



PUBLICACIÓN DE INFORMACIÓN PERSONAL EN PROVIDENCIAS JUDICIALES Y LA ERA DIGITAL

Cartilla

PUBLICACIÓN DE INFORMACIÓN PERSONAL EN PROVIDENCIAS JUDICIALES Y LA ERA DIGITAL

Cartilla

• • •

2023

Defensoría del Pueblo

Defensoría Delegada para la Protección de Derechos
en Ambientes Digitales y Libertad de Expresión



#NosUnenTusDerechos



#NosUnenTusDerechos

© Defensoría del Pueblo, 2023

Obra de distribución gratuita.

El presente texto se puede reproducir, fotocopiar o replicar, total o parcialmente, citando la fuente.

Colombia. Defensoría del Pueblo. Cartilla:
Publicación de información personal en providencias judiciales y la era digital.

Páginas:32

Bogotá, D. C., 2023

Equipo de la Defensoría Delegada
para la Protección de Derechos en Ambientes
Digitales y Libertad de Expresión

Autores

EVML

Diseño y diagramación

EVML

Diseño de portada

Sonia Villalba

Corrección de estilo

Fotografías

Banco de fotos de la Defensoría del Pueblo

Impresión

Impreso en Colombia

CARLOS CAMARGO ASSIS
Defensor del Pueblo

LUIS ANDRÉS FAJARDO ARTURO
Vicedefensor del Pueblo

OSCAR JULIÁN VALENCIA LOAIZA
Secretario General

NELSON FELIPE VIVES CALLE
Secretario Privado

JULIO SOLANO JIMÉNEZ
**Defensor Delegado para la Protección de
Derechos en Ambientes Digitales y Libertad
de Expresión**

Coordinación y edición general
GISSELA ARIAS GONZÁLEZ
**Directora Nacional de Promoción y Divulga-
ción de los Derechos Humanos.**
Secretaría Técnica del Comité Editorial

• • •

*Este documento debe citarse así:
Defensoría del Pueblo - Defensoría Del pueblo.
[2023]. Cartilla: Publicación de información per-
sonal en providencias judiciales y la era digital.*

PUBLICACIÓN DE INFORMACIÓN PERSONAL EN PROVIDENCIAS JUDICIALES Y LA ERA DIGITAL

Cartilla

• • •

2023

Defensoría del Pueblo

Defensoría Delegada para la Protección de Derechos
en Ambientes Digitales y Libertad de Expresión

CONTENIDO

Presentación	5
Introducción	7
1 La administración de justicia en Colombia y la publicación de providencias judiciales en medios digitales	7
1.1 Las providencias judiciales y el principio de publicidad.....	7
1.2 Sentencias de la justicia penal y los fines de la pena	8
2 Derechos humanos susceptibles de vulneración ante la publicación de providencias judiciales en medios digitales	10
2.1 Derecho a la privacidad.....	10
2.1.1 Origen del reconocimiento del derecho a la privacidad ..	10
2.1.2 La privacidad como derecho	10
2.1.3 Características y límites del derecho a la privacidad.....	11
2.1.4 Marco normativo de la protección de la privacidad y de los datos personales en Colombia	12
2.2 Derecho al olvido	13
2.2.1 Origen y concepto del derecho al olvido	13
2.2.2 Primeros esbozos del derecho al olvido en Colombia	17
2.2.3 Protección del derecho al olvido en los motores de búsqueda digitales.....	17
2.2.4 Límites del derecho al olvido	19
2.3 Otros derechos: el buen nombre y la honra.....	19
3 Recomendaciones para la publicación digital de información personal en providencias judiciales	21
3.1 Los derechos humanos y la publicación digital de providencias judiciales en la jurisprudencia colombiana.....	21
3.2 Las Reglas de Heredia	26
4 Conclusiones	29
Referencias	30

PRESENTACIÓN

La Defensoría del Pueblo de Colombia constituyó la Defensoría Delegada para la Protección de Derechos en Ambientes Digitales y Libertad de Expresión, con el propósito de institucionalizar la integración de tecnologías de la información en beneficio de la dignidad humana y desarrollar estrategias innovadoras para la promoción y protección de los derechos humanos en los escenarios digitales del país. Esto se enmarca en el Plan Estratégico Institucional “Nos unen tus derechos”, que potencia la promoción y difusión de los derechos humanos mediante la transformación tecnológica y la creación de novedosos sistemas de información.

La misión de esta Defensoría Delegada es analizar las dinámicas de los entornos digitales a la luz de la teoría universal de los derechos humanos, con el fin de establecer criterios que aseguren los derechos de la población colombiana, inclusive en el ciberespacio. Entre los principales objetivos de la Defensoría Delegada se destacan:

1. Centralizar la información pública y privada relacionada con la protección y promoción de los derechos humanos en entornos digitales, para crear una ruta de protección 4.0.
2. Establecer marcos de colaboración interinstitucionales entre el Estado colombiano, las redes sociales y las empresas que ofrecen servicios de redes, telecomunicaciones, contenidos digitales y, en general, aquellas plataformas basadas en la interacción tecnológica humana.
3. Desarrollar campañas de educación dirigidas a prevenir las vulneraciones en línea, con un enfoque en la reparación de las víctimas, los sujetos de especial protección constitucional y la población más afectada en línea.
4. Fomentar la protección de los derechos humanos en entornos digitales a través de la organización de encuentros académicos interinstitucionales.

5. Colaborar con organizaciones de la sociedad civil, líderes y expertos en tecnología para desarrollar guías y recursos informativos que empoderen a la población colombiana para navegar de manera segura y ética en el mundo digital.

Esta cartilla sobre la publicación de información personal en providencias judiciales en escenarios digitales es un ejemplo de la materialización de los nuevos tipos de estudios y estrategias que se llevan a cabo en la Defensoría del Pueblo de Colombia. La finalidad es actualizar las estrategias de promoción y protección de derechos en el universo digital, para brindar orientación a organizaciones públicas y privadas en el desarrollo de herramientas y en la toma de decisiones relacionadas con la protección de datos personales presentes en autos y sentencias publicados en páginas web, buscadores y plataformas digitales. Además, se busca mejorar los índices de reconocimiento y protección del derecho al olvido y de derechos análogos, como la privacidad, la honra y el buen nombre.

*“Vamos a conectar con los millones de colombianos que pasan parte de su vida en estos entornos digitales y que necesitan de nuestro apoyo constante para proteger y garantizar sus derechos. Hay mucho por hacer y es hora de comenzar. Hoy, sin titubeos, podemos afirmar que es una realidad que estaremos activos también en los territorios digitales y que, con la colaboración de todas las instituciones, redes sociales y, por supuesto, los actores clave en el mundo de las tecnologías de la información y comunicación, buscaremos establecer vías de protección concretas y sólidas”.**

CARLOS CAMARGO ASSIS,

Bogotá, D. C., 15 de marzo de 2022

Palabras en el discurso de instalación del lanzamiento de la Defensoría Delegada para la Protección de Derechos en Ambientes Digitales y Libertad de Expresión.

PUBLICACIÓN DE INFORMACIÓN PERSONAL EN PROVIDENCIAS JUDICIALES Y LA ERA DIGITAL

Introducción

La incorporación de las nuevas tecnologías en la administración y difusión de información judicial ha generado tensiones entre derechos fundamentales. Por un lado, se encuentran derechos como el buen nombre, *habeas data*, privacidad y el derecho al olvido, que parecen entrar en conflicto con derechos como la libertad, acceso, publicidad, opinión y transparencia de la información judicial. Esta colisión de derechos ha impulsado la necesidad de establecer pautas específicas para el manejo digital de datos personales en el ámbito judicial, un proceso que en Colombia se define a través de las decisiones de las altas cortes y la revisión de recomendaciones internacionales en la materia.



1. LA ADMINISTRACIÓN DE JUSTICIA EN COLOMBIA Y LA PUBLICACIÓN DE PROVIDENCIAS JUDICIALES EN MEDIOS DIGITALES

1.1 Las providencias judiciales y el principio de publicidad

Los jueces emiten decisiones al administrar justicia mediante dos formas de comunicación: los autos, que suelen abordar cuestiones procedimentales relacionadas con la gestión y desarrollo de un proceso judicial, y las sentencias, que resuelven definitivamente el caso en cuestión. Autos y sentencias se agrupan bajo el término ‘providencias judiciales’. De acuerdo con el principio de publicidad, presente en la administración de justicia, es esencial que las providencias judiciales se divulguen a través de diversos medios. La transición hacia el ámbito digital también ha tenido un impacto en la difusión de estas providencias, ahora accesibles para las partes, intervinientes y la opinión pública a través de Internet y aplicaciones digitales, entre otra inmensa gama de tecnologías basadas en la información y las comunicaciones.

