, este concepto se ha expandido mucho más, pues también es común que se hagan solicitudes a periódicos, blogs y periodistas para remover o eliminar contenidos, en lugar de realizar solicitudes de desindexación de los motores de búsqueda[17]. Esto puede tener un efecto muy negativo para la libertad de expresión, pues el derecho al olvido puede usarse para cancelar información de interés público mediante acciones sustentadas en el derecho al olvido. La RELE señaló en dicho informe que el derecho internacional de los derechos humanos no protege o reconoce el derecho al olvido en los términos de la sentencia del TJUE en el caso de Google España v. Gonzalez: "Por el contrario, la Relatoría Especial estima que la aplicación en las Américas de un sistema de remoción y desindexación privada de contenidos en línea con límites tan vagos y ambiguos resulta particularmente problemática a la luz del amplio margen normativo de protección de la libertad de expresión bajo el artículo 13 de la Convención Americana sobre Derechos Humanos."[18] Adicionalmente, la RELE indicó que los Estados que implementen legislaciones de derecho al olvido deben hacerlo de forma excepcional, específica, clara y limitada para que exista un respeto de la libertad de expresión y acceso a la información al momento de proteger la privacidad y dignidad de las personas, además de brindando una distinción entre información y datos personales, al igual que los casos en los que la acción no procede, especialmente cuando se trate de expresiones sobre asuntos de interés público.[19] Igualmente, la RELE razonó que las solicitudes cubiertas por esta legislación solo aplicarán cuando el solicitante demuestre la existencia de un daño sustancial a su privacidad y dignidad a través de una orden judicial en el marco de un proceso que respete las garantáis judiciales y que brinde la oportunidad para la defensa de todas las personas involucradas, incluyendo a quien realiza la expresión, el medio de comunicación o sitio web afectado y los intermediarios de internet involucrados.

En cuanto al reconocimiento de este concepto en instancias nacionales, se puede resaltar el caso de Colombia. En este país no se contempla el derecho al olvido en las legislaciones sobre datos personales. Sin embargo, la Corte Constitucional ha sentado jurisprudencia sobre la materia. Un caso emblemático al respecto es *Gloria v. El Tiempo*[20], donde la Corte Constitucional resolvió una tutela interpuesta contra el medio El Tiempo, mediante la cual una ciudadana buscaba que una noticia de doce años de antigüedad relacionada con su vinculación en un proceso penal por trata de personas no pudiese ser consultada en línea. El proceso contra la ciudadana había concluido por prescripción y la disponibilidad de dicha noticia en Google afectaba sus derechos, entre esos el de buscar un trabajo. Durante el trámite de la tutela, la Corte vinculó a Google para que se pronunciara sobre los hechos del caso. La Corte determinó que en este caso no aplicaba la legislación de habeas data en razón de la excepción de bases de datos periodísticos que contempla la legislación de ese país sobre esa materia. En su lugar, decidió analizar el caso a la luz de los derechos a la honra, buen nombre, dignidad humana

[17] Relatoría Especial para la Libertad de Expresión (2017). *Estándares para una Internet Libre, Abierta e Incluyente*, pág. 53, párr. 130. Obtenido de: https://www.oas.org/es/cidh/expresion/docs/publicaciones/INTERNET_2016_ESP.pdf
[18] *Ibídem.* Párr. 137.
[19] *Ibídem.* Párr. 140.
[20] Corte Constitucional. *Sentencia T-277 de 2015*. MP: Maria Victoria Calle Correa.

y libertad de información por tener prerrogativas equiparables a lo protegido por el derecho de habeas data. Adicionalmente, la Corte consideró que aplicar un sistema como el dispuesto en la sentencia del TJUE implica "un sacrificio innecesario del principio de neutralidad de internet y, con ello, de las libertades de expresión e información". En esta línea, Google consideró que no tenía ningún tipo de responsabilidad porque actuaba como un intermediario. La Corte Constitucional consideró que la forma de garantizar los derechos de la demandante sin afectar gravemente los derechos del medio era permitir que la noticia siguiera en línea pero se ordenara al medio actualizar la información publicada y utilizar una herramienta técnica para impedir que los buscadores identificaran la noticia escribiendo su nombre.

