

Datos personales en información pública:

oscuridad en lo
privado y luz en
lo público

Vivian Newman Pont



DOCUMENTOS 20

Datos personales en información pública: oscuridad en lo privado y luz en lo público

Vivian Newman

VIVIAN NEWMAN

Abogada de la Universidad Javeriana y licenciada en derecho por homologación en la Universidad de Barcelona, con especialización en derecho administrativo (D.S.U.) y maestrías en derecho público interno (D.E.A.) de la Universidad de París II, y en Cooperación y Desarrollo de la Universidad de Barcelona. Ha prestado servicio público en la Procuraduría General de la Nación; ha ejercido el derecho privado en Avianca S.A. y Bavaria S.A., y el derecho público como abogada independiente. Coordinó el Departamento de Derecho Público de la Universidad Javeriana, donde fue docente en derecho administrativo. Actualmente es subdirectora de Dejusticia.

Documentos Dejusticia 20

DATOS PERSONALES EN INFORMACIÓN PÚBLICA:
oscuridad en lo privado y luz en lo público

Este trabajo fue realizado gracias a la contribución de
Open Society Foundations (OSF), Privacy International (PI)
y el Centro Internacional de Investigaciones para el Desarrollo de Canadá (IDRC).

ISBN: 978-958-58858-1-3 Versión impresa
978-958-58858-0-6 Versión digital

Centro de Estudios de Derecho, Justicia y Sociedad, Dejusticia
Carrera 24 N° 34-61, Bogotá, D.C.
Teléfono: (57 1) 608 3605
Correo electrónico: info@dejusticia.org
<http://www.dejusticia.org>

Este texto puede ser descargado gratuitamente en <http://www.dejusticia.org>
Creative Commons Attribution-Non Commercial Share-Alike License 2.5.



Revisión de textos: María José Díaz Granados
Preprensa: Marta Rojas
Cubierta: Alejandro Ospina

Bogotá, enero de 2015

Contenido

Introducción..... 9

CAPÍTULO I.
MARCO CONCEPTUAL Y NORMATIVO 13

Origen conceptual 14

Conceptualización normativa..... 19

**Clasificaciones de datos personales
 y de información pública**..... 27

CAPÍTULO II.
**GUÍA DE ARMONIZACIÓN FRENTE A LA TENSIÓN
ENTRE LOS DATOS PERSONALES Y EL DERECHO
DE ACCESO A LA INFORMACIÓN PÚBLICA**..... 35

Carga de la prueba 36

Test de daño 41

Armonización..... 42

 Armonización de conceptos 42

 Selección de principios
 con posibilidades de colisión 47

 Armonización de principios y divulgación parcial..... 49

**Distinción entre diversas esferas
 de la intimidad y la autonomía**..... 55

Tratamiento diferencial
para datos personales de interés público 61

Conclusiones generales..... 69

ANEXO 1.
**Selección de ley especial aplicable a bases
de datos en la tensión entre *habeas data*
y acceso a información pública 75**

**Bases de datos con información
de seguridad, inteligencia y justicia 77**

Otras bases de datos con norma especial 80

Referencias..... 85

Agradecimientos

Agradezco los valiosos comentarios al contenido de este documento que hicieron Carlos Cortés, Nina Chaparro, Diana Esther Guzmán, Carlos Malagón, Juan Pablo Remolina, Silvia Rojas, Elvia Sáenz y Rodrigo Uprimny, así como a Alejandra Abondano por su colaboración en la revisión jurisprudencial y al equipo administrativo de Dejusticia por su apoyo constante.

Introducción

En una democracia constitucional, la transparencia en la esfera pública y el secreto en la esfera privada son valores necesarios, prioritarios y complementarios. En la cosa pública se requiere luz que nos permita ejercer el control ciudadano, exigir la garantía de los derechos, vigilar los dineros públicos, monitorear el funcionamiento estatal y, en general, facilitar la participación en las decisiones que nos afectan. La vida privada, en cambio, amerita sombras para el florecimiento de la autonomía, la autodeterminación y la libertad (Uprimny, Fuentes, Botero y Jaramillo 2006: 113 y ss.). La protección y el secreto en la vida privada nos permitirán desarrollarnos y ser personas despreocupadas de las consecuencias negativas derivadas de la exposición de nuestra intimidad intrascendente para terceros, al tiempo que la transparencia enriquecerá nuestra posibilidad de participar e intervenir en materias de importancia pública.

La luminosidad y la oscuridad se predicán de la información compuesta por datos de los ámbitos público y privado, y generan una disyuntiva importante, pues, por un lado, hay que revelarlos, y, por otro, darles protección.¹ Estos datos pueden ser personales o impersonales,

1 Después de la publicación en 1890, en la revista de derecho de la Universidad de Harvard, de un artículo titulado “The Right to Privacy” (El derecho a la privacidad), uno de sus autores, Louis Brandeis, escribió una serie de cartas y un artículo compañero sobre el deber de publicidad, *The Duty of Publicity*, analizando las tensiones entre la privacidad y la publicidad, y reconociendo el poder de la transparencia y la apertura como elementos purificadores, en el mismo sentido que la luz solar funciona como desinfectante. Sus estudios, primero para criticar a los periodistas invasivos y paparazzi, y luego para valorar el periodismo investigativo y de denuncia, resumen la ética del periodismo a la que se pretendía llegar en Estados

según si atañen a una persona natural o jurídica.² La información impersonal no tiene un fuerte límite constitucional de protección debido a la prohibición expresa de la censura, así como a los principios de publicidad, eficiencia y transparencia que rigen el acceso a la información pública, y la actividad de la administración pública y de la administración de justicia.³ La información personal, en cambio tiene una protección especial en Colombia y en general en los países con un relativo nivel de avance garantista en el acceso a la información pública.⁴

En la práctica, los datos personales llegan a repositorios públicos por diversos motivos y surgen dificultades para discernir cuándo es legal y constitucional un rechazo de acceso a la información por razones de privacidad, y cuándo no lo es. Esto sucede, pues existen múltiples datos personales que entregan las personas o recolectan terceros, incluido el Estado, a través de censos, encuestas, registros públicos, formulación de

Unidos a finales del siglo XIX y principios del siglo XX. Para mayor información ver Coyle (2009).

- 2 Según la Corte Constitucional en la sentencia C-1011 de 2008, que analizó la exequibilidad de la Ley 1266 del mismo año, tanto las personas naturales como las jurídicas son titulares de los derechos derivados de los datos personales, pero en la sentencia C-748 de 2011, que estudió la constitucionalidad de la Ley 1581 de 2012, las personas jurídicas tienen datos personales en la medida en que están compuestas por personas naturales, pero no por su propia naturaleza. De una lectura sistemática de ambas sentencias, se concluye que las personas jurídicas pueden ser titulares de datos personales comerciales, financieros, de servicios o de terceros países (Ley 1266 de 2008), pero no son titulares de datos personales en los demás casos.
- 3 Corte Constitucional, sentencia T-729 de 2002, M P. Eduardo Montealegre Lynett.
- 4 Por ejemplo, la Ley Federal de Acceso a la Información Pública Gubernamental de México de 2002, pionera y modelo en la región, menciona la “información confidencial”. Este concepto integra, según el artículo 18, los datos personales (datos personales son la información concerniente a una persona física, identificada o identificable, v.gr., el origen étnico o racial, el domicilio, el patrimonio, el número telefónico, la ideología o las preferencias sexuales) y que requieran el consentimiento de los individuos para su difusión, así como la información que los particulares entreguen a las autoridades siempre que tengan el derecho de reservarse dicha información de conformidad con una disposición legal (art. 19). Esta información tiene un trato excepcional: no está sujeta a un plazo de reserva y debe permanecer indefinidamente fuera del dominio público; y salvo que el titular de dicha información otorgue el consentimiento expreso para divulgarla, su acceso se encuentra restringido, no admite prueba de daño y solo puede acceder a ella el titular (López-Ayllón y Posadas (2011).

quejas o, en general, huellas que quedan en Internet y que luego constan en documentación pública. Esta documentación estará en poder o control de sujetos estatales, a través de diversas agrupaciones de datos que van desde un simple acto administrativo hasta sistemas informativos o bases de datos con patrones de comportamiento que tienen gran valor económico, social, científico, político y cultural.

Cuando esos datos se encuentran en poder o bajo el control de personas que están obligadas a hacer pública su actuación, se generan tensiones derivadas de la libertad informativa y la protección de la intimidad. Surgen entonces preguntas como: frente a una solicitud ordinaria de acceso a la información de datos personales ¿prima el acceso a la información o la protección de los datos personales? Los documentos públicos que contienen datos personales, ¿pueden divulgarse en su totalidad? ¿Qué hacer si los datos se encuentran en una providencia judicial que es pública por esencia? Y si se trata de los datos personales de un funcionario público que son necesarios para ejercer control social de su gestión ¿también se protegen del escrutinio público? ¿Y si se trata de datos personales para hacer una investigación o un estudio que sirva de soporte a un documento de política pública? ¿Y si hay interés público en verificar, por ejemplo, la autenticidad de las firmas y la existencia de los ciudadanos que votan por la revocatoria del mandato de un alcalde o gobernador elegido popularmente?⁵

-
- 5 En Bogotá, la revocatoria del mandato del alcalde Gustavo Petro es caso de estudio en esta materia. Por un lado, la Registraduría Nacional del Estado Civil, como en otras oportunidades, consideró que la solicitud de revocatoria con todas sus firmas y cédulas era información pública de libre acceso. Frente al requerimiento de la Superintendencia Delegada para la Protección de Datos Personales, respondió que a su modo de ver dicha información no constituía una base de datos y que no entregaba copia del archivo nacional de identificación (ANI), pues contenía datos biográficos, filiación política y la fórmula dactiloscópica, reservados por aplicación del artículo 213 del Código Electoral. La tutela derivada de este caso fue fallada en primera instancia por el Tribunal Administrativo de Cundinamarca en sentencia del 8 de julio de 2003, con una ponencia de Alfonso Sarmiento Castro, que despachó en un párrafo lo que consideró ausencia de violación del *habeas data*, pues los peritos tendrían acceso a las firmas con el exclusivo objeto de “verificar la autenticidad de las rúbricas y la figuración del firmante en el censo electoral respectivo, sin posibilidad de sustraer dato o documento alguno, protección encomendada a la accionada como autoridad encargada legalmente de su custodia y cuidado, con las responsabilidades que puede conllevar su uso para un objeto distinto al autorizado”. Ver el caso, que se encuentra bajo apelación, en <http://>

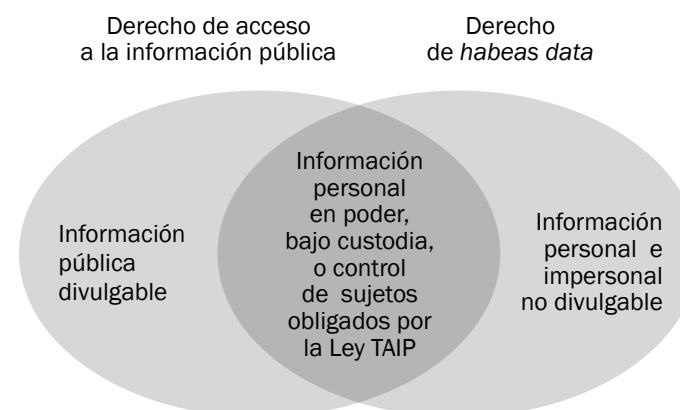
Para responder a las anteriores preguntas, en este documento exploramos cuál ha sido la respuesta de la ley y la jurisprudencia colombianas frente a las tensiones entre la intimidad y la publicidad de los datos. Lo haremos a partir de un primer capítulo dedicado a la revisión de la normativa existente en materia de publicidad y protección de datos personales, así como a su conceptualización legal y jurisprudencial (I), y seguiremos con un segundo capítulo que analiza la legislación y las principales decisiones de la Corte Constitucional que han aplicado dicho marco normativo en la práctica para definir unos estándares de implementación en ciertas hipótesis (II). Finalmente, extraeremos unas conclusiones básicas que esperamos sean útiles en la armonización de esta tensión.

En este sentido, el estudio de la normativa resulta útil por cuanto configura el marco dentro del cual debe tener lugar la respuesta estatal a la tensión entre lo público y lo privado, y permite identificar su filosofía. Por su parte, las decisiones constitucionales nos ofrecen la posibilidad de analizar cómo el tribunal encargado de la guarda de la Constitución de ambos derechos fundamentales resuelve la problemática frente a los casos concretos. En conjunto, aspiramos a que el análisis nos permita establecer cuál es el enfoque que ha tenido la respuesta del Estado y sus alcances o límites frente a los datos personales y su publicidad.

CAPÍTULO I. MARCO CONCEPTUAL Y NORMATIVO

Si una persona quiere acceder a información que pertenece a la órbita privada, pero se encuentra en poder o bajo custodia de una entidad que estaría obligada a divulgarla, se genera una tensión que el derecho resuelve ya sea mediante una protección (información pública clasificada) o mediante una obligación de revelación. Una gráfica de la teoría de conjuntos¹ puede ser útil para mostrar que en el cruce de ambos círculos se encuentra la tensión entre los derechos que aquí examinamos:

GRÁFICA 1
Datos personales en información pública



¹ Esta gráfica se inspira en otra imagen elaborada por el funcionario público Juan Pablo Remolina, del Grupo de Transparencia y Acceso a la Información Pública de la Procuraduría General de la Nación, que a su vez refleja las tensiones entre estos dos derechos y el derecho de petición.

En este capítulo presentamos los elementos conceptuales a partir de los cuales haremos nuestra aproximación a la armonización de esta tensión entre los dos extremos que representan valores y derechos igualmente importantes en un Estado social de derecho.

Origen conceptual

El primer paquete de documentos que se refirió a la importancia de la protección de datos personales provino del Consejo de Europa, la Organización de las Naciones Unidas (ONU), la Organización para la Cooperación y el Desarrollo Económicos (OCDE) y el Parlamento Europeo.² Estas menciones, producidas en el marco del contexto tecnológico de los años ochenta, articulaban la protección de los datos personales al derecho a la intimidad, de manera que los primeros gravitaban alrededor de la segunda.

La noción de intimidad, que se confundía y confunde con la de privacidad,³ fue mencionada originalmente por el jurista norteamericano

² Ver Nelson Remolina (2013: 32 y ss.) sobre el artículo 1 del Convenio 108 de 1981 del Consejo de Europa, y el prólogo de las directrices relativas a la protección de la privacidad y flujos transfronterizos de datos personales del 23 de septiembre de 1980 de la OECD, Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995.

³ Para efectos de este documento, el derecho a la intimidad y el derecho a la privacidad serán considerados sinónimos pues en el derecho colombiano no ha predominado ninguna distinción significativa. Sin embargo, para algunos académicos, como el profesor español de filosofía del derecho Megías Quirós, existe una diferencia entre intimidad y privacidad en la medida en que la primera entraña una dimensión negativa, de no permitir que otros accedan, y la segunda una dimensión positiva o de control. Al respecto, dice que la intimidad “tiene como objeto propio excluir a los extraños del conocimiento de nuestros datos íntimos, mientras que la segunda conlleva no solo el respeto de éstos, sino también su control, así como el secreto de las comunicaciones y las circunstancias en que se producen, el control de otros datos públicos que dan acceso a la intimidad”. Ver en este sentido su publicación *Privacidad e Internet: intimidad, comunicaciones y datos personales*. Recuperado de: <http://revistas.ucm.es/index.php/ANDH/article/viewFile/ANDH0202110515A/20978> (Consultada el 19 de junio de 2014). Para otros académicos, de la mano de Garzón Valdés, la intimidad es “el ámbito de los pensamientos de cada quien [...] lo aún no expresado y que probablemente nunca lo será”, mientras que privacidad es “la esfera personal reconocida [...] el ámbito reservado para las relaciones interpersonales”, de tal suerte que la privacidad debe ser estrictamente respetada por el Estado y por los poderes fácticos, pero regulada en ciertos aspectos críticos, y la intimidad debe permanecer absolutamente invulnerable (Garzón 2008).

Luis Brandeis en un artículo escrito con Warren Samuel en la *Revista jurídica* de la Universidad de Harvard, en 1890, bajo el título “El derecho a la privacidad” (Brandeis y Warren 1890). En los estudios de Brandeis se menciona por primera vez “el derecho a ser dejado solo” (*the right to be let alone*) como un principio para impedir que terceros (en particular periodistas invasivos) publiquen determinada información sin contar con la voluntad del implicado. El jurista se basó en la idea del incumplimiento de un contrato o confianza implícitos, por oposición a la propiedad de la imagen, la idea, la historia, etc. Para el efecto, Brandeis alegó que “... el principio puede ser invocado para proteger la privacidad del individuo de la invasión de la prensa, fotógrafos, o el poseedor de cualquier aparato moderno para grabar o reproducir escenas y sonidos”.

En ese entonces, y hasta muy entrado el siglo XX, la privacidad se había venido caracterizando por un cierto ámbito estático, sujeto al espacio donde se encuentran la persona y sus relacionados. Así, la intimidad se definía de múltiples maneras, pero siempre haciendo referencia a la vida privada y familiar en un espacio determinado: el derecho a ser dejado solo, con los suyos, en su propio entorno.

Sin embargo, con el avance de la tecnología, comienza una circulación de la información que se predica de una persona y la intimidad asume una movilidad que hasta entonces había sido escasa. Además, y como consecuencia de la puesta en marcha de los avances tecnológicos, aparece una capacidad ilimitada de registro y almacenamiento de los datos que a su vez se pueden correlacionar, difundir y casi nunca desaparecer.

Esta capacidad de recoger y conjugar la información relativa a las actuaciones pasadas y preferencias de una persona, es el paso previo para armar su perfil, individualizarla y asumir así poder sobre ella. En efecto, los datos son susceptibles de ser convertidos en información cuando se insertan en un modelo que los relaciona con otros y que, juntos, hace que adquieran sentido. Se constituyen, sin duda, en un instrumento que sirve para identificar a una persona y solo a ella, y que, por tanto, puede usarse para coartarla, muy a pesar de que los datos sean de su propiedad o de su intimidad y de que, por consiguiente, tenga el derecho de rechazar su divulgación o publicidad.

El conjunto de datos de este tipo son sus señales particulares: relaciones de propiedad y de familia, aspectos de su personalidad y señales de identidad de diversa índole que van emergiendo en las actividades de

la vida y que, combinados en un modelo, son equivalentes a una «huella digital» que identifica al individuo o al menos lo hace identificable.⁴

Por las características propias de los datos, una vez producidos pueden diseminarse con relativa facilidad. Usados, en combinación con otros de procedencias distintas pero predicables de la misma persona, van configurando lo que se ha dado en llamar el «perfil de datos de una persona». Los perfiles pueden ser contruidos, agregados, procesados e incluso descontextualizados por quienes tengan bancos de datos, bien sean manuales o sistematizados. Es evidente, entonces, el riesgo, muy concreto, de que la circulación de datos, por inocente que sea, permita acceder a la intimidad de los titulares, como si les hiciera seguimiento a sus movimientos físicos con un detective.

El «perfil de datos» del individuo se constituye entonces en una especie de «persona virtual» sobre la cual pueden ejercerse muchas acciones que tendrán repercusión sobre la persona real, desde el envío de propaganda no solicitada, hasta la coerción o el «ostracismo» social. Un buen manejo de bancos de datos permitiría identificar perfiles poblacionales desde distintos puntos de vista, con el peligro de que aquellos que ostentan «poder informático» puedan ejercer control social, no solo sobre la libertad de las personas individuales, sino sobre la de sectores sociales más amplios. Baste recordar que los proveedores e intermediarios de servicios de Internet y de comunicaciones, tales como las compañías de telefonía móvil, los motores de búsqueda y las aplicaciones digitales, tienen la capacidad de acceder a datos personales sobre horas en las que se hacen llamadas telefónicas, destinatarios de tales llamadas, asuntos de interés que motivan búsquedas en Internet, ubicación general y temporal, etc.

La era digital contribuye entonces a alejar al individuo de sus propios datos, mediante una amplia variedad de sistemas que los inmateria- lizan, y le hacen perder control sobre esta información que le es propia, tanto porque pertenece a su intimidad como porque representa su propio rastro, la huella de su ser y estar.

4 Ver en este sentido la intervención del ingeniero Ernesto Lleras, profesor investigador de la Facultad de Ingeniería de Sistemas y Computación de la Universidad de los Andes, invitado por la Corte Constitucional a presentar un concepto sobre el manejo y uso de los datos personales, que resultó de gran valor para la discusión y conclusiones de la sentencia T-414 de 1992 de la Corte Constitucional, y que a su vez nutrió este apartado.

Es clara entonces la importancia de controlar esta información que fluye en diferentes espacios, trascendiendo incluso fronteras, y de que para ese propósito se le brinden a cada persona herramientas distintas que le permitan gobernar su difusión.

Esta nueva categoría, si bien se elabora a partir del derecho a la privacidad, se perfila también muy cercana al libre desarrollo de la personalidad y, en cierta medida, al derecho de propiedad sobre uno mismo. De esta manera, el poder que se tiene sobre los propios datos adquiere características distintas de los derechos que conjuga y se conocen bajo la expresión latina *habeas data*.

El origen del *habeas data* se encuentra estrechamente vinculado a la expresión *habeas corpus* (que tengas el cuerpo), figura consagrada para devolverle la libertad corporal a una persona que esté detenida en condiciones no satisfactorias o ilegítimas. Trazando una analogía, el *habeas data* (que tengas/vengan los datos) se refiere a poder “...tomar conocimiento de datos propios en poder de otro” (Pierini, Lorences y Tornabene 1998: 22-23). Esta toma de conocimiento se extiende al control de los propios datos, al punto de definir el *habeas data* como “...un derecho autónomo que procura la protección frente al registro y utilización informática, ya no solo de datos personales considerados íntimos o informaciones sensibles, sino también de otros datos que a pesar de no tener estrictamente dicho carácter, igualmente merecen ser objeto de preservación, control y reserva” (Urioste 2008: 155 y ss.). La Constitución de Brasil de 1988 bautiza la protección de este derecho con la garantía del *habeas data*, bajo inspiración de la Constitución portuguesa.⁵

Simultáneamente, y por las mismas razones que fundamentan la evolución de los datos personales en otras partes, en el sistema normativo colombiano el derecho a la protección de los datos personales, que ya también se conoce como *habeas data*, se aleja un poco del núcleo exclusivo del derecho a la intimidad. Se empieza a conjugar con el libre desarrollo de la personalidad y la autodeterminación informática, asumiendo cada vez más independencia y autonomía, y permitiendo al titular de los

5 Señala Dallari, citado por Urioste, que dicha creación brasilera se apoyó en la intención de los ciudadanos portugueses de acceder a los registros de la policía política de Salazar, pues los iberoamericanos “...al salir de los largos años de gobiernos militares, también querían conocer los datos consignados en los registros del Servicio Nacional de Información” (Urioste 2008: 157).

derechos a acceder a su propia información, disponer de sus datos personales, actualizarlos y asegurar en parte su confidencialidad.

