ISSN 1794-2918
JURÍDICAS

COMO CITAR ESTE ARTÍCULO:

Vargas-Lozano, R. y Upegui-Villegas, C. (2016). La publicidad de las providencias penales en Internet. Una revisión a su constitucionalidad. *Revista Jurídicas*, *13* (1), 100-115.
DOI: 10.17151/jurid.2016.13.1.7.

Recibido el 12 de abril de 2016
Aprobado el 03 de junio de 2016

LA PUBLICIDAD DE LAS PROVIDENCIAS PENALES EN INTERNET. UNA REVISIÓN A SU CONSTITUCIONALIDAD

Renato Vargas-Lozano*
Carolina Upegui-Villegas**

RESUMEN

La divulgación de providencias judiciales de índole penal a través de Internet, mediante la página institucional de la Corte Suprema de Justicia, genera varios interrogantes de cara a la regulación colombiana vigente sobre el tratamiento y la protección de datos personales. Este artículo da cuenta de la evolución jurisprudencial en la materia y propone alternativas para limitar el acceso indiscriminado e incontrolado por Internet a los datos personales negativos y sensibles de quienes han sido vinculados a las actuaciones penales.

Palabras clave: datos personales, datos personales negativos, datos personales sensibles, *hábeas data*, antecedentes penales, derecho al olvido, Internet, divulgación de decisiones judiciales.

* Doctor en Derecho. Profesor de Derecho Penal de la Universidad Sergio Arboleda, Bogotá, Colombia. Investigador del grupo en derecho penal y ciencias criminológicas 'Emiro Sandoval Huertas'. Abogado en ejercicio vinculado a la firma Álvaro Vargas Abogados, Bogotá, Colombia. E-mail: renato.vargas@usa.edu.co. ORCID: 0000-0002-8558-2657.

** Doctora en Derecho. Abogada en ejercicio y consultora vinculada a la firma Álvaro Vargas Abogados, Bogotá, Colombia.
E-mail: carolina.upegui@alvarovargasabogados.com.
ORCID: 0000-0002-3773-7079.

THE PUBLICITY OF CRIMINAL PROVISIONS ON THE INTERNET. A REVIEW OF ITS CONSTITUTIONALITY

ABSTRACT

Web publishing of criminal judicial decisions by the Colombian Supreme Court of Justice, triggers some serious difficulties related to the processing and protection of personal data under the current national regulation. Besides reviewing the judge-made law evolution in the matter, this article proposes alternatives to limit the indiscriminate and uncontrolled access by Internet to the negative and sensitive personal data of those who have been subjected to criminal proceedings.

Key words: personal data, negative personal data, sensitive personal data, habeas data, criminal record, the right to be forgotten, Internet, publishing of judicial decisions.

INTRODUCCIÓN

Existe un derecho general de acceder a la información contenida en las decisiones judiciales en firme —salvo cuando exista reserva legal— y una obligación correlativa en cabeza de las autoridades que administran justicia de divulgarlas (inciso 3, artículo 64, Ley 270 de 1996; Corte Constitucional, sentencia C-872 de 2003). En su día, la Corte Constitucional consideró que esa facultad general de acceder a las "bases de datos" que contenían las decisiones era desproporcionada, contrariaba lo previsto en el artículo 74 de la Constitución y la seguridad jurídica, e interfería con cierta autonomía administrativa de las autoridades judiciales a la hora de reglamentar la materia y decidir qué medios empleaban para dar a conocer al público las providencias (sentencia C-037 de 1996).

Hoy en día la Sala de Casación Penal de la Corte Suprema de Justicia, por conducto de la Relatoría, divulga sus decisiones a través de una página Web oficial; permitiendo que cualquier persona con acceso a Internet pueda consultar, descargar y reproducir sus providencias (García, 2013). En tal virtud, la Relatoría gestiona documentalmente los autos y las sentencias y administra tanto los archivos como las bases de datos necesarios para cumplir con sus funciones de información y divulgación y la de garantizar el derecho de los ciudadanos a consultar las providencias judiciales (artículo 6, Ley 169 de 1896; artículo 40, Decreto Ley 052 de 1987; artículo 64, Ley 270 de 1996; artículos 74, 228, Constitución; Acuerdo 006 de 2002).

Empero, los desarrollos tecnológicos en materia de telecomunicaciones y procesamiento de datos hacen que la preocupación manifestada por la Corte Constitucional en 1996, cuando consideró inconveniente facilitar el acceso a las bases de datos judiciales, retome vigencia: los riesgos hoy, son todavía mayores; pues difundir providencias judiciales penales a través de la Internet, sin control e indiscriminadamente, puede afectar los derechos fundamentales de los ciudadanos. En este sentido, el *hábeas data* y la regulación sobre datos personales —aspectos no considerados en 1996— juegan un papel trascendental en orden a resolver la tensión entre, por un lado, los derechos de los individuos cuya información figura en las decisiones penales; y, por el otro, la obligación de darle publicidad a tales providencias y el derecho del público a conocerlas por medios óptimos y confiables.