El principio de publicidad es un mandato general del derecho, que en el ámbito de la ad-

ministración de justicia tiene dos escenarios de aplicación. El primero, como garantía del debido proceso, relacionado con la responsabilidad de los jueces de asegurarse de que las partes y los sujetos procesales, legitimados para consultar la información de los procesos, estén al tanto de las providencias judiciales. El segundo, como garantía del derecho al acceso a la información pública, derivado del derecho de los ciudadanos a conocer las sentencias judiciales, salvo una norma expresa en contrario.

Las providencias judiciales involucran el uso de información personal, clasificada según la ley colombiana en datos de carácter público, privado, semiprivado o sensible. Aunque existen etapas judiciales con carácter reservado que implican la privacidad de los datos personales, al final de los procesos se busca la transparencia de la administración judicial al publicar las sentencias. Esta tensión entre la privacidad de los datos personales y la necesidad de publicación de las sentencias se hace más evidente, especialmente en la justicia penal, que supone el relacionamiento de datos personales con la comisión de delitos, particularmente antecedentes penales, considerados en el ordenamiento jurídico colombiano como datos personales semiprivados.

1.2 Sentencias de la justicia penal y los fines de la pena

Las sentencias emitidas por jueces penales determinan, entre otras, las penas a las que serán o no sometidos los investigados por la presunta comisión de uno o varios delitos. Francesco Carrara (1973), mayor exponente de la escuela clásica penal italiana, definió la pena como el castigo que la autoridad impone a un culpable por su delito. Franz von Liszt, famoso profesor de Derecho Penal y político alemán, concibió a su vez la pena como la consecuencia más importante en términos jurídicos para el autor de un delito, aplicada bajo los fundamentos retributivos y preventivos (Monroy Sierra, 2005).

En el sistema penal colombiano la pena tiene tres objetivos principales: prevenir, castigar y resocializar. Esta triada se refleja en la Sentencia C-430 de 1996 de la Corte Constitucional, en la que se explica que el fin preventivo se cumple al establecer la sanción, el fin retributivo se manifiesta al imponer la pena judicialmente y el fin resocializador guía su ejecución conforme a los principios y normas del Derecho Internacional adoptadas por Colombia (1996). Es en estos objetivos donde se hace más clara la razón detrás de la publicidad de las sentencias.

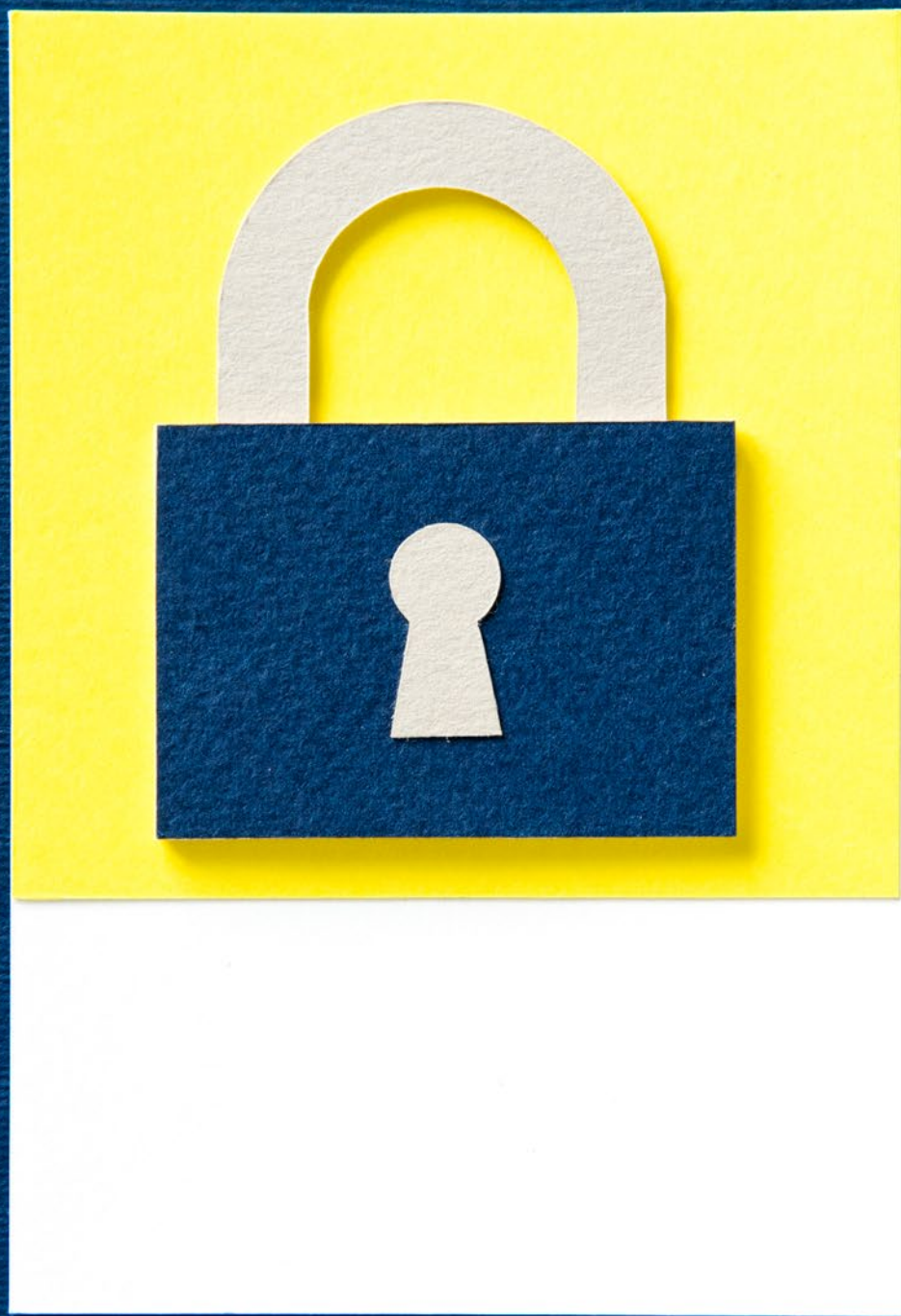
Los principios generales del derecho guían las penas impuestas por los jueces penales para cumplir con los objetivos que persiguen. En su influyente obra *De los delitos y de las penas*, Cesare Beccaria (1968) enfatizó que una pena, para no convertirse en una forma de violencia contra un ciudadano, debe ser pública, rápida, necesaria y la más mínima

posible dadas las circunstancias; además debe estar en proporción con los delitos y ser dictada por las leyes. En la actualidad, el principio de legalidad, el principio de necesidad de la sanción y el principio de proporcionalidad, entre otros, guían la imposición de las penas en la administración de justicia penal.

Las penas tienen varias características fundamentales que se derivan de los principios que las guían, como se detalla a continuación:

- a. La pena debe ser impuesta conforme a lo establecido en la ley (Velásquez, 2010).
- b. La responsabilidad penal es personal, lo que significa que se aplica únicamente a la persona declarada culpable y no a terceros (Monroy Sierra, 2005).
- c. La pena debe cumplirse estrictamente y, en principio, no es modificable. Se vuelve irrevocable cuando el juez, a través de una sentencia ejecutoriada, determina y emite una decisión final (Velásquez, 2010).

En virtud de estos presupuestos, la administración de justicia cumple con varias de sus funciones al publicar las providencias judiciales. Especialmente en la justicia penal, considerando las características, objetivos y principios que guían las penas y la necesidad de la transparencia y acceso público a las decisiones judiciales, las autoridades podrían enfrentarse a escenarios propicios para la vulneración de derechos humanos, como resultado de un inadecuado tratamiento de datos personales, si no se tienen en cuenta las medidas suficientes para la correcta publicación en escenarios digitales de información personal en providencias judiciales.



2. DERECHOS HUMANOS SUSCEPTIBLES DE VULNERACIÓN ANTE LA PUBLICACIÓN DE PROVIDENCIAS JUDICIALES EN MEDIOS DIGITALES

2.1 Derecho a la privacidad

2.1.1 Origen del reconocimiento del derecho a la privacidad

A finales del siglo XIX, los profesores estadounidenses Samuel Warren y Louis Brandeis (1890) definieron por primera vez la privacidad como el derecho a estar solos, es decir, a que se respete el espacio personal, lejos del escrutinio público. Esta reinterpretación de la idea se originó a partir de una frase acuñada en 1879 por el juez Thomas M. Cooley en la primera edición de su *Tratado sobre la Ley de Responsabilidad Civil Extracontractual*.