Por otro lado, en el caso de Brasil, el Supremo Tribunal Federal (STF) concluyó a inicios de 2021 que el derecho al olvido es incompatible con el sistema constitucional brasileño. Según el Tribunal, el paso del tiempo no es una restricción legítima para la divulgación de contenido verídico, por lo cual permitir el derecho al olvido significa restringir de forma excesiva la libertad de expresión:

> "Es incompatible con la Constitución Federal la idea de un derecho al olvido, entendido como la facultad de impedir, por el paso del tiempo, la divulgación de hechos o datos verídicos y legalmente obtenidos y publicados en los medios de comunicación social, analógicos o digitales. Cualquier exceso o abuso en el ejercicio de la libertad de expresión e información debe ser analizado caso por caso, con base en parámetros constitucionales, especialmente los relativos a la protección del honor, la imagen, la privacidad y la personalidad en general, y las disposiciones legales expresas y específicas en el ámbito penal y de los derechos civiles"[21].

En el caso de Argentina, se reconoce legalmente que las personas pidan la corrección o eliminación de sus datos. Por ejemplo, la Ley 25.326 dispone que el término de archivo de los antecedentes crediticios de una persona es de cinco años y que este plazo disminuye a dos años cuando los deudores pagan la obligación[22]. Además, en el 2020 la Cámara Nacional en lo Civil aplicó por primera vez el "derecho al olvido"[23] a favor de Natalia Denegri[24], una actriz y productora que había demandado a Google solicitando la desindexación de una serie de artículos con más de dos décadas de antigüedad que la vinculaban con el "caso Coppola", un famoso evento noticioso en Argentina relacionado con el allanamiento de la residencia del entonces representante de Diego Maradona[25].

---

[21] Tribunal Supremo Federal de Brasil. *Sentencia del 11 de febrero de 2021*. RE1010606. Obtenido de: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=755910773

[22] Centro de Estudios de Libertad de Expresión y Acceso a la Información (CELE). *Derecho al olvido: entre la protección de datos, la memoria y la vida personal en la era digital.* Obtenido de: https://www.palermo.edu/cele/pdf/DerechoalolvidoiLEI.pdf

[23] Cámara Nacional de Apelaciones en lo Civil. *Natalia Degeri v. Google Inc.*. Sentencia del 10 de agosto de 2020. ID SAIJ: FA20020049. Obtenido de: http://www.saij.gob.ar/camara-nacional-apelaciones-civil-nacional-ciudad-autonoma-buenos-aires-denegri-natalia-ruth-google-inc-derechos-personalisimos-acciones-relacionadas-fa20020049-2020-08-10/123456789-940-0200-2ots-eupmocsollaf

[24] La Nación (12 de agosto de 2020). *Caso Natalia Denegri: por primera vez en la Argentina, la justicia aplicó el "derecho al olvido" en una demanda contra Google*. Obtenido de: https://www.lanacion.com.ar/sociedad/por-primera-vez-argentina-se-promulgo-fallo-nid2418606/

[25] Resofworld. *Natalia Denegri no quiere ser definida por un escándalo de Maradona. Ahora lucha por que el Internet la olvide.* Obtenido de: https://restofworld.org/2021/denegri-google-maradona-derecho-olvidar/

Límites del derecho al olvido.

No obstante, existen límites al ámbito del derecho al olvido. En 2017, el TJUE recibió una petición de decisión prejudicial en el caso *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni.* El señor Manni, basándose en la decisión González, solicitó que se ordenara a la Cámara de Comercio borrar, anonimizar o bloquear cualquier dato que lo vinculara a la liquidación de su empresas. El TJUE se negó a estimar la solicitud del señor Manni, y sostuvo que, a la luz de la gama de posibles usos legítimos de los datos en los registros de empresas y de los diferentes plazos de prescripción aplicables a dichos registros, era imposible determinar un período máximo de conservación adecuado. En consecuencia, el TJUE se negó a declarar la existencia de un derecho general al olvido de los registros públicos de empresas.