El presente escrito se ocupa, entonces, de los problemas jurídicos suscitados en punto de la divulgación de las providencias judiciales penales que hace la Corte Suprema mediante su página de Internet; permitiendo un acceso indiscriminado e ilimitado a sus decisiones. Así, en primer lugar, se analiza lo atinente al tratamiento de datos, el *hábeas data* y la divulgación de providencias; y, en segundo término, se examina críticamente la posición de la Corte Suprema acerca de la publicación de las providencias penales a través de Internet y en especial su conformidad con

los principios, las normas y algunas decisiones de la Corte Constitucional atinentes al tratamiento de datos personales en Colombia.

LA DIVULGACIÓN DE PROVIDENCIAS, EL TRATAMIENTO DE DATOS PERSONALES Y EL *HÁBEAS DATA*

La Ley 1266 de 2008 —de marcado carácter sectorial— y la Ley Estatutaria 1581 de 2012, son las fuentes normativas principales del tratamiento de datos personales en Colombia; ambas se ocupan de los derechos a conocer, actualizar y rectificar la información personal alojada en bases de datos o archivos (el *hábeas data*), así como de los derechos, libertades y garantías previstos en los artículos 15 —intimidad personal y familiar y buen nombre— y 20 de la Constitución —derecho a la información y libertades de expresión, difusión e información— (Blume, 2012; Diorio, 2015).

Los datos personales: clasificación y tratamiento

Al margen de las propuestas doctrinales (Brian, 2012; Bru, 2007; Conde, 2005; Garriga, 2009, 2016; Hernández, 2012; Martínez, 2013; Rebollo y Serrano, 2008), lo cierto es que, en Colombia, un dato personal es "cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables" (artículo 3, literal c, Ley 1581 de 2012); vale decir, es la información relativa a una persona que permite identificarla o asociarla a una cosa, otra persona, una actividad, un hecho o una actuación concreta.

La Corte Constitucional precisó que los datos personales se refieren a aspectos exclusivos y propios de una persona natural que posibilitan su identificación (incluso, a través de un análisis de conjunto con otros datos), su propiedad reside exclusivamente en su titular y su tratamiento (captación, administración y divulgación) está sometido a reglas o principios especiales (Corte Constitucional, sentencia C-748 de 2011). En sentido similar, la Corte Suprema expresó que un dato personal es la información que permite identificar o que hace identificable a una persona natural, v. gr., sus datos de identificación (nombres, apellidos, fecha de nacimiento, documento de identidad, nacionalidad, estado civil, entre otros) (Corte Suprema, Auto Rad. 18837, de diez de junio de 2015).

Sin perjuicio de las propuestas de los especialistas (Murillo, 2007; Palacios, 2012; Remolina, 2013), el legislador clasifica los datos personales en 'públicos', 'semiprivados', 'privados' y 'sensibles'.

Los primeros son tales por mandato legal o constitucional, incluyendo los que no sean semiprivados, privados o sensibles, por ejemplo: los contenidos en documentos y registros públicos, gacetas y boletines oficiales, sentencias judiciales debidamente ejecutoriadas (no sometidas a reserva), los relacionados con el estado civil entre otros. Los segundos no tienen naturaleza íntima o reservada y su conocimiento o divulgación interesa a su titular, a cierto grupo de personas o a la sociedad en general, tales como los financieros y crediticios. Los terceros son de naturaleza íntima o reservada y solo importan a su titular, v. gr., la historia clínica; y los cuartos afectan la intimidad del titular, están estrechamente vinculados con los derechos fundamentales de las personas y su uso indebido puede generar discriminación, es el caso de los datos biométricos y de origen racial (literales f), g) y h), artículo 3 de la Ley 1266; literal f), artículo 3 Ley 1581; numeral 2, artículo 3 Decreto 1377 de 2013; numeral 3, artículo 3 Ley 1581 de 2012; Corte Constitucional, sentencias T-414 de 1992, T-729 de 2002, C-336 de 2007, C-1011 de 2008, C-334 de 2010, C-748 de 2011; Remolina, 2013; Gutiérrez, 2001; Voss, 2014).

El tratamiento (cualquier operación o conjunto de operaciones con o sin ayuda de la informática como la recolección, almacenamiento, uso, circulación o supresión) (literal g), artículo 3 Ley 1581 de 2012; Corte Constitucional, sentencia C-748 de 2011) de datos públicos no requiere autorización del titular; el de los semiprivados y los privados precisa de una orden de autoridad administrativa o judicial en cumplimiento de sus funciones, atendiendo los principios de la administración de datos personales o con la autorización de su titular (Corte Constitucional, sentencias T-443 de 1994, T-729 de 2002); y el de los sensibles, requiere autorización expresa o que esta sea innecesaria (artículos 6, 9, 10 Ley 1581 de 2012; Corte Constitucional, sentencia C-748 de 2011).

La divulgación de providencias judiciales

La divulgación de las providencias judiciales es fruto del ejercicio de una competencia atribuida al poder judicial, es decir, de una función pública y no del ejercicio de un derecho o una libertad de información en estricto sentido (Corte Constitucional, sentencia T-040 de 2013). Tales decisiones son el resultado de la función de administrar justicia y se vierten en documentos públicos; razón por la cual cualquiera puede consultarlas una vez ejecutoriadas, salvo las limitaciones legales expresas (inciso 3, artículo 64 Ley 270 de 1996; artículos 74, 228 Constitución). No obstante, los datos personales privados o sensibles contenidos en ellas siguen siendo tales mientras puedan asociarse a una persona e identificarla, exponiendo su intimidad y revelando, por ejemplo, que fue procesada, condenada o absuelta por un delito.

