EL HÁBEAS DATA EN LA ACTUALIDAD

Posibilidades y límites

Centro de Estudios Constitucionales
Tribunal Constitucional del Perú

EL HÁBEAS DATA EN LA ACTUALIDAD

Posibilidades y límites

EL HÁBEAS DATA EN LA ACTUALIDAD

Posibilidades y límites

DOCTRINA CONSTITUCIONAL

Coordinador
Luis R. Sáenz Dávalos

Centro de Estudios Constitucionales
Tribunal Constitucional del Perú

Colección «Doctrina Constitucional»
Ernesto Blume Fortini (dir.)

Centro de Estudios Constitucionales
Los Cedros núm. 209 · San Isidro · Lima

El hábeas data en la actualidad.
Posibilidades y límites
Luis R. Sáenz Dávalos (Coordinador)
Primera Edición: Noviembre 2020
Número de la Colección: 3

Hecho el Depósito Legal en la Biblioteca Nacional del Perú: N° 2020-08429
ISBN: 978-612-4464-04-1

Impreso en Perú
Tiraje: 500 ejemplares

Impresión: Q&P Impresores S.R.LTDA.
Av. Ignacio Merino N° 1546
Teléfono: 470 1788 Celular: 998 171 665
informes@qypimpresores.com

Contenido

Presentación

La incorporación en nuestro sistema jurídico de un proceso como el habeas data impuso, desde sus orígenes y más allá de las discusiones que en algún momento suscitó, la necesidad de abrir el debate académico sobre su naturaleza, reales alcances, límites y retos que implicaba, así como constituyó un desafío a la judicatura constitucional en la aplicación del mismo en las diversas controversias constitucionales que se presentaban, teniendo en cuenta la peculiaridad y especificidad de cada caso.

Ello fue así, porque a diferencia del habeas corpus y del amparo, que contaban con una indudable tradición en el derecho comparado y cuya recepción por nuestro constitucionalismo había dado lugar a un cierto desarrollo jurisprudencial, que se venía consolidando de a pocos, el habeas data apareció recién en los debates del Congreso Constituyente Democrático que tuvo el encargo del pueblo peruano de elaborar la Constitución de 1993, actualmente vigente, que lo incorporó en su Título V, dedicado a las garantías constitucionales, específicamente en el artículo 200°, inciso 3), en el que estipuló que el habeas data procede contra el hecho u omisión de cualquier autoridad, funcionario o persona que lesione o amenace los derechos a los que se refiere el artículo 2, incisos 5 y 6, de la Constitución; incisos que consagran, en esencia, el derecho fundamental de acceso a la información pública y el derecho fundamental a la autodeterminación informativa, respectivamente.

De otro lado, el manejo de la información en el mundo contemporáneo, caracterizado por el impresionante desarrollo de la tecnología comunicacional, presenta una serie de dimensiones provenientes de la avasalladora globalización, el avance de la cibernética, los progresos de

la telemática y, en general, la realidad virtual, entre otros aspectos, que constituyen todo un reto frente a lo que podríamos denominar la problemática comunicacional tradicional, emergente de las realidades vividas por la humanidad en los siglos XIX y XX, que reclaman respuestas acordes con tal modernidad y exigen ajustes en los instrumentos procesales de rescate, defensa y guardianía de los antes referidos derechos fundamentales.

Este último requerimiento ha llevado al Centro de Estudios Constitucionales a convocar a un grupo de especialistas para que aporten sus reflexiones sobre el proceso constitucional de habeas data a la luz de los nuevos tiempos, en la línea de procurar esas respuestas frente a los problemas propios de la llamada sociedad de la información. Todos ellos han colaborado con importantes contribuciones desde diversas, actuales e interesantes perspectivas, y el producto de tal esfuerzo es el volumen que en esta ocasión presento, el que viene a sumarse al repertorio bibliográfico de la institución que dirijo; volumen que sigue la línea trazada por mi antecesor, el Magistrado Carlos Ramos Núñez, a cuyo cargo estuvieron las obras colectivas referidas al proceso de amparo y al proceso de habeas corpus.

El presente colectivo cuenta con el valioso concurso de notables juristas extranjeros como Óscar Raúl Pucinelli (Argentina), Alan E. Vargas Lima (Bolivia), Martha Cecilia Paz (Colombia) y Artur Ricardo Ratc (Brasil). A ellos se suman los aportes de nuestros connacionales, Milushka Carrasco Gallardo, Luis R. Sáenz Dávalos, Leny Palma Encalada, Gonzalo Carlos Muñoz Hernández, Heidi Soraya Cárdenas Arce, María Candelaria Quispe Ponce, Susana Távara Espinoza, Bruno Novoa Campos, Lourdes Zamudio Salinas, Oscar Andrés Pazo Pineda, Sebastián Linares Luna, Enrique Pestana Uribe, Alfredo Orlando Curaca Kong, Astrid Kelly Cabezas Poma y Nadia Paola Iriarte Pamo.

A todos ellos mi sincero agradecimiento por sus valiosos aportes académicos, agradecimiento que extiendo al Director de Publicaciones y Documentación del Centro de Estudios Constitucionales, el profesor

Luis R. Sáenz Dávalos, por haber coordinado de manera eficiente la obra propuesta. Al respecto, anuncio que a esta le seguirán nuevas publicaciones relativas al resto de procesos constitucionales.

Finalmente, debo relievar que esta obra ha sido impulsada e implementada en el marco de las tareas que cumple el Centro de Estudios Constitucionales como órgano de investigación, académico y técnico de apoyo al desarrollo y cumplimiento de los objetivos del Tribunal Constitucional del Perú, en armonía con lo dispuesto por el artículo 22 de la Ley 28301, Ley Orgánica del Tribunal Constitucional del Perú.

Ernesto Blume Fortini
Director General del Centro de Estudios Constitucionales

Prólogo

El estudio de los procesos constitucionales definitivamente se hace más útil a la par que atractivo cuando la perspectiva que se asume no solo abarca una pluralidad de temas sistemáticamente seleccionados, sino cuando los enfoques que se otorgan a los mismos resultan totalmente abiertos, es decir, estructurados a partir de diversas visiones o corrientes de pensamiento.

Desde que se estableció la colección Doctrina Constitucional como una de las secciones de nuestro Centro de Estudios Constitucionales y se optó por promover publicaciones orientadas al análisis de cada uno de los instrumentos de protección de nuestra norma constitucional, se decidió que la opción de apostar por obras colectivas tenía que estar basada en la orientación variada. Carecería de todo sentido, que se pretenda hablar de un auténtico aporte doctrinario, cuando la explicación a dispensarse solo pueda encontrarse sustentada en un exclusivo y excluyente modo de entender las cosas.

Si los desarrollos que la jurisprudencia realiza de los institutos constitucionales desatan la necesidad de profundos debates o contrastes de opinión, está claro que el mejor producto académico reside en la existencia de una diversidad de pensamientos. Las convocatorias de grupos cerrados donde todos piensan de manera semejante o fotográficamente igual representa un remedo de academicismo donde las posiciones asumidas se traducen en autocomplacencias y maquillados pluralismos que en nada contribuyen a mejorar lo que por una u otra razón no se desenvuelve de la manera más adecuada o aun marchando en forma óptima, bien podría aspirar a un mayor desarrollo.

Es comprensible que el mundo académico a veces se contagie de una cierta dosis de perfeccionismo elitista, cuando se piensa que lo que se postula o defiende no admite otra posibilidad de visibilizarse. Pero ello a la larga resulta nocivo pues no permite la natural evolución o elemental depuración de defectos que toda institución jurídica se merece. La perspectiva del Centro de Estudios Constitucionales es decididamente y si nos atenemos a sus antecedentes, una distinta. Por ello y en cada oportunidad que se promueve estudios como el que ahora se presenta se procura que todos los pensamientos académicos sean recogidos independientemente de su orientación. Bajo tal contexto y mientras más abierta resulte la convocatoria, mucho más satisfactorio será el objetivo.