Se puede entonces entender el *habeas data* con una doble condición: una acción, teniendo en cuenta sus orígenes, y un derecho por haber sido consagrado de esta forma en la Constitución Política de 1991. De esta manera, el *habeas data* ha sido definido en ocasiones como “...un interdicto o acción judicial, rápida y expedita y sin el rito de un procedimiento judicial para amparar el derecho de toda persona a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ella en bancos de datos y en archivos de entidades públicas y privadas” (Camargo 2014: 61). Por otra parte, desde la doctrina también se ha aceptado que se trata de un derecho fundamental, teniendo en cuenta que “...el artículo 15 de la Carta Política indica que todas las personas ‘tienen derecho’ a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas”. Esta doble calidad de derecho y acción también se recoge en las normas legales colombianas que veremos en el próximo apartado.

Por su parte, el derecho de acceso a la información pública como derecho fundamental también ha tenido un reciente desarrollo. Desde la Ley 57 de 1985, que luego se incorporó al Código Contencioso Administrativo de 1984, se entronizó la solicitud de acceso a documentos públicos como un derecho del administrado a conocer y participar en la cosa pública. Con posterioridad, la Constitución de 1991 reconoció el derecho de acceso a la información pública, pero su consagración como derecho fundamental independiente no era clara en ese entonces. Tanto la jurisprudencia contencioso administrativa, como la constitucional, reconocían la existencia de este derecho, pero de manera cambiante. En ocasiones lo consideraban como una materialización del derecho de petición, y en otras oportunidades era un insumo o parte de la libertad de expresión. Solo a partir del siglo XXI comenzó la jurisprudencia a reconocer el acceso a la información pública como un derecho fundamental, ya no solo administrativo, sino además independiente y autónomo. La Corte Interamericana de Derechos Humanos fue el primer tribunal internacional en reconocer el derecho de acceso a la información pública como un derecho humano autónomo en la conocida sentencia *Claude Reyes y otros vs. Chile* del 19 septiembre de 2006. Por su parte, la Corte Constitucional colombiana en la sentencia C-491 de 2007, consolidó la independencia y autonomía de este derecho fundamental en nuestro

país.⁶ En el mes de marzo de 2014, luego de un arduo impulso de algunas organizaciones de la sociedad civil, reunidas en la Alianza Más Información, Más Derechos,⁷ desde la construcción hasta su examen en la Corte Constitucional, el presidente Santos sancionó la Ley estatutaria de transparencia y acceso a la información pública, Ley 1712 de 2014.

Pasamos a analizar entonces la Constitución de 1991 y sus desarrollos legislativos respecto al *habeas data* y el acceso a la información pública.

Conceptualización normativa

Los derechos relevantes para nuestro análisis se encuentran definidos en la Constitución Política y en la ley escrita que para nuestros efectos se compone principalmente de tres leyes estatutarias: Ley 1266 de 2008, a la que llamaremos Ley de *habeas data* sectorial; Ley 1581 de 2012 o Ley estatutaria de datos personales, y Ley 1712 de 2014 o Ley de transparencia y acceso a la información pública o Ley TAIP.

Como primera medida, en la Constitución Política⁸ el artículo 15 fija el contenido tanto del derecho a la intimidad como a la protección de los datos personales. La mencionada norma establece:

-
- 6 Para una explicación más detallada ver Uprimny y Newman (2013).
 - 7 La Alianza Más Información, Más Derechos está integrada por Transparencia por Colombia, Fundación para la Libertad de Prensa, Corporación OCASA, Proyecto Antonio Nariño y Centro de Estudios de Derecho, Justicia y Sociedad (Dejusticia).
 - 8 Por aplicación del bloque de constitucionalidad, artículo 92 constitucional, los tratados y convenios internacionales ratificados por el Congreso, que reconocen los derechos humanos, prevalecen en el orden interno y constituirán un criterio de interpretación. De esta manera, debemos también considerar los siguientes instrumentos que consagran el derecho a la intimidad y a los datos personales y que se entienden como parte de nuestro ordenamiento constitucional:
 - El artículo 12 de la Declaración Universal de Derechos Humanos (Naciones Unidas, 1948) que establece: “Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra y su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques”.
 - El artículo 17 del Pacto Internacional de Derechos Civiles y Políticos (ICCPR, 1966) que señala: “1) Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación. 2) Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques”.
 - El artículo 11 de la Convención Interamericana de Derechos Humanos que reza: “Protección de la honra y la dignidad. Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad. Nadie

Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre y el Estado debe respetarlos y hacerlos respetar. De igual modo tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.

La intimidad consagrada en la primera línea del artículo 15 —según la jurisprudencia colombiana que en cierta medida desarrolla ese principio del “derecho a ser dejado solo” de la doctrina norteamericana—, es definida por lo negativo: lo que impide la intervención de los demás. Es esa

... esfera o espacio de vida privada no susceptible de la interferencia arbitraria de las demás personas, que al ser considerada un elemento esencial del ser, se concreta en el derecho a poder actuar libremente en la mencionada esfera o núcleo, en ejercicio de la libertad personal y familiar, sin más limitaciones que los derechos de los demás y el ordenamiento jurídico.⁹

No menciona la Corte que la intimidad es el resultado de una construcción social, ni que la sociedad y sus usos van decidiendo qué es muy privado y debe protegerse, pero sí ahonda en ejemplos y menciona un recuento de conductas que pertenecen al individuo y que generalmente deben permanecer en su fuero interno pues no está interesado en compartirlos con la sociedad.¹⁰

puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques”.

El derecho a la intimidad también es definido en la convención de los Derechos del Niño de 1990 (art. 16), la Carta de Derechos fundamentales de la Unión Europea de 2000 (art. 7), la Convención Europea de Derechos Humanos de 1950 (art. 8) y la Convención Asiática (art. 21).

9 Corte Constitucional, sentencia C-1011 de 2008, M. P. Jaime Córdoba Triviño.

10 La sentencia SU-082 de 1995 transcribe un recuento empírico del autor Eduardo Novoa Monreal, sobre las actividades, situaciones y fenómenos pertenecientes a la vida privada, que incluye: “a) ideas y creencias religiosas, filosóficas, mágicas y políticas que el individuo desee sustraer del conocimiento ajeno; b) aspectos concernientes a la vida amorosa y sexual; c) aspectos no conocidos por extraños de la vida familiar, especialmente los de índole embarazosa para el individuo o para el grupo; d) defectos o

En la interpretación de la naturaleza del derecho consagrado en el segundo aparte del anterior artículo, referido al derecho a conocer, actualizar y rectificar las informaciones recogidas en bancos de datos, la jurisprudencia varió de fundamento. En un primer momento, consideró que se trataba del derecho a la intimidad, para luego adscribirlo a la autodeterminación y al libre desarrollo de la personalidad, y finalizar considerando que el núcleo del derecho al dato personal está compuesto por la autodeterminación y libertad informáticas. Así lo resumió en el 2011 el máximo tribunal:

En la jurisprudencia constitucional, el derecho al *habeas data* fue primero interpretado como una garantía del derecho a la intimidad, de allí que se hablara de la protección de los datos que pertenecen a la vida privada y familiar, entendida como la esfera individual impenetrable en la que cada cual puede realizar su proyecto de vida y en la que ni el Estado ni otros particulares pueden interferir. También, desde los primeros años de la nueva Carta, surgió al interior de la Corte una segunda línea interpretativa que consideraba el *habeas data* una manifestación del libre desarrollo de la personalidad. Según esta línea, el *habeas data* tiene su fundamento último [...] en el ámbito de autodeterminación y libertad que el ordenamiento jurídico reconoce al sujeto como condición indispensable para el libre desarrollo de la personalidad y en homenaje justiciero a su dignidad. Ya a partir de 1995, surge una tercera línea interpretativa que es la que ha prevalecido desde entonces y que apunta al *habeas data* como

anomalías físicas o psíquicos no ostensibles; e) comportamiento del sujeto que no es conocido de los extraños y que de ser conocido originaría críticas o desmejoraría la apreciación de éstos hacen de aquél; f) afecciones de la salud cuyo conocimiento menoscabe el juicio que para fines sociales o profesionales formulan los demás acerca del sujeto; g) contenido de comunicaciones escritas u orales de tipo personal, esto es, dirigidas únicamente para el conocimiento de una o más personas determinadas; h) la vida pasada del sujeto, en cuanto pueda ser motivo de bochorno para este; i) orígenes familiares que lastimen la posición social y, en igual caso, cuestiones concernientes a la filiación y a los actos de estado civil; j) el cumplimiento de las funciones fisiológicas de excreción, y hechos o actos relativos al propio cuerpo que son tenidos por repugnantes o socialmente inaceptables (ruidos corporales, intromisión de dedos en cavidades naturales, etc.); k) momentos penosos o de extremo abatimiento; y, j) en general, todo dato, hecho o actividad personal no conocidos por otros, cuyo conocimiento por terceros produzca turbación moral o psíquica al afectado (desnudez, embarazo prematrimonial)”. Cfr. Novoa (1979: 45 y 46).

un derecho autónomo, en que el núcleo del derecho al *habeas data* está compuesto por la autodeterminación informática y la libertad —incluida la libertad económica—.¹¹

La autodeterminación informática se convierte así en la facultad de la persona de autorizar la conservación, uso y circulación de sus datos, de conformidad con las regulaciones legales. La libertad, por otro lado, puede verse vulnerada por la circulación de datos no veraces o por la circulación de los mismos sin la autorización de su titular o de la ley. Esta connotación es relevante para el presente estudio, porque es con la autorización del titular del *habeas data* que en la mayoría de los casos se podrán transparentar los datos personales presentes en información pública.

La información pública, por su parte, se protege mediante varios artículos constitucionales. Si bien el artículo 74 tiene una concepción más específica en relación con el derecho de acceso a documentos públicos, es muy importante recordar que el artículo 20 garantiza la libertad de expresión y opinión, así como la de informar y recibir información veraz e imparcial que conlleva el derecho de acceder a dicha información veraz e imparcial, y que finalmente el artículo 23 consagra el derecho de presentar peticiones respetuosas y obtener pronta resolución, derecho que puede ser ejercido como medio o vehículo para lograr el acceso a la información pública.¹²

11 Corte Constitucional, sentencia C-748 de 2011, M. P. Jorge Pretelt Chaljub; ver también Corte Constitucional, sentencia T-729 de 2002, M. P. Eduardo Montealegre Lynett. En esta última providencia se dice “[A] partir de los enunciados normativos del artículo 15 de la Constitución, la Corte Constitucional ha afirmado la existencia-validez de tres derechos fundamentales constitucionales autónomos: el derecho a la intimidad, el derecho al buen nombre y el derecho al *habeas data*”.

12 Como ya se ha comentado previamente, por aplicación del bloque de constitucionalidad, artículo 92 constitucional, los tratados y convenios internacionales ratificados por el Congreso, que reconocen los derechos humanos, prevalecen en el orden interno y constituirán un criterio de interpretación. En consecuencia, debemos también considerar los siguientes instrumentos que consagran el derecho a acceder a la información pública como parte de nuestro ordenamiento constitucional:

- Según el artículo 19 de la Declaración Universal de los Derechos Humanos: “Todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión”.

- Según el artículo 13 de la Convención Americana sobre Derechos Huma-

Teniendo en cuenta las anteriores normas, es posible definir el derecho fundamental de acceso a la información pública como aquel en ejercicio del cual toda persona, sin necesidad de acreditar un interés directo ni una afectación personal, puede conocer sobre la existencia y acceder a la información en posesión o bajo control de las entidades públicas o privadas que cumplen función pública, prestan servicio público o ejecutan recursos públicos.

El Congreso colombiano, en varias ocasiones y sin seguir una línea única —pues varía en sus fundamentos—, se ha encargado de definir y conceptualizar los dos derechos fundamentales materia de nuestro estudio.

La primera regulación de *habeas data* en nuestro país, posterior a la Constitución de 1991, fue la Ley 1266 de 2008 sobre el tratamiento de datos personales en relación con el cumplimiento de obligaciones económicas o dinerarias. Se trata de una norma de carácter parcial, pues su ámbito de aplicación está sectorizado a datos comerciales, financieros, de servicios y provenientes de terceros países. Dicha regulación de índole estatutaria fue declarada exequible por la Corte Constitucional, pero destacando que se trataba de una regulación sectorial y parcial del *habeas data*.¹³ Las insuficiencias de la Ley 1266 condujeron a la aprobación de la Ley 1581 de 2012 que tampoco fue considerada por la Corte Constitucional como una regulación exhaustiva pero sí más completa y con relación “al punto en que convergen o entran en tensión los derechos al *habeas data*

nos que consagra la libertad de pensamiento y expresión: “1. Toda persona tiene derecho a la libertad de pensamiento y de expresión. Este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección. 2. El ejercicio del derecho previsto en el inciso precedente no puede estar sujeto a previa censura sino a responsabilidades ulteriores, las que deben estar expresamente fijadas por la ley y ser necesarias para asegurar: a. el respeto a los derechos o a la reputación de los demás, o b. la protección de la seguridad nacional, el orden público o la salud o la moral públicas”.

- Según el artículo 19 del Pacto Internacional de Derechos Civiles y Políticos: “1. Nadie podrá ser molestado a causa de sus opiniones. 2. Toda persona tiene derecho a la libertad de expresión; este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección”.

13 En adelante, la Ley 1266 de 2008 será también identificada en este escrito como ley de *habeas data* sectorial.

y a la información”.¹⁴ A lo largo de este texto entenderemos como ley de *habeas data* sectorial o primera ley de *habeas data* a la Ley 1266 de 2008, y como segunda ley de *habeas data* o Ley estatutaria de datos personales a la Ley 1581 de 2012.

La Ley estatutaria 1266 de 2008 o Ley de *habeas data* sectorial, define el dato personal y lo clasifica en público, privado y semiprivado. Sin embargo, la definición y la clasificación, como veremos a continuación, son de utilidad relativa pues no aportan mucho en cuanto a la naturaleza sino en cuanto a la relevancia de los datos para el titular y para terceros.

Según el artículo 3, literal e) de la mencionada ley del 2008, dato personal es cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que puedan asociarse con una persona natural o jurídica.¹⁵ A pesar de esta definición relativamente general, es cierto que dicha norma no se concentró en los datos personales de manera genérica. Más bien hizo énfasis y armó el régimen del dato financiero, comercial, de servicios y de otros países como lo anuncia su propio título, así como muchos de sus artículos, entre los cuales, la totalidad del título IV. En consecuencia, se necesitó una norma posterior para que fijara los alcances, límites, y, en general, para que se estableciera un régimen más integral del dato personal. Fue así como se aprobó la Ley 1581 de 2012.

Infelizmente, y a pesar de avances en otros campos, en materia de conceptualización la Ley 1581 de 2012 volvió a definir el dato personal y lo hizo en términos muy similares a su antecesora. Lo anterior, pues consideró que a esta noción correspondía cualquier información vinculada o que pudiera asociarse a una o varias personas naturales determinadas o determinables. El gran avance de esta norma posterior en el punto es haber hecho énfasis en que se trata de información relacionada con una

persona natural y no jurídica, tal y como aclaró la Corte Constitucional en su examen de constitucionalidad.

Pero no nos quedemos solo con el concepto legal y pasemos a su caracterización. Según la sentencia T-729 de 2002, las características del dato personal son: a) se refiere a aspectos propios y exclusivos de una persona natural; b) ayuda a identificar a una persona en mayor o menor medida; c) su propiedad reside permanentemente en cabeza del titular del mismo; d) su tratamiento está sometido a principios en cuanto a su captación, administración y divulgación.¹⁶ Podríamos entonces decir que los datos sirven para identificar a las personas, armar sus perfiles, definirlos y luego, indirectamente, esta identificación puede usarse en beneficio o en detrimento de los titulares, y por esto les incumbe y atañe todo lo que se haga con la información que resulta de su propiedad.

A título ilustrativo en materia de datos personales protegidos, podemos traer a colación el listado de datos personales considerados como tales por los *Lineamientos generales para la clasificación y desclasificación de la información de las dependencias y entidades de la Administración Pública Federal de México*. Dicho documento, en su artículo 32, elabora una lista de información de la persona física identificada o identificable que es considerada confidencial. Con una rápida lectura a dicho listado podremos tener algunas luces sobre lo que se debe incluir en el concepto de datos personales: origen étnico o racial; características físicas, morales y emocionales; vida afectiva; vida familiar; domicilio particular; número telefónico particular; patrimonio; ideología; opinión política; creencia o convicción religiosa; creencia o convicción filosófica; estado de salud física; estado de salud mental; preferencia sexual, y otras análogas que afecten su intimidad, como la información genética.¹⁷

Por su parte, la Ley 1712 de 2014 no define el dato personal pero conceptualiza el derecho de acceso a la información pública en su artículo cuarto, así: “En ejercicio del derecho fundamental de acceso a la información, toda persona puede conocer sobre la existencia y acceder a la información pública en posesión o bajo control de los sujetos obligados”. Este derecho solo podrá ser restringido excepcionalmente y genera la obligación correlativa de divulgar de forma proactiva la información y

¹⁴ Corte Constitucional, sentencia C-748 de 2011, M. P. Jorge Pretelt Chaljub.

¹⁵ En la sentencia de la Corte Constitucional C-1011 de 2008, se aclara que los datos, al menos los económicos en los que se especializa la ley de *habeas data* sectorial, son predicables de personas naturales y jurídicas. Así dice la Corte cuando declara la exequibilidad del artículo 3-a que define el titular de la información: “Sobre el particular, basta señalar que la condición de titular de información es predicable tanto de las personas naturales como jurídicas, en la medida en que las dos son susceptibles de producir información que puede ser recolectada por las bases de datos, lo que impone el deber de otorgar un nivel de protección suficiente y adecuado a esa información personal”. Sin embargo, en la sentencia C-748 de 2011, que estudia la constitucionalidad de la ley de *habeas data* posterior o general, se aclara que el titular solo es la persona natural.

¹⁶ Corte Constitucional, sentencia T-729 de 2002, M. P. Eduardo Montealegre Lynett.

¹⁷ <http://www.conafor.gob.mx:8080/documentos/ver.aspx?articulo=4855&grupo=8> (Consultado el 13 de junio de 2014).

responder de buena fe, de manera adecuada, veraz, oportuna y accesible a las solicitudes.

La Ley TAIP también definió la información pública clasificada en su artículo sexto:

Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal,¹⁸ pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de esta ley.

De manera que si el conjunto de datos cumple con los requisitos del artículo 18, no habrá acceso por tratarse de información pública clasificada. Así también lo entendió la sentencia de constitucionalidad de la Ley TAIP cuando, en respuesta a la petición de la Superintendencia de Industria y Comercio de crear una excepción especial para los datos personales, le indicó que dichos datos formaban parte del concepto amplio de la intimidad cobijado en el mencionado artículo 18.¹⁹

18 Los sujetos obligados están definidos por el artículo 5 de la Ley 1712 de 2014 que, dentro de su ámbito de aplicación, incluye: a) toda entidad pública, incluyendo las pertenecientes a todas las ramas del poder público, en todos los niveles de la estructura estatal, central o descentralizada por servicios o territorialmente, en los órdenes nacional departamental, municipal o distrital; b) los órganos, organismos y entidades estatales independientes o autónomos y de control; c) las personas naturales y jurídicas, públicas o privadas, que presten función pública, que presten servicios públicos respecto de la información directamente relacionada con la prestación del servicio público; d) cualquier persona natural o jurídica o dependencia de persona jurídica que desempeñe función pública o de autoridad pública, respecto de la información directamente relacionada con el desempeño de su función; e) las empresas públicas creadas por ley, las empresas del Estado y sociedades en que este tenga participación (en el entendido de que las personas obligadas en relación con su actividad propia no están sujetas al deber de información con respecto a dicha actividad); f) los partidos o movimientos políticos y los grupos significativos de ciudadanos, y g) las entidades que administren instituciones parafiscales, fondos o recursos de naturaleza u origen público, pero si estas últimas no cumplen los otros requisitos solo estarán obligadas respecto de aquella información que se produzca en relación con fondos públicos territoriales o nacionales que reciban o intermedien.

19 Corte Constitucional, sentencia C-274 de 2013, M. P. María Victoria Calle.

Una vez definidos los conceptos, pasemos al recuento de las varias clasificaciones que nuestra legislación hace de los datos, para poder así determinar qué criterios son aplicables en la tensión entre lo público y lo privado que se esconde detrás de nuestro objeto de estudio.

Clasificaciones de datos personales y de información pública

La Ley 1266 de 2008, o Ley de *habeas data* sectorial, clasifica los datos personales según el interés que se pueda tener en ellos. Esta división le otorga el carácter de privado al dato que “por su naturaleza íntima o reservada solo es relevante para el titular”. El dato semiprivado atañe no solo al dueño o titular del dato, sino también a un sector o grupo de personas, como es el caso del dato financiero y crediticio. Finalmente, el dato público es calificado como tal ya sea por la ley o la Constitución Política, o por exclusión al no pertenecer a ninguna de las categorías anteriores. El ejemplo por excelencia del dato personal público es el estado civil. También lo son aquellos datos contenidos en documentos públicos que no estén sometidos a reserva.²⁰

Esta tipología se asimila a una clasificación hecha por la sentencia T-729 de 2002 de la Corte Constitucional, “dirigida a clasificar la información desde un punto de vista cualitativo en función de su publicidad y la posibilidad legal de obtener acceso a la misma”, logrando cuatro grandes tipos cuyo acceso puede ser directo por parte de la ciudadanía o mediante autorización administrativa o judicial: la información pública o de dominio público, la información semiprivada, la información privada y la información reservada o secreta.²¹

20 Artículo 3, Ley 1266 de 2008.

21 La sentencia T-727 de 2002, con ponencia de Eduardo Montealegre Lynett, establece lo siguiente: Así, la información pública será, según la Corte, calificada como tal por ley o la Constitución y puede ser “obtenida y ofrecida sin reserva alguna y sin importar si la misma sea información general, privada o personal. La información semiprivada será aquella que por versar sobre información personal o impersonal y no estar comprendida por la regla general anterior, presenta para su acceso y conocimiento un grado mínimo de limitación, de tal forma que la misma solo puede ser obtenida y ofrecida por orden de autoridad administrativa en el cumplimiento de sus funciones o en el marco de los principios de la administración de datos personales. Es el caso de los datos relativos a las relaciones con las entidades de la seguridad social o de los datos relativos al comportamiento financiero de las personas. [...] La información privada

La conjugación de lo establecido por la norma legal y la jurisprudencia produce una tipología valiosa porque contribuye, aunque parcialmente, a resolver la tensión entre el acceso a la información pública y el *habeas data*, y porque ayuda a identificar a las personas y autoridades que se encuentran legitimadas para acceder o divulgar dicha información.