Casi cuarenta años después del ensayo sobre el derecho a la privacidad, el profesor Brandeis, esta vez como magistrado de la Corte Suprema de Estados Unidos, reafirmó su postura académica en el caso *Olmstead vs. United States* (1928). En este caso, se estableció que cualquier intrusión injustificada del Gobierno en la privacidad de los individuos debe ser considerada una violación a la cuarta enmienda, relacionada

con registros y allanamientos arbitrarios (Guerreiro Peralta, 2009). A partir de estos precedentes judiciales, se ha buscado abordar de manera legal la protección del derecho fundamental a la privacidad (Nieves Saldaña, 2011).

2.1.2 La privacidad como derecho

El reconocimiento del derecho a la privacidad marcó el inicio de un esfuerzo constante por proteger la vida privada de los individuos frente a los múltiples riesgos que pueden surgir en el manejo de la información personal. Tras la revolución digital del siglo XXI, en la que la información se convirtió en un recurso poderoso susceptible de ser utilizado por cualquier entidad (ya sea un individuo u organización), Gobiernos de todo el mundo comenzaron a promover leyes y políticas públicas centradas en la protección de los datos personales. Esta priorización de los datos personales como un derecho fundamental surge de la fuerte convicción de que esta información es una extensión de la propia identidad, a la cual nadie debería tener acceso sin consentimiento, y las sentencias judiciales publicadas en medios di-

giales no son, en principio, una excepción a esta máxima.

En la tradición europea, la privacidad ha estado asociada con la noción de dignidad humana. Siguiendo este enfoque, Leturia (2016) sostiene que la privacidad se relaciona con el derecho al libre desarrollo de la forma de vida y con la protección del derecho de cada individuo a vivir como el dueño y arquitecto de su propio destino. En consecuencia, el derecho fundamental a la privacidad goza de una amplia esfera de protección, superando concepciones tradicionales de control y adoptando una forma subjetiva o individual para resguardar a las personas como individuos frente a cualquier intromisión injustificada del poder público o la prensa en su ámbito personal (Guerrero Peralta, 2009).

Según Daniel Solove y Neil Richards, la privacidad de la información implica el derecho a controlar el flujo de nuestra información personal (Manheim & Kaplan, 2019), lo que podría entenderse como la totalidad de la información que mantenemos en privado o de forma confidencial, como medida preventiva ante la intromisión de terceros. Se considera además que la privacidad es una cuestión de poder, ya que influye en cómo las personas se comportan, toman decisiones y actúan en general (Solove, 2002). Comúnmente, las personas están preocupadas por cómo se utiliza su información para tomar decisiones o clasificarla, lo que podría afectar su disfrute de una personalidad inviolable (Barocas et al., 2017).

Por otro lado, la Declaración Universal de Derechos Humanos (DUDH) en el artículo 12 establece: “Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o reputación”, principio que se refrenda en el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos.

2.1.3 Características y límites del derecho a la privacidad

Así como la intimidad, el buen nombre o la honra (Guerrero Peralta, 2009), la privacidad representa uno de los derechos que materializa la dignidad humana (Leturia, 2016). Desde la perspectiva teórica, que concibe la privacidad como un derecho autónomo (Conde Ortiz, 2005), se reconoce su universalidad al ser inherente a todas las personas, independientemente de su raza, género, religión o nacionalidad. Al respecto y como resultado de su desarrollo histórico, la privacidad es mundialmente reconocida como un derecho civil y político.

La privacidad, en principio, se orienta de manera negativa, implicando que los Estados tienen la obligación de evitar cualquier tipo de interferencia o coerción en su ejercicio. Tanto agentes públicos como privados son considerados responsables en la medida en que se afecte de manera adversa la privacidad, lo que a su vez activa el aparato judicial y administrativo dependiendo de la gravedad de la vulneración. Además, la privacidad se percibe como un pilar fundamental de la democracia y el pluralismo, especialmente en la era de la información y las tecnologías de la comunicación, donde la sociedad busca cada vez más resguardar su órbita de acción.

Como sucede con cualquier otro derecho dentro de un Estado de derecho, la privacidad tiene límites; esto implica que los derechos en sí mismos no son absolutos ni ilimitados (Tórtora Aravena, 2010). Siguiendo la teoría jurídica, los límites de los derechos pueden ser de dos tipos: externos, determinados en el momento de su ejercicio, o internos, es decir, establecidos desde su concepción misma como derecho (Maldonado Muñoz, 2021).

En el caso de la privacidad, las principales limitaciones externas corresponden a la consideración del interés general, que en situaciones específicas puede restringirla, en aras de preservar la voluntad pública, la seguridad del Estado o cualquier otro interés legítimo establecido por una normativa (Convención Americana sobre Derechos Humanos - Pacto de San José, 1978). Por ejemplo, un límite externo es la necesidad de la publicidad de las providencias judiciales, en búsqueda del interés general y la seguridad jurídica, entre otros.

Para determinar los límites internos de la privacidad, las autoridades judiciales aplican, entre otros criterios, el concepto de la expectativa razonable de intimidad, establecido a finales de la década de 1920 por la Corte Suprema de los Estados Unidos y adoptado a nivel global (Guerrero Peralta, 2009). Este concepto hace referencia a los actos inequívocos que una persona realiza para establecer una expectativa subjetiva de intimidad (como estar en un lugar privado, cubrirse el rostro o bajar el tono de voz), la cual debe ser reconocida como razonable por la sociedad. En otras palabras, los individuos actúan en pro o en contra de su privacidad a través de una expectativa que es valorada por la sociedad.

2.1.4 Marco normativo de la protección de la privacidad y de los datos personales en Colombia

El artículo 15 de la Constitución Política colombiana establece el derecho de todas las personas a acceder, actualizar y corregir la información almacenada en bases de datos o archivos. Este conjunto de prerrogativas deriva de la antigua y popular locución latina '*habeas data*', que literalmente significa 'tener

los datos', pero que, como institución, engloba los principios y derechos que garantizan la protección de la privacidad y de los datos personales. En este mismo campo, el artículo 20 aborda el derecho a la información, junto con el derecho a la libertad de expresión.

Con base en estos mandatos constitucionales, se promulgó la Ley 1266 de 2008, que establece disposiciones generales sobre el *habeas data* y regula la información contenida en bases de datos personales, especialmente en los ámbitos financiero, comercial y crediticio. Posteriormente y dado que el enfoque de esta ley es en datos comerciales y financieros, se emitió en el país la Ley 1581 de 2012, que se enfocó en resguardar el derecho de *habeas data* en el contexto de los datos personales. Adicionalmente, esta ley introdujo una nueva categoría de datos personales conocidos como 'sensibles', que abarcan aspectos como la vida sexual, el estado de salud, datos biométricos, creencias religiosas, filosóficas, políticas, entre otros, los cuales pueden afectar la intimidad del titular o, si se utilizan de manera indiscriminada, propiciar su discriminación. Una serie de decretos reglamentarios han establecido los procedimientos y guías para materializar las reglas de protección creadas en la Ley 1581.



2.2 *Derecho al olvido*

2.2.1 Origen y concepto del derecho al olvido

La vertiginosa evolución de la tecnología basada en la información ha transformado la manera en cómo se aborda y protege el derecho a la privacidad. En la actualidad, el transcurso del tiempo ya no asegura el olvido; las providencias judiciales y las noticias y artículos relacionados quedan almacenados de forma ilimitada en bases de datos y motores de búsqueda digitales. Esta situación plantea desafíos para la administración de justicia, principalmente en aspectos como la resocialización (mencionada anteriormente como objetivo de las penas) y la ponderación, dado que es necesario equilibrar la necesidad de publicar las providencias con la afectación de otros derechos, como la privacidad. En este contexto, el derecho al olvido surge como una prerrogativa encaminada a proteger a las personas contra el indefinido tratamiento de datos personales en el tiempo.

Ayala Pérez (2016) concibe el derecho al olvido como un componente de la protección de datos personales, encargado de mantener un nivel adecuado de privacidad a través de controles sobre la información personal. Martínez Otero (2015) lo define como una respuesta a los avances tecnológicos que exponen públicamente el pasado de una persona de manera inmediata a través de Internet. Por su parte, Azurmendi (2015) identifica el derecho al olvido como la facultad de solicitar al responsable de un dato personal su cancelación o eliminación, así como la abstención de su difusión.