En esta ocasión y dando continuidad a los valiosos volúmenes que en el pasado se dedicaron a los procesos de amparo y de hábeas corpus, ahora se presenta un colectivo dedicado específicamente al proceso habeas data, instrumento que como bien lo sabemos, tuvo ciertos reparos en su recepción a nivel de nuestro Derecho, por lo menos en lo que fueron sus orígenes.

Reconocido como un mecanismo que por sus alcances podía generar ciertos riesgos, bien pronto mereció una reforma constitucional que lo circunscribió a lo que representa su verdadera naturaleza, la de proteger específicos derechos que siendo novedosos para lo que era nuestro constitucionalismo histórico, aparecían sin embargo como propios de una sociedad moderna y mucho más compleja que la tradicional.

Asumir el derrotero que ha venido recorriendo desde su reconocimiento hasta su posterior desarrollo legislativo y jurisprudencial, representa todo un reto que exigía tomar en cuenta variados temas que, como lo podrá observar el lector, han sido recogidos en el presente volumen.

Para cumplir con dicho propósito se convocó a un numeroso grupo de estudiosos no solo nacionales sino también extranjeros y que por una u otra razón ya habían abordado estos aspectos en algún otro momento o que mucho más recientemente han venido efectuado

valiosísimos aportes que vale la pena relievar. Naturalmente no todos los invitados pudieron acudir por diversas razones, pero los que lo han hecho han puesto lo mejor de sus esfuerzos para que este análisis resulte de singular utilidad. Ello nos motiva a seguir adelante y a emprender en un futuro próximo, desafíos similares con el resto de mecanismos de defensa de la Constitución.

Les estamos muy reconocidos a todas las personas que han colaborado en este colectivo, haciendo hincapié en la interesante paridad de género que en esta ocasión se puede apreciar y que ha permitido que un selecto grupo de académicos y académicas pueda participar. Sin proponernos tal resultado, ello se ha visto evidenciado, lo que de paso nos permite acreditar que los temas jurídicos contemporáneos viene despertando en todos quienes creen en el Derecho un interés cada vez más notorio que es de saludar y por supuesto fortalecer.

Nuestro agradecimiento final es para el Magistrado Ernesto Blume Fortini, Director General del Centro de Estudios Constitucionales, por haber apostado en nuestro concurso para coordinar la presente obra y por ratificar lo más positivo de la senda establecida por gestiones anteriores que habían puesto las primeras piedras para que el trabajo intelectual pudiera tener la relevancia y proyección que actualmente posee.

Coordinador

Luis R. Sáenz Dávalos

VIEJOS Y NUEVOS DERECHOS. VIEJOS Y NUEVOS TIPOS Y SUBTIPOS DE HÁBEAS DATA

A propósito de las novedades aportadas por el Reglamento General de Protección de Datos de la Unión Europea y los "Estándares" de la RIPD

Óscar Raúl Puccinelli*

1. Introducción

Cuatro generaciones de leyes de protección de datos se sucedieron hasta la actualidad y todas ellas trajeron novedades significativas que impactaron en el desarrollo de los principios que las regulan y de los derechos que reconocen. La primera generación arrancó en 1970, cuando recién aparecía Arpanet, con la primera ley de protección de datos del Länd de Hesse (Alemania) y se extendió hasta que se dictara el Convenio nº 108, del Consejo de Europa, "para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal" de 1981, que fue adoptado apenas antes del surgimiento de Internet y obligó a adecuar todas las leyes nacionales dictadas anteriormente.

* Doctor en Derecho por la Universidad de Buenos Aires. Doctor honoris causa por la Universidad Privada Antonio Guillermo Urrello (Cajamarca). Profesor adjunto en Derecho Constitucional de la Universidad Nacional del Rosario. Juez de la Sala Segunda de la Cámara de Apelación en lo Civil y Comercial de Rosario, Santa Fé, Argentina.

Esa segunda generación se extendió hasta la aprobación de la Directiva Europea 95/46, "relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos", que comenzó la tercera etapa, cuatro años después de que la *world wide web* se hiciera públicamente disponible, y provocó el dictado de nuevas leyes nacionales de adecuación a esa normativa y así como de otras relevantes reglas comunitarias que la fueron complementando.

La cuarta y por ahora última generación de leyes de protección de datos se inició a partir de la aprobación del Reglamento 2016/679 UE, "relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos" (RGPD), pero estas normas son mucho más escuetas que las anteriores, pues el reglamento, a diferencia de las leyes nacionales que se dictaron para ajustarse a la Directiva que deroga, es directamente aplicable en todos los Estados parte sin necesidad de la adopción de normas de transposición nacionales y por lo tanto no deben reiterar conceptos vertidos en el reglamento (ver en este sentido, v.gr., en el caso español, las sustanciales diferencias entre la "Ley Orgánica de Protección de Datos de Carácter Personal" 15/99 (LOPD) y la Ley Orgánica 3/2018 "de Protección de Datos Personales y garantía de los derechos digitales").

Si bien ya desde aquellos tiempos de Arpanet y de los sistemas de información mecanizados fueron gradualmente reconociéndose nuevos derechos, los mayores avances respondieron a los vertiginosos desarrollos de las TICs que provocara la aparición de la "web 2.0", la "web participativa", donde la aparición y desarrollo de las redes sociales y múltiples desarrollos tecnológicos (v.gr., los smartphones, la tecnología para llevar puesta, el big data, la computación en la nube, la inteligencia artificial, etc.) cambiara sustancialmente el panorama precedente y en un contexto donde ya no serían sólo los gobiernos, las universidades y las empresas los principales proveedores de información en la red, comenzaron a generarse nuevos riesgos para las personas en lo relativo

al tratamiento de sus datos personales y con ello la preocupación por generar nuevas herramientas jurídicas para la protección de éstos y de los derechos que en definitiva se pretenden cobijar a través de su tutela.

Así, en este último tramo que recién se inicia, se produjo el cambio normativo más sustancial desde que fueran dictadas las primeras leyes de protección de datos, en un fenómeno simétrico al vivenciado cuando Warren y Brandeis, en 1890, publicaran su célebre opúsculo "*The right to privacy*", en la *Harvard Law Review*, propiciando el reconocimiento de nuevos derechos frente a los avances tecnológicos (en especial, la fotografía, el telégrafo y la prensa rotativa) que estaban permitiendo una grave intrusión en la vida íntima de las personas[1].

[1] Entre sus interesantes reflexiones puede leerse: "Que el individuo debería tener protección de su persona y sus propiedades es un principio tan antiguo como la ley, pero de vez en cuando es necesario definir de nuevo la naturaleza exacta y el alcance de esa protección. Los cambios políticos, sociales y económicos, suponen el reconocimiento de nuevos derechos, y el *common law*, en su eterna juventud, debe crecer para satisfacer las nuevas demandas de la sociedad.

"Así, en los primeros tiempos, el *common law* dio un remedio a la interferencia física con la vida y la propiedad. Más tarde se reconoció la naturaleza espiritual del hombre, de sus sentimientos y de su intelecto. Poco a poco el alcance de estos derechos se amplió y ahora el derecho a la vida se convirtió en el derecho a disfrutar de la vida –el derecho a ser dejado solo, a asegurar el ejercicio de los amplios privilegios civiles, y el término "propiedad" ha crecido hasta incluir toda forma de posesión, tanto tangible como intangible–... lo que se refiere a las emociones humanas pronto se extendió el alcance de la inmunidad personal más allá del cuerpo del individuo, a su reputación y el prestigio entre sus semejantes… se protegieron las relaciones familiares… De bienes corporales surgieron los derechos inmateriales que emiten fuera de él…

"Invenciones recientes y métodos comerciales llaman la atención sobre el siguiente paso que debe tomarse para la protección de la persona, y para asegurar que el individuo lo que el juez Cooley llama el derecho "a ser dejado solo".

"Fotografías instantáneas y periódicos han invadido el sagrado recinto de la vida privada y doméstica; y numerosos dispositivos mecánicos amenazan con hacer buena la predicción de que 'lo que se susurraba en el armario será proclamado desde los tejados'.