Una segunda clasificación de datos personales, que obedece esta vez a la sensibilidad del dato o al riesgo que representa para el titular del mismo, resulta de la interpretación del artículo quinto de la Ley 1581 de 2012 o Ley estatutaria de datos personales. Son entonces datos sensibles aquellos que: i) afectan la intimidad del titular o ii) podrían afectar el derecho a la igualdad o su colección genera una propensión a la discriminación. La intimidad ya la hemos desarrollado previamente por lo que no nos detendremos en ella ahora, pero la propensión a la discriminación consiste en datos cuyo

...uso indebido puede generar su discriminación, como sería el caso en el que se coleccionen datos sobre el origen racial o étnico, la organización política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promuevan intereses de cualquier partido político o que garanticen los derechos y garantía de partidos políticos de oposición así como los datos relativos a la salud, la vida sexual y los datos biométricos.²²

Este listado no es taxativo, sino más bien cambiante dependiendo de los tiempos.

será aquella que por versar sobre información personal o no, y que por encontrarse en un ámbito privado, solo puede ser obtenida y ofrecida por orden de autoridad judicial en el cumplimiento de sus funciones (v. gr. libros de los comerciantes, de los documentos privados, de las historias clínicas o de la información extraída a partir de la inspección del domicilio). [...] Finalmente, encontramos la información reservada, que por versar igualmente sobre información personal y sobre todo por su estrecha relación con los derechos fundamentales del titular—dignidad, intimidad y libertad—se encuentra reservada a su órbita exclusiva y no puede siquiera ser obtenida ni ofrecida por autoridad judicial en el cumplimiento de sus funciones. Cabría mencionar aquí la información genética, y los llamados ‘datos sensibles’ o relacionados con la ideología, la inclinación sexual, los hábitos de la persona, etc.”.

22 Corte Constitucional, sentencia C-748 de 2011, M. P. Jorge Ignacio Pretelt Chaljub.

Esta segunda clasificación se pudo haber derivado de otra tipología que hiciera la Corte Constitucional en la recién mencionada sentencia T-729 de 2002. En esa ocasión, la Corte atendió a la especialidad del régimen aplicable y dividió entre información personal e impersonal, justificando la importancia de la tipología por tres razones:

...la primera, es la que permite afirmar que en el caso de la información impersonal no existe un límite constitucional fuerte²³ al derecho a la información, sobre todo teniendo en cuenta la expresa prohibición constitucional de la censura (art. 20 inciso 2º), sumada en algunos casos a los principios de publicidad, transparencia y eficiencia en lo relativo al funcionamiento de la administración pública (art. 209) o de la administración de justicia (art. 228). Una segunda razón, está asociada con la reconocida diferencia entre los derechos a la intimidad, al buen nombre y al *habeas data*, lo cual implica reconocer igualmente las diferencias entre su relación con la llamada información personal y su posible colisión con el derecho a la información. La tercera razón, guarda relación con el régimen jurídico aplicable a los llamados procesos de administración de datos inspirado por principios especiales y en el cual opera, con sus particularidades, el derecho al *habeas data*.

Una tercera clasificación resulta del numeral segundo del artículo 3 del Decreto 1377 de 2013, que reglamenta parcialmente la Ley 1581 de 2012, y que en cierta medida retoma la primera clasificación de la ley de *habeas data* sectorial. En dicha norma se define el dato personal público como aquel que no es semiprivado, privado ni sensible, y que por su naturaleza puede estar contenido en registros o documentos públicos, gacetas y boletines oficiales, y sentencias judiciales. Se incluye entonces un listado a título ilustrativo de datos que tienen esta condición, tales como aquellos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. No se menciona en la norma si el dato público es personal o impersonal, pero siendo el Decreto 1377 de 2013, reglamentario de la Ley 1581 de 2012 sobre protección de datos personales, suponemos que es lógico que se esté refiriendo al dato personal público. En otras normas, y sin mencionar que se trata de dato privado, sino más bien de un dato reservado o protegido, existe informa-

23 La sentencia citada cita a su vez la sentencia T-414 de 1992.

ción personal con tendencia fuerte a no ser compartida con la ciudadanía. Este es el caso de los datos en el registro único de víctimas (art. 29 Ley 1448 de 2011), la información tributaria (art. 583 Estatuto Tributario), los datos de personas acogidas al programa de protección de testigos, víctimas e intervinientes en el proceso penal (art. 5, Decreto 1843 de 1992), la información registrada bajo reserva bancaria, los libros y papeles del comerciante (arts. 61 a 62 del Código de Comercio), los registros de la Registraduría sobre la identidad de las personas como sus datos biográficos, su filiación y fórmula dactiloscópica (art. 51, Ley 96 de 1985) y la información de los suscriptores de un proceso de firma digital (art. 25, Decreto 1740 de 2000).

Respecto de la tercera clasificación, es importante tener en cuenta que cuando el dato es público, no hay objeción alguna para su divulgación. Pero esta situación se presenta solo cuando hay claridad absoluta sobre la publicidad del dato y, como la definición del dato público a su vez depende de la de los datos privados y semiprivados, con frecuencia habrá dudas. Por el momento, la pertenencia a los ejemplos de datos públicos que trae la ley ya es un indicador claro del triunfo del derecho de acceso a la información pública en tensión con el *habeas data*. Así, se define primero qué dato es público y qué dato no lo es. Si el dato no pertenece a los ejemplos de datos públicos, se agudiza la necesidad de ponderación y es necesario buscar criterios para balancear los dos valores en conflicto y la autorización, para luego resolver la tensión a favor del acceso a la información pública si hay autorización del titular. Dicha autorización debe ser expresa e inequívoca, pues la naturaleza privada de un dato no se pierde por el solo hecho de haber sido publicado o ser de fácil acceso en Internet u otros medios generales.²⁴ Además, se podrán hacer públicos los datos si su divulgación se requiere para salvaguardar el interés vital del titular en incapacidad de decidir, pero con autorización de su representante legal; se requieren dichos datos para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial, o cuando tenga finalidad histórica, estadística o científica con supresión de la identificación de los titulares.²⁵

²⁴ Corte Constitucional, sentencia C-748 de 2011, M. P. Jorge Ignacio Pretelt Chaljub, que declaró inexecutable el aparte del artículo 6, literal d) de la Ley 1581 de 2012, según el cual era posible tratamiento de datos sensibles cuando su titular los había hecho manifiestamente públicos.

²⁵ Artículo 6, Ley 1581 de 2012.

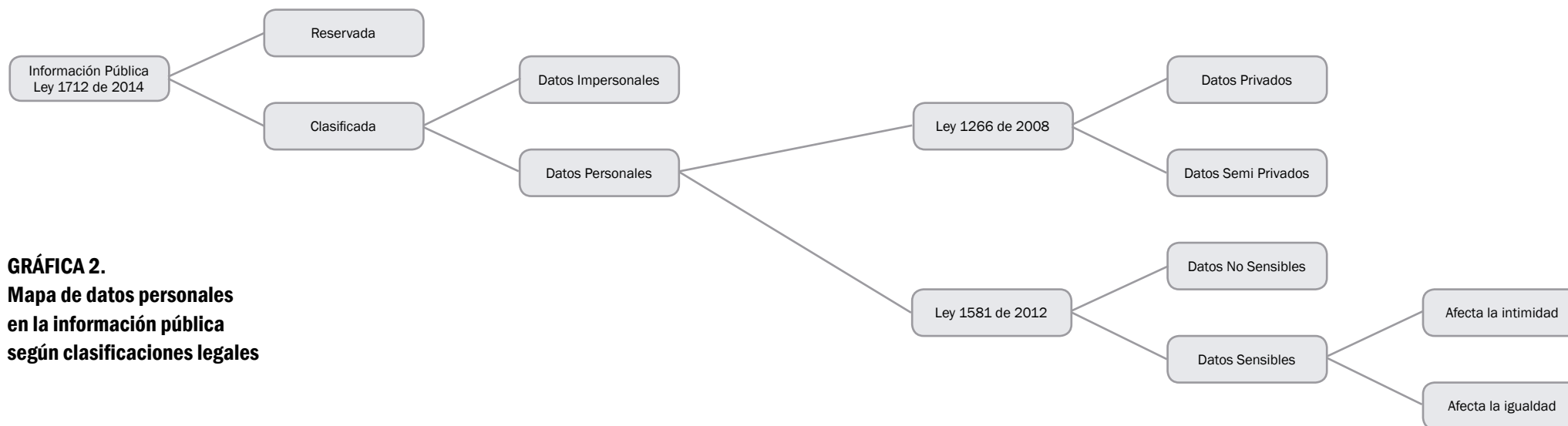
La cuarta y última clasificación que importa para el presente estudio es la que ofrece la Ley 1712 de 2014. Esta norma estatutaria define información pública como el conjunto organizado de datos contenido en cualquier documento que se encuentre bajo control de los sujetos obligados y la divide en pública clasificada y pública reservada. La primera pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica, y la segunda pertenece al ámbito público pero no está permitido divulgarla por las siguientes razones de interés público: defensa y seguridad nacional, seguridad pública, relaciones internacionales, salud pública, estabilidad macroeconómica y financiera nacional, derechos de la infancia y la adolescencia, debido proceso e igualdad de las partes, y prevención, investigación y persecución de los delitos y faltas disciplinarias. Si la información pública, es decir, si el conjunto de datos bajo control de un sujeto obligado incluye datos privados, semiprivados o personales a los que se refieren los dos párrafos anteriores, quedaría, *prima facie*, clasificada.²⁶

La gráfica 2 permite conjugar las diversas clasificaciones legales de datos personales en la información pública.

Al analizar las clasificaciones arriba mencionadas, encontramos que: i) definitivamente hay tensión frente a la protección y la divulgación de datos personales en información pública, pero con tendencia a la protección de todos los datos personales privados, semiprivados y sensibles; (ii) los datos sensibles están protegidos bajo el principio de confidencialidad y solo podría accederse a ellos previa autorización de su titular o en las circunstancias previstas por el artículo 6 de la Ley 1581 de 2012;²⁷ iii)

²⁶ Corte Constitucional, Sentencia C-274 de 2013, M. P. María Victoria Calle, al analizar la exequibilidad del artículo 6 de la Ley 1712 de 2014, considera que estos datos serían clasificados porque “su difusión afecta gravemente el derecho a la intimidad de las personas”.

²⁷ El artículo 6 de la Ley 1581 de 2012 impide que los datos personales sensibles puedan ser divulgados sin autorización de su titular, salvo que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial, y en este caso solo serán divulgados para que se integren al expediente de dicho proceso judicial; o cuando tengan una finalidad histórica, estadística o científica, caso este último en el cual deberán adoptarse las medidas conducentes a la supresión de identidad de los titulares. Tampoco podrán ser divulgados los datos personales sensibles de niños y adolescentes, salvo aquellos que sean de naturaleza pública, de acuerdo con lo previsto en el artículo 7° —Derechos de los niños, niñas y adolescentes— de la Ley 1581 de 2012.



GRÁFICA 2.
Mapa de datos personales
en la información pública
según clasificaciones legales

la primera y la tercera clasificación podrían fusionarse en una sola, en la cual la tensión entre la protección de datos personales y el acceso a la información pública se presentaría en los datos personales privados, y, en ocasiones, en los datos semiprivados; iv) la cuarta clasificación es indicativa de la tensión y de las excepciones establecidas para lidiar con ella, pero para mantener un adecuado equilibrio de derechos fundamentales y bienes constitucionales su aplicación debe conjugarse con otras normas existentes que contienen las otras clasificaciones, fundamentadas en la

protección de otros intereses, así como con la aplicación del test de daño consagrado en la Ley TAIP.

Para tender al anterior equilibrio de derechos fundamentales y bienes constitucionales en juego debemos estudiar algunos criterios útiles al abordar tensiones en los datos privados involucrados con la información pública, criterios derivados del precedente jurisprudencial y de la propia normativa.

CAPÍTULO II.

GUÍA DE ARMONIZACIÓN FRENTE A LA TENSIÓN ENTRE LOS DATOS PERSONALES Y EL DERECHO DE ACCESO A LA INFORMACIÓN PÚBLICA

Frente a la tensión entre el derecho a la intimidad/autodeterminación informática y el derecho a la información, a lo largo de sus primeros casi veinticinco años de jurisprudencia, la Corte ha oscilado en otorgar el énfasis entre uno y otro derecho fundamental sin que finalmente se pueda afirmar el carácter absoluto de ninguno. Juan Carlos Upegui Mejía, en su texto sobre el *habeas data*, resume y sistematiza las diversas posiciones en cuatro tesis (2008:130 y ss.) que acogemos y nos permitimos resumir a continuación:

1. La de la prevalencia, que otorga prioridad al derecho a la intimidad “como consecuencia necesaria de la consagración de la dignidad humana como principio fundamental y valor esencial” del Estado social de derecho,¹ y que fue paulatinamente abandonada y solo retomada de manera aislada por la Corte.²
2. La del equilibrio, armonización o ponderación mediante el *habeas data*, según la cual lo que realmente se valora son los intereses que obedecen a la finalidad de cada derecho en el caso específico, rodeado de reglas concretas propias de los datos personales que finalmente fueron recogidas en dos leyes estatutarias actualmente vigentes.³

¹ Corte Constitucional, sentencia T-414 de 1992, M. P. Ciro Angarita Varón.

² Corte Constitucional, sentencia C-877 de 2005, M. P. Jaime Córdoba Triviño.

³ Corte Constitucional, sentencias T-022 de 1993, M. P. Ciro Angarita Barón

3. La de la ponderación mediante el juicio de proporcionalidad que somete el análisis a los principios de idoneidad (medida adecuada para obtener el fin), de necesidad (si todas las medidas son idóneas, debe ser la más benigna posible al fin buscado), finalidad (que busque la garantía de bienes o derechos constitucionales) y proporcionalidad estricta (que su divulgación no suponga un sacrificio de valores constitucionales mayor al que implica conservarla o viceversa).⁴
4. La de los límites de los derechos en juego, que supone que los contornos o los ámbitos de los derechos, o incluso las clases de información involucrada en los derechos como privada, semiprivada y pública, nos permitirán resolver la tensión.⁵

Las dos primeras tesis parecen haber sido fruto de momentos históricos superados, ya sea por una interpretación reconocedora de la integralidad y la interdependencia de los derechos, o por legislación compiladora. En cambio, las dos últimas tesis se siguen encontrando en la jurisprudencia como justificación de las decisiones en los respectivos casos, aunque sin olvidar algunos elementos, en especial de la segunda.

Recientemente, la declaratoria de constitucionalidad, que dio paso a la sanción y vigencia de la Ley 1712 de 2014 sobre transparencia y acceso a la información pública, arroja algunas luces al respecto que nos permitiremos recoger seguidamente en una suerte de guía que conjuga las tesis 3) y 4) que consideramos aún vigentes.

Carga de la prueba

Cuando un ciudadano pretenda conocer información pública y un sujeto obligado retenerla, por considerarla reservada o confidencial (clasificada), es el sujeto obligado quien debe justificar su posición debidamente, pues el artículo 28 de la Ley TAIP invierte la carga de la prueba. En este caso, el sujeto obligado debe, por escrito,⁶ “aportar las razones y pruebas que fundamenten y evidencien” por qué la información no debe divulgarse.

y SU-082 de 1995, M. P. Jorge Arango Mejía.

4 Corte Constitucional, sentencias C-1147 de 2001 y C-872 de 2003, M. P. Clara Inés Vargas.

5 Corte Constitucional, sentencias C-691 de 2003, M. P. Clara Inés Vargas y T-846 de 2004, M. P. Alfredo Beltrán Vargas.

6 Artículo 18, Ley 1712 de 2014 y título IV, artículo 24 y siguientes del Decreto Reglamentario 103 de enero 20 de 2015 por el cual se reglamenta

Los argumentos que justifiquen la protección de la información deberán a su vez, siguiendo las palabras de la Corte al examinar la constitucionalidad de este artículo, demostrar “que su decisión no es acto arbitrario, sino el resultado de una decisión administrativa legítima, responsable, juiciosa y respetuosa de los derechos ciudadanos y acorde con los deberes que tienen los servidores públicos”.⁷ Además, en conjunción con el propio análisis que hace la Corte de la definición de información pública clasificada y de documento en construcción en la Ley TAIP, así como del funcionamiento en general de las excepciones, quien niega acceso a información debe sujetarse a los principios de razonabilidad y proporcionalidad que recogen, en parte, la tesis de la ponderación recogida por Upegui y enunciada previamente. Así, habrá que dar cuenta de que se emplee la medida más adecuada posible y menos dañina al interés público de la transparencia y los valores constitucionales que conlleva.⁸ Además, en caso de existir pruebas, estas se deben aportar para demostrar que el beneficio obtenido con la retención de información pública clasificada es mayor a la lesión causada al derecho de acceso a la información pública.

Pero no bastará una justificación abstracta de razones y proporciones. Se requiere, según el mismo artículo 28, una demostración concreta de que se cumplen las siguientes condiciones:⁹ 1) demostrar que la in-

la Ley 1712 de 2014 y se dictan otras disposiciones.

7 Corte Constitucional, sentencia C-274 de 2013, acápite 3.2.29, M. P. María Victoria Calle.

8 Y desde el ángulo del *habeas data*, la sentencia C-1011 de 2008 lo corrobora cuando examina el artículo segundo de la ley de *habeas data* sectorial con mucho cuidado para no afectar el principio general de publicidad de las actuaciones del Estado y el ejercicio del derecho a la información. La Corte asevera que el establecimiento de excepciones a ese principio de publicidad no debe afectar las garantías del derecho a la información, “por lo que solo serán oponibles aquellos modos de reserva o confidencialidad que i) tengan carácter excepcional y respondan a un criterio de proporcionalidad y razonabilidad; ii) estén expresamente previstas por el legislador; y iii) respondan a fines constitucionalmente legítimos, en especial la protección del derecho a la intimidad del sujeto concernido, cuando se trate de información personal de carácter privado que, según lo expuesto en esta sentencia, no tiene vocación de circulación, habida cuenta su vínculo inescindible con la órbita íntima y familiar del individuo”. Por último, la Corte asegura que la consagración de excepciones al principio de publicidad de las actuaciones del Estado, no lleva de suyo el desconocimiento del derecho al *habeas data*.

9 Ver artículo 28 de la Ley 1712 de 2014: “Carga de la prueba. Le corresponde al sujeto obligado aportar las razones y pruebas que fundamenten

formación debe relacionarse con un objetivo legítimo establecido legal o constitucionalmente; 2) indicar cómo el interés o bien que se pretende proteger está catalogado en calidad de excepción en los artículos 18 o 19 de la Ley de transparencia y acceso a la información, y 3) evidenciar que la revelación de la información causaría un daño presente, probable y específico que excede el interés público que representa el acceso a la información.¹⁰ Estos tres elementos, que adicionalmente se consagran en el artículo 33 del Decreto Reglamentario 103 del 20 de enero de 2015, “son compatibles con la protección constitucional que en nuestro ordenamiento tiene el derecho fundamental a acceder a la información pública”,¹¹ y garantizan un examen ponderado para resolver la tensión de derechos y bienes protegidos que se presentan en estas circunstancias.

Pues bien, como primera medición, siendo los datos personales un objetivo legítimo consagrado de manera expresa en el artículo 15 de la Constitución Política, consideramos cumplida la primera condición de la valoración que debe realizar todo encargado de resolver una tensión entre el *habeas data* y el acceso a la información pública para lograr proteger datos. Además, la propia Corte ha dicho que cuando “se trata de excepciones al principio de publicidad, la posibilidad de establecer una reserva depende no solo de que una ley consagre esta opción de manera general sino que precise qué información es la que goza de este tratamiento excepcional”.

y evidencien que la información solicitada debe permanecer reservada o confidencial. En particular, el sujeto obligado debe demostrar que la información debe relacionarse con un objetivo legítimo establecido legal o constitucionalmente. Además, deberá establecer si se trata de una excepción contenida en los artículos 19 y 20 [sic deberían ser 18 y 19] de esta ley y si la revelación de la información causaría un daño presente, probable y específico que excede el interés público que representa el acceso a la información”.

10 Las excepciones, según la Relatora Especial para la Libertad de Expresión, Catalina Botero, en el *Informe de la Oficina del Relator Especial para la Libertad de Información*, OEA/Ser. L/V/II.134 Doc. 5, aprobado por la Comisión Interamericana de Derechos Humanos el 25 de febrero de 2009, deben pasar una prueba de tres partes: a) estar relacionada con uno de los objetivos legítimos que la justifican; b) demostrarse que la divulgación de la información efectivamente amenaza causar un perjuicio sustancial a ese objetivo legítimo; y c) demostrarse que el perjuicio al objetivo es mayor que el interés público en contar con la información.

11 Corte Constitucional, sentencia C-274 de 2013, acápite 3.2.29, M. P. María Victoria Calle.

Considerando esto último, es necesario mencionar que hay dos normas estatutarias que protegen los datos privados, semiprivados y sensibles, así:

- a) La Ley 1266 de 2008 protege la circulación de los datos privados y semiprivados pues en su artículo 3, literales g) y h), define el dato privado como el que solo es relevante para el titular, y el semiprivado como aquel que solo interesa a un sector o grupo de personas o a la sociedad en general sin ser público; en su artículo 4 literal c) consagra el principio de circulación restringida que sujeta la administración a la naturaleza de los datos, de lo cual se desprende que los datos privados y semiprivados no tienen circulación pública como regla general.¹²
- b) La Ley 1581 de 2013, en su artículo 4, consagra el principio de libertad (literal c), el principio de acceso y circulación restringida (literal f) y el principio de confidencialidad (literal h), los cuales definen que los datos personales que no son públicos, deben ser protegidos del acceso público, salvo autorización del titular. Se añade la definición de datos sensibles del artículo 5 que ya hemos comentado y que también se encuentra en el artículo 3 del decreto 1377 de 2013, el refuerzo de la prohibición expresa del tratamiento de datos sensibles establecida en el artículo 6 de la misma ley que corrobora la negativa del acceso público para los datos personales que posean esta calidad, y la prohibición expresa de tratar los datos personales de niños, niñas y adolescentes del artículo 7.