Rodrigo Pica (2016) lo presenta como un derecho que garantiza la privacidad y el desarrollo de las personas, evitando la constante

persecución del pasado. Para el autor, este derecho otorga la posibilidad de que los datos de una persona dejen de ser accesibles en la web por decisión propia. Francisco Leturia (2016), guiado por el principio de proporcionalidad, argumenta que el derecho al olvido implica que cierta información del pasado no debe ser difundida si puede causar más perjuicio que beneficio, y enfoca la discusión hacia la teoría del daño.

Laura Silberleib (2016) aporta en el esfuerzo conceptualizador del derecho al olvido, al combinar el factor tiempo con la noción de necesidad y relevancia de la información. Afirma que este derecho materializa el principio de limitación temporal e indica que los datos deben ser eliminados una vez que ya no son necesarios o pertinentes para los fines para los cuales fueron recopilados. Estas características implican que la posibilidad de destruir información depende de criterios temporales y de pertinencia.

Siguiendo esta perspectiva académica, José López (2013) plantea que el derecho al olvido implica el poder de la ciudadanía para cancelar y oponerse al tratamiento de sus datos personales cuando estos dejan de ser útiles o necesarios para el propósito con el que fueron recopilados o publicados.

En este sentido, Leturia (2016) destaca que se trata del legítimo interés de cada individuo de no estar permanentemente expuesto a datos que puedan perjudicar su honor o reputación, especialmente en el caso de noticias previamente difundidas en el pasado. Por otro lado, Vaninetti subraya la facultad que tiene un individuo o su familia de evitar que hechos verídicos del pasado, independientemente de su naturaleza deshonrosa o no, sean traídos al presente y puedan ocasionar un descrédito público al ser divulgados, dado el paso del tiempo

y su desconocimiento social (Silberleib, 2016). Una de las más reconocidas autoridades en el campo de la protección de datos, la Agencia Española de Protección de Datos (AEPD), establece que la información se elimina cuando se considera obsoleta debido al paso del tiempo o cuando su divulgación vulnera derechos fundamentales, incluida la reputación (AEPD, 2020).

Rodrigo Pica articula la definición de derecho al olvido citada anteriormente con la noción de rectificación de información, el paso del tiempo y la desnaturalización del uso, bajo el concepto de ilegitimidad sobrevenida. Según su perspectiva, el derecho al olvido implica la posibilidad de rectificar o cancelar el uso de datos en la web, planteando la idea de que el uso de información y noticias se vuelve ilegítimo con el tiempo y al desnaturalizarse su propósito original debido a cambios de circunstancias. Esto implica, según el autor, que el derecho al olvido, como derecho a la cancelación, rectificación u oposición respecto al uso informático de un dato personal, está intrínsecamente ligado a la utilización de la información. Si bien en un momento su uso fue legítimo, con el paso del tiempo dejó de serlo, y su efecto inevitable tras su vencimiento es que el dato debe ser borrado (Pica, 2016).

El Tribunal de Justicia de la Unión Europea, una autoridad destacada en este campo por aplicar las normas de protección de datos del continente, advierte que cuando el tratamiento de datos es inadecuado, desactualizado, se prolonga más allá de lo necesario o es excesivo para su finalidad, podría vulnerar los derechos fundamentales de los titulares. En este sentido, señala que un tratamiento que inicialmente fue lícito de datos precisos podría volverse incompatible con las normas cuando dichos datos ya no sean necesarios

para los fines para los que fueron recogidos o tratados (Tribunal de Justicia de la Unión Europea, 2014).

De acuerdo el Reglamento General de Protección de Datos (RGDP), norma vigente en Europa, el derecho de supresión, conocido como derecho al olvido, otorga a los seres humanos la facultad de solicitar al responsable del tratamiento de sus datos personales la eliminación inmediata en determinadas circunstancias. Estas incluyen: a) cuando los datos ya no son necesarios para los fines originales de su recopilación o procesamiento; b) si el interesado retira su consentimiento y no hay otro fundamento legal para el tratamiento; c) si el interesado se opone al tratamiento y no hay razones legítimas que prevalezcan; d) si los datos han sido tratados de manera ilegal; e) si la supresión es requerida por una obligación legal; o f) si los datos fueron obtenidos en relación con una oferta de servicios de la sociedad de la información (Parlamento Europeo & Consejo de la Unión Europea, 2016).

El reglamento también establece que, en caso de que el responsable del tratamiento haya hecho públicos los datos y esté obligado a suprimirlos, deberá tomar medidas razonables, incluyendo las técnicas, para informar a otros responsables que están tratando esos datos sobre la solicitud de supresión del interesado. Esto implica eliminar enlaces, copias o réplicas de los datos. Para los fines de este documento, corresponde a los enlaces, copias o réplicas de las providencias judiciales publicadas en medios digitales (Parlamento Europeo & Consejo de la Unión Europea, 2016). Sin embargo, de acuerdo con la norma, existen situaciones en las que el derecho de supresión o de olvido no se aplica. Esto ocurre cuando el tratamiento es necesario para: a) el ejercicio del derecho a la libertad de expresión e información; b) el cumplimiento de una

obligación legal, o para el desempeño de una misión de interés público o en el ejercicio de poderes públicos conferidos al responsable; c) razones de interés público en el ámbito de la salud pública; d) fines de archivo, investigación científica, histórica o estadística; o e) la formulación, ejercicio o defensa de reclamaciones (Parlamento Europeo & Consejo de la Unión Europea, 2016). En el caso concreto, estas limitaciones determinan el tiempo adecuado, necesario y proporcional en el que una providencia judicial, bajo el principio de publicidad, supone el tratamiento de datos personales en bases de datos digitales.

El derecho al olvido es, bajo esta reconstrucción teórica, un derecho fundamental, autónomo e independiente. Su objetivo es suprimir los datos personales almacenados en bases de datos soportadas en medios digitales cuando, por el paso del tiempo, carecen de una finalidad legítima, causando un daño a los derechos a la reputación, al buen nombre y a la privacidad, entre otros. Esta información se convierte en inútil, innecesaria e impertinente.

2.2.2 Primeros esbozos del derecho al olvido en Colombia

En el ordenamiento jurídico colombiano, el derecho al olvido no tiene una consagración expresa, se ha protegido a través de algunas decisiones judiciales y ha evolucionado en virtud del garantismo de los jueces constitucionales, en procesos derivados de acciones constitucionales, principalmente acciones de tutela. En 2021, el Congreso de la República introdujo nuevas regulaciones sobre la retención de información negativa en las centrales de riesgo y bases de datos financieros, a través de la Ley 2157 de 2021, comúnmente conocida

como la “Ley del borrón y cuenta nueva”. Esta ley tiene el potencial de brindar a las personas que en algún momento recibieron una calificación negativa, pero que cumplieron con sus obligaciones económicas, la oportunidad de comenzar de nuevo en su historial crediticio y comercial. Esta normativa aborda un campo muy particular del llamado derecho al olvido.

2.2.3 Protección del derecho al olvido en los motores de búsqueda digitales

Las personas, como titulares de datos personales, pueden solicitar la eliminación de información al buscar su nombre o un dato específico en los motores de búsqueda digitales, siempre que detecten un uso indebido de sus datos. Esta facultad está respaldada por el Tribunal de Justicia de la Unión Europea (TJUE), que se ha pronunciado sobre los resultados obtenidos en búsquedas realizadas en motores de búsqueda. En un caso concreto de 2014, este Tribunal consideró que, dada la naturaleza delicada de una información contenida en determinados anuncios y el hecho de que su publicación original databa de 5 años atrás, el interesado tenía el derecho a que esta información ya no estuviera vinculada a su nombre en esa respectiva lista (Tribunal de Justicia de la Unión Europea, 2014). En esta decisión, el administrador del motor de búsqueda adujo que no ejercía ningún control sobre los datos que gestionaba en Internet. Sin embargo, procurando esclarecer su responsabilidad, el TJUE expresamente determinó que el gestor de un motor de búsqueda lleva a cabo una exploración automatizada, constante y sistemática de la información disponible en Internet. Durante este proceso, recopila datos, los extrae, registra y organiza en el contexto de sus programas de

indexación. Posteriormente, almacena esta información en sus servidores y, cuando es necesario, la comunica y facilita el acceso a los usuarios en forma de listas de resultados de búsquedas. Todas estas operaciones deben ser consideradas como un proceso de tratamiento de datos personales, sin que sea relevante que el gestor del motor de búsqueda también realice estas mismas operaciones con otros tipos de información y no haga distinción entre estos activos y los datos personales (Tribunal de Justicia de la Unión Europea, 2014). Adicionalmente, el TJUE estableció que, bajo ciertas condiciones, el administrador del motor de búsqueda tiene la obligación de eliminar los resultados obtenidos a partir del nombre de una persona, incluyendo los enlaces a páginas web publicadas por terceros que contengan información sobre esa persona (Tribunal de Justicia de la Unión Europea, 2014). Además, subrayó que esta obligación puede persistir incluso si el nombre o la información no se eliminan previa o simultáneamente de esas páginas web, e incluso si la publicación en dichas páginas es en sí misma lícita (2014).