"Durante años se ha producido una sensación de que la ley debe permitirse algún remedio para la circulación no autorizada de retratos de personas privadas y el mal de la invasión de la privacidad de los periódicos… De la conveniencia –de hecho, de la necesidad– de alguna tal protección, no puede dudarse. La prensa está excediendo en todas las direcciones de los límites evidentes de la polémica y de la decencia… La intensidad

Con el marco regulatorio emergente de las leyes de protección de datos de la tercera generación, apareció en Iberoamérica una acción constitucional específica para la protección de los datos personales, que se despliega también a través de un proceso constitucional específico: el hábeas data de la Constitución del Brasil de 1988, norma que generó una inmediata adhesión en prácticamente todas las reformas constitucionales sucesivas de la región.

En el caso del Perú, la Constitución de 1993 consagró la acción de hábeas data en el artículo 200, inc. 3, el cual, reformado en 1995, limitó al instituto a la tutela de los derechos reconocidos por el artículo 2, incs. 5 y 6, que regulan, respectivamente los derechos de acceso a la información pública y a la protección de los datos personales[2]. La norma fue reglamentada inmediatamente, en lo procesal, por la ley 26.301, "de hábeas data y acción de cumplimiento", que fue sustituida con la entrada en vigencia del Código Procesal Constitucional (ley 28.237, de 2004). Ya con respecto a los derechos de fondo (que son los que enriquecen la tipología de los hábeas data), éstos están desarrollados por las leyes 27.806 de transparencia y acceso a la información pública, y 29.733, de protección de datos, además de las normas secundarias dictadas por las sucesivas autoridades de aplicación de ambas leyes, actualmente la Autoridad Nacional de Protección de Datos Personales (ANPD) y la Autoridad Nacional de Transparencia y Acceso a la Información Pública (ANTAIP), ambas concentradas dentro de la órbita del Ministerio de Justicia y Derechos Humanos.

y la complejidad de la vida, concomitantes con el avance de la civilización, han hecho necesario un poco de retiro del mundo, y el hombre, bajo la influencia refinadora de la cultura, se ha vuelto más sensible a la publicidad, por lo que la soledad y la privacidad se han vuelto más esenciales para el individuo… el individuo tiene derecho a decidir si lo que es suyo habrá de darse a publicidad..." (Samuel Warren y Louis Brandeis, "The Right to Privacy", Harvard Law Review, vol. IV, núm. 5, 15/12/1890, págs. 194/220).

[2] Originalmente también cubría el inc. 7 (que regula los derechos al honor, a la buena reputación, a la voz, a la imagen y a la intimidad personal y familiar, además de reconocer específicamente el derecho de réplica), remisión que fue eliminada por la ley 26.470, de 1995.

En tiempos de la reforma constitucional del artículo 200, y partiendo de la primigenia clasificación de Sagüés de los tipos emergentes de la Constitución argentina[3], realizamos por aquél entonces una primera clasificación tentativa de los tipos y subtipos de hábeas data vigentes en Latinoamérica, en la que no nos limitamos a la tipología constitucional sino que también abarcamos la emergente de las normas sobre protección de datos europeas, y en posteriores versiones de ese primigenio artículo, fuimos incorporando los de las leyes que se fueron dictando en la región (proceso que ocurrió y sigue ocurriendo gradualmente desde la aprobación de la ley chilena de 1999, de protección de la vida privada y la ley de protección de datos argentina, de 2000).

Mucha agua ha pasado bajo el puente desde entonces y recientes desarrollos normativos han reconocido nuevos principios y derechos específicos en el marco de la protección de datos, de modo que aquellas primitivas tipologías se tornaron claramente insuficientes y ameritan ser actualizadas, ajustándolas especialmente a los nuevos paradigmas que propone el RGPD[4], cuya relevancia deviene no sólo de ser el instrumento más potente y actualizado en la materia (fue aprobado en abril de 2016 y entró plenamente en vigencia desde el 25 de mayo de 2018), sino de haber sido recogido por los "Estándares de Protección de Datos Personales para los Estados Iberoamericanos"[5], un relevante instrumento de *soft law* aprobado en 2017 por la Red Iberoamericana de Protección de Datos (RIPD), elaborado consensuadamente por las autoridades de control iberoamericanas con competencias específicas sobre protección de datos que integran la RIPD.

[3] Néstor P. Sagüés, "Subtipos de Hábeas data", J.A. 20/12/95, pág. 31 y sigs.

[4] "Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)", disponible en https://www.boe.es/doue/2016/119/L00001-00088.pdf.

[5] Disponibles en https://www.redipd.org/sites/default/files/inline-files/Estandares_Esp_Con_logo_RIPD.pdf.

A fin de mostrar correctamente las diferencias entre la tipología previa a estos dos instrumentos y a la ampliada por efecto de la aparición de éstos, volcaremos primeramente la clasificación realizada en 2008 por el Tribunal Constitucional peruano (la cual, en gran medida, aunque con terminología diferente, coincide con la nuestra[6]), para luego analizar los avances normativos provocados por el RGPD y los "Estándares" de la RIPD y, finalmente, volcarlos en nuestra *aggiornada* clasificación.

2. La tipología adoptada por el Tribunal Constitucional Peruano

Con base en los artículos 200, inc. 3 y 2, incs. 5 y 6 de la Constitución y en las normas del Código Procesal Constitucional, el Tribunal Constitucional peruano (TC, en adelante) delineó los distintos tipos de hábeas data vigentes en el Perú, en una muy citada "sentencia académica", en la que consideró expedirse al respecto por considerarlo "pertinente, a efectos de cumplir la función pedagógica de sus resoluciones, precisar los tipos de hábeas data que se encuentran establecidos tanto en la Constitución Política (art. 200, inciso 3) como en el Código Procesal Constitucional (art. 61°)".

Al realizar esa clasificación aclara el Tribunal que, pese a que el código "hace una relación de los posibles casos de acumulación objetiva, las pretensiones en el hábeas data no tienen por qué entenderse como limitadas a los casos que establece la ley", y que por ello puede "extender su alcance protector a otras situaciones o alternativas que pudiesen darse en la realidad", dado que la propuesta "del artículo 64° es simplemente enunciativa".

Hechas estas aclaraciones, la sentencia trata, literalmente, la existencia de los siguientes tipos de hábeas data, del siguiente modo:

[6] Oscar R. Puccinelli, "Tipos y subtipos de hábeas data en el derecho constitucional latinoamericano. A propósito del hábeas data peruano para acceder a información pública". La Ley, Buenos Aires, Tomo 1997-D, 215.

"**I. Hábeas Data Puro**: Reparar agresiones contra la manipulación de datos personalísimos almacenados en bancos de información computarizados o no.

"**1.1. Hábeas Data de Cognición**: No se trata de un proceso en virtud del cual se pretende la manipulación de los datos, sino efectuar una tarea de conocimiento y de supervisión sobre la forma en que la información personal almacenada está siendo utilizada.

"**1.1.1. Hábeas Data Informativo:** Está dirigido a conocer el contenido de la información que se almacena en el banco de datos (qué se guarda).

"**1.1.2. Hábeas Data Inquisitivo:** Para que se diga el nombre de la persona que proporcionó el dato (quién).

"**1.1.3. Hábeas Data Teleológico:** Busca esclarecer los motivos que han llevado al sujeto activo a la creación del dato personal (para qué).

"**1.1.4. Hábeas Data de Ubicación:** Tiene como objeto que el sujeto activo del poder informático responda dónde está ubicado el dato, a fin de que el sujeto pasivo -el accionante- pueda ejercer su derecho (dónde).

"1.2. Hábeas Data Manipulador: No tiene como propósito el conocimiento de la información almacenada, sino su modificación.

"1.2.1. Hábeas Data Aditivo: Agrega al banco de datos una información no contenida. Esta información puede consistir: en la actualización de una información cierta pero que por el paso del tiempo se ha visto modificada; también puede tratarse de una información que tiene como objeto aclarar la certeza de un dato que ha sido mal interpretado; o incorporar al banco de datos una información omitida que perjudica al sujeto pasivo.