Además, en el caso Google v. CNIL, la Corte de Justicia de la Unión Europea sostuvo que "el derecho al olvido" no requiere que un motor de búsqueda elimine los resultados de todos sus dominios. Sin embargo, sí se requiere que se eliminen todos los resultados de búsqueda en todos los Estados que pertenecen a la Unión Europea[26]. Con esta decisión, se restringió el alcance territorial del derecho al olvido, lo cual significa que este "derecho" sólo aplicaría en las fronteras de la Unión Europea, restringiendo su aplicación extraterritorial.

En esa misma decisión, al igual que en la del caso de GC y otros v. Google, afirmó que las tensiones entre el derecho de protección de datos personales y las libertades de expresión e información deben tener un balance inspirado en la jurisprudencia del Tribunal Europeo de Derechos Humanos en casos de privacidad y libertad de expresión.

Adicionalmente, la normativa actual a nivel europeo con respecto al derecho al olvido, el Reglamento General de Protección de Datos, establece en su artículo 17.3.a que este no será aplicable en aquellos casos en que el tratamiento de datos sea necesario para el ejercicio de la libertad de expresión o con fines de archivo de interés público.

Además, otras jurisdicciones se han negado a defender el derecho al olvido frente a los motores de búsqueda. En Brasil, por ejemplo, se sostuvo que no se puede obligar a los motores de búsqueda a eliminar los resultados de búsqueda relacionados con términos o expresiones específicas. Asimismo, el Tribunal Supremo de Japón se negó a hacer valer el derecho al olvido frente a Google, al considerar que la eliminación "sólo puede permitirse cuando el valor de la protección de la intimidad supera significativamente al de la divulgación de la información ".

Según los Principios Globales sobre la Libertad de Expresión y la Privacidad, este derecho —en la medida en que esté reconocido en una jurisdicción concreta— debe limitarse al derecho de las personas, en virtud de la legislación sobre protección de datos, a solicitar a los motores de búsqueda suprimir los resultados de búsqueda inexactos producidos a partir de una búsqueda de su nombre, y debe limitarse al nombre de dominio correspondiente en casos donde el individuo afectado ha demostrado un daño sustancial. Afirma, además, que las solicitudes de supresión de la lista deben estar sujetas a la resolución final de un tribunal o de un órgano jurisdiccional independiente con la experiencia pertinente en materia de libertad de expresión y derecho de protección de datos.

[26] Corte de Justicia de la Unión Europea. *Google v. CNIL*. Caso C-507 de 2017. Sentencia del 10 de enero de 2019. Obtenido de: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62017CC0507

CIFRADO Y ANONIMATO EN INTERNET

La encriptación se refiere a un proceso matemático que convierte los mensajes, la información o los datos en una forma ilegible para cualquiera, excepto para el destinatario previsto, protegiendo así la confidencialidad y la integridad del contenido contra el acceso o la manipulación de terceros[27]. Con un "cifrado de clave pública" —la forma dominante de seguridad de extremo a extremo para los datos en tránsito— el remitente utiliza la clave pública del destinatario para cifrar el mensaje y sus anexos, y el destinatario utiliza su propia clave privada para descifrarlos[28]. También es posible cifrar los datos en reposo que se almacenan en el propio dispositivo, como un ordenador portátil o un disco duro[29].

El anonimato puede definirse como el hecho de actuar o comunicarse sin utilizar o dar a conocer el propio nombre o identidad, o cómo actuar o comunicarse de forma que se proteja la determinación del nombre o la identidad, o la posibilidad de utilizar un nombre inventado o supuesto que no esté necesariamente asociado a la identidad legal o habitual[30]. El anonimato puede distinguirse del pseudo anonimato: el primero se refiere a no adoptar ningún nombre, mientras que el segundo se refiere a adoptar un nombre supuesto[31].