Martínez Otero (2015) destaca que los motores de búsqueda han implementado procedimientos específicos en sus términos y condiciones para evaluar solicitudes de supresión de ciertos datos personales. Por ejemplo, Google sostiene que llevará a cabo una ponderación entre los derechos de privacidad de los usuarios y el derecho del público a conocer y distribuir información al considerar dicha solicitud. En este proceso, el buscador examinará si los resultados incluyen información obsoleta sobre el solicitante y si existe un interés público legítimo en esa información. Frente al análisis de este documento, Google expresamente señala que podría negarse a retirar cierta información relacionada con condenas penales.

En cuanto al ordenamiento jurídico colom-

biano y la administración de justicia en Colombia, si bien la Ley 1581 de 2012 determina el régimen general de protección de datos personales, no existe en esta ni en otra norma una mención expresa sobre el derecho al olvido ni a ninguna prerrogativa con un contenido semejante. Ha sido la Corte Constitucional colombiana la que, a partir del año 2015, ha emitido pronunciamientos encaminados a la materialización de este derecho. Estos pronunciamientos se centran en la implementación de medidas técnicas que directamente pretenden modificar o suprimir los datos personales alojados en los motores de búsqueda, con el fin de evitar la correspondiente identificación o individualización de los titulares de los datos y, en consecuencia, proteger su derecho al olvido. Estas importantes decisiones judiciales y la estrategia técnica dispuesta por los operadores judiciales en Colombia son detalladamente analizadas en el aparte 3.1. de este documento, titulado “Los derechos humanos y la publicación digital de providencias judiciales en la jurisprudencia colombiana”.

2.2.4 Límites del derecho al olvido

Como la privacidad, el derecho al olvido tiene límites. En términos prácticos, el derecho a divulgar información o el derecho a la libertad de expresión pueden considerarse limitaciones externas del derecho al olvido. Desde esta perspectiva, los expertos sostienen que, por regla general, el derecho a la información prevalecerá sobre el derecho al olvido, incluso con el paso del tiempo, cuando implica datos de relevancia histórica o se relaciona con hechos asociados al ejercicio de la actividad pública o por parte de una figura pública (De Terwangne, 2012).

En el contexto de la publicación de providen-

cias judiciales en medios digitales, el derecho a la información puede prevalecer en ciertos casos, especialmente cuando los hechos objeto del proceso judicial revelan un interés legítimo para su divulgación. Esto puede ocurrir, por ejemplo, cuando una decisión judicial se convierte (además de su carácter público) en una noticia de interés público. En este contexto, es legítimo recordar esta decisión, incluyendo los nombres de las partes (excepto si se trata de menores de edad, en cuyo caso se aplican normativas de protección diferentes). Sin embargo, con el paso del tiempo, cuando la cuestión ya no es de actualidad o no es considerada noticiable, y siempre que no exista una razón justificada para una nueva divulgación de la información como noticia, el derecho al olvido anula el derecho a la información (De Terwangne, 2012).

Por lo tanto, el derecho a la información, como límite al derecho al olvido, prevalece en aquellos casos en los que es necesario difundir información personal judicial, especialmente penal, en una noticia. No obstante, una vez que la relevancia actual del acontecimiento ha cesado, o más específicamente, después de que se ha cumplido la condena y se han alcanzado los objetivos de la pena, se configuran las circunstancias para que prevalezca el derecho al olvido (Silberleib, 2016).

2.3 Otros derechos: el buen nombre y la honra

De manera específica y solo en determinados casos, las garantías fundamentales asociadas con la publicación de datos personales en decisiones judiciales se centran en nociones de reputación, juicios y valoraciones sociales. Uno de estos derechos, el derecho al buen nombre, según la interpre-

tación de la Corte Constitucional, se refiere al juicio que los demás miembros de una sociedad hacen sobre una persona en particular. Su propósito radica en proteger a este individuo de expresiones ofensivas, injuriosas o información falsa o tendenciosa (Sentencia C-489 de 2002).

Aunque la Corte no establece una separación total entre los derechos a la honra y al buen nombre, reconoce que ambos están interconectados. El derecho al buen nombre se relaciona con la reputación de una persona en actividades públicas, mientras que la honra se refiere a la consideración que merece como miembro de la especie humana y a aspectos más privados de su vida (Sentencia C-442 de 2011).

En términos de dignidad humana, la Corte sostiene que el derecho a la honra está estrechamente ligado, ya que involucra la valoración de la persona como individuo, así como la evaluación de aspectos íntimos no cubiertos por la intimidad personal y familiar. Por su parte, el buen nombre también guarda una estrecha relación con la dignidad humana, al proteger contra ataques que restrinjan la proyección de la persona en el ámbito público o colectivo (Sentencia C-442 de 2011).

La Declaración Universal de los Derechos Humanos de 1948 respalda estos conceptos al prohibir injerencias arbitrarias en la vida privada, la familia, el domicilio y la correspondencia, así como ataques a la honra o la reputación, destacándose el empleo de los términos como equivalentes o intercambiables. En la Declaración, la Asamblea General de las Naciones Unidas enfatiza que toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques (Asamblea General de las Naciones Unidas, 1948, artículo 12).



3. RECOMENDACIONES PARA LA PUBLICACIÓN DIGITAL DE INFORMACIÓN PERSONAL EN PROVIDENCIAS JUDICIALES

La incorporación de las nuevas tecnologías en la gestión y difusión de la información judicial en la era digital puede dar lugar a conflictos entre derechos fundamentales. Por un lado, el derecho al buen nombre, *habeas data*, privacidad, derecho al olvido, etc., y por otro, los derechos a la libertad, acceso, publicidad, opinión y transparencia de la información judicial, entre otros. Esta colisión de derechos determina el establecimiento de pautas específicas para el manejo de datos personales en el ámbito judicial, cuyo enfoque debe procurar la comprensión de la decisión judicial y sus fundamentos jurídicos, manteniendo al mismo tiempo estándares de protección de la información personal involucrada.

Como se pudo observar, en Colombia el derecho al olvido, a diferencia de la privacidad, la honra y el buen nombre, no tiene una consagración expresa. Sin embargo, en conjunto, estos

derechos se han protegido a través de decisiones judiciales innovadoras y han evolucionado en virtud del garantismo de los jueces constitucionales en sede de tutela que, a corte del primer semestre de 2023, registran 42.591 procesos por acciones de tutela interpuestas deprecando la protección de derechos a la privacidad, *habeas data*, o análogos (Corte Constitucional, 2023).

A continuación, la Defensoría Delegada para la Protección de Derechos en Ambientes Digitales y Libertad de Expresión presenta un análisis de las decisiones más importantes de las altas cortes colombianas en la materia y de las recomendaciones internacionales denominadas Reglas de Heredia. El objetivo es concluir el mejor escenario posible en relación con los derechos que pueden vulnerarse como resultado de un tratamiento inadecuado de datos personales adscritos a providencias judiciales publicadas en medios digitales.

3.1 *Los derechos humanos y la publicación digital de providencias judiciales en la jurisprudencia colombiana*

La duración indeterminada e innecesaria de datos personales en una providencia judicial, publicada en una relatoría digital, constituye el escenario principal en el que surge la tensión entre el derecho a la información, el principio de publicidad de las sentencias, el principio de transparencia y el derecho de acceso a la información, en contraposición a los derechos a la privacidad, olvido y *habeas data*, entre otros derechos derivados del uso de datos personales.