"1.2.2. Hábeas Data Correctivo: Tiene como objeto modificar los datos imprecisos y cambiar o borrar los falsos.

"1.2.3. Hábeas Data Supresorio: Busca eliminar la información sensible o datos que afectan la intimidad personal, familiar o cualquier otro derecho fundamental de la persona. También puede proceder

cuando la información que se almacena no guarda relación con la finalidad para la cual ha sido creado el banco de datos.

"1.2.4. Hábeas Data Confidencial: Impedir que las personas no autorizadas accedan a una información que ha sido calificada como reservada. En este tipo, se incluye la prohibición de datos que por el paso del tiempo o por sentencia firme se impide su comunicación a terceros.

"1.2.5. Hábeas Data Desvinculador: Sirve para impedir que terceros conozcan la identificación de una o más personas cuyos datos han sido almacenados en función de determinados aspectos generales como la edad, raza, sexo, ubicación social, grado de instrucción, idioma, profesión.

"1.2.6. Hábeas Data Cifrador: Tiene como objeto que el dato sea guardado bajo un código que sólo puede ser descifrado por quien está autorizado a hacerlo.

"1.2.7. Hábeas Data Cautelar: Tiene como propósito impedir la manipulación o publicación del dato en el marco de un proceso, a fin de asegurar la eficacia del derecho a protegerse.

"1.2.8. Hábeas Data Garantista: Buscan el control técnico en el manejo de los datos, a fin de determinar si el sistema informativo, computarizado o no, garantiza la confidencialidad y las condiciones mínimas de seguridad de los datos y su utilización de acuerdo con la finalidad para la cual han sido almacenados.

"1.2.9. Hábeas Data Interpretativo: Tiene como objeto impugnar las valoraciones o conclusiones a las que llega el que analiza la información personal almacenada.

"1.2.10. Hábeas Data Indemnizatorio: Aunque no es de recibo en nuestro ordenamiento, este tipo de hábeas data consiste en solicitar la indemnización por el daño causado con la propalación de la información.

"2. Hábeas Data Impuro: Solicitar el auxilio jurisdiccional para recabar una información pública que le es negada al agraviado.

> **"2.1. Hábeas Data de Acceso a Información Pública:** Consiste en hacer valer el derecho de toda persona a acceder a la información que obra en la administración pública, salvo las que están expresamente prohibidas por la ley"[7].

3. Los nuevos contenidos aportados por el Reglamento 2016/679 UE (RGPD) a la protección de los datos personales

Esta novel norma comunitaria fue adoptada luego de un intenso proceso de elaboración participativa, en especial de las autoridades de protección de datos instauradas en los países europeos, y responde a la necesidad de dar nuevas respuestas normativas a los avances tecnológicos habidos desde la aprobación de la Directiva 95/46, en especial por la aparición de la "web 2.0" (la web "participativa", donde se incorporan las redes sociales, la computación en la nube, la internet de las cosas y los datos masivos, entre otros nuevos fenómenos), cuyos acelerados desarrollos empezaron a reconfigurar la red hacia nuevos formatos, en concreto una web semántica ("web 3.0") que nos prepara para la etapa tal vez final de la "web 4.0" (la web "simbiótica", que se redimensionará permanentemente a partir de los desarrollos de la robótica, las nanotecnologías, la inteligencia artificial, etc.).

Puesto de modo sintético, este nuevo Reglamento, de cara a dichos avances, realiza una serie de modificaciones al marco normativo anterior vigente (al Directiva 95/46, que deroga), siendo las relevantes las siguientes:

a) Se extiende subjetivamente de modo expreso el alcance de sus disposiciones a responsables o encargados de tratamiento de datos no establecidos en la Unión Europea que realicen tratamientos derivados de una oferta de bienes o servicios

[7] EXP. N. 0 06164-2007-HD/TC - AREQUIPA - JHONNY ROBERT COLMENARES JIMÉNEZ - 21/12/07, disponible en https://tc.gob.pe/jurisprudencia/2008/06164-2007-HD.pdf.

destinados a ciudadanos de la Unión o como consecuencia de una monitorización y seguimiento de su comportamiento, quienes quedan sujetos a la norma y por ello deben designar representantes en la Unión Europea que actuarán como punto de contacto de las autoridades de supervisión y de los ciudadanos.

b) Sobre el principio del consentimiento para el tratamiento de los datos personales, se exige que sea libre, informado, específico e inequívoco (mediante una declaración de los interesados o una acción positiva que indique el acuerdo, pero no puede deducirse del silencio o de la inacción) y además, para ciertos tratamientos (v.gr., los datos sensibles, cuyo listado se amplía a los datos genéticos y biométricos y a las infracciones y condenas penales, aunque no las administrativas), se exige que sea explícito y verificable.

Se introducen reglas específicas sobre el consentimiento de los menores en los servicios de la sociedad de la información, quienes pueden prestarlos autónomamente a partir de los 16 años (aunque cada Estado puede rebajarlo a no menos de los 13 años de edad, y en esta dirección, v.gr., España lo fijó en 14 años). Dicho consentimiento además debe ser verificable y el aviso de privacidad debe estar redactado en un lenguaje que puedan entender.

c) Se agregan los principios de transparencia e información, por virtud de los cuales las políticas de privacidad y los avisos legales deben ser más simples, inteligibles y completos, incluso a través de íconos normalizados. Por consecuencia, las empresas deben revisar sus avisos de privacidad, rediseñándolos en un lenguaje claro y conciso, la base legal para el tratamiento de los datos, los períodos de retención y el derecho de los interesados de dirigir sus reclamaciones a las autoridades de protección de datos.

d) Se reconoce explícitamente derecho a la limitación del tratamiento, donde el titular del dato puede solicitar el bloqueo temporal del tratamiento de sus datos cuando existan controversias sobre su licitud, tal como en el caso argentino está previsto en la ley de protección de datos personales, al prever las medidas cautelares que pueden solicitarse dentro de un proceso de hábeas data.

e) Se incorporan dos nuevos derechos: al olvido (anteriormente reconocido por el Superior Tribunal de Justicia de la Unión Europea en el célebre caso "Costeja") y a la portabilidad de los datos, que implica la posibilidad de transferirlos en formatos interoperables, en concreto, que permitan su reutilización por parte del titular de los datos o de otro responsable.

f) Se adiciona además el principio "responsabilidad proactiva" (*accountability*) que se traduce en los de prevención y actuación proactiva por parte de los responsables y encargados del tratamiento, trasladándose a las organizaciones el deber de demostrar que cumple con tales exigencias. En la misma dirección, se promueve la utilización de sellos y certificaciones y se limita la posibilidad de selección del encargado del tratamiento por parte del responsable del tratamiento, dado que deberá elegir alguno que aporte suficientes garantías de cumplimiento normativo.

g) Se agregan los principios de protección de datos desde el diseño y por defecto (hardware y software deben ser diseñados para proteger la privacidad ya desde el diseño mismo de los sistemas y aplicaciones, y, además, v.gr., en las opciones que otorgan estas últimas al momento de la instalación, se debe ofrecer como primera opción la que más protege a la privacidad del individuo. Se intenta garantizar así el cumplimiento de la norma desde el mismo momento en que se diseñe una empresa, producto, servicio o actividad que implique tratamiento de dato, como regla y desde el origen).

h) Se exige a los responsables y encargado del tratamiento el mantenimiento de un registro de tratamientos como medio de control interno que sustituye a la obligación de inscribir los ficheros y se prevén garantías más estrictas y mecanismos de seguimiento respecto de las transferencias de datos fuera de la UE.

   También se los obliga la realización de evaluaciones de impacto sobre la privacidad frente a nuevos tratamientos (donde se establezcan los riesgos específicos de tratar ciertos datos y se prevean medidas para mitigar o eliminar dichas amenazas) y al nombramiento de un delegado de protección de datos (DPO), interno o externo (un técnico similar al oficial de privacidad que voluntariamente tienen muchas empresas), quien deberá asistir a las organizaciones en el proceso de cumplimiento, actuando como un verdadero delegado de la autoridad de control.