Finalmente, en el cumplimiento de esta condición habrá que tener en cuenta que hay normas especiales que protegen datos personales como pueden ser los casos de las bases de datos de la ley de inteligencia y contra-inteligencia (Ley 1621 de 2013) y de censos de población y vivienda (Ley 79 de 1993); el registro único de víctimas (art. 29, Ley 1448 de 2011); la información tributaria (art. 583 Estatuto Tributario); los datos de personas acogidas al programa de protección de testigos, víctimas e intervi-

12 El párrafo del artículo 4, literal c de la Ley 1266 de 2008, dice lo siguiente: “Los datos personales, salvo la información pública, no podrán ser accesibles por Internet o por otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido solo a los titulares o los usuarios autorizados conforme a la presente ley”.

nientes en el proceso penal (art. 5, Decreto 1843 de 1992); los registros de la Registraduría sobre la identidad de las personas, tales como sus datos biográficos, su filiación y fórmula dactiloscópica (art. 51, Ley 96 de 1985), y la información de los suscriptores de un proceso de firma digital (art. 25, Decreto 1740 de 2000). Aunque también habrá que considerar que los principios sobre protección de datos, como la legalidad, la transparencia, la seguridad, la confidencialidad y la calidad son aplicables a todas las bases de datos incluidas las exceptuadas en la Ley 1581 de 2012 y para los datos que tengan naturaleza especial se aplicarán de forma concurrente.¹³ Para un análisis no exhaustivo de bases de datos mencionadas en las leyes de protección de datos personales, hemos incluido un anexo de selección de ley aplicable al caso, que puede constituir una guía.

Para cumplir con la segunda condición, debemos evaluar si los datos personales constituyen una excepción a la Ley TAIP. Para el efecto, consideramos que siendo el *habeas data* en sus orígenes parte del derecho a la intimidad, y después un derecho independiente, pero relacionado al fin y al cabo, es lógico pensar que los datos personales forman parte de las excepciones al acceso a la información consagradas en el artículo 18, literal a) de la Ley de transparencia y acceso a la información pública. Así lo consideró la Corte Constitucional al examinar la constitucionalidad de la Ley TAIP y estimar que no era necesario otorgar una categoría especial de reserva legal a los datos personales pues los datos sensibles afectan “el derecho a la intimidad y otros derechos fundamentales que pueden ser reservas al derecho de acceso a la información pública, y que resultan compatibles con las reglas específicas que fijará este proyecto de ley estatutaria una vez sea sancionado”.¹⁴ De manera que se puede considerar cumplida

¹³ Artículo 2, parágrafo Ley 1581 de 2012.

¹⁴ Nótese que la Corte hace referencia a los “datos sensibles” y no a todos los datos personales. Corte Constitucional, sentencia C-274/13, numeral 3.2.5, examen de constitucionalidad del artículo 5 de la Ley 1712 de 2014, M. P. María Victoria Calle. Es pertinente recordar, como ya mencionamos previamente, que la Superintendencia de Industria y Comercio, encargada de la protección del dato personal intervino en la revisión de constitucionalidad de la ley TAIP. En su escrito, dicha entidad pública solicitó que mediante un fallo modulado se incluyera como excepción al acceso a información pública, toda la información protegida por la Ley 1581 de 2012 sobre datos personales. Sin embargo, la Corte Constitucional consideró que la regulación de la ley en estudio era suficiente para exceptuar esta información consignada en una ley precisa y de carácter estatutaria y desestimó la petición por innecesaria.

Tabla de preguntas básicas para clasificar datos personales en información pública

Pregunta	Respuesta
¿Es un objetivo legítimo establecido de forma precisa por la Constitución o por la ley?	Si se trata de datos privados, semi-privados o sensibles es un objetivo legítimo establecido en artículo 15 de la Constitución, Ley 1266 de 2008, artículos 3 g y h y 4 c, y Ley 1581 de 2012, artículos 4 c, f, h. Además, pueden existir normas especiales aplicables a ciertas bases de datos.
¿Se trata de una excepción contenida en los artículos 18 o 19 de la Ley TAIP?	Si se trata de datos privados, semi-privados o sensibles, es una excepción contenida en el artículo 18 de la Ley TAIP y confirmada, al menos para datos sensibles, por la sentencia C-274 de 2013, numerales 3.2.5 y 3.2.6.
¿Cumple con el test de daño presente, probable y específico?	Acudir según cada caso a los criterios de armonización de conceptos y principios, esferas de la intimidad y enfoque dual.

la segunda condición respecto de los datos sensibles, al tiempo que se desprende una tendencia de protección de los datos personales en general.

Por último, nos quedaría analizar si la revelación de la información causaría un daño presente, probable y específico que exceda el interés público representado en el acceso a la información. Habría entonces, y luego de analizar la tabla que recoge este apartado en conjugación con el Capítulo IV del Decreto 103 del 20 de enero de 2015, que aplicar el test de daño sustancial o test de interés público bajo el cual no basta para exceptuar del acceso que la información se encuentre protegida por una norma sobre un tema predeterminado, sino que se requiere adicionalmente que la revelación de la información pueda generar daño claro y probable, es decir, concreto y no remoto, que exceda el interés público que representa el acceso a la información.

Test de daño

El test de daño presente, probable y específico, es equivalente al test conocido en la doctrina como de daño al interés público. Según la Relatoría para la Libertad de Expresión del sistema interamericano, al aplicar la prueba de daño al interés público, “debe elegirse la opción de excepción que menos restrinja el derecho de acceso a la información pública”. La excepción, atendiendo a nuestra jurisprudencia, debe entonces: i) ser adecuada para el logro del objetivo; ii) ser proporcionada para el interés que

la justifica, y iii) interferir lo menos posible con el derecho de acceso a la información. Si luego de hecho el test se concluye que el interés público exige la revelación de los datos personales, y que no revelarlos causaría más daño que el que se genera al no protegerlos, se deberán divulgar.

Para poder desarrollar mejor el test de daño —que en todo caso forma parte de la carga de la prueba— acudiremos a continuación a diferentes criterios que ayudarán al encargado a dilucidar la manera equilibrada, necesaria y legítima de proteger al máximo ambos derechos, y, en últimas, a resolver proporcionadamente el camino que se debe seguir. Comenzaremos por sugerir una armonización de conceptos y principios, en consonancia con la tesis de la ponderación recogida por Upegui en el capítulo anterior; luego ofreceremos la perspectiva de diferentes esferas de la intimidad que atiende a la tesis de los límites también mencionada previamente; por último, propondremos el enfoque dual, cuando se trate de información de funcionarios públicos que sea de interés público.

Armonización

El artículo 1 de la Ley 1581 de 2012 regula el ámbito de aplicación de esta ley de datos personales que conjuga el *habeas data* del artículo 15 y el derecho de acceso a la información del artículo 20, ambos de la Constitución Política. Pero como la intimidad y la autodeterminación de los datos personales buscan la reserva, y el derecho de acceso a la información pública pretende todo lo contrario, debemos intentar armonizar los principios que rigen cada extremo para así guiar a quien tiene que decidir si divulga o si protege un dato personal contenido en información pública. Para hacerlo, previa una armonización de conceptos, haremos una breve mención de los principios básicos de ambos derechos para luego seleccionar los principios más relevantes y concentrarnos en una posible fórmula que contribuya a resolver la tensión.

Armonización de conceptos

La dificultad se presenta de manera pronunciada cuando el dato personal, que debe ser protegido, considerado confidencial y condicionado a una autorización del titular, se encuentra presente o forma parte de información pública. A su vez, la colisión se presenta por la necesidad de aplicar el principio de máxima divulgación o máxima publicidad que se halla inmerso en la esencia del derecho de acceso a la información pública, según el cual es público todo lo que no cumple con unos requisitos específicos;

mientras que en la protección del dato personal impera el adagio según el cual es privado y secreto todo lo que no es designado como público por su naturaleza o por designación legal.

Para intentar armonizar esta tensión, que es la nuez del problema, debemos partir de la definición de dato público que, según el artículo 3 f de la Ley 1266 de 2008, es “el dato calificado como tal según los mandatos de la ley o de la Constitución Política y todos aquellos que no sean semi-privados o privados, de conformidad con la presente ley”.

De la anterior definición se desprende que es la ley la que debe determinar cuándo un dato personal de carácter financiero, crediticio, comercial, de servicios o proveniente de terceros países es público. Esta primera interpretación enfrenta el dato personal dinerario al principio de máxima divulgación y pareciera darle una primera victoria al *habeas data*. Pero para complementar su lectura, se debe añadir el segundo aparte de la definición que aclara que dato personal público es todo aquel que no sea ni privado ni semiprivado. En el análisis de la constitucionalidad de este segundo aparte, la Procuraduría General de la Nación intervino alegando que se establecía una especie de presunción de dato público, lo que daría al traste con la intimidad y el *habeas data*.

En respuesta, la Corte Constitucional acepta que podría en principio haber confusión, pero acude a una interpretación sistemática de dato público, privado y semiprivado, pues las definiciones existentes en los literales correspondientes a los dos últimos conceptos son suficientemente claras y no se pueden desconocer para llegar también a la definición del primero.¹⁵ Se concluye, entonces, que el dato público no se presume

15 Corte Constitucional, sentencia C-1011 de 2008: “...la Corte considera que aunque la redacción del literal f) pudiera ofrecer confusión, su interpretación concreta se logra a partir del análisis de los literales g) y h). En efecto, estas previsiones definen adecuadamente los datos privados y semiprivados, distinguiéndolos del dato público en razón al mayor o menor nivel de interés para el titular que tenga la información en ellos contenida. Así las cosas, la previsión del legislador estatutario de considerar como datos públicos “todos aquellos que no sean semiprivados o privados” es inane, en la medida en que la misma norma se encarga de establecer qué datos pertenecen a esas categorías y, a su vez, las definiciones propuestas delimitan suficientemente el espectro material en el que son aplicables. Por ende, no es posible concluir que la citada expresión del literal f) permita la adscripción indiscriminada de datos personales a la condición de públicos, puesto que las definiciones de datos semiprivados y privados son igualmente amplias, de modo tal que no resulta viable sostener una interpretación que permita que un dato personal vinculado al contenido

y que para llegar a su definición —que en este caso es solo aplicable como la generalidad de la ley al dato personal dinerario y económico— habría que descartar la presencia de dato privado y semiprivado, que a su vez responden al interés exclusivo de su titular en el primer caso, y a un grupo específico en el segundo. Como la propia ley sectorial define la información dineraria y económica como semiprivada, no gozará entonces de las características de información pública, necesarias para que haya acceso general inmediato de la ciudadanía a ella.

Pero el dato personal no es solo dinerario o económico, y aunque la Ley 1581 de 2012, que cubre un rminos muy similares a los de su antecesora decreto 1377 de 2013 si decidi vez responden al inter a los dos o, que se considera coámbito mayor de aplicación, decidió no enfrentarse a la discusión interpretativa que se generó en la norma antecesora y obvió la definición de dato público, su decreto reglamentario, en una posible extralimitación de facultades reglamentarias, sí lo hizo. Así, el Decreto 1377 de 2013, decidió participar en la discusión y, desoyendo la consideración de inane que le había otorgado la Corte Constitucional a la previa definición, ofreció en su artículo 3-2 un concepto del dato público en términos muy similares a los de su antecesora, aunque ampliando los ejemplos:

Dato público: es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.

y alcance del derecho a la intimidad resulte incorporado al concepto de dato público, pues es indudable que por sus características particulares se ubicaría bien en la categoría de dato semiprivado o de dato privado. Adicionalmente, debe tenerse en cuenta que para los efectos de la regulación sectorial que se predica del Proyecto de Ley, el legislador estatutario ha previsto que la información financiera, comercial y crediticia es una modalidad de información semiprivada. En consecuencia, no será válido que en la aplicación de las reglas contenidas en la iniciativa, que como se ha insistido, solo resultan aplicables a la administración de datos personales de contenido comercial y crediticio, se establezca que dicha información tiene carácter público, puesto que existe un mandato legal que establece, de forma expresa, lo contrario” (énfasis agregado).

En esta ocasión, se decidió no definir el dato público como aquel considerado como tal por la ley o la Constitución, y se evitó el enfrentamiento directo con el principio de máxima divulgación o máxima publicidad de la jurisprudencia sobre acceso a la información y la Ley TAIP. Sin embargo, al definirlo por oposición al dato semiprivado, privado o sensible, tampoco se aportó de manera definitiva a su significado. Sabemos que el dato público puede solicitarse por cualquier persona, sin requisitos ni condiciones, pues forma parte de sus derechos fundamentales,¹⁶ pero no hay aún definición clara del mismo.

Corresponde entonces acudir a una interpretación sistemática de la Ley 1581 y su decreto reglamentario, con el principio de máxima publicidad. Para el efecto, como ya hemos mencionado, según el artículo 2 de la Ley de TAIP, “toda información *en posesión, bajo control o custodia* de un sujeto obligado es pública y no podrá ser reservada o limitada sino por disposición constitucional o legal” (énfasis agregado).

Los datos personales, por decisión de dos leyes estatutarias (la Ley 1266 de 2008 y la 1581 de 2012), NO son información pública, sino protegida y, por estar bajo el control o la custodia de un sujeto obligado, no son automáticamente revelables, puesto que su esencia, la de ser datos personales, constituye una excepción a la información pública y mientras no pierdan su naturaleza de tales y cumplan con las condiciones del test de daño de la Ley TAIP, seguirán siendo privados o personales o, en los términos de esta última norma, información pública clasificada.

El principio de máxima publicidad o divulgación, que ya estaba entronizado como garantía constitucional¹⁷ cuando se aprobaron las leyes estatutarias sobre datos personales, seguirá aplicándose, pero en armonía con los principios de confidencialidad, de libertad y de acceso y circulación restringida de los datos personales. No habrá revelación automática de dichos datos personales mientras sigan sirviendo para identificar a las personas, pues nos encontramos ante una excepción legal que exige autorización para su tratamiento y divulgación. Ni siquiera si media autorización para publicarlos, o si han sido recolectados en ejercicio de una función legal, parecieran perder su naturaleza.

¹⁶ Corte Constitucional, sentencias T-729 de 2002, C-336 de 2007, C-334 de 2010 y C-748 de 2011.

¹⁷ Corte Constitucional, sentencia T-1025 de 2007, M. P. Manuel José Cepeda y C-491 de 2007, M. P. Jaime Córdoba Triviño, que fijaron la línea jurisprudencial en materia de acceso a la información pública, lo que incluye el principio de máxima divulgación.

Seguimos sin embargo, con la incertidumbre de saber a cabalidad qué es un dato público, tarea en la cual creemos que los ejemplos que dan ambas normas comentadas pueden arrojar luces.

En la categoría de datos de registros públicos, denominados por la ley como datos públicos, encontramos los datos relativos al estado civil de las personas. El estado civil es la situación jurídica de una persona en la familia o en la sociedad,¹⁸ y todos los hechos y actos relativos al mismo deben ser inscritos en el registro civil, v. gr., nacimientos, matrimonios, cambios de nombre, adopciones, alteraciones de la patria potestad, etc. También se incluyen los datos en el registro de instrumentos públicos, en el registro público mercantil, un alto porcentaje de datos de funcionarios públicos que se conservan en toda entidad pública, además de algunos propios de entidades que los aglutinan en diferentes modalidades y en distintas entidades públicas (Departamento Administrativo de la Función Pública, Procuraduría General de la Nación, etc.).

Así, la información privada que, en ejercicio de las funciones de entidades públicas, es capturada y aglutinada por registros o documentación catalogados como públicos por la ley, se transforma en dato público. En consecuencia, si esa información se extrae del registro público, no es necesario el consentimiento o la autorización del titular del dato.

En este último caso, es importante tener en cuenta que se cumplen los requisitos para divulgar información bajo control de sujetos obligados, pues el derecho a la intimidad es uno de los objetivos legítimos consagrados por el artículo 18 de la Ley estatutaria, que le da tratamiento de excepción al principio de máxima divulgación; aplicado el test, resultaría que el daño al acceso a la información sería de menor entidad al que causaría divulgar datos personales.

Además de los ya nombrados, existen muchos registros públicos en nuestro sistema jurídico. En la lista podríamos incluir, de manera no taxativa, los siguientes: el registro mercantil (art. 26 del código de comercio), el registro único de proponentes (art. 6, Ley 1150 de 2007), el registro único nacional de tránsito (RUNT) (art. 9, Ley 1676 de 2013), la licencia de conducción (art. 2, Ley 769 de 2002), el registro de propiedad de vehículos y la tarjeta que se expida con base en él (art. 2, Ley 769 de 2002).

Pero, ¿qué sucede cuando los registros no son catalogados como públicos por la ley? Para responder a esta pregunta, debemos primero se-

leccionar los principios que pueden colisionar y luego resolver la tensión entre ambos extremos.

Selección de principios con posibilidades de colisión

Los principios de la protección de datos personales ya habían sido producidos por la jurisprudencia constitucional, y la Ley 1581 de 2012 los recogió en su artículo cuarto bajo el siguiente listado:

- Principio de legalidad en el tratamiento de datos.
- Principio de finalidad.
- Principio de limitación temporal del tratamiento de datos personales.
- Principio de pertinencia y proporcionalidad.
- Principio de libertad o autorización del titular del dato.
- Principio de veracidad o calidad.
- Principio de transparencia.
- Principio de acceso y circulación restringida.
- Principio de seguridad.
- Principio de confidencialidad.

Adicionalmente, en su sentencia de constitucionalidad de la Ley 1581, la Corte recogió otros principios aplicables, como los de no discriminación, la indemnización por los daños causados por uso indebido, y la interpretación integral. Finalmente, la Corte incluyó otros tres principios derivados de la lectura sistemática de la mencionada ley: principio de proporcionalidad del establecimiento de excepciones (las excepciones deben ser motivadas), principio de independencia de la autoridad de control y principio de exigencia de estándares de protección equivalentes para la transferencia internacional de datos.

La mayoría de los anteriores principios se refieren a asuntos no relacionados con la tensión entre la protección de los datos personales y el acceso a la información pública, de manera que no daremos mayor explicación de sus contenidos. Además de tener en cuenta el principio de proporcionalidad, por ser directamente relevante, seleccionaremos entonces los principios de libertad o de autorización del titular del dato y circulación restringida.¹⁹ Estos exigen la autorización o el consentimiento

¹⁸ Decreto 1260 de 1970, artículo 101, entre otros.

¹⁹ El principio de libertad equivale, bajo el entendido de que se trata de una legislación sectorial, al de circulación restringida consagrado en el artículo

previo, expreso, inequívoco e informado del titular, por cualquier medio que pueda ser objeto de consulta posterior, para legitimar el tratamiento de los datos. El tratamiento incluye el acceso de dichos datos a terceros.

No se requiere, sin embargo, autorización del titular —ya lo advertimos—, cuando se trata datos públicos o de naturaleza pública, lo que nos remite a la anterior sección de datos públicos. Tampoco debe mediar autorización cuando se trate de información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial, en casos de urgencia médica o sanitaria o cuando el tratamiento es autorizado por la ley para fines históricos, estadísticos o científicos.²⁰

Por su parte, la Ley TAIP también cuenta con un listado de principios, de los cuales el más importante es el de máxima publicidad para titular universal, íntimamente relacionado con el de transparencia, según los cuales toda información en posesión, bajo control o custodia de un sujeto obligado se presume pública y no podrá ser reservada o limitada, sino por disposición constitucional o legal.²¹ De esta manera, se entroniza la fórmula esencial para la transparencia, es decir, que no se requiere de una norma para acceder a información que es de todo el mundo, sino, por el contrario, se requiere de una norma para impedirlo.

Adicionalmente, el artículo tercero de la ley en comento establece otros principios:

- Principio de buena fe.
- Principio de facilitación.
- Principio de no discriminación.
- Principio de gratuidad.
- Principio de celeridad.
- Principio de eficacia.

lo 4c) de la Ley 1266 de 2008. Según la norma “Los datos personales, salvo la información pública, no podrán ser accesibles por Internet o por otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido solo a los titulares o los usuarios autorizados conforme a la presente ley” (énfasis agregado). Pero también habrá que tener en cuenta el parágrafo del artículo 6 de esa misma ley, pues exige de autorización del titular a la administración de la información pública, así: “La administración de información pública no requiere autorización del titular de los datos, pero se sujeta al cumplimiento de los principios de la administración de datos personales y a las demás disposiciones de la presente ley”.

²⁰ Ver artículos 8, 9 y 10 de la Ley 1581 de 2012.

²¹ Ver artículos 2 y 3 de la Ley 1712 de 2014.

- Principio de la calidad de la información.
- Principio de la divulgación proactiva de la información.

Nos parece que la mayoría de estos principios, cuyos contenidos se encuentran debidamente desarrollados en ley y jurisprudencia, gravitan en torno y son aplicables al dato personal inmerso en la información pública y no representan mayor conflicto. Concentrémonos entonces en los principios que podrían generar conflicto, transparencia, máxima divulgación, libertad y autorización restringida, y cómo su entendimiento adecuado ayuda a dilucidar si se divulgan o se protegen los datos personales.

Armonización de principios y divulgación parcial

Nos encontramos, pues, ante el test de daño como herramienta para solventar la tensión entre los principios de máxima divulgación y transparencia, y el principio de libertad o necesidad de autorización del titular. Si un documento es público, porque está bajo posesión, control o custodia de un sujeto obligado de la Ley TAIP, debe ser divulgado por aplicación del primer grupo de principios. Sin embargo, si el documento contiene datos personales, no puede revelarse sin autorización del titular, por aplicación del segundo principio.

Frente a este difícil equilibrio, en los casos en los que no existe normativa que permita entregar información personal sin consentimiento del titular, existe el deber de adoptar una interpretación equilibrada de los datos personales y del acceso a la información pública. Es en este momento, en el que cobra más importancia la tesis de la ponderación mediante el juicio de proporcionalidad ya mencionado. En cada caso concreto, el análisis debe someterse a los principios de idoneidad, necesidad, finalidad y proporcionalidad estricta.

La armonización que se propone es una herramienta valiosa, en especial para tratar de resolver la tensión que se presenta con frecuencia en situaciones como las de acceso a subsidios y otros beneficios públicos de programas sociales. Así, mientras la ciudadanía quiere ejercer control social y político solicitando el listado de beneficiarios de este tipo de programas, la entidad estatal respectiva lo niega, alegando protección de datos personales. El sujeto obligado debe decidir si entregar los listados de beneficiarios de subsidios, con todos sus datos personales, es una medida adecuada para ejercer control social, o si hay otras fórmulas más idóneas; si es la más benigna o si existe alguna manera menos dañina de verificar el manejo de los dineros públicos; si con ella se logra la garantía de la par-

ticipación ciudadana, y si no supone un sacrificio mayor a la intimidad y autodeterminación de los subsidiados, generando, por ejemplo, estigmatización o discriminación.