Cuando el archivo que contiene una providencia judicial se aloja en una base de datos y se facilita su consulta pueden vulnerarse derechos fundamentales tales

como el *hábeas data*, la intimidad, la honra o el honor (Gordillo y Restrepo, 2004; Lucena, 2014). Por consiguiente, si las decisiones contienen datos personales, su titular debe poder ejercer el derecho al *hábeas data*; además, su divulgación ha de ajustarse a las previsiones legales y constitucionales relativas a la protección de datos personales y a la finalidad respectiva de la base de datos.

Esto explica porque resulta difícil justificar el acceso indiscriminado a la información que solo contribuye a generar sospechas sobre las personas, a estigmatizarlas o a etiquetarlas (Corte Constitucional, sentencia SU-458 de 2012). Asimismo, como entre los datos personales y la intimidad de su titular existe una relación estrecha, se entiende que este no pierde la facultad de incidir en la gestión de aquéllos cuando la información es incluida en un banco o base de datos dado que tal actividad no le confiere al que la realiza la posibilidad de apropiarse del dato (Corte Constitucional, sentencia T-414 de 1992).

La divulgación de providencias judiciales y los principios aplicables a la protección de datos personales

La divulgación de las decisiones judiciales debe respetar la normativa atinente a la protección de datos personales y al *hábeas data* (Corte Constitucional, sentencias T-729 de 2002, C-1011 de 2008, C-748 de 2011; artículos 17 y ss. de la Ley 1581 de 2012). La pregunta a responder es si la administración de archivos y bases de datos de acceso libre en Internet, que contienen información altamente sensible (incluso datos personales negativos), atiende a los principios que rigen la gestión de datos personales y proscriben el uso abusivo del poder informativo.

La respuesta es negativa, pues divulgar las providencias judiciales, sobre todo por Internet y permitiendo un acceso generalizado e incontrolado a la información contenida en ellas, atenta contra varios de los principios sobre tratamiento de datos personales y el *hábeas data,* en especial, tratándose de los datos privados o sensibles.

El de legalidad, en primer lugar, acorde con el cual el manejo de información personal es una actividad reglada sometida a las normas y los límites fijados por la ley, resulta infringido si no se toman las medidas necesarias para evitar la difusión de datos personales que podrían vulnerar derechos fundamentales, si se facilita la difusión indiscriminada de información personal negativa o desfavorable (Corte Constitucional, sentencias T-120 de 1997, T-1479 de 2000, T-761 de 2004), se ejerce un poder informativo —generar información y divulgarla— que desborda las funciones legales y constitucionales o se favorece el ejercicio inorgánico del poder informativo (Warso, 2013; Pazos, 2015).

El de finalidad, en segundo lugar, implica que toda gestión de datos personales debe obedecer a una finalidad legítima, expresa y específica que ha de estar conforme a la Constitución y a la ley; el suministro de datos personales debe realizarse en un contexto delimitado y la información destinarse exclusivamente a los fines para los cuales fue entregada por el titular o los autorizados por la ley (Corte Constitucional, sentencias C-748 de 2011, T-987 de 2012). Este principio se vulnera al dejar la información personal a disposición del público —en Internet— y permitir un acceso irrestricto e indiscriminado a la misma.

En tercer lugar, el principio de necesidad consiste en que los datos personales tratados tienen que ser los estrictamente necesarios para cumplir con las finalidades de las bases de datos (Corte Constitucional, sentencia C-1011 de 2008). Sin embargo, la divulgación de las decisiones judiciales con los datos personales de los implicados luce innecesaria, en tanto los fines de comunicación y divulgación pueden cumplirse perfectamente sin identificar, hasta el detalle de su individualidad, a las partes.

El de utilidad, en cuarto lugar, supone que el tratamiento de datos personales debe tener una función determinada, es decir, una "utilidad clara o determinable" (Corte Constitucional, sentencia C-748 de 2011), so pena de favorecer "conductas lesivas del derecho a la autodeterminación informativa ante el riesgo de excesos en el ejercicio del derecho a informar" (Corte Constitucional, sentencia C-185 de 2003). Por ello, el hecho mismo de divulgar las decisiones por Internet o un medio de comunicación masivo parece excesivo y desproporcionado, pues va más allá de lo estrictamente útil.

El principio de acceso y circulación restringida, en quinto lugar, prevé que la administración de datos personales está sometida a la naturaleza de aquéllos, al objeto de las bases de datos, a la autorización del titular, a los mandatos de la ley y a los demás principios de tratamiento de datos personales que evitan su divulgación indiscriminada. Con base en esto, los datos personales no pueden ser accesibles por Internet —u otros medios de comunicación masiva— sino en la medida en que el acceso a la información pública pueda controlarse y restringirse a los titulares o usuarios autorizados por las leyes (Corte Constitucional, sentencia C-748 de 2011). Si la divulgación indiscriminada de datos personales privados y/o sensibles está prohibida en términos generales, la circulación restringida de las decisiones que los contienen debe imponerse.