   Se establece la obligación de notificación inmediata a la autoridad de control y en algunos casos a los titulares de datos acerca del acaecimiento de incidentes de seguridad, y se refuerzan las medidas de seguridad, que deben aplicarse considerando especialmente el tipo de tratamiento de que se trate, los costos de implantación o el riesgo que el tratamiento presenta para los derechos y libertades, y todas las organizaciones que tratan datos deben realizar un análisis de riesgo de sus tratamientos.

   Finalmente, en este aspecto, se destaca la promoción de códigos de conducta sectoriales y esquemas de certificación ante la autoridad de control.

i) Se fortalece el sistema de control institucional, creándose el sistema de "ventanilla única", de modo que las empresas multinacionales tendrán como interlocutora a una sola autoridad de control nacional, en concreto la del establecimiento

principal de la entidad), y se concibe un procedimiento de cooperación entre autoridades de los países involucrados, de forma tal que un afectado puede dirigirse a su autoridad de control para que atienda a los reclamos contra responsables establecidos en varios Estados miembros o que, estando en uno, hagan tratamientos que afecten significativamente a ciudadanos en varios.

También se dispone que las denuncias podrán ser presentadas a través de asociaciones de usuarios y que pueden exigirse indemnizaciones de los daños y perjuicios derivados del tratamiento indebido de los datos personales.

Se agrava, asimismo, el marco sancionatorio, previéndose multas severas a quienes violen las reglas emergentes del Reglamento (incluso si fueran Administraciones públicas, aunque cada Estado puede optar por excluirlas), para cuya graduación se puede considerar el volumen de negocios de la empresa que incurra en infracción a dichas normas (en concreto, las sanciones pueden llegar a 20 millones de Euros o el 4% de la facturación global anual).

Por último, en cuanto a las controversias que puedan surgir entre las autoridades, se deriva su resolución al Comité Europeo de Protección de Datos (organismo integrado por los directores de todas las autoridades de protección de datos de la UE).

4. Los "Estándares de protección de datos personales para los Estados Iberoamericanos" de la RIPD.

En junio de 2017, en el marco del XVI Encuentro Iberoamericano de la Red Iberoamericana de Protección de Datos (RIPD) celebrado en Santiago de Chile, se aprobaron los "Estándares de Protección de Datos Personales para los Estados Iberoamericanos", que con el apoyo de la propia Comisión Europea han supuesto un verdadero

revulsivo para la regulación de la protección de los datos personales en la región. Se trata de un documento de *soft law* que consta de 26 considerandos y 45 artículos, distribuidos en 10 capítulos que siguen, en líneas generales, los parámetros del RGPD europeo, y que, conforme se expresa al final de sus considerandos, es adoptado a fin de contribuir, con el carácter de directrices orientadoras, a la emisión de iniciativas regulatorias de protección de datos personales en la región de los países que aún no cuentan con estos ordenamientos, o en su caso, sirvan como referente para la modernización y actualización de las legislaciones existentes.

Entre sus considerandos se destaca, respecto del derecho a la protección de las personas físicas en relación con el tratamiento de sus datos personales; que éste es un derecho fundamental y autónomo que difiere de los derechos a la vida privada y familiar, a la intimidad, al honor, al buen nombre y otros derechos similares; que tiene por objeto salvaguardar el poder de disposición y control que tiene toda persona física con respecto a la información que le concierne fundamentalmente en atención al empleo de las tecnologías de la información y las comunicaciones que cobran cada vez mayor relevancia en todos los quehaceres de la vida cotidiana, y que es un derecho que puede extenderse a las personas jurídicas según lo disponga cada ordenamiento interno.

Se recuerda luego que la RIPD, en la reunión celebrada en Santa Cruz de la Sierra, Bolivia, en 2006, elaboró las "Directrices para la Armonización de la Protección de Datos en la Comunidad Iberoamericana" (el antecedente de estos Estándares); que la Unión Europea adoptó el RGPD, marco normativo que se posiciona como un referente obligado y determinante para la elaboración de las legislaciones nacionales de protección de datos en Iberoamérica, y que ante la falta de armonización en los Estados Iberoamericanos respecto al reconocimiento, adopción, definición y desarrollo de las figuras, principios, derechos y procedimientos que dan contenido al derecho a la protección de datos personales resulta apremiante, en el marco de una constante innovación

tecnológica, la adopción de instrumentos regulatorios que garanticen la protección de las personas y el libre flujo de los datos personales para el desarrollo, fortalecimiento e intercambio de bienes y servicios en una economía global y digital.

Se pone de resalto también que se debe garantizar un nivel alto de protección de los derechos y libertades de las personas y que es imperioso establecer un equilibrio entre los intereses de todos los actores del sector público, privado y social y titulares involucrados, incluyendo el establecimiento de excepciones por cuestiones de interés público que sean razonables y compatibles con los derechos y libertades, para evitar incurrir en restricciones o limitaciones injustificadas o desproporcionadas que no sean acordes con los fines perseguidos en sociedades democráticas.

Se afirma asimismo que los riesgos potenciales por el tratamiento de datos a gran escala efectuado por parte de organismos públicos y privados afecta especialmente a sectores vulnerables como las niñas, niños y adolescentes, cuyos intereses superiores cabe preservar; que es necesario arribar a un consenso mínimo respecto de la categorización de los datos sensibles o especialmente protegidos y establecer reglas uniformes para su tratamiento, y que no todos los Estados Iberoamericanos tienen legislación en la materia por lo que debe arribarse a un marco regulatorio armonizado sobre el cual existen consensos suficientes y donde además se coincide respecto de los principios y derechos que deben reconocerse, inclusive en el contexto de tratamientos efectuados por motores o buscadores de Internet.

Se enfatiza luego en que debe arribarse a un régimen regulatorio de los servicios que tratan datos personales por encargo del responsable, sin eximir a éste de sus obligaciones y responsabilidades; que es necesario establecer una base mínima respecto de las transferencias internacionales de datos personales con pleno respeto a los derechos de los titulares; que la posibilidad de obtener información en Internet respecto de millones de personas desde cualquier lugar del mundo

no debería constituirse en un factor que impida la efectiva protección de los derechos y libertades en el ciberespacio, y que deben adoptarse medidas preventivas que permitan al responsable responder proactivamente, como la adopción de esquemas de autorregulación vinculante o sistemas de certificación en la materia, la designación de un oficial de protección de datos personales, la elaboración de evaluaciones de impacto a la protección de datos personales y la privacidad por defecto y por diseño, entre otras.

Sobre los mecanismos institucionales para asegurar el cumplimiento de las normas de protección de datos, se expresa que debe existir en cada Estado Iberoamericano una autoridad de control independiente e imparcial, cuyas decisiones estén únicamente sujetas a control judicial y sean ajenas a toda influencia externa; que cuente con facultades de supervisión e investigación en su materia y esté encargada de vigilar el cumplimiento de la legislación nacional en la materia; que cuente con recursos humanos y materiales suficientes para garantizar el ejercicio de sus poderes y el desempeño efectivo de sus funciones. Asimismo se destaca que los titulares deben contar con una serie de mecanismos y procedimientos para presentar sus reclamaciones ante la autoridad de control y para ser indemnizados por los daños y perjuicios que pudieran sufrir; y, finalmente, se afirma que en este terreno es indispensable establecer una base mínima para la cooperación internacional entre las autoridades de control latinoamericanas y entre éstas y las de terceros países, con la finalidad de favorecer y facilitar la aplicación de la legislación en la materia y una protección efectiva de los titulares.