En estos casos, a nuestro modo de ver, el razonamiento o test deberá tener en cuenta la contraposición de la intimidad/*habeas data*, en especial con datos privados, semiprivados o sensibles, y el acceso a la información pública, para concluir que la información para el ejercicio del control social se podría entregar, si y solo si, se puede hacer de manera proporcionada. Es decir, sin violentar los valores que encierran la intimidad y el *habeas data*, para lo cual debería rechazarse la individualización de beneficiarios que suponga la revelación de datos sensibles, privados o semiprivados de personas naturales, tales como los hábitos personales, la dirección exacta, el origen social, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos, y la vida sexual.

Esta armonización²² supone que hay protección al *habeas data* al tiempo que se propende por el máximo de transparencia que se predica de información pública, lo cual generalmente conlleva la divulgación parcial consagrada en el artículo 21 de la Ley 1712 de 2014. La divulgación parcial conjugaría el principio de circulación restringida, con dos principios de transparencia y una regla de acceso a la información que resultan de contribuciones de la jurisprudencia constitucional de 2007: i) el principio de circulación restringida, según el cual los datos personales, salvo la información pública, no podrán ser accesibles por Internet o por otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido solo a los titulares o los usuarios autorizados; ii) el principio de máxima publicidad para titular universal; iii) el principio según el cual la reserva opera respecto del contenido de un documento público pero no de su existencia, y iii) la regla según la cual, cuando parte de la información contenida en un documento público esté protegida por una excepción, “debe hacerse una versión pública que mantenga la reserva únicamente de la parte indispensable”.²³

22 En este documento no estudiamos directamente la tensión con otros derechos como la libertad de expresión o la libertad de prensa de los artículos 20 y 73 de la CP, pero es claro que en el juicio de proporcionalidad que conlleva el test de daño se deberá tener en cuenta la prohibición constitucional de la censura y el análisis frente a otros derechos fundamentales.

23 Artículo 21 de la Ley 1712 de 2014. Divulgación parcial y otras reglas.

De manera que la presencia de datos personales privados, semiprivados o sensibles en un documento público puede generar un impedimento en la transparencia integral, pero no autoriza negar la existencia de los datos, por lo que procedería una divulgación parcial. Y la sola existencia del documento no sería suficiente si existiere la posibilidad de presentar la información de manera parcial, pues se impondrá, por ejemplo, el deber de comunicar los datos agregados generales sin identificar a los propietarios de dichos datos.

La norma exige que se haga una versión especial que mantenga bloqueado, reservado o protegido únicamente lo estrictamente necesario, para cumplir tanto con la protección del *habeas data* como con la apertura del derecho de acceso a la información pública. De esta manera, no se negará el acceso a la información pública sino que se filtrarán los datos que no sean públicos o no tengan autorización de publicidad por parte de su titular.

Esta posibilidad la corrobora la sentencia C-748 de 2011 que examina la constitucionalidad de la Ley 1581 de 2012. Al analizar las excepciones al tratamiento de datos, declara exequible el literal e) del artículo 6 sobre excepciones al tratamiento de datos sensibles, pero solo cuando se trata de lograr fines estadísticos, históricos o científicos, que para el presente caso propondríamos se extendiera a fines de garantía de la participación ciudadana. Como condición previa, eso sí, la ley exige que se tomen las medidas necesarias para suprimir la identidad de los titulares.

La Corte encuentra exequible esta excepción porque: i) cumple con fines imperiosos y favorece los intereses de la colectividad, pues se contribuye al mejor diseño de políticas públicas, al funcionamiento del Estado y a la satisfacción de derechos (incluso el derecho colectivo a la verdad); ii) se prevé un medio adecuado al exigir que se suprima la identidad del titular y, iii) hay un balance adecuado entre el derecho al *habeas data* y los derechos que se satisfacen con las actividades históricas estadísticas y científicas. Los tres fines se podrían cumplir, a nuestro modo de ver, respecto de la veeduría ciudadana.

Dice la sentencia que el tratamiento con fines históricos, estadísticos y científicos se permite sin autorización y debe ceñirse a lo estipulado en el artículo 6, según el cual debe tomarse las medidas para la supresión de la identidad del titular. Por último, establece —también en una expresión que se puede trasponer respecto de la solicitud de beneficiarios de subvenciones— que el acceso a la información contenida en el registro civil

no puede interpretarse como una autorización abierta para el acceso a los datos del titular, y debe adecuarse a los principios y protecciones establecidos en esta ley.

Mención aparte merecen los datos personales contenidos en providencias judiciales, que también son datos públicos según la definición del Decreto 1377 de 2013. No obstante, pueden presentarse tensiones entre la privacidad de partes y testigos en un proceso, y la publicidad de las decisiones judiciales, ya que los fallos judiciales son de público conocimiento, pues son requeridos para conocer el estado de la jurisprudencia y divulgar el contenido de sus precedentes que luego serán citados, preservando el derecho a la igualdad. Simultáneamente, existen derechos de la infancia y la adolescencia que hay que proteger para evitar daños o revictimizaciones con su publicación. Para armonizar estas tensiones, el principio de divulgación parcial recién mencionado es muy valioso.

Adicionalmente, y si se tratare de la publicidad de estas decisiones en Internet o en cualquier otro formato electrónico, habría igualmente tensiones pues mientras que los fallos judiciales son de público conocimiento, contienen en algunos casos información privada que debe permanecer reservada o, en los términos de la Ley TAIP, clasificada. Para atender esta problemática, la sociedad civil de los países latinoamericanos ha producido lo que se conoce como Reglas de Heredia,²⁴ que son recomendaciones mínimas que conllevan la “anonimización” de autos y sentencias con datos personales reservados. Destacaremos la regla 5, que puede ser útil en este acápite de nuestro estudio, en la medida en que se apoya en la armonización de principios que pretendemos impulsar:²⁵

24 http://www.ijusticia.org/heredia/Reglas_de_Heredia.htm (Consultado el 1 de junio de 2014).

25 También es útil en este estudio la Regla de Heredia número 7: “Regla 7. En todos los demás casos se buscará un equilibrio que garantice ambos derechos. Este equilibrio podrá instrumentarse: a) en las bases de datos de sentencias, utilizando motores de búsqueda capaces de ignorar nombres y datos personales; b) en las bases de datos de información procesal, utilizando como criterio de búsqueda e identificación el número único del caso. Se evitará presentar esta información en forma de listas ordenadas por otro criterio que no sea el número de identificación del proceso o la resolución, o bien por un descriptor temático”.

Estas reglas de Heredia no son contrarias a los criterios que estamos mencionando en este capítulo y que continuaremos analizando a continuación en relación con ciertas hipótesis de bases de datos con leyes especiales.

Regla 5. Prevalecen los derechos de privacidad e intimidad, cuando se traten datos personales que se refieran a niños, niñas, adolescentes (menores) o incapaces; o asuntos familiares; o que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos; así como el tratamiento de los datos relativos a la salud o a la sexualidad; o víctimas de violencia sexual o doméstica; o cuando se trate de datos sensibles o de publicación restringida según cada legislación nacional aplicable o hayan sido así considerados en la jurisprudencia emanada de los órganos encargados de la tutela jurisdiccional de los derechos fundamentales.

En este caso, se considera conveniente que los datos personales de las partes, coadyuvantes, adherentes, terceros y testigos intervinientes, sean suprimidos, anonimizados o definidos por letras o números, salvo que el interesado expresamente solicite que no sean suprimidos sus datos y ello sea pertinente de acuerdo con la legislación.

De esta manera, y bajo la autorización de la divulgación parcial prevista en la Ley TAIP y en la Ley de datos personales para ciertos casos, se accederá a información útil cuando, existiendo tensión, se revele un objetivo de interés general en acceder a dicha información que pueda cumplirse sin violentar el *habeas data*.

No obstante nuestra posición respecto del test de daño para subvencionados, en el derecho comparado ha habido casos en los cuales ha primado el derecho de acceso a la información pública. Véase, para el efecto, la sentencia de la Corte Suprema de Argentina que enfrentó a la solicitud de divulgación de un listado de beneficiarios de subvenciones estatales y concluyó que: a) la estigmatización de las personas pobres receptoras de la subvención es un riesgo conjetural que en todo caso sería consecuencia de una acción posterior de terceros y no del acceso a los datos en sí mismos y, b) el acceso en este caso no tenía por objeto presumible una conducta de ese estilo.²⁶

Por otro lado, en un caso chileno de patentes municipales (C610-10), el Consejo de la Transparencia resolvió sobre si la eventual publicidad de unas patentes municipales autorizaba necesariamente la divulga-

26 Corte Suprema de Justicia de la Nación, Buenos Aires, 26 de marzo de 2014, CIPECC c/Ministerio de Desarrollo Social, 11702/03 amparo Ley 16.986.

ción de los datos que interesaban al reclamante, es decir, nombre o razón social de los contribuyentes, su dirección, incluyendo calle y número, la ciudad en que ejercen su actividad y su giro comercial. El Consejo estimó que dicha información no había sido recolectada de fuentes accesibles al público (antecedentes proporcionados por el contribuyente al solicitar el otorgamiento de la patente respectiva para este solo efecto), razón por la cual tampoco podía entenderse que había consentido en su publicidad, y confirmó que no existía una norma legal que estableciera su carácter público en términos generales. Sin embargo, entendió que

...datos de las personas naturales contribuyentes de patentes municipales, especialmente los que son de interés del reclamante, en cuanto están directamente vinculados con la actividad gravada, revisten relevancia especialmente sobre las siguientes dos cuestiones, a saber: 1) el cumplimiento de los requisitos necesarios para el ejercicio de la actividad que se autoriza por medio de la patente; y 2) la publicidad del giro o actividad desarrollada por el contribuyente, que permitiría conocer si este cumple con la regulación sectorial correspondiente, y los ingresos que se perciben por concepto de patentes municipales.²⁷

Para el efecto, aplicó el test de interés público y consideró que la reserva de los datos personales que interesan al reclamante podría ceder en beneficio de su publicidad, por el manifiesto interés público que revisten.

El Supervisor Europeo de Protección de Datos para este tipo de tensiones considera que se debe preferir la protección de datos personales en poder de la Administración Pública, frente al acceso a la información. Adicionalmente, ofrece unas recomendaciones prácticas que contribuyen a tomar decisiones en estos casos. En esta calidad, la autoridad europea considera que: a) “El mero hecho de que un documento contenga datos personales de carácter general, como el nombre de una persona, no debería —normalmente—, impedir su divulgación”; b) los datos sensibles son un claro indicador de que la intimidad está en juego, por ejemplo, “sobre su salud; cuando se refiere al honor y la reputación de la persona; cuando pudiera dar una imagen falsa de la persona; cuando divulga hechos embarazosos,

y cuando divulga información dada o recibida por la persona con carácter confidencial”; c) el perjuicio a la intimidad no puede ser nimio o superficial, por ejemplo, “cuando dichos datos personales ya han sido divulgados anteriormente”; y d) “Es posible que determinadas informaciones que de forma directa no identifican a un titular puedan ser consideradas datos de carácter personal cuando dicha identificación es posible sin suponer la misma un tiempo o esfuerzo desproporcionado” (Matus 2013: 197-228).

Al aplicar el test de daño o interés público, cristalizando el juicio de proporcionalidad, y teniendo en cuenta las referencias de derecho comparado latinoamericano y las recomendaciones del Supervisor Europeo, creemos que es posible armonizar la tensión existente entre estos derechos fundamentales, con el mínimo de daño y el máximo de beneficio a los derechos fundamentales involucrados. Habrá que proteger la intimidad y la autodeterminación, sin olvidar que hay que valorar todos los principios que obliguen al sujeto a inclinarse por la transparencia, así como la finalidad de la difusión de los datos. De este modo, puede anticiparse que cuando la revelación de la información cumple con las mismas finalidades democráticas que el ámbito de mayor protección de la libertad de expresión, hay tendencia a que la intimidad ceda a favor de la ampliación de un debate vigoroso y amplio en la ciudadanía, por lo que se debe propender por aplicar la fórmula que permita dicho debate.

Teniendo en cuenta esta armonización de principios que se acompaña de la divulgación parcial, pasaremos entonces a explicar el criterio de las diversas esferas o límites de la intimidad y la autonomía, como criterio auxiliar en nuestro objeto de estudio.

Distinción entre diversas esferas de la intimidad y la autonomía

Un segundo criterio para definir qué información íntima correspondiente a datos personales debe permanecer clasificada y secreta, articulando la interpretación de la ley de transparencia y las normas de datos personales, hace referencia a la distinción entre diversas esferas de la vida personal, lo que a su vez conlleva diferentes esferas de los datos personales. Este criterio se acerca a la tesis de los límites de los derechos que mencionamos en acápite previo, para explicar las formas como, según lo había resumido Upegui, la jurisprudencia colombiana había intentado resolver la tensión en cuestión. Y a pesar de que la consideramos en parte superada, sigue siendo un insumo para considerar en la armonización.

²⁷ Ver Matus (2013: 197-228). Además, en virtud de lo dispuesto en la letra c del artículo 17 de la Ley 19.880 de Chile, y sólo en la medida en que el titular solicite la prestación de un servicio o la concesión de un beneficio determinado a un organismo público específico, su consentimiento no será necesario para la cesión de esos datos.

Para distinguir las diversas esferas de la vida interior de cada individuo, resulta valioso acudir a la jurisprudencia alemana, que otorga protección diferencial según la mayor cercanía al núcleo del derecho fundamental de que se trate. De esta manera, es posible encontrar una esfera más íntima dotada de mayores garantías, una esfera privada pero compartida con un grupo reducido de allegados en la que la protección es intermedia y, finalmente, un ámbito personal en el que necesariamente se debe interactuar con otras personas, en el cual la protección es mucho menor.²⁸

Así explica la academia colombiana la clasificación de la intimidad en la jurisprudencia alemana:

La jurisprudencia alemana ha distinguido además entre diversas esferas de la intimidad y la autonomía personales, de suerte que en ellas el grado de protección constitucional es diverso. *La esfera más íntima* corresponde en general a los pensamientos o sentimientos más personales que un individuo solo ha expresado a través de medios muy confidenciales, como cartas o diarios estrictamente privados, y es, según el Tribunal Constitucional, un ámbito intangible de la dignidad humana. La garantía en este campo es casi absoluta, de suerte que solo situaciones o intereses excepcionalmente importantes justifican una intromisión. Luego encontramos la *esfera privada en sentido amplio*, que corresponde a la vida en ámbitos usualmente considerados reservados, como la casa o el ambiente familiar de las personas, en donde también hay una intensa protección constitucional, pero hay mayores posibilidades de injerencia ajena legítima. Y, finalmente, el Tribunal habla de la *esfera social o individual* de las personas, que corresponde a las características propias de una persona en sus relaciones de trabajo o públicas, en donde la protección constitucional a la intimidad y a la autonomía es mucho menor, aún cuando no desaparece, pues no se puede decir que se puede informar sobre todo lo que una persona hace por fuera de su casa sin violar su intimidad (énfasis agregado) (Uprimny, Fuentes, Botero y Jaramillo 2006: 66-67).

La jurisprudencia colombiana, y en particular la sentencia T-787 de 2004 de la Corte Constitucional, con ponencia de Rodrigo Escobar Gil

28 Estas esferas que distinguen la intimidad y la privacidad tienden también a acercarse a la visión de Garzón Valdés (Garzón, 2008), para quien la intimidad es el fuero más interno (yo con yo), y la privacidad se predica de la relación interpersonal (yo con otro).

sobre una caricatura denominada “La flor del trabajo”, en la cual se hace mofa de una profesora sometida a incapacidades consecutivas y publicada en diversos medios, estableció lo siguiente en materia de ámbitos de intimidad:

Dependiendo del nivel en que el individuo cede parte de su interioridad hacia el conocimiento público, se presentan distintos grados de intimidad. Dichos grados de intimidad se suelen clasificar en cuatro distintos niveles, a saber: la intimidad personal, familiar, social y gremial (CP art. 15). La primera, alude precisamente a la salvaguarda del derecho de ser dejado solo y de poder guardar silencio, es decir, de no imponerle a un determinado sujeto, salvo su propia voluntad, el hecho de ser divulgados, publicados o fiscalizados aspectos íntimos de su vida. La segunda, responde al secreto y a la privacidad en el núcleo familiar, una de cuyas principales manifestaciones es el derecho a la inmunidad penal, conforme al cual, “nadie podrá ser obligado a declarar contra sí mismo o contra su cónyuge, compañero permanente o parientes dentro del cuarto grado de consanguinidad, segundo de afinidad o primero civil”. La tercera, involucra las relaciones del individuo en un entorno social determinado, tales como, las sujeciones atinentes a los vínculos laborales o públicos derivados de la interrelación de las personas con sus congéneres en ese preciso núcleo social, a pesar de restringirse —en estos casos— el alcance del derecho a la intimidad, su esfera de protección se mantiene vigente en aras de preservar otros derechos constitucionales concomitantes, tales como el derecho a la dignidad humana. Finalmente, la intimidad gremial se relaciona estrechamente con las libertades económicas e involucra la posibilidad de reservarse —conforme a derecho— la explotación de cierta información, siendo, sin lugar a dudas, uno de sus más importantes exponentes, el derecho a la propiedad intelectual.

El primer nivel de intimidad, el personal, hace referencia al derecho a ser dejado solo o en paz. Este nivel de intimidad, que está respaldado constitucionalmente por la inviolabilidad de la correspondencia y demás formas de comunicación privada (art. 15), y por la inviolabilidad del domicilio (art. 28),²⁹ permite que las personas construyan y desarrollen su

29 La noción de domicilio en derecho constitucional difiere del concepto clásico civilista. La Corte, en la sentencia C-024 de 1994, en la que revisó algunos artículos del Código Nacional de Policía relativos al registro o alla-

personalidad sin intervención de terceros. El segundo nivel es el familiar, que está anclado constitucionalmente en el artículo 15, cuando se menciona la intimidad familiar, y en el artículo 33 que prohíbe obligar a alguien a declarar contra sí mismo o contra sus familiares más próximos. El tercer nivel es el de intimidad social, en el que la Corte incluye los vínculos laborales o más públicos que tienen una protección intermedia en aras de la dignidad humana.

Finalmente, el último nivel es el de la intimidad gremial, que está atada a la facultad de mantener en secreto cierta información vinculada con el ejercicio profesional o económico. En la Constitución, la intimidad gremial se expresa principalmente en el artículo 74 sobre el secreto profesional, en el artículo 61 sobre la propiedad intelectual y, más lejanamente, en el artículo 150 sobre la propiedad industrial. También puede considerarse que la intimidad gremial se relaciona con el secreto comercial e industrial protegido por la Decisión 486 de 2000 de la Comunidad Andina de Naciones (CAN), conocida también como del Acuerdo de Cartagena.

Es válido anotar que esta división de ámbitos más y menos privados suele coincidir con la clasificación de información privada y semiprivada derivada de la Ley 1266 de 2008 que mencionamos en acápites anteriores. En efecto, si la información privada es aquella que protege el fuero más íntimo, de suerte que solo interesa a su titular, y la semiprivada es un poco menos íntima e interesa, además de al titular, a un grupo determinado con el que este último interactúa, es posible concluir que atienden a categorías muy similares que además nos servirán para considerar que hay mayor razonabilidad y proporcionalidad en solo entregar información semiprivada a las personas o grupos directamente involucrados, en lugar de a la ciudadanía en general.

Así, si por ejemplo aplicamos a bases de datos personales los anteriores criterios de ámbitos de la intimidad y su coincidencia con el interés que puedan tener terceros en ella, podríamos considerar que las bases de datos personales pertenecientes a los dos primeros niveles gozan de la

mayor protección. Las bases de datos del tercer ámbito de intimidad, que es el social, y que equivale a lo semiprivado, interesan al usuario y a un grupo de personas cuyos intereses pertenecen a este escenario social. Esta divulgación excede el estrecho círculo de la intimidad y debe ser publicada en el círculo social al que interesa, pero si se tratare de su divulgación al público en general, dependerá del caso concreto, aunque en principio tendrá menos facilidad su detentor en demostrar el daño presente, probable y específico que conlleva transparentar información de esta índole, daño que a su vez debe exceder el interés público de conocer este tipo de información.

En esta línea, los datos sobre orientación sexual no solo son extremadamente cercanos al núcleo de la intimidad, sino que además conllevan una cierta propensión a la discriminación. Pertenecen, sin duda, al primer nivel de intimidad y ameritan la mayor de las protecciones. En este campo, la Corte se enfrentó en la sentencia T-256 de 2002 a un caso en el que una autoridad de salud publicó en medios de comunicación información sobre las causas de la muerte de una persona que tenía sida y sobre su comportamiento sexual; la Corte protegió el derecho a la intimidad familiar de la actora que era la madre de la persona que había fallecido.

El caso de la información crediticia es ilustrativo de la tercera esfera de privacidad, y para el efecto nos vamos a referir a la sentencia SU-082 de 1995, en la cual la Corte se pregunta si el manejo que una persona haga de sus obligaciones de contenido económico pertenece a su esfera privada o, por el contrario, tiene incidencia social y por tanto es objeto del derecho a la información de los demás. En su respuesta, la Corte estima que la calidad de deudor no debe quedar en la intimidad por dos razones principales: por un lado, el contenido económico del crédito no puede equipararse a aquello que pertenece a planos superiores como la dignidad humana y, por otra parte, el cumplimiento crediticio no es de mero interés personal, sino que también atañe a acreedores actuales y potenciales.

En efecto, el préstamo de dinero es una actividad que conlleva un riesgo, y que es además de interés general bajo la inspección, vigilancia y control por parte del Gobierno, por lo cual el comportamiento crediticio no puede ser secreto. La circulación de información acerca de los deudores ayuda al fortalecimiento de la confianza pública y su valor económico la aleja de la intimidad que pertenece solo al individuo.³⁰ Pero esta infor-

namiento del domicilio, sostuvo que: "...por inviolabilidad de domicilio se entiende en general el respeto a la casa de habitación de las personas [...] además de [...] todos aquellos espacios cerrados, en donde las personas desarrollan de manera más inmediata su intimidad y su personalidad mediante el libre ejercicio de su libertad. La defensa de la inviolabilidad del domicilio protege así más que a un espacio físico en sí mismo al individuo en su seguridad, libertad e intimidad".