El cifrado y el anonimato son herramientas necesarias para el pleno disfrute de los derechos digitales y gozan de protección en virtud del papel fundamental que desempeñan para garantizar la libertad de expresión y la privacidad. Como describe el Relator Especial de las Naciones Unidas sobre la libertad de expresión[32]:

> "El cifrado y el anonimato, por separado o conjuntamente, crean una zona de privacidad para proteger la opinión y las creencias. Por ejemplo, permiten las comunicaciones privadas y pueden proteger una opinión del escrutinio exterior, algo especialmente importante en entornos políticos, sociales, religiosos y jurídicos hostiles. Cuando los Estados imponen una censura ilegal mediante el filtrado y otras tecnologías, el uso de la encriptación y el anonimato puede permitir a los individuos sortear las barreras y acceder a la información y las ideas sin la intromisión de las autoridades. Los periodistas, los investigadores, los abogados y la sociedad civil confían en la encriptación y el anonimato para protegerse (y proteger a sus fuentes, clientes y socios) de la vigilancia y el acoso. La capacidad de buscar en la red, desarrollar ideas y comunicarse de forma segura puede ser la única manera en que muchos pueden explorar aspectos básicos de la identidad, como el género, religión, etnia, origen nacional o sexualidad. Los artistas confían en el cifrado y el anonimato para salvaguardar y proteger su libre expresión, especialmente en situaciones en las que no es sólo el Estado el que crea limitaciones, sino también la sociedad que no tolera opiniones o expresiones no convencionales".

---

[27] Report of the UNSR on Freedom of Expression (22 de mayo de 2015). *Report on anonymity, encryption and the human rights framework*. A/HRC/29/32, Obtenido de: http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx

[28] *Ibídem.*

[29] *Ibídem.*

[30] Electronic Frontier Foundation (10 de febrero de 2015). *Anonymity and encryption*, pág. 3. Obtenido de: https://www.ohchr.org/Documents/Issues/Opinion/Communications/EFF.pdf

[31] *Ibídem.*

[32] OHCHR (22 de mayo de 2015). *Report on encryption, anonymity, and the human rights framework.* Obtenido de: https://www.ohchr.org/en/issues/freedomopinion/pages/callforsubmission.aspx

El cifrado y el anonimato son especialmente útiles para el desarrollo y el intercambio de opiniones en línea, sobre todo en circunstancias en las que las personas pueden estar preocupadas por la posibilidad de que sus comunicaciones sean objeto de interferencias o ataques por parte de agentes estatales o no estatales. Se trata, por tanto, de tecnologías específicas a través de las cuales los individuos pueden ejercer sus derechos.

Según el Reporte de las Naciones Unidas sobre cifrado y anonimato, aunque estas herramientas pueden frustrar a los funcionarios encargados de la aplicación de la ley y de la lucha contra el terrorismo, las autoridades estatales generalmente no han proporcionado una justificación pública adecuada para apoyar la restricción o para identificar las situaciones en las que la restricción ha sido necesaria para lograr un objetivo legítimo[33]. Las prohibiciones absolutas del uso individual de la tecnología de encriptación restringen de forma desproporcionada el derecho a la libertad de expresión, ya que privan a todos los usuarios en línea de una jurisdicción concreta del derecho a forjarse un espacio para la opinión y la expresión, sin que se alegue en particular que el uso de la encriptación tiene fines ilícitos[34]. Asimismo, la regulación estatal de la encriptación puede equivaler a una prohibición, por ejemplo, mediante la exigencia de licencias para el uso de la encriptación, el establecimiento de normas técnicas débiles para la encriptación o el control de la importación y la exportación de herramientas de encriptación[35].

El Reporte de las Naciones Unidas sobre cifrado y anonimato ha pedido a los Estados que promuevan el cifrado fuerte y el anonimato, y ha señalado que las órdenes de descifrado sólo deberían ser permisibles cuando sean el resultado de leyes transparentes y accesibles al público, aplicadas únicamente de forma selectiva y caso a caso a los individuos (no a una masa de personas), y sujetas a una orden judicial y a la protección de los derechos de las personas a un proceso justo[36].