En desarrollo de esos fundamentos, en su Capítulo I (Disposiciones generales) establece su objeto, las definiciones, el ámbito de aplicación (subjetivo, objetivo y territorial); las excepciones generales al derecho a la protección de datos personales (seguridad nacional, seguridad pública, salud pública, la protección de los derechos y las libertades de terceros y cuestiones de interés público), cuyo reconocimiento debe reunir determinados requisitos (ser establecidas de manera expresa por medio de ley, contemplar ciertos aspectos mínimos y ser necesarias,

adecuadas y proporcionales en una sociedad democrática, respetando los derechos y las libertades fundamentales de los titulares); la posibilidad de limitar el derecho a la protección de datos personales a través de la ponderación con otros derechos y libertades fundamentales; las reglas para el tratamiento de los datos personales de niñas, niños y adolescentes (que incluye la necesaria formación académica de este grupo vulnerable respecto del uso responsable, adecuado y seguro de las tecnologías de la información y comunicación y los eventuales riesgos a los que se enfrentan en ambientes digitales), y las reglas para el tratamiento de los datos sensibles.

En el Capítulo II (Principios de protección de datos personales), se desarrollan con gran grado de detalle los de legitimación, licitud, lealtad, transparencia, finalidad, proporcionalidad, calidad, responsabilidad, seguridad y confidencialidad.

En el Capítulo III (Derechos del titular), se reconocen los derechos de los titulares de los datos personales, refiriendo a los "Derechos ARCO", entre los cuales se incluye a los tradicionales que dan origen a su denominación (acceso, rectificación, cancelación y oposición) y se agrega el recientísimamente reconocido de portabilidad de los datos personales, regulando con detalle el modo de ejercerlos.

En el Capítulo IV (Encargado), regula la actividad y responsabilidades de quien realiza las actividades de tratamiento de los datos personales por encargo, sin ostentar el poder de decisión sobre el alcance y contenido de los tratamientos característico del responsable del tratamiento.

En el Capítulo V (Transferencias internacionales de datos personales), se regulan precisamente los supuestos y condiciones en que pueden realizarse ese tipo de transferencias y se habilitan ciertos límites que, para ser válidos, deben ser establecidos expresamente por las legislaciones internas (seguridad nacional, seguridad pública, protección de la salud pública, protección de los derechos y libertades de terceros, y cuestiones de interés público).

En el Capítulo VI (Medidas proactivas en el tratamiento de datos personales), se habilita a reconocer medidas que promuevan el mejor cumplimiento de la legislación sobre protección de datos y coadyuven a fortalecer y a elevar los controles implementados por el responsable del tratamiento, entre las cuales menciona: a) privacidad por diseño y privacidad por defecto; b) la designación, por parte del responsable, de un oficial de protección de datos personales o figura equivalente (cuando los tratamientos: sean realizado por una autoridad pública; tengan por objeto una observación habitual y sistemática de la conducta del titular, o puedan entrañar un alto riesgo de afectación de los titulares); c) la adopción de mecanismos de autorregulación vinculante, y d) la realización de evaluaciones de impacto a la protección de datos personales.

En el Capítulo VII (Autoridades de control), se alude a la necesidad de contar, en cada Estado Iberoamericano, con una o más autoridades de control en materia de protección de datos personales(, que pueden ser unipersonales o pluripersonales pero que deben contar con plena autonomía; actuar con carácter imparcial e independiente, estar exentas de toda influencia externa directa o indirecta; no estar sujetas a orden ni instrucción alguna; estar integradas por personas que cuenten con experiencia y aptitudes específicas, sean designadas mediante un procedimiento transparente y removidas únicamente por causales graves; cuenten con suficientes poderes de investigación, supervisión, resolución, promoción y sanción; sus decisiones estén únicamente sujetas al control jurisdiccional y cuenten con recursos humanos y materiales necesarios para el cumplimiento de sus funciones.

En el Capítulo VIII (Reclamaciones y Sanciones), se establecen las reglas que deben observarse al crearse ese régimen, tanto al reconocer el derecho de los titulares a presentar reclamaciones administrativas y judiciales para hacer efectivos sus derechos, como al establecer medidas correctivas y sancionar las conductas que contravengan los principios y derechos contenidos en la norma.

En el Capítulo IX (Derecho de indemnización), se estipula que las legislaciones nacionales deben reconocer el derecho que tiene el titular a ser indemnizado frente a los daños y perjuicios derivados de una violación a su derecho a la protección de datos personales y que también deben señalar qué autoridad resulta competente para conocer de este tipo de acciones, así como los plazos, requerimientos y términos a través de los cuales procederán las indemnizaciones respectivas.

En el Capítulo X (Cooperación internacional) se refiere a la necesidad de establecer mecanismos de cooperación internacional que faciliten la aplicación de las legislaciones nacionales dictadas en la materia y que permitan reforzar la asistencia y cooperación internacional, la asistencia entre las autoridades de control a través de la notificación y remisión de reclamaciones, la asistencia en investigaciones y el intercambio de información, y, finalmente, la adopción de mecanismos orientados al conocimiento e intercambio de mejores prácticas y experiencias en materia de protección de datos personales, inclusive en materia de conflictos de jurisdicción con terceros países.

5. Nuestra propuesta original *aggiornada*.

Tal como lo indica el TC peruano en la sentencia citada *supra*, la labor de clasificación en los distintos tipos y subtipos de hábeas data pretende cumplir fines meramente didácticos, y no es de ningún modo excluyente de otros tipos que no estén contenidos en la tipología resultante que puedan eventualmente surgir. Además, no se trata de encasillar en tipos que constituyan compartimentos estancos y que por ello sólo puedan ser utilizados aisladamente, ya que, por el contrario, pueden ser incoados en cualquier proceso de manera conjunta, sucesiva e incluso alternativa (v.gr., peticionando el acceso a una información determinada de la que ya se tomó conocimiento indirecto y exigiendo que una vez producido ese acceso y sea confirmada la existencia de esa información, se proceda, según corresponda, a la rectificación de los datos, su confidencialización o a la exclusión del registro).

Nos ocuparemos en adelante de aportar tal clasificación, incorporando, como se dijo, las novedades aportadas en esta cuarta generación de leyes de protección de datos que estamos transitando, al calor del RGPD europeo y de los Estándares de la RIPD.

A. Tipologías genéricas:

1. Hábeas data "propio" e "impropios" ("puro" e "impuro", según el TC)

Atendiendo a las finalidades perseguidas por el hábeas data y al legitimado pasivo de la acción, cabe distinguir entre dos especies principales del instituto.

El hábeas data "propio" o "tradicional" (hábeas data "puro", en la terminología del TC), se dirige a prevenir o reparar lesiones que pudieran producirse en el tratamiento de datos de carácter personal realizado en bases y bancos de datos.

El "hábeas data impropio" ("impuro", según el TC), diseñado a fin de:

a) obtener información pública negada al legitimado activo por parte del legitimado pasivo ("de acceso a la información pública" según el TC), o

b) replicar información de carácter personal publicada a través de los medios de difusión tradicionales (como estaba inicialmente previsto en la Constitución peruana de 1993).

Cada una de estas especies pueden a su vez ser objeto de clasificaciones secundarias –distinguiéndoselas entre subespecies, tipos y subtipos–, considerando los objetivos que cada una de ellas persigue.

2. Hábeas datas "preventivos" y "reparadores"

Esta segunda clasificación genérica atiende al momento en que se incoa la acción y al tipo de tutela que persigue su promotor. Surgen así, los tipos que se refieren de inmediato.

Los hábeas datas *preventivos*, que son aquellos que procuran evitar la consumación de lesiones aún no producidas, por ejemplo, obteniendo información sobre los datos colectados, la localización de los bancos de datos que los contienen, la finalidad de su creación, el tipo y contenido de los datos registrados, las fuentes de las cuales se obtuvo información almacenada y los potenciales y efectivos recipiendarios de los datos colectados, toda información que puede resultar de suma utilidad para solicitar otros tipos de tratamientos sobre los datos registrados o los sistemas de información.