30 Corte Constitucional, sentencia SU 082 de 1995, M. P. Jorge Arango Mejía.

mación crediticia, que debe ser completa, actual y veraz, interesa a la comunidad crediticia, que ejerce sus funciones de otorgamiento de crédito, y solo atañe a la ciudadanía en general en la medida en que se combine con otros criterios de armonización, como por ejemplo que esta información le permita participar en la gestión de la cosa pública.

El caso de los datos de catastro y de salud,³¹ aunque anterior a la ley de protección de datos personales, también es relevante para ilustrar este tipo de información que, a pesar de estar bajo control o custodia de entidades estatales, pertenece a la categoría semiprivada que interesa, *prima facie*, a un grupo reducido de personas, es decir, al nivel de intimidad gremial. En esta ocasión, la tutela fue interpuesta porque un ciudadano consideró vulnerado su derecho a la intimidad y puestos en riesgo sus derechos y los de su familia por el acceso a cierta información jurídica y económica acerca de los bienes dispuesta por el Departamento Administrativo de Catastro del Distrito Capital, así como la información también accesible acerca de la afiliación al régimen social en salud de los individuos dispuesta por la Superintendencia Nacional de Salud. En relación con catastro, la Corte encontró que la información accesible mediante el solo documento de identidad gozaba de protección precaria que solo se superaba exigiendo la inserción de datos confidenciales, pues estos impiden el acceso de terceros. Además, estimó que existía un desconocimiento indirecto del principio de finalidad, puesto que Catastro permite el acceso indiscriminado a datos que, en principio, están llamados a ser conocidos por determinadas personas naturales y jurídicas. Esto distorsiona la finalidad de los datos puesto que se permite que extraños, sin intereses visibles, accedan a la información del titular. En tercer lugar, debido al acceso indiscriminado, existe un riesgo para el principio de individualidad pues no hay un cuidado suficiente para evitar que se combinen los datos de distintas bases de datos y la construcción de perfiles individuales.

En cuanto a la información accesible a través de la página de Internet de la Superintendencia Nacional de Salud, la Corte encontró que se desconoce la libertad, finalidad y circulación restringida debido al acceso indiscriminado que se permite desde dicha página. El máximo tribunal no dudó en considerar dicha información como semiprivada y, por tanto, de uso privado entre las entidades de seguridad social y el titular. De esa

manera, se estableció que la finalidad de esos datos personales se enmarca en esa relación, y que dicha información no tendría por qué ser conocida por terceros.

Asimismo, la Corte advirtió que el acceso indiscriminado a las bases de datos bajo examen, podría llegar a permitir el cruce de datos y la construcción de al menos una pequeña semblanza del titular, que podría incluso completarse con otras bases de datos. Esta situación, se consideró, afecta los derechos fundamentales del actor y, en específico, compromete sus derechos a la autodeterminación informática, la intimidad, libertad e integridad física, entre otros. El aumento de bases de datos (publicadas ahora por Internet), así como el fortalecimiento del poder informático, en carencia casi absoluta de controles, generan un riesgo para los derechos fundamentales de los titulares de datos personales contenidos en esas bases. Por estas razones, la Corte decidió conceder la tutela e invitó al legislador a expedir urgentemente una regulación integral, comprensiva y suficiente en la materia para proteger los derechos fundamentales, urgencia que se materializó en la Ley 1581 de 2012.

Finalmente, la Corte recordó que para que exista un equilibrio entre los derechos a la información y al *habeas data*, es necesario que tanto la entidad administradora (en calidad de garante) como el peticionario se conduzcan según el principio de responsabilidad compartida y de cargas mutuas, lo que en cierta medida nos remite a la necesidad de justificar la relevancia y el interés del solicitante de acceso a dicha información pública.

Podemos entonces concluir que, según la esfera de la intimidad o autonomía de que se trate, se amplía o disminuye la tendencia de publicidad. Así, se va reduciendo la protección de los datos personales, y un sujeto obligado a divulgar información pública estaría más naturalmente inclinado a entregar información semiprivada, que privada. Además, esta tendencia a la divulgación disminuye si el dato se acerca al ámbito de intimidad más cercano a la individualidad, y se iría matizando a medida que se aleje del mismo, teniendo en cuenta que los círculos social, laboral o gremial también gozan de protección.

Tratamiento diferencial para datos personales de interés público

Un segundo criterio auxiliar para analizar la obligación de transparencia o clasificación frente a datos personales obedece a la naturaleza de la persona de cuyos datos se trate y, en cierta medida, también evidencia la

31 Corte Constitucional, sentencia T-729 de 2002, M. P. Eduardo Montealegre Lynett.

tesis de los límites de los derechos narrada previamente y aplicada en el anterior apartado. En efecto, la protección de la intimidad y de los datos personales no es igual para todas las personas. Hay quienes, por diversas razones, tienen un tratamiento diferencial con unos límites diversos. Este tratamiento especial, que exige unos parámetros de protección diferentes para personas públicas y personas privadas, se deriva del modelo de protección dual reconocido por la jurisprudencia constitucional nacional y por la interamericana, que explicaremos seguidamente.

El modelo de protección dual acepta un menor grado de protección de los derechos al *habeas data*, al buen nombre y a la intimidad en relación con la divulgación de información que se refiere a funcionarios públicos y personas de interés público, porque la vida privada de estos últimos es observada de manera más detallada por el interés general. Los personajes públicos, incluidos políticos o artistas, asumen pues el riesgo de ser afectados por la exposición de muchas de sus actividades personales, cuando atañen al interés público, son de trascendencia y causan impacto social, superando la mera curiosidad.

Ahora bien, este modelo de protección diferencial se debe conjugar con el principio de relevancia pública. De acuerdo con este principio, para que la información sea de relevancia pública y, en consecuencia, sea más importante conocerla que proteger la intimidad o los datos personales de la persona involucrada, hay que tener en cuenta no solo la calidad de la persona sino también el contenido mismo de la información.

Sobre la calidad de la persona, la jurisprudencia ha reconocido que a medida que aumente el reconocimiento público de una persona que lo ha buscado voluntariamente, menores son los límites de protección de su intimidad. Así, habrá más reserva para la intimidad de la persona privada que en nada afecta a la sociedad, menos protección para la persona que se vuelve pública por su profesión (artistas, personas populares), aún menos protección para la intimidad del funcionario público que ha sido nombrado o designado para un cometido público, hasta llegar al servidor público de elección popular, respecto del cual hay la máxima necesidad de escrutinio por parte de la sociedad a quien representa, y para quien constituye modelo, por lo que recibe la menor protección a su intimidad.

La disminución de protección basada en el sujeto se articula con el tipo de información íntima de que se trata, y el valor que tiene el debate abierto para una sociedad democrática. Los funcionarios públicos ven su esfera privada reducida e integrada a la esfera del debate público en virtud

de la prevalencia del interés general en un Estado democrático, y así lo consienten desde el momento en que aspiran o aceptan su cargo. Se reconoce, entonces, que si bien la información que manejan pueda ser en principio personal, si su conocimiento es de preocupación pública o ya es de conocimiento público, no debe ser de acceso reservado ni clasificado.³²

No obstante el anterior principio, en una ocasión la jurisprudencia, de manera aislada y sin que sus observaciones pertenecieran al núcleo de la discusión, manifestó la necesidad de autorización del funcionario público, en su calidad de data-habiente, para poder publicar su información. Se trató de una sentencia que estudió una acción de inconstitucionalidad contra varios artículos de la Ley 190 de 1995 sobre preservación de la moralidad pública y erradicación de la corrupción administrativa. Se estudió entonces el artículo 3 sobre el valor probatorio de la información contenida en el Sistema Único de Información de Personal (SUIP), artículo cuya parte final contenía la prohibición según la cual las hojas de vida y las causales de despido no podrían constituir prueba en procesos judiciales o administrativos laborales, así como la limitación de que solo podrían comunicarse la identificación del funcionario y las causales de su desvinculación del servicio o de la terminación anormal de sus contratos.³³ En esta oportunidad, la Corte declaró la inexecutable de aquel inciso que limitaba la información y el uso de las hojas de vida como prueba, y, de paso, aprovechó para hacer algunas anotaciones sobre la protección de las hojas de vida.³⁴ Dijo entonces que “hay aspectos de la hoja de vida

32 Para el detalle y la evolución de esta línea jurisprudencial, ver Uprimny, Fuentes, Botero y Jaramillo (2006), y la siguientes sentencias: T-80/93 en relación con el senador Dájer llamado campeón del ausentismo; T-322/96 en relación con el Secretario de Gobierno de Antioquia, Pedro Juan Moreno, acusado de vínculos con el paramilitarismo.

33 Artículo 3, Ley 190 de 1995: “A partir de la vigencia de la presente Ley, las hojas de vida de las personas que ocupan cargos o empleos públicos o de quienes celebren contratos de prestación de servicios con la administración, permanecerán en la unidad de personal de la correspondiente entidad, hasta su retiro. Producido este, la mencionada Unidad enviará al Sistema Único de Información de Personal de que trata el artículo anterior, la hoja de vida con la información relativa a la causa del retiro. *Dicha información no podrá utilizarse como prueba en procesos judiciales o administrativos de carácter laboral y de ella solo se comunicarán la identificación del funcionario y las causales de su desvinculación del servicio o de la terminación anormal de sus contratos* (lo que aparece en cursiva fue declarado inexecutable). ”

34 Corte Constitucional, sentencia C-038/96, M. P. Eduardo Cifuentes Muñoz.

de quien es o ha sido funcionario o contratista del Estado, cuyo conocimiento indiscriminado puede vulnerar su intimidad y buen nombre”. Dijo también que “Las hojas de vida tienen un componente personal elevado, de suerte que así reposen en archivos públicos, sin la expresa autorización del data-habiente, no se convierten en documentos públicos destinados a la publicidad y a la circulación general”. Estas dos frases han sido utilizadas por ciertos funcionarios públicos para responder negativamente a peticiones ciudadanas de estas hojas de vida y ocultar esta información.

¿Cuál podría ser la parte personal o vulnerable de una hoja de vida a la que, en calidad de *obiter dicta*, se refería la Corte? ¿Qué información es tan sensible en una hoja de vida que está vedada a la ciudadanía y, consecuentemente, le impide ejercer muchos otros derechos fundamentales (arts. 20, 23, 40, 73, 74) que en esa misma sentencia protegió el alto tribunal?

¿Podrían ser los datos personales sobre la formación de un empleado público? ¿Los datos sobre la experiencia laboral? ¿Sobre la participación en sociedades y asociaciones? ¿La edad? ¿Puede existir, por razones de seguridad, la necesidad de reservar la información sobre los bienes de un funcionario? Consideramos que ninguno de los datos mencionados debe mantenerse oculto porque, precisamente, se ofrece para poder acceder a un cargo o contrato públicos y su ocultamiento impide el control ciudadano.

Un año después,³⁵ en otra sentencia de constitucionalidad contra otros artículos de la misma Ley 190 de 1995, la Corte aclararía que no se refería ni a la información académica ni a la laboral. Dijo el tribunal:

La información de carácter académico y laboral no está sustraída al conocimiento público, con base en ella la persona se da a conocer en el ámbito social y se promociona en el mercado laboral, sin que su consignación en un sistema de información público amenace su derecho fundamental a la intimidad, mucho menos cuando ella ha sido voluntariamente suministrada por quien expresamente ha manifestado su interés de ofrecer sus servicios a la administración pública, que es lo que hace la persona natural cuando diligencia el formato único de hoja de vida que se le exige como condición previa para considerar su contratación con el Estado, o la persona natural o jurídica que en su calidad de consultor se inscribe en el correspondiente registro. El Estado,

a través del legislador, está habilitado para diseñar e imponer la utilización de esos instrumentos técnicos, que de una parte le permiten garantizar la vinculación de los más capaces y de los más idóneos a la administración, bien sea como servidores públicos o como contratistas, y de otra le permiten impulsar la realización de los principios rectores de la administración pública, siempre y cuando el contenido de dichos instrumentos no desconozca principios fundamentales de las personas, y contemplen, ellos mismos, mecanismos de control que eviten un uso indebido de la información que los nutre.

Así, se concluye que si un funcionario público quiere ocultar datos de su hoja de vida, solo podrá hacerlo respecto de aquellos que se refieren a su fuero íntimo, como su dirección o su correo electrónico personal. Solo de manera excepcional, filtrando o bloqueando esta información y permitiendo el acceso a los datos restantes, podrá limitarse el conocimiento sobre las hojas de vida de quienes se encuentran sometidos al escrutinio público.

Una vez aclarado que la sentencia C-038 de 1996 solo se refirió a la intimidad de las hojas de vida de funcionarios públicos tangencialmente, y cuando tuvo oportunidad se dedicó a rescatar la importancia de acceder a información sobre juicios de dichos funcionarios para poder así ejercer el derecho a la participación ciudadana, por lo que no puede considerarse como línea jurisprudencial propiamente dicha, podemos seguir considerando que el modelo dual de protección de la privacidad de la función pública sigue siendo sólido y robusto.³⁶

35 Corte Constitucional, sentencia C-326/97, M. P. Fabio Morón Díaz.

36 Ver, en este sentido, la sentencia de la Corte Constitucional T-066 de 1998, en la cual se consideró que primaba el derecho a la información frente a personas y hechos públicos porque son objeto de interés general; ver también la sentencia SU-1723 de 2000, en la cual el cantante Diomedes Díaz perdió frente a una programadora que expuso sus detalles y datos íntimos, así como la investigación penal por el delito de homicidio de la cual era objeto; sentencia T-437 de 2004 sobre la reducción del espacio de privacidad de Pedro Juan Moreno, quien fuera señalado por la revista *Semana* como muy cercano al presidente Uribe, sin que este último lo hubiera nombrado en un cargo público; sentencia T-218 de 2009 sobre la intimidad del exvicepresidente y exgobernador del Valle del Cauca, Angelino Garzón, donde se concluye que no es que las personas públicas carezcan de intimidad sino que frente a colisiones con la libertad informativa se hará un juicio más estricto para probar el desbalance en el ejercicio de la libertad de prensa.

Pero no solo la jurisprudencia nacional, sino también la interamericana han mantenido una posición similar de tratamiento diferenciado para funcionarios públicos en relación con ciudadanos ordinarios.³⁷ En el año 2009, en un caso de responsabilidad internacional del Estado por interceptación y divulgación (esto último por parte de un funcionario: el procurador) de la conversación telefónica de un abogado con el padre de su cliente, la Corte Interamericana recordó:

La Corte ha señalado que en una sociedad democrática los funcionarios públicos están más expuestos al escrutinio y la crítica del público. Este diferente umbral de protección se explica porque se han expuesto voluntariamente a un escrutinio más exigente. Sus actividades salen del dominio de la esfera privada para insertarse en la esfera del debate público. Este umbral no se asienta en la calidad del sujeto, sino en el interés público de las actividades que realiza.³⁸

37 También se adopta este enfoque en las Reglas de Heredia creadas por la sociedad civil y disponibles en: http://www.ijusticia.edu.ar/heredia/Reglas_de_Heredia.htm (Consultado el 20 de julio de 2014). En especial, en la regla sexta según la cual: “Prevalece la transparencia y el derecho de acceso a la información pública cuando la persona concernida ha alcanzado voluntariamente el carácter de pública y el proceso esté relacionado con las razones de su notoriedad. Sin embargo, se considerarán excluidas las cuestiones de familia o aquellas en las que exista una protección legal específica. En estos casos podrán mantenerse los nombres de las partes en la difusión de la información judicial, pero se evitarán los domicilios u otros datos identificatorios”.

38 Corte Interamericana de Derechos Humanos, sentencia del 27 de enero de 2009, caso Tristán Donoso vs. Panamá; excepción preliminar, fondo, reparaciones y costas, párr. 115. Ver también los siguientes casos de la Corte Interamericana: Kimel vs. Argentina (2008), Herrera Ulloa vs. Costa Rica (2004), Ricardo Canese vs. Paraguay (2004) y Fontevecchia y D’Amico vs. Argentina (2011). En esta última decisión, la Corte consideró que los medios de comunicación tienen un rol fundamental en una sociedad democrática, por lo que el Estado debe asegurarse de que sus restricciones sean mínimas. Asimismo, el Tribunal aseveró que la protección de la libertad de expresión es mayor si se trata de discusiones concernientes a la idoneidad de una persona en el desempeño de un cargo público o sus actuaciones en desempeño de este tipo de labores. Afirmó también la Corte que los funcionarios públicos ven su esfera privada reducida e integrada a la esfera del debate público en virtud del interés general, por su propio consentimiento desde el momento en que aceptan su cargo. Sobre el punto, la Corte concluyó que existen dos criterios relevantes a la hora de examinar una posible vulneración del derecho a la vida privada por la expresión de opiniones: 1) el menor umbral de protección de los funcionarios públicos, especialmente de los electos popularmente, respecto

Por último, debemos citar la sentencia C-274 del 9 de mayo de 2013 por medio de la cual la Sala Plena de la Corte Constitucional declaró exequible el proyecto de ley de transparencia y del derecho de acceso a la información pública nacional. En esta decisión, al examinar la constitucionalidad de los literales c) y e) del artículo 9 sobre divulgación proactiva de información mínima obligatoria respecto a la estructura del sujeto obligado, rechazó la petición de algunos intervinientes que consideraban que era inconveniente la publicidad sobre el nivel salarial o el valor de los contratos de prestación de servicios, pues en su opinión ello podía implicar la publicidad de información que ponía en riesgo al titular de la misma. Para explicar su posición, la Corte señaló que no encontraba que tal preocupación, considerada en abstracto, fuera fundada “en la medida en que la información a la que se refieren esos dos literales está relacionada con la gestión y el uso de recursos públicos sobre cuya utilización se debe garantizar el acceso más transparente posible”. Seguidamente, la Corte enfatiza que para que esta información mínima pueda ser reservada se requiere que se cumplan los requisitos propios de rechazo al acceso contemplados en los artículos 18, 19 y 29 del proyecto de ley de transparencia y acceso a la información pública.

Adicionalmente, cuando este máximo tribunal analiza la conformidad con la Constitución del artículo 18 sobre información exceptuada por daño de derechos a personas naturales o jurídicas, reafirma que el tratamiento diferencial a la intimidad de servidores públicos y ciudadanos es legal y constitucional. Al respecto establece que las referencias al artículo 24 de la Ley 1437 de 2011 deben ser reemplazadas por la norma estatutaria que se expida en lugar de esta que fuera declarada inconstitucional. Pero, más importante aún, al continuar refiriéndose al literal b) (aunque se está refiriendo en realidad al literal a), hace la ya tradicional distinción entre el derecho a la intimidad de quienes sean funcionarios públicos y el de las demás personas. La Corte estima que

... esta excepción resulta pertinente, como quiera que cuando se trata de funcionarios públicos, el escrutinio de ciertos datos personales está permitido, de conformidad con los parámetros de constitucionalidad señalados, por lo cual no encuentra la Corte que sea incompatible con el artículo 74 de la Carta ni con otras disposiciones constitucionales.

de otras figuras públicas y los particulares, y 2) el interés público en las actuaciones que ellos realizan.

Para responder a la pregunta de cuáles serían esos “ciertos datos personales” bastaría, por un lado, considerar el principio de relevancia pública que hemos mencionado previamente. Por otro lado, también deberíamos referirnos a la misma Ley de transparencia y acceso a la información pública que establece una información mínima obligatoria en su artículo 9 que incluye datos sobre salarios, formación y experiencia.

En efecto, según el mencionado artículo, por lo menos la información concerniente a la educación, formación académica, experiencia laboral y profesional, salario y remuneración por servicios de funcionarios públicos y contratistas es de obligada divulgación y no puede permanecer reservada. Suponemos, entonces, que la Corte Constitucional, además de mantener su línea jurisprudencial de la relevancia pública para divulgar datos personales de personas públicas, adoptó una posición que tuvo en cuenta una interpretación sistemática del proyecto de ley, en el cual señaló que el artículo 9 de la mencionada ley (declarado exequible) contiene información mínima obligatoria que incluye en el parágrafo la obligación del Departamento Administrativo de la Función Pública de establecer:

...un formato de información de los servidores públicos y de personas naturales con contratos de prestación de servicios, el cual contendrá los nombres y apellidos completos, ciudad de nacimiento, formación académica, experiencia laboral y profesional de los funcionarios y de los contratistas [...] Se omitirá cualquier información que afecte la privacidad y el buen nombre de los servidores públicos y contratistas, en los términos definidos por la constitución y la ley.

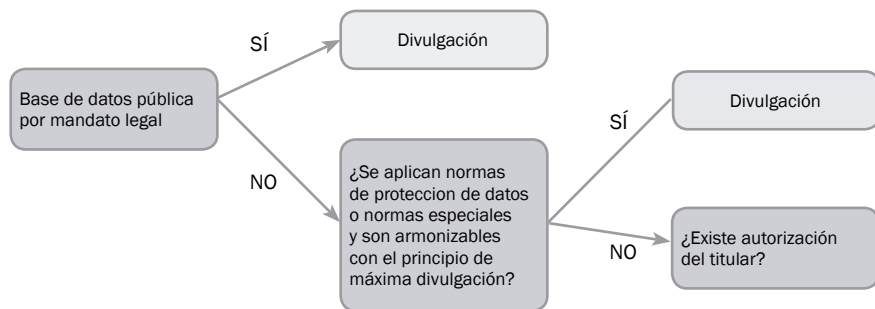
La anterior evolución de la línea jurisprudencial constitucional colombiana, que junto con la jurisprudencia interamericana señalan como idóneo el modelo dual de protección de la intimidad para personas de interés público y particulares comprende un esquema diferencial que combina una mayor garantía del derecho de acceso a la información pública, sin vulnerar el núcleo esencial del derecho a la intimidad y del derecho a la protección de los datos personales. Esta interpretación armónica resuelve tensiones de forma más garantista que la protección simple de la intimidad de funcionarios públicos, por lo que deberá preferirse. De otra forma, no se podrían mantener las conquistas derivadas de la progresividad de las libertades informativas y, por el contrario, se daría un paso atrás en la protección de los derechos fundamentales de libertad de expresión y acceso a la información pública.

Para terminar con esta aproximación que, para resolver la tensión entre la intimidad y el *habeas data*, por un lado, y el acceso a la información pública por otro, propone un criterio de armonización principal basado en la proporcionalidad y acompañado de dos criterios desarrollados jurisprudencialmente en torno a la delimitación de los derechos fundamentales, pasamos a las conclusiones generales del presente escrito.