En sexto lugar, el principio de confidencialidad indica que los datos personales que no sean públicos deben mantenerse en reserva salvo que exista una autorización legal o del titular de la información o de un juez. Así, aunque las providencias judiciales ejecutoriadas son documentos públicos que contienen información pública y pese a que los ciudadanos pueden conocer —por razones legítimas—

dichas decisiones, las mismas incluyen información personal sensible cuya divulgación ha de hacerse en forma controlada; lo cual es muy difícil cuando el medio empleado es Internet.

Por último, en séptimo lugar, el principio de interpretación integral de derechos constitucionales acorde con el cual las leyes de protección de datos deben interpretarse de forma armónica con el *hábeas data*, el buen nombre, la honra, la intimidad y la información.

El *hábeas data*

La necesidad de evitar los excesos del poder informativo en el tratamiento de datos personales, especialmente de los negativos, justifica la entrada en escena del *hábeas data*; un derecho fundamental autónomo y una garantía de otros derechos y libertades susceptibles de afectarse con el tratamiento indebido de datos personales, consagrado en el artículo 15 de la Constitución; que faculta al titular de la información personal para exigir a quienes administren sus datos personales conocerlos, actualizarlos, rectificarlos, autorizarlos, incluirlos, excluirlos, suprimirlos y certificarlos (Corte Constitucional, sentencias T-307 de 1999, T-129 de 2002, T-729 de 2002, C-1011 de 2008, SU-458 de 2012, T-058 de 2013; Corte Suprema, Sala de Casación Penal, sentencias Rad. 72260 de 20 de marzo de 2014, 62605 de 13 de diciembre de 2012; Cifuentes, 1997; de la Calle, 2009).

Por consiguiente, si una providencia judicial divulgada por Internet expone datos personales sensibles de un individuo, este puede ejercer su derecho fundamental al *hábeas data* para controlar la información que le concierne y la forma en que ella es administrada o divulgada en Internet; así como para garantizar otros derechos (al trabajo o al buen nombre) y libertades (económicas).

La divulgación de providencias judiciales penales en Internet

La Relatoría de la Sala de Casación Penal de la Corte Suprema se encarga de divulgar las decisiones judiciales penales con el propósito de que los ciudadanos puedan conocerlas —publicidad— y sepan cómo se interpreta y aplica la ley —seguridad jurídica—; en desarrollo de esta función gestiona archivos y bases de datos mediante los cuales administra la información contenida en dichas providencias. En tal sentido, si bien hay un interés legítimo de la sociedad en conocer las sentencias aludidas, lo cierto es que su divulgación generalizada e incontrolada —posibilidad que se maximiza con el uso de la Internet— puede afectar algunos derechos fundamentales de los procesados, someterlos a discriminación y exclusión social e impedir su derecho al trabajo, su resocialización o su reinserción (Koops, 2014); además, de informar inapropiadamente sobre sus antecedentes penales (Corte Constitucional, sentencias T-632 de 2010, T-648 de 2012; Corte Suprema,

Sala de Casación Penal, Sala Segunda de Decisión de Tutelas, Rad. 4992 de 09 de septiembre de 2010).

Los antecedentes penales y el derecho al olvido

En Colombia no es viable suprimir totalmente los antecedentes penales —datos personales negativos—, de ahí que no pueda alegarse un eventual "derecho al olvido" (Newman, 2015; Ausloos, 2012; Bennet, 2012; Rees and Heywood, 2014; Mantelero, 2013; Remolina, 2014; Roig, 2012); pero ello no siempre ha sido así, pues el artículo 11 del Decreto 2398 de 1986 lo admitía cuando la pena se hubiere cumplido o se la hubiera declarado prescrita o se la considerare prescrita "por haber transcurrido un tiempo igual o mayor al estipulado en el Código Penal" (Corte Constitucional, sentencia T-022 de 1993).

En otras materias —disciplinaria, financiera o crediticia (Corte Constitucional, sentencias T-414 de 1992, T-022 de 1993, C-1066 de 2002)— este derecho al olvido ha sido reconocido; de hecho, en 2002, al ocuparse de los antecedentes disciplinarios, la Corte Constitucional consideró posible extenderlo a otros ámbitos (sentencia C-1066 de 2002; Puccinelli, 2012). Sin embargo, en 2012, la Corte se pronunció expresamente en contra de ampliar sus efectos a los antecedentes penales y negó la posibilidad de exigir al administrador de bases de datos de antecedentes penales la supresión total de dicha información negativa (Corte Constitucional, sentencia SU-458 de 2012).

De esta forma, a día de hoy, no es posible pedir la supresión completa de la información personal contenida en las bases de datos; aunque sí pueden solicitarse su almacenamiento y circulación restringidos.

La divulgación de los antecedentes penales

Los antecedentes penales se refieren a las sanciones penales impuestas a una persona mediante sentencias ejecutoriadas (Corte Constitucional, sentencia T-023 de 1993) y son los datos negativos por excelencia, al asociar al condenado con circunstancias "no queridas, perjudiciales, socialmente reprobadas o simplemente desfavorables" (Corte Constitucional, sentencia SU-458 de 2012). Es una información de carácter sensible y semiprivada producto del ejercicio de una función pública legal y constitucionalmente legítima que no posee actualmente un término de vigencia puesto que la condena, en tanto registro o dato histórico, acompaña a quien se le impone por toda su vida (Corte Suprema, Sentencias de Tutela 46906, 49524, 50741; Cabezudo, 2011).