Los hábeas datas *reparadores*, que son los que están previstos para conjurar lesiones que se están consumando y por ello están dirigidos no ya a obtener información, sino a producir modificaciones tanto sobre los datos colectados en el sistema de información (v.gr., para rectificar o suprimir datos) como respecto del sistema de información en sí mismo (v.gr., a fin de que se realicen modificaciones sobre sus medidas de seguridad o permitan una portabilidad de los datos que no sea factible por cuestiones técnicas) e incluso también proceden cuando tales lesiones ya se produjeron (v.gr., en los ordenamientos que lo permiten por esta vía procesal, para obtener el resarcimiento derivado de un tratamiento ilegal o ilegítimo de datos de carácter personal).

3. Hábeas datas "individuales" y "colectivos"

Una tercera tipología genérica clasifica a los hábeas datas según los alcances de la legitimación del promotor de la acción y los efectos que producirá la sentencia que se dicte en el proceso de hábeas data. Surgen así los tipos que se consignan a continuación:

El hábeas data *individual*, que representa la tipología más extensa, y que es el ejercido sólo por los titulares de los datos respecto de sus datos personales (en legitimación ampliada en el derecho argentino en otros ordenamientos a sus sucesores universales), donde la sentencia tiene efecto ordinariamente *inter partes,* y

El hábeas data *colectivo*, que es articulable con el objetivo específico, del sujeto demandante, de tutelar los datos de carácter personal de un grupo determinado o indeterminado de personas afectadas frente a un tratamiento indebido de datos, supuesto en el cual la sentencia que se dicte en el proceso de hábeas data tiene –o debería tener- efecto *erga omnes*.

En concreto, puede ser incoado tanto por la persona registrada (cuando considera que además de ella existen otras personas afectadas igualmente por un tratamiento ilegal), como por ciertas asociaciones de la sociedad civil (vulgarmente conocidas bajo las siglas ONG) constituidas en pro de determinados fines de bien común (v.gr., de defensa del consumidor, de lucha contra la discriminación, etc.) y por el defensor del pueblo (en virtud de su usual legitimación procesal a fin de tutelar judicialmente los derechos de las personas).

Así, en este hábeas data no se tutela ya un mero interés individual, sino el de muchas individualidades y a la vez uno general, y por ello se acude a la representación colectiva.

Su origen fue doctrinario, en concreto a propuesta nuestra y de Palazzi, frente a la inserción del hábeas data como subtipo de amparo en la reforma constitucional argentina de 1994 (se entendió que el constituyente, al remitir a la acción de amparo en el mismo artículo regulada –en concreto, tratada en sus especies individual y colectivo– también habilitaba ambas posibilidades del hábeas data, en especial por funcionar, al igual que el amparo colectivo, frente a supuestos de discriminación).

Luego fue reconocido normativamente de manera expresa en la Constitución venezolana de 1999, al disponer, en su artículo 281, inc. 3°, que: *"entre las atribuciones del Defensor del Pueblo se encuentra la de interponer las acciones de inconstitucionalidad, amparo, hábeas corpus, hábeas data y las demás acciones o recursos necesarios para ejercer las atribuciones señaladas en los ordinales anteriores, cuando fuere procedente de conformidad con la ley"*.

Desde luego, tal legitimación colectiva nunca podrá servir para acceder directamente a los datos de personas distintas del impetrante (en especial, en los casos en que es incoado por una persona física o de existencia ideal), sino para reparar lesiones de orden colectivo (cuando, v.gr., se solicita la eliminación de una determinada categoría de datos que son incompatibles con la finalidad del registro y pueden causar discriminación), en cuyo caso sólo el juez del hábeas data y en todo caso el funcionario legalmente legitimado para ello (v.gr., el defensor del pueblo, o el titular del órgano de control) podrán tener contacto con ellos (en el caso mencionado, a fin de verificar su eliminación).

B. Tipologías específicas

Realizadas estas primeras clasificaciones genéricas, dividiremos el análisis partiendo del hábeas data tradicional o propio, para luego referirnos a las versiones de hábeas data que tienen una finalidad distinta a la típica de aquél.

1. Hábeas data "propio" ("puro", en la terminología del TC)

Esta especie de hábeas data, como se dijo, está destinada a operar respecto del contenido de las bases o bancos de datos de carácter personal, o a fin de obtener un resarcimiento económico del responsable de aquéllos.

Exhibe dos subespecies principales (hábeas data preventivos y reparadores) y una interesante diversidad de tipos y subtipos, a los que nos referiremos a continuación.

1.1. Hábeas data preventivos

Los hábeas data preventivos, como se dijo, apuntan a obtener información respecto de los datos o de los sistemas de información que los contienen, precisamente para prevenir violaciones al derecho a la protección de datos. Desde luego, más allá de su finalidad objetivamente

preventiva, cuando la información que se pretende obtener al momento de su interposición ya es conocida por otros medios por el perjudicado, pasa a funcionar (subjetivamente y para la persona que ya conoce el contenido del registro) como hábeas data reparador, a fin de, v.gr., motivar con el acceso la supresión de un dato erróneo, o de colectar prueba para el ejercicio de un hábeas data reparador.

1.1.1. Hábeas data informativo: subtipos localizador, exhibitorio, finalista y autoral ("de cognición", "informativo", "inquisitivo", "teleológico" y "de ubicación", en la terminología del TC)

El hábeas data **informativo ("de cognición", según el TC)**, como se anticipó, es aquel que no está destinado a operar sobre los datos registrados, sino que solamente procura recabar la información necesaria para permitir a su promotor decidir a partir de ésta –si es que la información no la obtuvo antes por vía extrajudicial– si los datos y el sistema de información está funcionando legalmente o si, por el contrario no lo está y por lo tanto solicitará operaciones sobre los asientos registrados o sobre el sistema de información en sí mismo.

Se divide en tres subtipos:

a) el hábeas data **localizador ("de ubicación", según el TC)**, destinado a indagar sobre la existencia y ubicación de bancos y bases de datos, y encuentra su razón lógica en que, para poder ejercer los derechos reconocidos por las normas protectoras de datos de carácter personal, resulta necesario previamente localizar las fuentes potencialmente generadoras de información lesiva. Varios países (v.gr., Argentina, en su ley 25.326), con el objeto de garantizar el ejercicio de los derechos de aquellos que se encuentren potencialmente afectados, establecen la obligatoriedad de inscribir a las bases y bancos de datos ante el órgano de aplicación de la ley, siguiendo las reglas europeas vigentes por entonces (aunque a partir de la

aprobación del RGPD esta obligación, como regla que hace a la licitud de los tratamientos, ha cesado);

b) el hábeas data **exhibitorio ("informativo", según el TC)**, dirigido a conocer qué datos de carácter personal se encuentran almacenados en determinado sistema de información y verificar el cumplimiento de los demás requisitos que le exige la ley para proceder a la registración de aquéllos (v.gr., consentimiento informado del interesado);

c) el hábeas data **finalista ("teleológico, según el TC)**, reconocido con el objeto de determinar para qué se creó el registro, lo que permitirá luego a su promotor establecer si las categorías de los datos almacenados se corresponden con la finalidad declarada en el acto de su creación, y

d) el hábeas data **autoral ("inquisitivo, según el TC)**, cuyo propósito es inquirir acerca de quién proporcionó los datos con que cuenta la base o banco de datos.

De estos subtipos, el primero es ordinariamente de fuente legal, mientras que los tres restantes se encuentran regulados expresamente en las constituciones de Argentina, Brasil, Colombia, Ecuador, Guatemala, Paraguay, Perú y Venezuela.

También lo prevén expresamente la Constitución de Portugal, y en el plano de loes estados federados argentinos, se encuentra regulado por las constituciones de Buenos Aires (ciudad autónoma y provincia), Córdoba, Chaco, Chubut, Jujuy, Río Negro, San Juan, San Luis y Tierra del Fuego.

También se refieren a ellos, entre otras, la ley argentina de protección de datos (25.326), artículos 6, 13, 14, 15 y 21; la ley chilena sobre protección de la vida privada (19.628), artículos 9 y 12 y la ley peruana de protección de datos (29.733) artículos 18, 19 y 34.

El RGPD lo trae regulado en los artículos 13, 14 y 15 y los Estándares de la RIPD refieren a este tipo en el numeral 25.