Aunque el derecho al olvido ha cobrado vigencia con las nuevas tecnologías, la Corte Constitucional colombiana ha procurado reconocerlo desde su creación. En 1992, estableció: “[...] es bien sabido que las sanciones o informaciones negativas acerca de una persona no tienen vocación de perennidad y, en consecuencia, después de algún tiempo tales personas son titulares de un verdadero derecho al olvido” (Sentencia T-414 de 1992).

A partir de esta decisión, la Corte Constitucional, analizando la colisión entre la libertad y la privacidad, entre otros, ha subrayado la relevancia de los antecedentes penales como activos de información y datos personales al facilitar la identificación y reconocimiento de las personas. Para la Corte, una entidad encargada de administrar bases de datos sobre antecedentes penales podría violar el derecho al *habeas data* de los titulares, como resultado del desconocimiento de los principios de finalidad, necesidad, utilidad y circulación

restringida de la información personal sobre antecedentes penales contenida en dichas bases de datos (Sentencia SU-458 de 2012).

La Corte Suprema de Justicia de Colombia ha sostenido que las bases de datos destinadas a la difusión de la jurisprudencia “no podrán divulgar nombres, apellidos ni cualquier otro dato personal sensible de los sujetos procesales o intervinientes, cuando estos sean irrelevantes para el propósito de publicar las sentencias, de lo contrario se estaría violando el *habeas data*” (Auto 18837 de 2015).

En el mismo auto, la Corte Suprema estableció que las providencias en formato electrónico deben ser editadas, sustituyendo los nombres de los sujetos procesales por sus iniciales. Esto se debe a que la Relatoría de la Sala de Casación Penal, a través del sitio web de la Corte Suprema de Justicia, no tiene como propósito servir como una base de datos de antecedentes penales, sino para la divulgación de su jurisprudencia. Por lo tanto, se advierte que las bases de datos podrían tener un efecto adverso si se utilizan como medio para obtener referencias criminales de manera indefinida (Auto 18837 de 2015).

Por tanto, la jurisprudencia ha subrayado la necesidad de aplicar un cuidado especial cuando la información recolectada o sometida a algún tipo de procesamiento se refiere a antecedentes legales, procesos judiciales o investigaciones de naturaleza penal relacionadas con presuntas conductas delictivas. Estos datos son considerados como sensibles según lo establecido en la Ley 1581 de 2012, artículo 5. En otro pronunciamiento, la Corte Constitucional determinó que, si con el paso del tiempo el tratamiento de los datos personales se modifica o desvía de su propósito original, es necesario que las autoridades tomen las medidas necesarias para preservar la garantía de los derechos a la privacidad, buen nombre

o *habeas data*. Sin embargo, la Corte reconoció que la publicidad de las sentencias sirve a propósitos constitucionales y que, debido a su amplia difusión, la información contenida en estas se vuelve de dominio público (Sentencia T-020 de 2014).

En consecuencia, el tratamiento de antecedentes penales, como datos personales semiprivados y tras la extinción de los fines de la pena, constituye una trasgresión del derecho al *habeas data*. La clasificación de antecedentes penales como datos semiprivados se mantiene a lo largo de las decisiones judiciales de la Corte. En la Sentencia T-450 de 2022, el alto tribunal destacó el carácter práctico de las categorías de datos personales y enfatizó en los principios de finalidad, utilidad y circulación restringida que el administrador de la base de datos de antecedentes penales debe cumplir para impedir el acceso a terceros que no estén expresamente autorizados o que no tengan un interés constitucional o legalmente reconocido (al mismo tenor de la Sentencia SU-458 de 2012, previamente analizada).

El reconocimiento de la protección de datos sensibles en sentencias judiciales implicó también medidas de protección empleadas por los jueces colombianos para evitar que con la publicación de las respectivas providencias en medios digitales se pudieran vulnerar derechos o producir actos discriminatorios. Un ejemplo de esta práctica es la Sentencia T-124 de 2015, en la que la Corte Constitucional optó por suprimir los nombres reales de sujetos de especial protección, particularmente defensores de derechos humanos, víctimas de desplazamiento forzado y víctimas de violencia sexual, entre otros, para evitar su posterior identificación (Sentencia T-124 de 2015).

En el mismo año, la Corte Constitucional abordó el caso de una noticia con informa-

ción incompleta que vinculaba a una persona con hechos delictivos, aunque nunca se le declaró culpable. La Corte concedió el amparo de los derechos fundamentales a la intimidad, debido proceso y petición de la accionante, y ordenó al medio de comunicación utilizar herramientas técnicas como “robots.txt”, “metatags” u otros medios similares para evitar que, al introducir el nombre de la persona en el buscador, se pudiera acceder a la noticia (Sentencia T-277 de 2015). Este fue un paso significativo hacia la incorporación de herramientas técnicas en las decisiones judiciales para garantizar la protección de los derechos fundamentales.

En la Sentencia T-512 de 2016, la Corte Constitucional equilibró los derechos de aquellos individuos que buscan la privacidad de sus antecedentes penales, como datos personales derivados del cumplimiento de sus condenas, frente a los derechos fundamentales de los niños, niñas y adolescentes, sujetos a una protección especial por parte del Estado al representar un interés supremo para la sociedad. En este caso, se trataba del acceso a los antecedentes penales del rector de una institución educativa, condenado en el año 2000 por los delitos de acceso carnal abusivo en persona menor de 14 años, en concurso homogéneo agravado con pornografía infantil. Los magistrados determinaron que la disponibilidad de estos datos no contravenía los derechos de *habeas data* y de resocialización penal, ya que se trataba de información relevante que debía ser conocida previamente por las autoridades administrativas encargadas de llevar a cabo el proceso de selección de los directivos educativos. La Corte Constitucional no solo garantizó la especial protección de los derechos de los niños, niñas y adolescentes, sino que además instó a los distintos órganos constitucionales a adoptar un régimen de inhabilidades para los aspirantes a la carrera do-

cente que tuvieran antecedentes penales relacionados con violencia sexual o intrafamiliar (Sentencia T-512 de 2016). En consecuencia, la publicación de providencias judiciales que busquen un fin ulterior, como la protección de niños, niñas y adolescentes, prevalece sobre la intención de salvaguardar la privacidad o buen nombre de los sujetos infractores, incluso si estos han cumplido rigurosamente con lo dispuesto por la justicia penal.

Otro ejemplo de una providencia judicial que implementa medidas técnicas para salvaguardar los derechos al buen nombre, honra y *habeas data* se encuentra en la Sentencia T-693 de 2016. En este caso, la Corte Constitucional determinó que una columna de opinión afectaba los derechos del accionante, quien nunca estuvo involucrado ni vinculado a los presuntos delitos mencionados en la publicación. Luego de considerar los límites a la libertad de expresión, la Corte ordenó al periódico tomar medidas a través de herramientas técnicas como la desactivación de “etiquetas o metatags”, la implementación de “protocolos de exclusión” como “robots.txt” o códigos como “noindex” o “no archive”, así como cualquier otro recurso informático que impidiera que, al buscar el nombre del accionante en motores de búsqueda de Internet, se pudiera acceder a la versión digital de la columna de opinión.

Finalmente, a través de una sentencia unificadora, la Corte Constitucional determinó que el derecho al acceso a la información pública está regido por el principio de máxima divulgación. Esto implica que, en principio, la información en posesión de un sujeto obligado debe ser pública, en concordancia con los principios de transparencia y publicidad (Sentencia SU-355 de 2022). Además, destacó las reglas procedimentales para acceder a los expedientes judiciales establecidas en el artículo

123 de la Ley 1564 de 2012 o Código General del Proceso (Sentencia SU-355 de 2022).

La Corte a su vez subrayó que el principio de publicidad en el ámbito de la administración de justicia tiene dos facetas. Por un lado, como garantía del debido proceso, lo que implica que es responsabilidad de los jueces asegurarse de que las partes y los sujetos procesales estén al tanto de las actuaciones dentro de los procesos judiciales. Por otro lado, como garantía del derecho al acceso a la información pública, materializado en el derecho de los ciudadanos a conocer las decisiones judiciales. En términos generales, lo anterior significa que las decisiones judiciales pueden ser consultadas por cualquier persona, a menos que exista alguna reserva legal que lo impida (Sentencia SU-355 de 2022).

Por otra parte, la Corte Constitucional también reconoció que dada la llegada de la emergencia sanitaria por el COVID-19 y el consiguiente cambio de la presencialidad a la virtualidad en el sistema de administración de justicia de Colombia, el portal web de la Rama Judicial ha experimentado una transformación en su propósito. De ser una plataforma meramente informativa, ahora se ha convertido en un espacio donde se ejerce el principio de publicidad de las providencias judiciales (Sentencia SU-355 de 2022).