Conclusiones generales

No resulta fácil definir cuál de los dos extremos en tensión debería primar en nuestro estudio de datos personales en información pública: ¿el acceso a la información pública como derecho fundamental en sí mismo e instrumental para el ejercicio de otros derechos como la libertad de expresión, la participación ciudadana, los derechos políticos y los derechos sociales? o ¿la intimidad, la autodeterminación personal o la libertad personal que encarnan el *habeas data*? Lo más sensato es considerar que no debe primar ninguno porque no hay jerarquía entre los derechos fundamentales y ninguno debe pesar más que el otro. En consecuencia, es importante buscar opciones en la armonización de los derechos en juego.

Como sostuvimos al comienzo de este escrito, los datos personales llegan a repositorios públicos por diversos motivos y surgen dificultades para discernir cuándo es legal y constitucional un rechazo de acceso a la información por razones de privacidad y cuándo no. Esto sucede porque existen múltiples datos personales que entregan las personas o recolectan terceros, incluido el mismo Estado, a través de censos, encuestas, registros públicos o incluso datos personales que quedan en Internet o en poder de proveedores de servicios y que luego constan en documentación pública. Cuando esos datos se encuentran en poder o bajo el control de personas que están obligadas a transparentar su actuación, se generan tensiones derivadas de la libertad informativa y la protección de la intimidad. Entonces, para contribuir en la definición de la discusión entre el acceso a la información o la protección de los datos personales, si los documentos públicos que contienen datos personales pueden divulgarse en su totalidad, si se divulgan los datos personales de un funcionario público que son necesarios para ejercer control social de su gestión, o si se divulgan aquellos que se requieren para hacer una investigación o un estudio que sirva de soporte a un documento de política pública, se debe aplicar el artículo 28 de la Ley TAIP que, al ser la única norma que se plantea la dificultad,



NOTA 1: La divulgación parcial es aplicable a los casos de circulación restringida y conlleva una versión pública con reserva/clasificación únicamente de la parte indispensable.

NOTA2: La reserva/clasificación opera respecto del contenido de un documento pero no de su existencia, salvo que la sola reserva ponga en evidencia la información negada.

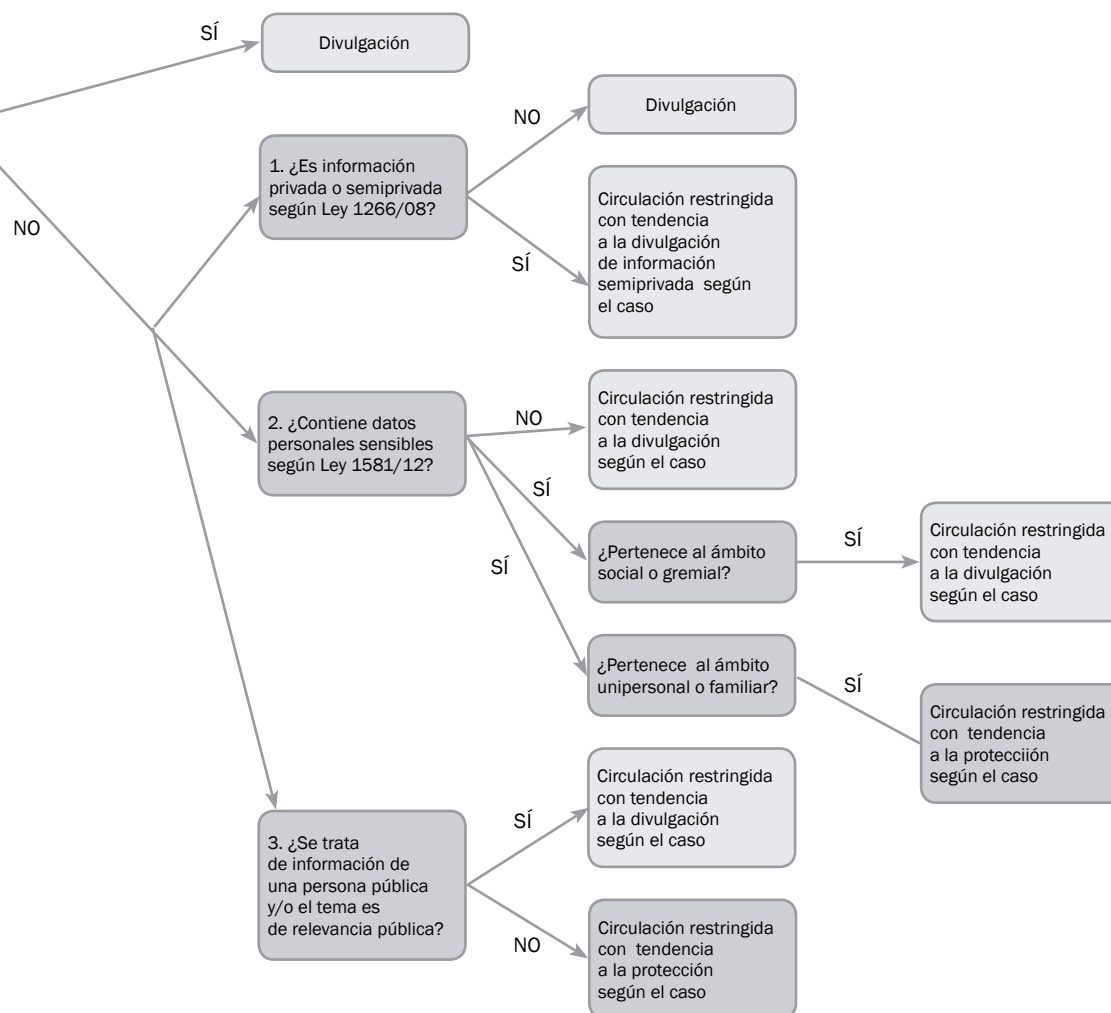
Ninguna autoridad pública puede negarse a indicar si un documento obra o no en su poder o negar la divulgación de un documento.

resulta la guía legislativa más adecuada para atender la tensión entre el *habeas data* y el acceso a la información pública.

En consecuencia, quien deba responder a una solicitud de acceso de bases de datos personales, deberá: i) definir si la base de datos o los datos que solicite la ciudadanía son un objetivo legítimo de protección que se enmarca dentro de lo consagrado en el artículo 15 de la CP y precisado en la Ley 1266 de 2008, en la Ley 1581 de 2012, o una tercera norma legal que precisa y explícitamente le otorgue protección; ii) establecer que se trate de la excepción a la privacidad prevista en el artículo 18 de la Ley TAIP, y iii) ponderar si la revelación de la información personal causaría un daño presente, probable y específico que exceda el interés público que representa el acceso democrático y ciudadano a dicha información.

El tercer paso consiste en valorar el daño, de tal suerte que sea cierto, objetivo y sustancial, no remoto o ínfimo, así como aportar las pruebas que acrediten la amenaza del daño en caso de que existan. Todo lo anterior apalancado en el razonamiento del juicio de proporcionalidad y de los límites de los derechos decantados por la propia jurisprudencia, para lo cual proponemos que en cada caso concreto la ponderación de derechos fundamentales en juego y los principios que los rigen sigan el siguiente camino representado, previamente al test de daño, en la gráfica 3.

GRÁFICA 3.
Lineamientos para valorar el acceso a datos personales en información pública



1. Comenzar definiendo si la información o el dato al que se pretende acceder es de naturaleza pública o privada por mandato legal o constitucional, pues ya existen algunos documentos que no presentan discusión en cuanto a su publicidad. Tal es el caso del registro público de la Cámara de Comercio, del registro civil, del registro servidores públicos o de aquellos registros que resultan del cumplimiento de funciones estatales.

2. Si hay claridad sobre la naturaleza pública de los datos, se debe proceder con un análisis de la normativa aplicable para definir si se aplican las normas de protección de datos o normas especiales. Si el ámbito de aplicación es de normativa especial, analizar si los principios de dicha normativa especial son armonizables con el principio de máxima divulgación. En particular, cuando los datos son catalogados como reservados o protegidos, hay una tendencia hacia su protección. Este es el caso de los datos en el registro único de víctimas (art. 29, Ley 1448 de 2011), la información tributaria (art. 583 Estatuto Tributario), los datos de personas acogidas al programa de protección de testigos, víctimas e intervinientes en el proceso penal (art. 5, Decreto 1843 de 1992), la información registrada bajo reserva bancaria, los libros y papeles del comerciante (arts. 61 a 62 del Código de Comercio), los registros de la Registraduría sobre la identidad de las personas como sus datos biográficos, su filiación y fórmula dactiloscópica (art. 51, Ley 96 de 1985) y la información de los suscriptores de un proceso de firma digital (art. 25, Decreto 1740 de 2000).
3. Establecer si existe autorización del titular para el tratamiento de datos, que debe incluir la publicidad de los mismos. Si existe la autorización, se pueden publicar esos datos.
4. Evaluar si se trata de información privada o semiprivada de conformidad con la Ley 1266 de 2008. Si la información es privada o semiprivada se debe aplicar el principio de circulación restringida.
5. Estudiar si el documento incluye datos personales, es decir, datos con los que se puede definir, distinguir e identificar personas. Si los datos no son personales, y se encuentran en un documento público, existe una tendencia a que prime el acceso a la información pública, pues el riesgo de daño a datos que no sirven para identificar a las personas es de menor entidad que la vulneración misma al derecho fundamental de conocer y acceder a la información pública.
6. Analizar si esos datos personales que componen las bases de datos son sensibles o no son sensibles. Con esto nos referimos a si son datos íntimos o si guardan en sí mismos un cierto riesgo o propensión a la discriminación por violación del derecho a la igualdad. Si los datos no son sensibles, existe la posibilidad de que prime el

acceso a la información pública, pues el riesgo de daño por divulgación de datos no sensibles puede ser de menor entidad que la vulneración misma al derecho fundamental de conocer y acceder a la información pública.

7. Establecer si los datos personales sensibles conllevan el riesgo de discriminación o violación a la intimidad. Para efectos de analizar si hay violación a la intimidad de datos personales, hay que estudiar a cuál ámbito de la intimidad pertenecen: a) a la esfera unipersonal o de información privada, b) a la esfera familiar o de información privada pero menos íntima, c) a la esfera de información semiprivada que interesa a ciertas personas únicamente pero no a toda la ciudadanía, o d) a la esfera de información gremial. Así, si los datos personales sensibles conllevan a) o b), la tendencia será de protección, y si conllevan c) o d) la tendencia de protección se relaja pues el grupo de interés es más amplio.
8. Especificar y acreditar el riesgo concreto o daño probable y específico a la discriminación, a la intimidad o a la autodeterminación, y compararlo con el riesgo que conllevaría mantener oculta información necesaria para la participación ciudadana y la transparencia, analizando el ámbito de aplicación que se encuentra involucrado. Entre mayor cercanía al núcleo duro de la intimidad (vida sexual, creencias personales, familia, vida social), se debe garantizar mayor protección a los datos personales, y entre más distancia con el núcleo duro de intimidad, mayor prevalencia al acceso a la información pública.
9. Establecer si estamos ante los datos personales de un funcionario público y, en ese caso, aplicar el enfoque diferencial de tal suerte que si la intimidad del funcionario afecta el núcleo esencial del interés público que motiva el interés de conocer dichos datos, existirá una tendencia mayor hacia la divulgación del contenido del documento público.
10. Si luego de hecho el test se concluye que el interés público exige la revelación de los datos personales, y que protegerlos causaría más daño que el que se genera al divulgarlos, se deberán hacer públicos o se podrá revelar una versión filtrada y parcial del documento que no permita la identificación de las personas si como resultado del anterior balance prevalece la protección a los datos personales.

ANEXO 1.

Selección de ley especial aplicable a bases de datos en la tensión entre *habeas data* y acceso a información pública

Como los datos personales se organizan en bases de datos, un criterio para proteger estos datos es establecer la legislación aplicable con apoyo en la cual se protege o rechaza el acceso a la información respectiva. Para nuestro estudio, es importante definir entonces si se trata de una base de datos que se rige por la Ley de *habeas data* sectorial (1266 de 2008), por la Ley de *habeas data* posterior (1581 de 2012), por la Ley de TAIP, por otras leyes especiales, o por una interpretación armoniosa de todas o algunas de las anteriores. En particular, analizaremos las normas de protección de datos personales que establecen su propio ámbito de aplicación y excluyen algunas bases de datos que deberán, sin embargo, en términos generales, regirse por sus principios.

La tipología que sugerimos emplear divide las bases de datos en dos categorías. Una primera atiende a conceptos de interés público como seguridad, inteligencia y justicia, asuntos que están esencialmente en manos de una persona pública, y la segunda categoría se refiere a bases de datos cuya custodia o tratamiento está a cargo de una persona privada que puede o no estar cumpliendo una función pública o prestando un servicio público como los registros de las cámaras de comercio y los de periodistas. No importa que algunos de esos registros sean públicos, lo clave en esta segunda categoría es la naturaleza de la persona natural o jurídica responsable de la base de datos.

Teniendo en cuenta que la Ley 1266 de 2008 es parcial y sectorial, partiremos de la Ley 1581 de 2012, que en su artículo segundo define su propio ámbito de aplicación. Esta ley se aplica a todos los datos de infor-

mación personal registrados en un banco de datos, sean estos administrados por entidades de naturaleza pública o privada. También se aplica a datos personales en territorio colombiano o extranjero, si el responsable o encargado del tratamiento está fuera del territorio nacional pero le es aplicable la legislación colombiana por normas y tratados internacionales.¹

Entonces, como punto de partida, el ámbito de protección de la Ley de *habeas data* posterior tiene una extensión superior a la de la Ley TAIP, pues esta última solo incluye como sujetos obligados a las personas privadas, en la medida en que administren fondos o recursos públicos, tengan función de autoridad pública, cumplan una función pública o presten un servicio público respecto de la información directamente relacionada con dicha prestación.² Además, la Ley TAIP no trasciende las fronteras colombianas.

Sin embargo, ni el carácter público o privado ni las conexiones con normas colombianas o extranjeras son el único criterio para definir las normas aplicables. La lista de bases de datos que el legislador excluyó de manera expresa es taxativa, pero larga. Y estas bases de datos excluidas o exceptuadas se regirán por los principios de protección de datos de esta ley estatutaria posterior en materia de datos personales, siempre y cuando no riñan “con los datos que tienen características de estar amparados por la reserva legal”. El texto entrecomillado corresponde al párrafo del artículo segundo de la Ley 1581 de 2012³ que establece una priorización de los principios regulados en dicha ley, sin importar que se trate de bases de datos exceptuadas o excluidas, pero exige una armonización con los prin-

cipios propios de la reserva legal que se encuentran definidos tanto en la Ley TAIP como en las leyes especiales de cada una de esas bases de datos.

Bases de datos con información de seguridad, inteligencia y justicia

Es frecuente, legítima y explicable la excepción del literal b) del artículo segundo de la Ley 1581 que establece que no regulará “las bases de datos y archivos que tengan por finalidad la seguridad y defensa nacional, así como la prevención, detección, monitoreo y control del lavado de activos y el financiamiento del terrorismo”. Se trata de proteger bienes e intereses públicos de justicia y seguridad.

Sin embargo, debemos notar los cambios que se dan del 2008 al 2012: en el 2008 la excepción en materia de justicia es amplia para bases de datos que sancionen delitos, y en el 2012 es estrecha y solo se refiere al lavado de activos y al terrorismo. En seguridad y defensa nacionales, la Ley 1581 de 2012 tiene un énfasis amplio que contrasta con la garantía de la seguridad nacional interna y externa, excluyente de la defensa, de la Ley de 2008. Los anteriores caprichos del legislador no tienen fácil explicación, pero, como primera anotación, creemos que la parcialidad regulatoria de la Ley de *habeas data* sectorial y la generalidad de la ley posterior apuntan a que cualquier solución deba pasar por privilegiar los contenidos de la ley posterior y general, es decir, la Ley 1581 de 2012. Así, la exclusión del régimen del *habeas data* debería aplicarse de manera restrictiva a bases de datos del lavado de activos y del financiamiento del terrorismo (y no a todas las bases de datos del sistema judicial) al igual que a las bases de datos que tengan por finalidad la seguridad y defensa nacional, muy similar pero al parecer con mayor cobertura que la sola seguridad interna y externa.

Independientemente de los cambios normativos del 2008 al 2012, y de la norma aplicable a las bases de datos judiciales, es importante tener en cuenta que en el 2012, la Corte Constitucional profirió la sentencia SU-458 en la que tuteló el derecho al *habeas data* de trece personas que interpusieron tutelas separadamente y exigió que el manejo de sus datos no contribuyera a su estigmatización. Las acciones de tutela que desataron esta sentencia de unificación involucran a trece personas que fueron condenadas penalmente. En el caso, a pesar de que una autoridad judicial había declarado la extinción de sus condenas o la prescripción de sus penas, en el certificado de antecedentes judiciales —que en ese momento administraba y expedía el Departamento Administrativo de Seguridad

- 1 No existen a la fecha tratados internacionales sobre tratamiento de datos que sean vinculantes para Colombia según informa la Superintendencia de Industria y Comercio en el radicado 13013509 del 7 de marzo de 2013, citado por Nelson Remolina Angarita (2013: 125).
- 2 Ver nota de pie de página 29 de dicha Ley, que transcribe el contenido del artículo 5 de la Ley 1712 de 2014.
- 3 El artículo segundo, párrafo de la Ley 1581 de 2012, establece: “Los principios sobre protección de datos serán aplicables a todas las bases de datos, incluidas las exceptuadas en el presente artículo, con los límites dispuestos en la presente ley y sin reñir con los datos que tienen características de estar amparados por la reserva legal. En el evento que la normatividad especial que regule las bases de datos exceptuadas prevea principios que tengan en consideración la naturaleza especial de datos, los mismos aplicarán de manera concurrente a los previstos en la presente ley”.

(DAS)— se leía: “registra antecedentes, pero no es requerido por autoridad judicial”. En la exposición de los hechos del caso, la Corte señaló que “[a]lgunos de los demandantes alegaron que esta práctica del DAS dificultaba la consecución de empleo; algunos afirmaron que habían sido despedidos o su contrato no renovado a causa de la exhibición del certificado judicial con el antedicho formato”. La Corte, entonces, precisó que:

...la publicidad indiscriminada de la información sobre antecedentes penales no cumple una finalidad legal o constitucional, no es útil ni necesaria. Por el contrario, considera la Corte que dicha información facilita el ejercicio incontrolado del poder informático, constituye una barrera de facto para el acceso o la conservación del empleo, y facilita prácticas de exclusión social y discriminación prohibidas por la Constitución.

Por esta razón, la Corte concedió la tutela y ordenó que en el certificado de antecedentes penales se utilizara otra leyenda que no permitiera inferir la existencia de antecedentes.

Una segunda excepción, la del literal c) del mismo artículo segundo de la Ley 1581, excluye las bases de datos que tengan objeto y contenido de inteligencia y contrainteligencia. En la Ley de *habeas data* sectorial se excluyen bases de datos atendiendo al criterio de entes responsables de la inteligencia y la seguridad (antiguo DAS y Fuerza Pública), mientras que la Ley de *habeas data* posterior es de mayor cobertura pues se refiere a todas las bases de datos relacionadas con la función de inteligencia y la contrainteligencia que, por aplicación de la Ley 1621 de 2013, es

...aquella que desarrollan los organismos especializados del Estado del orden nacional [...] con el objetivo de proteger los derechos humanos, prevenir y combatir amenazas internas o externas contra la vigencia del régimen democrático, el régimen constitucional y legal, la seguridad y la defensa nacional y cumplir los demás fines enunciados en la ley.

Lo que implica que una amplia gama de instancias desarrolla dicha función estatal y, en consecuencia, las bases de datos que crea o custodia se rigen por otras normas diferentes del *habeas data*, en este caso se registrarían por una norma especial.

Esta excepción de información de inteligencia en su sentido amplio también trató de incluirse en un párrafo en la Ley de TAIP. En dicha oportunidad, en el debate legislativo se trató de establecer un párrafo

segundo en el artículo quinto, según el cual toda la información, documentos, bases de datos y contratos relacionados con defensa y seguridad nacional, orden público y relaciones internacionales quedaban excluidos de la aplicación de la mencionada ley. No obstante, en su examen de constitucionalidad, la Corte consideró que una excepción tan amplia representaba negación del derecho a la información pública, lo que a su vez constituía, además de una voz contraria a los tratados internacionales, un impedimento al control ciudadano sobre las actuaciones de los servidores públicos y de las agencias estatales. Para el efecto, dijo la Corte: “Este tipo de expresiones genéricas o vagas constituye una habilitación general a las autoridades para mantener en secreto la información que discrecionalmente consideren adecuado, y es claramente contraria al artículo 74 CP”⁴

La remisión obligada es, entonces, a la ley especial. En consecuencia, debemos acudir a la propia ley de inteligencia y contrainteligencia (Ley 1621 de 2013 estatutaria y especial) cuyo capítulo quinto crea un centro de protección de datos de inteligencia y contrainteligencia en cada organismo que cumpla estas funciones. Dichos centros tendrán por finalidad controlar el ingreso y la salida de información a las bases de datos y archivos de inteligencia y contrainteligencia, garantizando de manera prioritaria su reserva constitucional y legal; asegurar que aquellos datos de inteligencia y contrainteligencia que una vez almacenados no sirvan para los fines establecidos sean retirados, y garantizar que la información no será almacenada en las bases de datos de inteligencia y contrainteligencia por razones de género, raza, origen nacional o familiar, lengua, religión, opinión política o filosófica, pertenencia a una organización sindical, social o de derechos humanos, o para promover los intereses de cualquier partido o movimiento político o afectar los derechos y las garantías de los partidos políticos de oposición. A su vez, el artículo 33 de dicha ley de inteligencia pareciera considerar reservada y, por tanto, secreta hasta por treinta años, toda información, documentos y elementos técnicos de los organismos que cumplen funciones de inteligencia y contrainteligencia, lo que incluiría los datos personales contenidos en estas bases de datos.