En ejercicio del *hábeas data*, el titular de la información puede solicitar su supresión relativa impidiendo su divulgación por Internet u otro medio que facilite el acceso

indiscriminado a ella. La supresión no es total debido a la utilidad de estos datos personales en asuntos penales y a otros usos legítimos en materias tales como la inteligencia, la ejecución de la ley o el control migratorio (Corte Constitucional, sentencias SU-458 de 2012; C-540 de 2012 y T-058 de 2015).

Las autoridades actúan conforme a la Constitución y a la ley cuando administran esta información, siempre que no se aparten de sus fines ni afecten derechos o libertades fundamentales de los individuos. Por ello si cualquiera puede acceder al pasado judicial de otro, indiscriminada e incontroladamente, se desborda la utilidad que la Constitución y las leyes le atribuyen al tratamiento de estos datos (Corte Constitucional, sentencia SU-458 de 2012; Álvarez, 2011). Es, por tanto, una información que debe tratarse con cautela y revelarse solo cuando realmente sea necesario; pues de lo contrario peligra el cumplimiento de los fines de la pena especialmente la reinserción social (Corte Suprema de Justicia, sentencia de Tutela 47807); así, aunque el interés de la sociedad en conocer este tipo de información es legítimo (Corte Constitucional, sentencia SU-458 de 2012; Hernández, 2016), esto no justifica un ejercicio inorgánico del poder informativo.

Precisar cuándo opera el derecho al olvido y bajo qué condiciones es una cuestión cuya regulación legal es urgente (*El Tiempo*, 2016); entre tanto, se podrían aplicar analógicamente a los antecedentes penales ciertas disposiciones referidas a los disciplinarios, por ejemplo, establecer un mecanismo general de acceso para los particulares que carecen de un interés legítimo y otro para aquellos que sí lo tienen (Corte Constitucional, sentencia SU-458 de 2012).

La divulgación de providencias judiciales en materia penal

Pese a que las reflexiones se enfocan en los antecedentes penales, la verdad es que el análisis propuesto vale para cualquier decisión judicial mediante la cual tenga lugar la publicidad indiscriminada de una sanción penal; aun cuando la providencia divulgada no sea la que impone la condena o, incluso, cuando la sentencia condenatoria misma no circule en Internet, v. gr., el auto de inadmisión de una demanda de casación que alude a las sentencias de las instancias.

Atendido lo dicho respecto de los antecedentes penales debe concluirse que no existe un derecho a evitar la gestión y, mucho menos, a prohibir la circulación de las providencias penales cuya divulgación ocurre por mandato legal. No obstante, las autoridades sí pueden administrar los archivos que contienen esas decisiones y divulgarlos de manera tal que el medio de difusión —la Internet— garantice que la circulación de datos personales sensibles respete las libertades y garantías constitucionales y que su utilización no sea incontrolada (Jacobs y Larrauri, 2010).

Si bien hay varias decisiones de constitucionalidad referidas al tema desde el 2002, el antecedente más reciente y pertinente es de 2014; cuando, al describir la manera en que puede ejercerse el derecho al *hábeas data* en su modalidad de supresión relativa respecto de sentencias judiciales penales, la Corte Constitucional apuntó que es posible pedir a la Relatoría de la Sala de Casación Penal que reemplace el nombre del interesado por una sucesión de letras o de números que impidan su identificación (sentencia T-020 de 2014). En ese momento se propuso una "regla de circulación restringida" y se determinó que la publicidad indiscriminada de las sentencias judiciales en Internet violaba los principios de finalidad, utilidad, necesidad y circulación restringida, produciéndose un ejercicio incontrolado del poder informativo.

En junio de 2015 la Corte Suprema indicó que, a partir de ese momento, la Relatoría de la Sala de Casación Penal debía cambiar la forma de publicar las decisiones en Internet y ordenó adoptar las medidas necesarias para cumplir con los principios y normas de protección de datos personales. Se dijo que la función de divulgar las decisiones penales a través de la página de Internet institucional podía cumplirse sin publicar el nombre de las partes ni de los intervinientes en los procesos penales y, por consiguiente, dispuso editar los textos de las providencias para reemplazar los nombres y apellidos o cualquier otro dato personal sensible de los sujetos procesales o intervinientes por sus respectivas iniciales; además, indicó que las búsquedas en sus bases de datos debían limitarse mediante "criterios inherentes a temas jurídicos" (Auto Rad. 18837 de 10 de junio de 2015). Dicha decisión, que parecía plegarse a la idea de la supresión relativa, no operaba automáticamente ni respecto de los registros ya existentes o pasados por lo cual el interesado debería ejercer expresamente su derecho al *hábeas data* ante la Relatoría de la Sala de Casación Penal.

Días después, la misma Sala, se negó a suprimir el nombre de un ciudadano en una sentencia; pero apuntó que la resonancia dada a sus decisiones por los servicios de búsquedas generalizadas en Internet, sin control por parte de la Corte Suprema, contrariaba la doctrina constitucional de la sentencia C-037 de 1996 (Sala de Casación Penal, sentencia Rad. 20889 de 19 de agosto de 2015). En consecuencia, determinó que la Relatoría y la División de Informática utilizaran las herramientas tecnológicas y los protocolos necesarios para que el fallo de tutela solo pudiera consultarse en los sistemas de información controlados por ella (Weber, 2015).