De esta manera, el cifrado y el anonimato en Internet permiten el desarrollo de un ámbito de privacidad para la protección de opiniones y creencias del escrutinio e injerencias externas, que puedan vulnerar la libertad de expresión de las personas. Por lo tanto, cuando los Estados imponen censura ilegal mediante filtros y otras tecnologías, el uso del cifrado y el anonimato puede empoderar a las personas para eludir barreras y acceder a información e ideas sin la intrusión de las autoridades, y así promover el derecho a la libertad de expresión.

VIGILANCIA ESTATAL CON MEDIOS DIGITALES

La vigilancia de las comunicaciones abarca el control, la interceptación, la recopilación, la obtención, el análisis, el uso, la conservación, la retención, la interferencia, el acceso o acciones similares llevadas a cabo con respecto a la información que incluye, refleja, surge o se refiere a las comunicaciones de una

[33] *Ibídem*, párr. 36.
[34] *Ibídem*, párrs. 30 y 40.
[35] *Ibídem*, párrs. 30 y 41.
[36] *Ibídem*, párrs. 59-60.

persona en el pasado, el presente o el futuro[37]. Esto se refiere tanto al contenido de las comunicaciones como a los metadatos. Con respecto a estos últimos, se ha señalado que la agregación de información —comúnmente denominados "metadatos"— pueden dar una idea del comportamiento, las relaciones sociales, las preferencias privadas y la identidad de una persona. En su conjunto, pueden permitir sacar conclusiones muy precisas sobre la vida privada de una persona.

La Observación General No. 16 del Comité de Derechos Humanos establece que "la vigilancia, ya sea electrónica o de otro tipo, la interceptación de las comunicaciones telefónicas, telegráficas y de otro tipo, las escuchas telefónicas y la grabación de conversaciones deben estar prohibidas"[38]. La vigilancia —tanto la recopilación masiva de datos[39], como la recopilación selectiva de datos— interfiere directamente en la intimidad y la seguridad necesarias para la libertad de opinión y de expresión, y debe evaluarse a través de un test tripartito para evaluar la permisibilidad de la restricción. En la era digital, las TIC han aumentado la capacidad de los gobiernos, las empresas y los particulares para llevar a cabo la vigilancia, la interceptación y la recopilación de datos, y han hecho que la eficacia en la realización de dicha vigilancia ya no esté limitada por la escala o la duración.

En una resolución adoptada por la Asamblea General de las Naciones Unidas sobre el derecho a la intimidad en la era digital, se destacó que la vigilancia y/o interceptación ilegal o arbitraria de las comunicaciones, así como la recopilación ilegal o arbitraria de datos personales, son actos altamente intrusivos que violan el derecho a la intimidad, pueden interferir con el derecho a la libertad de expresión y pueden contradecir los principios de una sociedad democrática, incluso cuando se llevan a cabo a escala masiva[40]. Señaló además que la vigilancia de las comunicaciones digitales debe ser coherente con las obligaciones internacionales en materia de derechos humanos y debe llevarse a cabo sobre la base de un marco jurídico, que debe ser accesible al público, claro, preciso, exhaustivo y no discriminatorio.

Para cumplir la condición de legalidad, muchos Estados han tomado medidas para reformar sus leyes de vigilancia con el fin de permitir los poderes necesarios para llevar a cabo estas actividades. De acuerdo con los principios de necesidad y proporcionalidad, la vigilancia de las comunicaciones debe considerarse un acto altamente intrusivo y, para cumplir el umbral de proporcionalidad, se debe exigir al Estado que, como mínimo, establezca la siguiente información a una autoridad judicial competente antes de llevar a cabo cualquier vigilancia de las comunicaciones:

---

[37] Necessary and Proportionate Principles (2014). *International principles on the application of human rights to communications surveillance*, pág. 4. Obtenido de: https://necessaryandproportionate.org/files/2016/03/04/en_principles_2014.pdf.