Sin embargo, no estimamos lógica esta conclusión en relación con la protección temporal de toda la información de estos centros de datos, pues no obedece a una lectura sistemática e integral. En efecto, si se analiza el estudio de este artículo hecho por la Corte, se concluye que no realizó

⁴ Corte Constitucional, sentencia C-274 de 2013, M. P. María Victoria Calle.

el test estricto de proporcionalidad que legitimaría en principio la reserva legal de esta información, limitándose a estudiar la constitucionalidad del término de treinta años para la reserva. Y no se ocupó la Corte de hacer tal examen de cumplimiento de las condiciones necesarias para exceptuar el principio general de acceso a la información, según lo viene exigiendo de tiempo atrás y que por supuesto realizó minuciosamente respecto de otros artículos de la misma ley, por varias razones: i) en el mismo artículo 33, parágrafo 2, se establece que cada organismo de inteligencia que pretenda cobijar con secreto la información que posee deberá hacer el test de proporcionalidad estricto; ii) en cinco artículos se consagró la reserva expresa de ciertos documentos de inteligencia, lo que hubiera sido inocuo si la reserva fuera general para toda la información, y iii) la interpretación integral del proceso analítico de la Corte Constitucional que decidió hacer un test de proporcionalidad de la reserva de cierta información pero dejó por fuera de este test el artículo 33, implica que no es viable la reserva general de la información que pudiera entenderse de una lectura rápida y superficial.⁵

Así, consideramos que la interpretación restrictiva de estas excepciones al *habeas data*, que a su vez lo son del acceso a la información pública, contribuyen a la garantía y protección de los derechos fundamentales que exceptúan. Pasemos entonces a la segunda categoría de bases de datos que se someten a norma especial.

Otras bases de datos con norma especial

Además de la justicia, la inteligencia en sentido amplio, y la seguridad y defensa nacional, existen otros fundamentos para la construcción y manipulación de bases de datos que también se acogen a regímenes especiales.

Nos referimos, como primera exclusión, a las bases de datos o archivos mantenidos en un ámbito exclusivamente personal o doméstico que no sean suministrados a terceros (en el momento en que se suministren a terceros los archivos se regirán por la Ley 1581 de 2012). Como segunda exclusión, la Ley de 2013 exceptúa de su ámbito de aplicación “las bases de datos y archivos de información periodística y otros contenidos edi-

toriales”, las de la Ley 79 de 1993 (sobre censos de población y vivienda) y las de la propia Ley 1266 de 2008 que ya hemos comentado, con un énfasis sectorial relativo a datos financieros, crediticios, comerciales, de servicios y de terceros países. Finalmente, el artículo segundo de la Ley de 2008 excluye de su ámbito de aplicación, de manera expresa, los registros públicos a cargo de las cámaras de comercio.

Para analizar las anteriores excepciones, es válido hacerlo por partes y lo haremos de los casos más fáciles a los más difíciles.

Primero, consideramos que la excepción de los datos domésticos es comprensible y no amerita mayor discusión pues se trata de datos que no circulan, por lo que la exclusión será aplicable en la medida de su no circulación. Los datos que circulan internamente no trascienden a terceros, pues permanecen en la misma fuente de información, la misma entidad, empresa o agente. Tómense como ejemplo las bases de datos caseras, las libretas telefónicas y los aparatos móviles que conjugan también los datos de nuestros corresponsales.

En este caso, la circulación externa cambiaría el régimen aplicable. No obstante no aplicarse la norma 1266 de 2008 por exclusión expresa, la Corte constitucional aclara que en todo caso “resultan predicables las garantías propias del derecho constitucional al *habeas data*, en cuanto resulten aplicables”, y, en caso de que el dato circule o trascienda a terceros,

serán exigibles todas las prerrogativas propias de la administración de datos personales, previstas en la Constitución y la norma estatutaria a favor del titular del dato. Especialmente, serán predicables los requisitos de autorización del sujeto concernido y especificidad de la materia del dato a aquellos de contenido comercial, crediticio, financiero, de servicios y proveniente de terceros países.⁶

Segundo, que los archivos y la información periodística y editorial gozan de una protección especial por contener las fuentes de información que constitucionalmente son reservadas, precisamente por la protección reforzada que tiene la libertad de expresión originada en la prohibición expresa a la censura de la Constitución Política. Además, porque la libertad de prensa que protege el artículo 20 de la Constitución Política amerita un cuidado especial para evitar la censura previa de contenidos, así

⁵ Estas razones son explicadas en otro escrito previo, en el cual argumentamos que bajo una lectura sistemática e integral de la sentencia de exequibilidad y de la propia ley de inteligencia la lógica señala que esta información no puede estar sometida a una reserva genérica (ver Uprimny y Newman 2013) Disponible en: www.dejusticia.org

⁶ Corte Constitucional, sentencia C-1011 de 2008, M. P. Jaime Córdoba Triviño.

como en general un juicio de proporcionalidad y razonabilidad propios en su tensión frente al *habeas data*.

Tercero, que la ley de censos de población y vivienda goza de sus propias reglas representadas principalmente en su artículo quinto, según el cual no hay acceso a la información del DANE derivada de censos y encuestas, ni por parte de la ciudadanía ni por parte de las autoridades públicas, salvo en “resúmenes numéricos” que no permitan la individualización de los contenidos para fines distintos de los estadísticos.⁷

Cuarto, que la Ley 1266 establece que los registros de las cámaras de comercio se registrarán “exclusivamente por las normas y principios consagrados en las normas especiales que las regulan”. Esta exclusión se deriva de la naturaleza de los tres registros que llevan las cámaras de comercio —el registro público mercantil, el registro de entidades sin ánimo de lucro y el de proponentes—, registros públicos en los que a todas luces debe primar el objetivo de publicidad y transparencia. En efecto, según el Código de Comercio (arts. 26 a 47) y las normas del registro público de proponentes, es al Estado y a la sociedad a quienes interesan los datos consignados en estos registros.⁸ Sin confundir, por supuesto, que los libros de los comerciantes no son datos personales pero tienen reserva constitucional y legal.⁹

7 Ley 79 de 1993, artículo 50. Las personas naturales o jurídicas, de cualquier orden o naturaleza, domiciliadas o residentes en el territorio nacional, están obligadas a suministrar al Departamento Administrativo Nacional de Estadística (DANE), los datos solicitados en el desarrollo de Censos y Encuestas. Los datos suministrados al DANE, en el desarrollo de los censos y las encuestas, no podrán darse a conocer al público ni a las entidades u organismos oficiales, ni a las autoridades públicas, sino únicamente en resúmenes numéricos, que no hagan posible deducir de ellos información alguna de carácter individual que pudiera utilizarse para fines comerciales, de tributación fiscal, de investigación judicial o cualquier otro diferente del propiamente estadístico.

8 El artículo 26 del Código de Comercio señala que “El registro mercantil tendrá por objeto llevar la matrícula de los comerciantes y los establecimientos de comercio, así como la inscripción de todos los actos, libros y documentos respecto de los cuales la ley exigiere esta formalidad. El registro mercantil será público. Cualquier persona podrá examinar los libros y archivos en que fuere llevado, tomar anotaciones de sus asientos o actos y obtener copia de los mismos”.

9 El artículo 61 del Código de Comercio consagra las excepciones a la reserva, así: “Los libros y papeles del comerciante no podrán examinarse por personas distintas de sus propietarios o personas autorizadas para ello, sino para los fines indicados en la Constitución Nacional y mediante orden de autoridad competente. Lo dispuesto en este artículo no restringirá el

No quiere esto decir, sin embargo, que por tener su propia normativa, no haya lugar a entregar la información pública que como sujeto obligado de la Ley TAIP le corresponde, o a desconocer la garantía de protección de datos personales que ofrece la Constitución Política. Esto último lo recordó la Corte en el análisis de exequibilidad de la Ley 1266 de 2008 cuando concluyó:

No obstante, sobre este particular la Sala considera oportuno aclarar que si bien la regulación de los registros públicos que administran las cámaras de comercio a través de normas especiales resulta constitucional, ello opera sin perjuicio de que [en] esos procesos de administración de datos personales resulten exigibles las prerrogativas y facultades que el derecho fundamental al *habeas data* consagra a favor del titular de la información.

Quinto, que la exclusión de la Ley 1266 de 2008 es extraña, pues ambas normas (la mencionada y Ley 1581 de 2013) parecieran o debieran ser complementarias y no excluyentes.

Al analizar la constitucionalidad de la norma de 2008, la Corte Constitucional la declara exequible pero llama la atención sobre la importancia de no afectar el principio general de publicidad de las actuaciones del Estado y el ejercicio del derecho a la información. La Corte asevera que el establecimiento de excepciones a ese principio de publicidad, no debe afectar las garantías del derecho a la información,

...por lo que solo serán oponibles aquellos modos de reserva o confidencialidad que i) tengan carácter excepcional y respondan a un criterio de proporcionalidad y razonabilidad; ii) estén expresamente previstas por el legislador; y iii) respondan a fines constitucionalmente legítimos, en especial la protección del derecho a la intimidad del sujeto concernido, cuando se trate de información personal de carácter privado que, según lo expuesto en esta sentencia, no tiene vocación de circulación, habida cuenta su vínculo inescindible con la órbita íntima y familiar del individuo.¹⁰

derecho de inspección que confiere la ley a los asociados sobre libros y papeles de las compañías comerciales, ni el que corresponda a quienes cumplan funciones de vigilancia o auditoría en las mismas”.

10 Corte Constitucional, sentencia C-1011 de 2008, M. P. Jaime Córdoba Triviño.

Aunado a lo anterior, la Corte asegura que la consagración de excepciones al principio de publicidad de las actuaciones del Estado, no lleva de suyo el desconocimiento del derecho al *habeas data*. En ese orden de ideas, aun en aquellos ámbitos donde no se aplique la Ley de *habeas data*, deberán permanecer vigentes las garantías, los derechos y los principios desarrollados en la propia ley y analizados en su sentencia de exequibilidad.

En conclusión, los registros de las cámaras de comercio deben mantener su máxima publicidad, pero sometidos a su propio ordenamiento, al igual que rigiéndose por la ley de TAIP pues cumplen función pública; las bases de datos domésticas no compartidas con terceros no se rigen por la ley de datos personales y no son consideradas domésticas las que constan en sistemas y documentos públicos y, por último, las bases de datos de inteligencia, seguridad y defensa nacional están excluidas de la aplicación de la Ley de *habeas data*, pero no de la aplicación de la Ley de TAIP, y, para su protección se requiere un test estricto de proporcionalidad, cuyos principios deberán prevalecer en una interpretación sistemática e integral en conjunto con la Ley de inteligencia y contrainteligencia. No obstante, todos los datos personales, aunque se rijan por leyes especiales, deben someterse a los principios, garantías y derechos del *habeas data* que sean armonizables.¹¹

11 Lo anterior, pues así lo establece el parágrafo del artículo segundo de la Ley 1581 de 2012 ya mencionado, como la sentencia 1011 de 2008 de la Corte Constitucional, M. P. Jaime Córdoba Triviño que dice de manera clara lo siguiente: “No obstante esta comprobación, la Corte advierte necesario estipular que la legitimidad constitucional de la consagración de ámbitos de exclusión a las reglas contenidas en el Proyecto de Ley no significa, de ningún modo, que tanto esos ámbitos, como todos aquellos en los que se llevan a cabo labores de recopilación, tratamiento y circulación de datos personales, estén excluidos de la protección que incorpora el derecho fundamental al *hábeas data* y, en general, la libertad y las demás garantías en la Constitución, según la fórmula establecida en el artículo 15 CP y conforme a los principios identificados por la jurisprudencia constitucional y descritos en el apartado 2 del presente análisis material. Por tanto, en cada una de las actividades de gestión de datos personales deberá cumplirse con el plexo de derechos, libertades y garantías propias del derecho fundamental al *habeas data*, según las consideraciones expresadas a lo largo de esta sentencia. Inclusive, la Sala advierte que las mismas normas de la ley estatutaria, en cuanto prevén los principios de administración de datos personales, al igual que los derechos y deberes de titulares, fuentes y usuarios, pueden servir de parámetro para la evaluación de la legitimidad de otras modalidades de tratamiento de información personal, en tanto dichos preceptos resulten pertinentes y aplicables”.

Referencias

- Botero, Catalina. 2009. *Informe de la Oficina del Relator Especial para la Libertad de Información*, OEA/Ser. L/V/II.134 Doc. 5, aprobado por la Comisión Interamericana de Derechos Humanos el 25 de febrero de 2009.
- Brandeis, Luis y Samuel Warren. 1890. *The Right to Privacy* IV (5). Consultado 19 de mayo de 2014. Recuperado de: http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html
- Camargo, Pedro Pablo. 2014. *Habeas Data, derecho a la intimidad*. Bogotá: Editorial Leyer.
- Cohen, Julie. 2000. “Examined Lives: Informational Privacy and the Subject as Object”. *Stanford Law Review* 52:1373.
- Coyle, Erin. 2009. “The Moral Duty of Publicity: Louis Dembitz Brandeis’ Crusades for Reform in the Press and Public Affairs, 1890-1916”. *Journalism History* 35:3. Recuperado de: <http://www.questia.com/library/journal/1P3-1900305841/the-moral-duty-of-publicity-louis-dembitz-brandeis>
- Garzón Valdés, Ernesto. 2008. “Lo íntimo, lo privado y lo público”. *Cuadernillo 6 del IFAI*, 140:1. Consultado 20 de junio de 2014. Recuperado de: <http://inicio.ifai.org.mx/Publicaciones/cuadernillo6.pdf>
- Kreimer, Seth. 1991. “Sunlight, Secrets and Scarlet Letters: The Tension Between Privacy and Disclosure in Constitutional Law”. *University of Pennsylvania Law Review*. Recuperado de: http://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=2410&context=faculty_scholarship
- Instituto Federal de Acceso a la Información Pública. 2003. “Lineamientos generales para la clasificación y desclasificación de la información de las dependencias y entidades de la Administración Pública Federal de México”. *Diario Oficial*, agosto 18. Consultado 13 de junio de 2014. Recuperado de: <http://www.conafor.gob.mx:8080/documentos/ver.aspx?articulo=4855&grupo=8>
- López Ayllón, Sergio y Alejandro Posadas. 2011. “Las Pruebas de daño e interés público en materia de acceso a la información. Una perspectiva comparada”. Consultado 13 de junio de 2014. Recuperado de: <http://www.juridicas.unam.mx/publica/rev/decoinc/cont/9/art/art2.htm>
- Matus Arenas, Jessica. 2013. “Derecho de acceso a la información pública y protección de datos personales”. *Revista chilena de derecho y tecnología*

2:1. Consultado 26 de junio de 2014. Recuperado de: <http://www.rchdt.uchile.cl/index.php/RCHDT/article/viewFile/26959/29080>

Novoa Monreal, Eduardo. 1979. *Derecho a la vida privada y libertad de información*. México: Siglo XXI.

Pierini, Alicia, Valentín Lorences, María Inés Tornabene. 1998. *Habeas Data, derecho a la intimidad*. Buenos Aires: Editorial Universidad.

Puccinelli, Oscar. 1999. *El Habeas Data en Indoiberoamérica*. Bogotá: Editorial Temis.

Quirós, José Justo Megías. 2002. "Privacidad e Internet: intimidad, comunicaciones y datos personales". *Anuario de Derechos Humanos. Nueva Época* 3. Consultado 19 de junio de 2014. Recuperado de: <http://revistas.ucm.es/index.php/ANDH/article/viewFile/ANDH0202110515A/20978>

"Reglas de Heredia". Consultado 1 de junio y 20 de julio de 2014. Recuperado de: http://www.iijusticia.org/heredia/Reglas_de_Heredia.htm

Salgado Seguí, Víctor. 2010. *Intimidad, privacidad y honor en Internet: nuestros derechos en riesgo*. Fundación Telefónica. Consultado 13 de junio de 2014. Recuperado de: http://telos.fundaciontelefonica.com/seccion=1268&idioma=es_ES&id=2010110409480001&activo=6.do

Remolina Angarita, Nelson. 2013. *Tratamiento de datos personales, aproximación internacional y comentarios a la Ley 1581 de 2012*. Bogotá: Legis.

Upegui, Juan Carlos. 2008. *Habeas Data Fundamentos, naturaleza, régimen*. Bogotá: Universidad Externado de Colombia.

Uprimny, Rodrigo, Adriana Fuentes, Catalina Botero y Juan Fernando Jaramillo. 2006. *Libertad de prensa y derechos fundamentales; análisis de la jurisprudencia constitucional en Colombia (1992-2005)*. Bogotá: Andiaros, Fundación Konrad Adenauer y Dejusticia.

Uprimny, Rodrigo y Vivian Newman. 2013. "Sub-reglas para acceder o rechazar el acceso a la información judicial y de seguridad nacional. Sistematización de la jurisprudencia constitucional en Colombia (2006-2012)". *Colección Más información, más derechos*. Recuperado de: <http://www.dejusticia.org/#/actividad/1515>

Urioste Braga, Fernando. 2008. *Derecho de la información*. Montevideo-Buenos Aires: Editorial Bdf.

• DOCUMENTOS 1

ETNORREPARACIONES: la justicia colectiva étnica y la reparación a pueblos indígenas y comunidades afrodescendientes en Colombia

Publicación digital e impresa

César Rodríguez Garavito, Yukyan Lam
2011

• DOCUMENTOS 2

LA CONSULTA PREVIA: DILEMAS Y SOLUCIONES. Lecciones del proceso de construcción del decreto de reparación y restitución de tierras para pueblos indígenas en Colombia

Publicación digital e impresa

César Rodríguez Garavito, Natalia Orduz Salinas
2012

• DOCUMENTOS 3

LA ADICCIÓN PUNITIVA:

La desproporción de leyes de drogas en América Latina

Publicación digital e impresa

Rodrigo Uprimny, Diana Esther Guzmán, Jorge Parra Norato
2012

• DOCUMENTOS 4

ORDEN PÚBLICO Y PERFILES RACIALES:

experiencias de afrocolombianos con la policía en Cali

Publicación digital e impresa

Yukyan Lam, Camilo Ávila
2013

• DOCUMENTOS 5

INSTITUCIONES Y NARCOTRÁFICO:

la geografía judicial de los delitos de drogas en Colombia

Publicación digital

Mauricio García Villegas, Jose Rafael Espinosa Restrepo, Felipe Jiménez Ángel
2013

• DOCUMENTOS 6

ENTRE ESTEREOTIPOS: Trayectorias laborales de mujeres y hombres en Colombia

Publicación digital

Diana Esther Guzmán, Annika Dalén
2013

• DOCUMENTOS 7

LA DISCRIMINACIÓN RACIAL EN EL TRABAJO:

Un estudio experimental en Bogotá

Publicación digital e impresa

César Rodríguez Garavito, Juan Camilo Cárdenas C., Juan David Oviedo M., Sebastián Villamizar S.
2013

• DOCUMENTOS 8

LA REGULACIÓN DE LA INTERRUPCIÓN VOLUNTARIA DEL EMBARAZO EN COLOMBIA

Publicación digital
Annika Dalén, Diana Esther Guzmán, Paola Molano
2013

• DOCUMENTOS 9

ACOSO LABORAL

Publicación digital
Diana Guzmán, Annika Dalén
2013

• DOCUMENTOS 10

ACCESO A LA JUSTICIA: Mujeres, conflicto armado y justicia

Publicación digital
Diana Esther Guzmán Rodríguez, Sylvia Prieto Dávila
2013

• DOCUMENTOS 11

LA IMPLEMENTACIÓN DE LA DESPENALIZACIÓN PARCIAL DEL ABORTO

Publicación digital e impresa
Annika Dalén
2013

• DOCUMENTOS 12

RESTITUCIÓN DE TIERRAS Y ENFOQUE DE GÉNERO

Publicación digital e impresa
Diana Esther Guzmán, Nina Chaparro
2013

• DOCUMENTOS 13

RAZA Y VIVIENDA EN COLOMBIA: la segregación residencial y las condiciones de vida en las ciudades

Publicación digital e impresa
María José Álvarez Rivadulla, César Rodríguez Garavito, Sebastián Villamizar Santamaría, Natalia Duarte
2013

• DOCUMENTOS 14

PARTICIPACIÓN POLÍTICA DE LAS MUJERES Y PARTIDOS. Posibilidades a partir de la reforma política de 2011.

Publicación digital
Diana Esther Guzmán Rodríguez, Sylvia Prieto Dávila
2013

• DOCUMENTOS 15

BANCADA DE MUJERES DEL CONGRESO: una historia por contar

Publicación digital
Sylvia Cristina Prieto Dávila, Diana Guzmán Rodríguez
2013

• DOCUMENTOS 16

OBLIGACIONES CRUZADAS: Políticas de drogas y derechos humanos

Publicación digital
Diana Guzmán, Jorge Parra, Rodrigo Uprimny
2013

• DOCUMENTOS 17

GUÍA PARA IMPLEMENTAR DECISIONES SOBRE DERECHOS SOCIALES

Estrategias para los jueces, funcionarios y activistas
Publicación digital e impresa
César Rodríguez Garavito, Celeste Kauffman
2014

• DOCUMENTOS 18

VIGILANCIA DE LAS COMUNICACIONES EN COLOMBIA El abismo entre la capacidad tecnológica y los controles legales

Publicación digital e impresa
Carlos Cortés Castillo
2014

• DOCUMENTOS 19

NO INTERRUPIR EL DERECHO Facultades de la Superintendencia Nacional de Salud en materia de IVE

Publicación digital
Nina Chaparro González, Annika Dalén
2015

La información personal llega a repositorios

públicos a través de censos, encuestas, registros o simplemente como rastro del uso de Internet. Cuando esos datos se encuentran en poder o bajo el control de personas que están obligadas a transparentar su actuación según la Ley de transparencia y acceso a la información pública (Ley 1712 de 2014), surgen dificultades para discernir cuándo es legal y constitucional rechazar su acceso y cuándo no, pues se generan serias tensiones. De un lado, está el acceso a la información pública, derecho fundamental en sí mismo e instrumental para el ejercicio de otros derechos como la libertad de expresión, la participación ciudadana y los derechos sociales y, de otro, la protección de la intimidad, la autodeterminación personal o la libertad personal que encarna el *habeas data* protegido por las leyes de datos personales (leyes 1266 de 2008 y 1581 de 2012).

Surgen, entonces, preguntas como: ¿frente a una solicitud ordinaria de acceso a la información de datos personales prima el acceso a la información o la protección de los datos personales? ¿Los documentos públicos que contienen datos personales pueden divulgarse en su totalidad? ¿Qué hacer si los datos se encuentran en una providencia judicial que es pública por esencia? Y si se trata de los datos personales de un funcionario público, que son necesarios para ejercer control social de su gestión, ¿también se protegen del escrutinio público? ¿Y si se trata de datos personales para hacer una investigación o un estudio que sirva de soporte a un documento de política pública? ¿Y si hay interés público en verificar, por ejemplo, la autenticidad de las firmas y existencia de los ciudadanos que votan por la revocatoria del mandato de un alcalde o gobernador elegido popularmente?

Para responder a los anteriores interrogantes, en este documento exploramos cuáles han sido las respuestas de la ley y la jurisprudencia colombianas frente a las tensiones entre la intimidad y la publicidad de los datos.

978-958-58858-1-3



9 789585 885813