En este contexto, la Corte ordenó al Consejo Superior de la Judicatura establecer las condiciones para las publicaciones de información judicial en el portal web de la Rama Judicial. Asimismo, lo instó a actualizar la normativa existente para adecuarla a las nuevas necesidades de publicación en la página, dada la priorización de las tecnologías de la información y las comunicaciones en la administración de justicia. Para la Corte, esta normativa deberá incluir pautas para garan-

tizar la protección del derecho a la intimidad personal y familiar de las personas.

Además, estableció que se debe diseñar un plan de capacitación del portal web de la Rama Judicial, con el fin de que los funcionarios encargados de publicar contenidos aprendan sobre el manejo técnico para llevar a cabo estas publicaciones en los micrositos web y encaminado a que conozcan las razones por las cuales estos contenidos se indexan en los motores de búsqueda y la manera en que deben proteger el derecho a la intimidad en las diversas publicaciones realizadas en el portal web de la Rama Judicial (Sentencia SU-355 de 2022).

3.2 *Las Reglas de Heredia*

En el Seminario de Internet y Sistema Judicial celebrado en la provincia de Heredia, Costa Rica, en 2003, se congregaron representantes de diversas organizaciones, tanto públicas como privadas de América Latina, con el propósito central de abordar los desafíos que supone la administración de justicia en el ámbito digital. Particularmente, se discutieron las tensiones derivadas de la presencia de sitios web de los poderes judiciales en la red. En Heredia también se debatieron los presupuestos de transparencia y publicidad, especialmente en lo concerniente a la protección de datos personales.

Como resultado de este encuentro, se formularon las reconocidas Reglas de Heredia, un conjunto de recomendaciones de carácter internacional dirigidas a los tribunales e instituciones encargadas del tratamiento de datos personales presentes en providencias judiciales publicadas en Internet y otros medios digitales. Estas reglas, sin menoscabar los derechos de acceso, libertad y transparencia

respecto a las providencias judiciales, buscan establecer procedimientos apropiados, necesarios y equilibrados para su publicación en la era digital. En otras palabras, persiguen promover una colaboración armoniosa entre el sistema judicial y la tecnología de la información, con el fin de mejorar los estándares de la administración de justicia en lo que respecta a la protección de datos en el ámbito digital, siempre garantizando que no se causen perjuicios antijurídicos a las personas que han sido objeto de procesos judiciales.

De acuerdo con Carlos Gregorio y Mario Lobato de Paiva es importante distinguir que estas recomendaciones legislativas se centran en la difusión de sentencias e información procesal en Internet o en otros formatos electrónicos, pero no abarcan la información judicial en formato físico ni los documentos almacenados en los despachos judiciales (Gregorio & Lobato, 2003).

También sugieren los expertos que las reglas establecen pautas mínimas para salvaguardar los derechos de intimidad y privacidad. Esto implica que cualquier autoridad, entidad privada o persona jurídica que difunda información judicial en Internet debe emplear procedimientos que cada vez más ofrezcan una mayor protección a estos derechos (Gregorio & Lobato, 2003). Al respecto, las reglas se aplican tanto a los sitios web de los Poderes Judiciales como a los proveedores comerciales de jurisprudencia o información judicial, en virtud de su posición como fuentes de información y consulta; es decir, aplican también a terceros en su rol de difusión. Las diez reglas creadas en Heredia pueden resumirse así (Instituto de Investigación para la Justicia, 2003):

1. La difusión de sentencias y resoluciones judiciales en Internet busca promover la transparencia en la administración de justicia y garantizar la igualdad ante la ley.

2. La difusión en Internet de la información procesal tiene como objetivo facilitar el acceso inmediato a los movimientos, citaciones o notificaciones a las partes y quienes tengan un interés legítimo en el caso.

3. Los interesados tienen el derecho de oponerse, sin costos, a la difusión de datos que les conciernan, por razones legítimas. Además, se permite la exclusión o rectificación de datos difundidos de manera ilegítima.

4. Los motores de búsqueda deben adecuarse al alcance y objetivos de la información judicial difundida.

5. Prevalecen los derechos de privacidad e intimidad en casos que involucren datos personales sensibles, como los relativos a menores, asuntos familiares, opiniones políticas, entre otros.

6. Cuando una persona se convierte en una figura pública y el proceso está relacionado con su notoriedad, prevalecen la transparencia y el derecho de acceso a la información pública, a menos que se trate de asuntos de familia u otros protegidos legalmente.

7. En los demás casos, se busca un equilibrio entre la protección de la privacidad

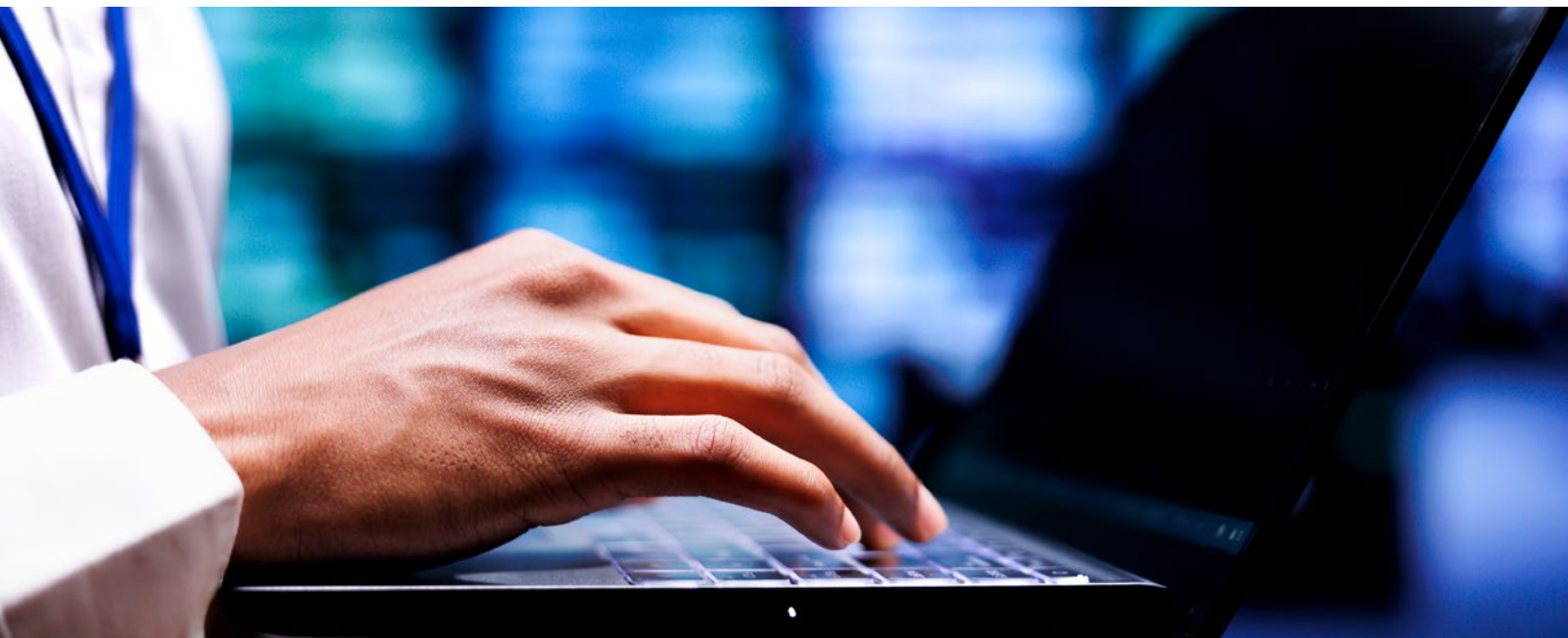
y el derecho de acceso a la información. Este equilibrio puede lograrse mediante el uso de motores de búsqueda que excluyan nombres y datos personales.

8. El tratamiento de datos sobre infracciones, condenas penales o medidas de seguridad debe ser supervisado por la autoridad pública.

9. Los jueces deben evitar mencionar hechos irrelevantes o relacionados con terceros en sus sentencias, proporcionando solo la información necesaria para fundamentar su decisión.

10. En los convenios con editoriales jurídicas, se deben cumplir las reglas establecidas previamente (Instituto de Investigación para la Justicia, 2003).