[38] Comité de Derechos Humanos (1988). *Observación General No. 36*. Vigésima tercera sesión. Recopilación de Comentarios Generales y Recomendaciones Generales Adoptadas por los Órganos de Tratados de Derechos Humanos. HRI/GEN/1/Rev.1, párr. 8.

[39] Edward Snowden, ha revelado que la Agencia de Seguridad Nacional de Estados Unidos y la Sede General de Comunicaciones en el Reino Unido habían desarrollado tecnologías que permitían el acceso a gran parte del tráfico global de Internet, registros de llamadas, libretas de direcciones electrónicas de individuos y grandes volúmenes de otros contenidos de las comunicaciones. Estas tecnologías se despliegan a través de una red transnacional que comprende las relaciones de inteligencia estratégica entre los gobiernos y otros actores.

[40] UNGA *Resolution on the right to privacy in the digital age* A/C.3/71/L.39/Rev.1, 16 November 2016 (2016 UN Resolution on Privacy). Obtenido de: http://www.un.org/ga/search/view_doc.asp?symbol=A/C.3/71/L.39/Rev.1

- Si existe un alto grado de probabilidad de que se haya cometido o se vaya a cometer un delito grave o una amenaza específica contra un objetivo legítimo.
- Si se han agotado otras técnicas menos invasivas o serían inútiles, de modo que la técnica utilizada es la opción menos invasiva.
- La información a la que se acceda se limitará a la que sea relevante y material para el delito grave o la amenaza específica a un objetivo legítimo alegado.
- El exceso de información recopilada no se conservará, sino que se destruirá o devolverá rápidamente.
- El acceso a la información sólo lo tendrá la autoridad especificada y se utilizará únicamente para el propósito y la duración para los que se dio la autorización.
- Las actividades de vigilancia solicitadas y las técnicas propuestas no atentan contra la esencia del derecho a la intimidad o de las libertades fundamentales.

La vigilancia constituye una injerencia evidente en el derecho a la intimidad. Además, también constituye una injerencia en el derecho a mantener opiniones sin interferencias y en el derecho a la libertad de expresión. Con especial referencia al derecho a mantener opiniones sin interferencias, los sistemas de vigilancia, tanto selectivos como masivos, pueden socavar el derecho a formarse una opinión, ya que el miedo a la revelación involuntaria de la actividad en línea, como la búsqueda y la navegación, probablemente disuade a las personas de acceder a la información, especialmente cuando dicha vigilancia conduce a resultados represivos.

La interferencia con el derecho a la libertad de expresión es particularmente evidente en el contexto de los periodistas y miembros de los medios de comunicación que pueden ser sometidos a vigilancia como resultado de sus actividades periodísticas. Como ha señalado el Secretario General de la ONU, esto puede tener un efecto amedrentador en el ejercicio de la libertad de los medios de comunicación, y dificulta la comunicación con las fuentes y el intercambio y desarrollo de ideas, lo que puede llevar a la autocensura. El uso de la encriptación y de otras herramientas similares se ha convertido en algo esencial para el trabajo de los periodistas, a fin de garantizar que puedan realizar su labor sin interferencias.

La revelación de las fuentes periodísticas y la vigilancia pueden tener consecuencias negativas para el derecho a la libertad de expresión debido a la violación de la confidencialidad de las comunicaciones de una persona. Una vez que la confidencialidad es socavada, no puede ser restaurada. Por lo tanto, es de suma importancia que las medidas que socavan la confidencialidad no se tomen de forma arbitraria.

La importancia de la protección de las fuentes está bien establecida. Por ejemplo, la Relatoría Especial para la Libertad de Expresión manifestó que la confidencialidad de las fuentes es un elemento esencial de la labor periodística y del papel de los periodistas para informar sobre cuestiones de interés público y recordó que conforme el Principio 8 de la Declaración de Principios sobre Libertad de Expresión de la CIDH, "todo comunicador social tiene derecho a la reserva de sus fuentes de información, apuntes y archivos personales y profesionales". En palabras de la Relatoría Especial:

> “La importancia del derecho a la confidencialidad de las fuentes reside en que, a fin de proveer al público de información necesaria para satisfacer su derecho a recibir información, los

> periodistas realizan un importante servicio al público cuando recaban y difunden información que no sería divulgada si la reserva de las fuentes no estuviera protegida. La confidencialidad, por lo tanto, es esencial para el trabajo de los periodistas y para el rol que cumplen en la sociedad de informar sobre asuntos de interés público"[41].