Esta postura supuso un viraje radical respecto del Auto que reconocía el derecho de *hábeas data* en su modalidad de supresión relativa, en la línea de la jurisprudencia constitucional. Para la Corte Suprema su labor consiste en proferir decisiones judiciales y, al divulgarlas, realizar los principios de publicidad y transparencia de la información pública; así cumple con los intereses de la sociedad en controlar y vigilar la actividad del poder judicial y en conocer a los responsables de las

infracciones penales, la dimensión de sus actos o la sanción impuesta, además de realizar el fin de prevención general de la pena. Lo anterior justifica la pérdida de una expectativa razonable de intimidad por parte de los condenados, pues el conocimiento social de las condenas "hace parte del padecimiento implícito en la expiación de la pena" (Corte Suprema, Sala de Casación Penal, sentencia Rad. 20889 de 19 de agosto de 2015).

En este caso la Corte Suprema entendió que no se podía obstaculizar el derecho de los ciudadanos a conocer el contenido de las providencias, ni quebrantar el principio de máxima publicidad consagrado en la Ley 1712 de 2014 (artículo 2); en consecuencia, no había motivo para limitar el acceso general a sus bases de datos o implementar protocolos para impedir su consulta mediante Internet.

Ante la ausencia de una ley estatutaria que determine el régimen específico de la administración de las bases de datos de decisiones judiciales, la Corporación estableció algunas reglas sobre la divulgación de datos personales en las providencias; aunque refiriéndolas exclusivamente a "los procesados vencidos en juicio, a quienes se les desvirtuó la presunción de inocencia y se les declaró penalmente responsables" (Corte Suprema, Sala de Casación Penal, sentencia Rad. 20889 de 19 de agosto de 2015); así, basándose en la sentencia SU-458 de 2012 —sobre los antecedentes penales—, manifestó que el derecho del condenado a la supresión de los datos personales tan solo procedía "a partir de la declaración de cumplimiento de la pena o de su prescripción" (Corte Suprema, sala de Casación Penal, sentencia Rad. 20889 de 19 de agosto de 2015).

Sin duda, las consideraciones de la Corte Suprema relativas a la divulgación de providencias judiciales en Internet tanto en sus versiones del 10 como del 30 de junio del año 2015, al igual que en las de agosto del mismo año, tienen fundamento en la ley, la Constitución y la jurisprudencia previa. Con todo, no puede dejar de advertirse que las finalidades atribuidas por la Corporación a la divulgación de las decisiones en el último pronunciamiento desbordan, por mucho, la atinente a la mera difusión de los argumentos jurídicos y las reglas aplicadas por los jueces en sus proveídos. Adicionalmente, en tanto que las precisiones efectuadas en la providencia reseñada aluden a los condenados, cabe suponer que para quien carezca de tal condición rigen las normas y principios del *hábeas data* conforme a lo indicado anteriormente en este documento.

Al margen de esto, queda por determinar si la Internet es el instrumento adecuado para divulgar decisiones de índole penal puesto que dicho medio, sin duda eficaz en clave de divulgación y comunicación, facilita un ejercicio inorgánico del poder informativo sobre datos personales sensibles. Pese a la "expectativa razonable de intimidad" que pierde el condenado tal proceder afecta excesivamente sus derechos fundamentales; por ello, en tanto la Internet propicia la difusión indiscriminada e

incontrolada de datos personales sensibles, no resulta descabellado afirmar que actualmente tiene lugar una gestión indebida de las bases de datos destinadas a la divulgación de providencias judiciales penales.

¿Cómo resolver esta cuestión? Una propuesta

En orden a conjurar esta situación, y mientras se expide una ley que aclare el tema, se propone que las bases de datos destinadas a la divulgación de las decisiones sean distintas a las internas que emplean los juzgados y las corporaciones judiciales; entendiendo, respecto de estas últimas, que los datos personales son indudablemente útiles para la administración de justicia y que sus contenidos pueden conocerse, sin perjuicio de las limitaciones legales, gracias al derecho general de acceso a documentos públicos. Ambas quedarían sujetas a las leyes sobre protección de datos personales para, además de garantizar los derechos legales y constitucionales del titular de la información, asegurar que esta última sea veraz, precisa, confiable y actual.

Las bases de datos cuya finalidad sea la divulgación en Internet exigen adoptar medidas de control de la información mucho más rigurosas, para evitar la circulación indiscriminada e incontrolada de datos personales. Las providencias judiciales deberían divulgarse luego de 'anonimizar' a los sujetos procesales e intervinientes; evitando así el engorroso trámite de verificar, caso por caso, si el condenado cumplió o no con la pena o si esta ha prescrito o implementar protocolos informáticos para restringir un acceso indiscriminado a la información personal.