A pesar de su importancia y reconocimiento, dada su naturaleza internacional, las recomendaciones de las Reglas de Heredia requieren en el ordenamiento colombiano un proceso formal de adhesión, a través del respectivo trámite legislativo, con el ánimo de fomentar un futuro en el que se alcance un equilibrio entre la transparencia, el acceso a la información pública y los derechos de privacidad, buen nombre, honra y olvido, entre otros.



4. CONCLUSIONES

1. La privacidad, el derecho al olvido, el buen nombre y la honra son derechos fundamentales susceptibles de protección, especialmente cuando se analiza el tratamiento de datos personales contenidos en providencias judiciales publicadas en medios digitales. Esto es relevante, sobre todo en sentencias penales publicadas en bases de datos con antecedentes penales, considerados como datos semi-privados, que con el paso del tiempo y solo en algunos casos específicos pierden las finalidades legítimas derivadas de su publicación.

2. Tanto la Corte Constitucional como la Corte Suprema de Justicia de Colombia han demostrado un compromiso significativo en la protección de los derechos fundamentales a la privacidad, el derecho al olvido, el buen nombre y la honra, entre otros. Estos derechos entran en tensión con el principio de publicidad y transparencia, así como con los derechos de acceso a la información y libertad de expresión y opinión, en el contexto de la publicación de providencias judiciales en medios digitales. Es esencial destacar que esta protección se garantiza a través de mecanismos de

supresión de datos personales para impedir la identificación o individualización de los titulares de los datos, a menos que surjan situaciones donde entren en juego derechos de sujetos de especial protección constitucional o cuando se persigan fines ulteriores en beneficio de la sociedad colombiana.

3. En Colombia, existe una oportunidad para fortalecer el marco jurídico en lo referente a la creación de estándares mínimos para la publicación de información personal en providencias judiciales a través de medios digitales. Esto puede lograrse mediante una implementación gradual y actualizada de las recomendaciones establecidas en las Reglas de Heredia, así como a través del seguimiento y aplicación de las órdenes establecidas por la Corte Constitucional en la Sentencia SU-355 de 2022. En conjunto, estos procesos están orientados a la creación de mecanismos innovadores que promuevan los derechos humanos en ambientes digitales, bajo la estrategia de transformación en la protección dispuesta por la Defensoría Delegada para la Protección de Derechos en Ambientes Digitales y Libertad de Expresión.

REFERENCIAS

- AEPD. Agencia Española de Protección de Datos [2020]. Derecho al olvido. Qué es el derecho de supresión.
- Asamblea General de las Naciones Unidas [1948]. Declaración Universal de los Derechos Humanos.
- Ayala Pérez, T. [2016]. Memoria versus olvido: la paradoja de internet. *Universum*, 31-44.
- Azurmendi, A. [2015]. Por un «derecho al olvido» para los europeos: Aportaciones jurisprudenciales de la sentencia del Tribunal de Justicia Europeo del caso Google Spain y su recepción por la Sentencia de la Audiencia Nacional Española de 29 de Diciembre de 2014. UNED. *Revista de Derecho Político*, 273-310.
- Barocas, S., Felten, E. W., Huey, J., Kroll, J. A., Reidenberg, J. R., Robinson, D. G. & Yu, H. [2017]. *Accountable Algorithms*. https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=9570&context=penn_law_review.
- Beccaria, C. [1968]. *De los delitos y de las penas*. Madrid: Alianza
- Brandeis, L. & Warren, S. [1890]. The Right to Privacy. *Harvard Law Review*, 193-220.
- Carrara, F. [1973]. *Programa del curso de derecho criminal*. 2 ed. Editorial Jurídica Continental.
- Conde Ortiz, C. [2005]. *La protección de datos personales. Un derecho autónomo con base en los conceptos de intimidad y privacidad*. Cádiz: Dykinson, S. L.
- Corral Talciani, H. [2000]. *Configuración jurídica del derecho a la privacidad II: concepto y delimitación*. <https://repositorio.uc.cl/dspace/bitstream/handle/11534/14814/000300261.pdf>.
- Corte Constitucional [2023]. Relatoría – estadísticas. <https://www.corteconstitucional.gov.co/lacorte/estadisticas.php>
- De Terwangne, C. [2012]. Privacidad en Internet y el derecho a ser olvidado/ derecho al olvido. IDP. *Revista de Internet, Derecho y Política*, 53-66.
- Gregorio, C., & Lobato, M. [2003]. *Las Reglas de Heredia comentadas*. <https://docplayer.es/39372906-Las-reglas-de-heredia-comentadas.html>
- Guerrero Peralta, O. J. [2009]. La expectativa razonable de intimidad y el derecho fundamental a la intimidad en el proceso penal. XXXI *Jornadas Internacionales de Derecho Penal*, 55-84. Bogotá : Universidad Externado de Colombia.
- Instituto de Investigación para la Justicia [2003] Reglas Mínimas para la Difusión de Información Judicial en Internet. Reglas de Heredia. <https://biblioteca.cejamericas.org/bitstream/handle/2015/4766/mx-reglas-minimas.pdf?sequence=1&isAllowed=y>
- Leturia I., F. J. [2016]. Fundamentos Jurídicos del derecho al olvido. ¿Un nuevo derecho de origen europeo una respuesta típica ante colisiones entre ciertos derechos fundamentales? *Revista Chilena de Derecho*, 91-113.
- López, J. M. [2013]. *El derecho a la protección de datos personales en la doctrina del tribunal constitucional*. España: Thomson Reuters Arazandi.
- Maldonado Muñoz, M. [2021]. Límites y contenido esencial de los derechos (un marco conceptual problemático). *Revista Derecho del Estado, Universidad Externado de Colombia* [47], 79-112.
- Manheim, K., & Kaplan, L. [2019]. *Artificial Intelligence: Risks to Privacy and Democracy*. https://edisciplinas.usp.br/pluginfile.php/6502070/mod_folder/content/0/Manheim-AI%2C%20risks%20to%20privacy%20and%20democracy%2C%202019.pdf.
- Martínez Otero, J. M. [2015]. El derecho al olvido en internet: debates cerrados y cuestiones abiertas tras la STJUE Google vs AEPD y Mario Costeja. UNED. *Revista de Derecho Político*, 103-142.
- Monroy Sierra, J. A. [2005]. *Tratado de Derecho Penal. Parte general. Actualizado con el nuevo Código Penal y sus reformas respectivas*. Barranquilla: Antillas.

Nieves Saldaña, M. (2011). El derecho a la privacidad en los Estados Unidos: aproximación diacrónica a los intereses constitucionales en juego. *Teoría y Realidad Constitucional* (28), 279-312.

Organización de los Estados Americanos [OEA]. (1978). *Convención Americana sobre Derechos Humanos [Pacto de San José]*. Suscrita en la Conferencia Especializada Interamericana sobre Derechos Humanos. https://www.oas.org/dil/esp/1969_Convenci%C3%B3n_Americana_sobre_Derechos_Humanos.pdf

Parlamento Europeo & Consejo de la Unión Europea. (2016). *Reglamento [UE] 2016/679*. Obtenido de Reglamento General de Protección de Datos: <https://www.boe.es/boe/2016/119/L00001-00088.pdf>.

Pica, R. (2016). El derecho fundamental al olvido en la web y el Sistema Constitucional chileno. *Estudios Constitucionales*. Centro de Estudios Constitucionales de Chile Universidad de Talca 14(1), 309-318.

Silberleib, L. (2016). El derecho al olvido y la persistencia de la memoria. *Información, cultura y sociedad: revista del Instituto de Investigaciones Bibliotecológicas* (35), 125-136.

Solove, D. J. (2002). Conceptualizing Privacy. <https://www.jstor.org/stable/pdf/3481326.pdf>.

Tórtora Aravena, H. (2010). The Limitations to the Fundamental Rights. *Estudios Constitucionales*, 8(2), 167-200.

Tribunal de Justicia de la Unión Europea (2014). Asunto C-131/12. Google Spain, S.L. y Google Inc. contra Agencia Española de Protección de Datos (AEPD) y Mario Costeja González. ECLI:EU:C:2014:317.

Velásquez Velásquez, F. (2010). Manual de Derecho penal, parte general. Bogotá: Ediciones jurídicas Andrés Morales.





**Defensoría
del Pueblo**
COLOMBIA

#NosUnenTusDerechos

Defensoría del Pueblo de Colombia
Calle 55 N° 10-32
Apartado Aéreo: 24299 - Bogotá, D. C.
Código Postal: 110231
Tels.: 314 73 00 - 314 40 00

www.defensoria.gov.co