En este sentido, las actividades de vigilancia llevadas a cabo contra los periodistas corren el riesgo de socavar fundamentalmente la protección de las fuentes a la que tienen derecho los periodistas.

Actualmente en la región, existe una moratoria normativa sobre la venta, la transferencia y el uso de la tecnología de vigilancia con enfoque de derechos humanos que anida una zona gris, donde los Estados arraigan prácticas de vigilancia con herramientas digitales[42]. En la región se ha evidenciado en los últimos años el repetido uso de softwares de vigilancia en múltiples países indican un patrón sumamente preocupante de intimidación de periodistas y defensoras y defensores de derechos humanos.

En agosto de 2021, La Comisión Interamericana de Derechos Humanos (CIDH), su Relatoría Especial para la Libertad de Expresión (RELE) y la Oficina en México del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (ONU-DH) expresaron su preocupación ante los nuevos hallazgos sobre la utilización del software Pegasus para espiar a periodistas, personas defensoras de derechos humanos y personas con liderazgo público que ejercían oposición al gobierno[43].

De modo similar, en enero de 2022, respecto del caso de El Salvador, la CIDH, RELE y OACNUDH expresaron preocupación ante los hallazgos sobre uso del software Pegasus para espiar a periodistas y organizaciones de la sociedad civil[44]. Al respecto, destacaron que "Ante situaciones de denuncia de vigilancia digital sobre actividades legítimas como el periodismo y la defensa de derechos humanos, es deber de los Estados notificar formal y oportunamente a las personas cuya privacidad ha sido invadida con el fin de que éstas puedan: i) conocer la información recolectada y ii) manifestar su opinión sobre el tratamiento futuro que se debe dar a esa información."

CONCLUSIÓN

A medida que el mundo se mueve en línea, la protección de datos es cada vez más necesaria. En el contexto americano, se han logrado algunos avances. Chile fue el primer país de América Latina que adoptó una ley de protección de datos en 1999, seguido de Argentina en el 2000. Varios países han

[41] Organización de Estados Americanos. *Relatoría Especial manifiesta preocupación por acciones para que periodistas revelen sus fuentes y materiales informativos en Perú*. Comunicado de Prensa R151/18 del 12 de julio de 2018. Obtenido de: https://www.oas.org/es/cidh/expresion/showarticle.asp?artID=1110&lID=2

[42] https://hchr.org.mx/comunicados/declaracion-de-la-alta-comisionada-de-la-onu-para-los-derechos-humanos-michelle-bachelet-sobre-el-uso-de-software-espia-para-vigilar-periodistas-y-personas-defensoras-de-derechos-humanos/

[43] https://hchr.org.mx/comunicados/la-cidh-su-rele-y-onu-dh-mexico-manifiestan-preocupacion-ante-nuevos-hallazgos-sobre-la-utilizacion-del-software-pegasus/

[44] http://www.oas.org/es/cidh/jsForm/?File=/es/cidh/prensa/comunicados/2022/022.asp

seguido este ejemplo, tales como Uruguay, México. Perú, Colombia, Brasil, Barbados y Panamá[45]. A medida que avanzamos, los activistas de los derechos digitales tienen un papel importante que desempeñar para garantizar que los Estados sigan el ritmo de la evolución de la protección de datos y promulguen marcos legislativos que protejan y promuevan plenamente el derecho de las personas a la privacidad.

[45] El Espectador. ¿Cómo se encuentra la protección de datos en Latinoamérica? 29 de septiembre de 2020. Obtenido de: https://www.elespectador.com/tecnologia/como-se-encuentra-la-proteccion-de-datos-en-latinoamerica-article/