La opción del anonimato halla respaldo en la jurisprudencia de la Corte Suprema, pues esta admitió que podía imponer la obligación de suprimir la información personal de procesados, víctimas y testigos a quienes entregue la información de las providencias o administren bases de datos y sistemas de información relacionados con ellas (Sala de Casación Penal, sentencia 20889 de 19 de agosto de 2015). La idea, siguiendo a Brian (2012), es que en materia de protección de datos y su gestión a través de la tecnología tiene vigencia la máxima "proactividad y no reacción, prevención y no corrección" (p. 9).

CONCLUSIONES

En principio, la divulgación de providencias judiciales de índole penal por parte de la Relatoría de la Sala de Casación Penal —empleando la Internet— puede verse como el ejercicio legítimo, en clave constitucional y legal, de la función de divulgación de información pública de las providencias judiciales, mediante la cual se satisface el interés público en controlar la actividad jurisdiccional, informar sobre las infracciones penales —sus particularidades y la identidad de los transgresores—

y permitir el conocimiento de los argumentos y las razones jurídicas de los jueces al administrar justicia en los casos concretos. Además, claro está, de cumplir con la función de prevención general de las penas.

A tono con la posición de la Corte Suprema del 19 de agosto de 2015 la legitimidad de esta actividad, sumada a la importancia de sus fines, permite excluir —con algunas salvedades— la aplicación del *hábeas data* en cualquiera de sus modalidades de supresión; asimismo, faculta a la Corporación para servirse de la Internet o de cualquier otro tipo de sistema de información en orden a comunicar sus decisiones.

No obstante, se demostró que la divulgación y consecuente publicidad de las sentencias judiciales en Internet vulnera la regulación sobre protección de datos personales y *hábeas data* en Colombia: es indiscriminada, facilita un ejercicio inorgánico del poder informático sobre los datos personales contenidos en soportes públicos y contraría algunos de los principios fundamentales (v. gr., los de finalidad, utilidad, necesidad y circulación restringida) llamados a guiar la actuación de quienes administran archivos y bases de datos personales o procesan y manejan información personal de terceros, incluidos quienes lo hacen en el marco de la función pública de impartir justicia.

Adicionalmente, se advierte una gestión indebida de las bases de datos destinadas a la divulgación de providencias penales, pues, si bien la Internet resulta eficaz como mecanismo general de acceso a la información, no es el medio tecnológico adecuado para el cumplimiento de las finalidades asignadas a la difusión de las decisiones penales, ya que su utilización excede las finalidades legales y constitucionales de la divulgación de esta clase de providencias judiciales y afecta derechos y garantías constitucionales básicas de los ciudadanos condenados o no.

Todos estos problemas podrían evitarse si se garantiza el anonimato de las personas —partes e intervinientes— que figuran en las decisiones alojadas en las bases de datos destinadas a la divulgación de información pública. Esta acción obviaría las discusiones sobre la procedencia o no del *hábeas data* y de la normativa sobre protección de datos personales en estos supuestos a más de evitar analogías, no necesariamente atinadas, con los antecedentes penales o los disciplinarios a la hora de precisar si el acceso a la información contenida en las providencias debe restringirse o no, ya sea en razón de un derecho al olvido (supresión total), por la aceptación de la supresión relativa de información personal de forma general o únicamente cuando se hubiere cumplido la pena o la misma hubiere prescrito.

Esta opción, claramente preventiva antes que reactiva, garantiza los derechos de las personas cuya información está contenida en las decisiones divulgadas, resulta sencilla de implementar y es bastante más efectiva que la de resolver caso por caso las peticiones elevadas por los ciudadanos y, por supuesto, es compatible con las funciones legales asignadas a la Relatoría de la Sala de Casación Penal de la Corte Suprema.

REFERENCIAS BIBLIOGRÁFICAS

Álvarez, F.J. (2011). El acceso por parte de las fuerzas y cuerpos de seguridad del Estado a ficheros de datos personales. En Pedraz Penalva, E. (Coord.). *Protección de datos y proceso penal* (pp. 48-83). Madrid, España: La Ley.

Ausloos, J. (2012). The 'Right to be Forgotten' — Worth remembering? *Computer Law and Security Review*, *28*, 143-152.

Bennet, S.C. (2012). The "Right to Be Forgotten": Reconciling EU and US Perspectives. *Berkeley Journal of International Law*, *30* (1), 161-195.

Blume, P. (2012). The Inherent contradictions in data protection law. *International Data Privacy Law*, *2* (1), 26-34.

Brian, A. (2012). La protección inteligente de los datos personales: Privacy By Design (PBD). *Revista Internacional de Protección de Datos Personales*, *1*, 1-15.

Bru, E. (2007). La protección de datos en España y en la Unión Europea. Especial referencia a los mecanismos jurídicos de reacción frente a la vulneración del derecho a la intimidad. *Revista de Internet, Derecho y Política*, *5*, 78-91.

Cabezudo, N. (2011). Ficheros automatizados y registros centrales de la Administración de justicia. La obtención de los datos y la gestión de las informaciones. En Pedraz Penalva, E. (Coord.). *Protección de datos y proceso penal* (pp. 141-174). Madrid, España: La Ley.

Cifuentes, E. (1997). El hábeas data en Colombia. *Derecho PUCP: Revista de la Facultad de Derecho*, *51*, 115-144.

Conde, C. (2005). *La protección de datos personales. Un derecho autónomo con base en los conceptos de intimidad y privacidad*. Madrid, España: Dykinson.

de la Calle, J.M. (2009). *Autodeterminación informativa y hábeas data en Colombia. Análisis de la Ley 1266 de 2008. Jurisprudencia y derecho comparado.* Bogotá, Colombia: TEMIS.

Diorio, S. (2015). Data Protection Laws: Quilts Versus Blankets. *Syracuse Journal of International Law and Commerce*, *42* (2), 485-513.

El Tiempo. (25 de febrero de 2016). ¿Derecho al olvido prima en casos con menores de edad? Las cortes han ordenado 'borrar' nombres de condenas, con algunas excepciones. Recuperado de http://www.eltiempo.com/politica/justicia/derecho-al-olvido-en-caso-de-abuso-contra-menores/16519752.

García, A. (2013). Reflexiones en torno a la protección de los datos personales en Internet y las redes sociales. Retos y perspectivas en un mundo hiperconectado. *Derecho Comprado de la Información*, *21*, 39-67.

Garriga, A. (2009). *Tratamiento de datos personales y derechos fundamentales*. Madrid, España: Dykinson.

Garriga, A. (2016). *Nuevos retos para la protección de datos personales. En la Era del Big Data y de la computación ubicua*. Madrid, España: Dykinson.

Gordillo, J. y Restrepo, O. (2004). Introducción al análisis del derecho fundamental del hábeas data. *Estudios Socio-Jurídicos*, *6* (2), 351-385.

Gutiérrez, J.D. (2001). *Los límites entre la intimidad y la información*. Bogotá, Colombia: Universidad Externado de Colombia.

Hernández, J.C. (2012). La protección de datos personales en Internet y el hábeas data. *Revista Derecho y Tecnología*, *13*, 61-85.

Hernández, S. (25 de febrero de 2016). El caso del rector de colegio que genera debate en Honda. El hoy directivo de un colegio público pagó condena por abuso de menores de edad. *El Tiempo*. Recuperado de http://www.eltiempo.com/colombia/otras-ciudades/debate-por-rector-condenado-por-abuso-de-menores-en-honda/16519747.

Jacobs, J. y Larrauri, E. (2010). ¿Son las sentencias públicas? ¿Son los antecedentes penales privados? Una comparación de la cultura jurídica de Estados Unidos y España. *Revista para el Análisis del Derecho InDret*, *4*, 1-52.

Koops, B. (2014). The trouble with European data protection. *International Data Privacy Law*, *4* (4), 250-261.

Lucena, I.V. (2014). El concepto de intimidad en los nuevos contextos tecnológicos. En Galán Muñoz, A. (Coord.). *La protección jurídica de la intimidad y de los datos de carácter personal frente a las nuevas tecnologías de la información y comunicación* (pp. 15-54). Valencia, España: Tirant Lo Blanch.

Mantelero, A. (2013). The EU Proposal for a General Data Protection Regulation and the roots of the 'right to be forgotten'. *Computer Law and Security Review*, *29*, 229-235.

Martínez, R. (2013). *Protección de datos de carácter personal*. Valencia, España: Tirant Lo Blanch.

Murillo de la Cueva, P.L. (2007). Perspectivas del derecho a la autodeterminación informativa. *Revista de Internet, Derecho y Política*, *5*, 18-32.

Newman, A.L. (2015). What the "right to be forgotten" means for privacy in a digital age. *Science*, *347* (6221), 507-508.

Palacios, M.D. (2012). El poder de autodeterminación de los datos personales en Internet. *Revista de Internet, Derecho y Política*, *14*, 61-74.

Pazos, R. (2015). El funcionamiento de los motores de búsqueda en Internet y la política de protección de datos personales, ¿una relación imposible? *Revista para el Análisis del Derecho InDret*, *1*, 1-50.

Puccinelli, O.R. (2012). El "derecho al olvido" en el derecho de la protección de datos. El caso argentino. *Revista Internacional de Protección de Datos Personales*, *1*, 1-22.

Rebollo, L. y Serrano, M. (2008). *Introducción a la protección de datos*. Madrid, España: Dykinson.

Rees, C. and Heywood, D. (2014). The 'right to be forgotten' or the 'principle that has been remembered'. *Computer Law and Security Review*, *30*, 574-578.

Remolina, N. (2013). *Tratamiento de datos personales: aproximación internacional y comentarios a la Ley 1581 de 2012*. Bogotá, Colombia: LEGIS.

Remolina, N. (8 de octubre de 2014). ¿Derecho al olvido y lista Clinton? Recuperado de http://oiprodat.com/2014/10/08/derecho-al-olvido-y-lista-clinton/.

Roig, M. (2012). *La cancelación de los antecedentes delictivos*. Valencia, España: Tirant Lo Blanch.

Voss, W.G. (2014). Looking at the European Union Data Protection Law Reform Through a Different Prism: The Proposed EU General Data Protection Regulation Two Years Later. *Journal of Internet Law*, *17* (9), 11-24.

Warso, Z. (2013). There's more to it than data protection — Fundamental rights, privacy and the personal/household exemption in the digital age. *Computer Law and Security Review*, *29*, 491-500.

Weber, R.H. (2015). The digital future — A challenge for privacy? *Computer Law and Security Review*, *31*, 234-242.