1.1.2. Hábeas data "transparentador" o "traslucidor"

Este tipo procura que se cumpla con las obligaciones de transparencia e información, que sólo se regulaban de una manera relativa en las leyes de protección de datos que precedieron al RGPD y a los Estándares de la RIPD, por lo que nos referiremos solo a ellas.

En el RGPD se encuentran claramente explicados los alcances de estas obligaciones en el considerando 78, según el cual: "La protección de los derechos y libertades de las personas físicas con respecto al tratamiento de datos personales exige la adopción de medidas técnicas y organizativas apropiadas con el fin de garantizar el cumplimiento de los requisitos del presente Reglamento. A fin de poder demostrar la conformidad con el presente Reglamento, el responsable del tratamiento debe adoptar políticas internas y aplicar medidas que cumplan en particular los principios de protección de datos desde el diseño y por defecto.

"Dichas medidas podrían consistir, entre otras, en reducir al máximo el tratamiento de datos personales, seudonimizar lo antes posible los datos personales, dar transparencia a las funciones y el tratamiento de datos personales, permitiendo a los interesados supervisar el tratamiento de datos y al responsable del tratamiento crear y mejorar elementos de seguridad. Al desarrollar, diseñar, seleccionar y usar aplicaciones, servicios y productos que están basados en el tratamiento de datos personales o que tratan datos personales para cumplir su función, ha de alentarse a los productores de los productos, servicios y aplicaciones a que tengan en cuenta el derecho a la protección de datos cuando desarrollan y diseñen estos productos, servicios y aplicaciones, y que se aseguren, con la debida atención al estado de la técnica, de que los responsables y los encargados del tratamiento están en condiciones de cumplir sus obligaciones en materia de protección de datos. Los principios de la protección de datos desde el diseño y por defecto también deben tenerse en cuenta en el contexto de los contratos públicos."

También el considerando 100 muestra su naturaleza preventiva, cuando se menciona: "A fin de aumentar la transparencia y el cumplimiento del presente Reglamento, debe fomentarse el establecimiento de mecanismos de certificación y sellos y marcas de protección de datos, que permitan a los interesados evaluar con mayor rapidez el nivel de protección de datos de los productos y servicios correspondientes".

Ya en el articulado, el artículo 5, al aludir a los principios relativos al tratamiento de los datos, expresa que deben ser tratados "de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»)", y se lo regula específicamente en el artículo 12[8].

[8] Artículo 12. Transparencia de la información, comunicación y modalidades de ejercicio de los derechos del interesado

1. El responsable del tratamiento tomará las medidas oportunas para facilitar al interesado toda información indicada en los artículos 13 y 14, así como cualquier comunicación con arreglo a los artículos 15 a 22 y 34 relativa al tratamiento, en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, en particular cualquier información dirigida específicamente a un niño. La información será facilitada por escrito o por otros medios, inclusive, si procede, por medios electrónicos. Cuando lo solicite el interesado, la información podrá facilitarse verbalmente siempre que se demuestre la identidad del interesado por otros medios.

2. El responsable del tratamiento facilitará al interesado el ejercicio de sus derechos en virtud de los artículos 15 a 22.

En los casos a que se refiere el artículo 11, apartado 2, el responsable no se negará a actuar a petición del interesado con el fin de ejercer sus derechos en virtud de los artículos 15 a 22, salvo que pueda demostrar que no está en condiciones de identificar al interesado.

3. El responsable del tratamiento facilitará al interesado información relativa a sus actuaciones sobre la base de una solicitud con arreglo a los artículos 15 a 22, y, en cualquier caso, en el plazo de un mes a partir de la recepción de la solicitud. Dicho plazo podrá prorrogarse otros dos meses en caso necesario, teniendo en cuenta la complejidad y el número de solicitudes. El responsable informará al interesado de cualquiera de dichas prórrogas en el plazo de un mes a partir de la recepción de la solicitud, indicando los motivos de la dilación. Cuando el interesado presente la solicitud por medios electrónicos, la información se facilitará por medios electrónicos cuando sea posible, a menos que el interesado solicite que se facilite de otro modo.

4. Si el responsable del tratamiento no da curso a la solicitud del interesado, le informará sin dilación, y a más tardar transcurrido un mes de la recepción de la solicitud, de las razones de su no actuación y de la posibilidad de presentar una reclamación ante una autoridad de control y de ejercitar acciones judiciales.

Los Estándares de la RIPD lo tratan específicamente en el numeral 20.

1.1.3. Hábeas data "evaluador preventivo de riesgos" o "verificador de impacto de los tratamientos"

El objetivo de este tipo es el de prevenir la realización de determinados tratamientos que puedan acarrear importantes riesgos para los derechos y libertades, y persigue que se realicen los estudios sobre impacto en la protección de datos con carácter previo al inicio de esos tratamientos y que esos tratamientos se ajusten de manera tal que esos riesgos se neutralicen o minimicen al máximo.

Este tipo aparece a partir de su incorporación en el RGPD, de modo que cabe remitir a sus previsiones y a las de los Estándares de la RIPD.

En el caso del RGPD, el considerando 84 expresa: "A fin de mejorar el cumplimiento del presente Reglamento en aquellos casos en los

5. La información facilitada en virtud de los artículos 13 y 14 así como toda comunicación y cualquier actuación realizada en virtud de los artículos 15 a 22 y 34 serán a título gratuito. Cuando las solicitudes sean manifiestamente infundadas o excesivas, especialmente debido a su carácter repetitivo, el responsable del tratamiento podrá:

a) cobrar un canon razonable en función de los costes administrativos afrontados para facilitar la información o la comunicación o realizar la actuación solicitada, o
b) negarse a actuar respecto de la solicitud.

El responsable del tratamiento soportará la carga de demostrar el carácter manifiestamente infundado o excesivo de la solicitud.

6. Sin perjuicio de lo dispuesto en el artículo 11, cuando el responsable del tratamiento tenga dudas razonables en relación con la identidad de la persona física que cursa la solicitud a que se refieren los artículos 15 a 21, podrá solicitar que se facilite la información adicional necesaria para confirmar la identidad del interesado.

7. La información que deberá facilitarse a los interesados en virtud de los artículos 13 y 14 podrá transmitirse en combinación con iconos normalizados que permitan proporcionar de forma fácilmente visible, inteligible y claramente legible una adecuada visión de conjunto del tratamiento previsto. Los iconos que se presenten en formato electrónico serán legibles mecánicamente.

8. La Comisión estará facultada para adoptar actos delegados de conformidad con el artículo 92 a fin de especificar la información que se ha de presentar a través de iconos y los procedimientos para proporcionar iconos normalizado.

que sea probable que las operaciones de tratamiento entrañen un alto riesgo para los derechos y libertades de las personas físicas, debe incumbir al responsable del tratamiento la realización de una evaluación de impacto relativa a la protección de datos, que evalúe, en particular, el origen, la naturaleza, la particularidad y la gravedad de dicho riesgo. El resultado de la evaluación debe tenerse en cuenta cuando se decidan las medidas adecuadas que deban tomarse con el fin de demostrar que el tratamiento de los datos personales es conforme con el presente Reglamento. Si una evaluación de impacto relativa a la protección de datos muestra que las operaciones de tratamiento entrañan un alto riesgo que el responsable no puede mitigar con medidas adecuadas en términos de tecnología disponible y costes de aplicación, debe consultarse a la autoridad de control antes del tratamiento".

Por su parte, el considerando 90 expresa: "En tales casos, el responsable debe llevar a cabo, antes del tratamiento, una evaluación de impacto relativa a la protección de datos con el fin de valorar la particular gravedad y probabilidad del alto riesgo, teniendo en cuenta la naturaleza, ámbito, contexto y fines del tratamiento y los orígenes del riesgo. Dicha evaluación de impacto debe incluir, en particular, las medidas, garantías y mecanismos previstos para mitigar el riesgo, garantizar la protección de los datos personales y demostrar la conformidad con el presente Reglamento".

Luego, el considerando 91 afirma: "Lo anterior debe aplicarse, en particular, a las operaciones de tratamiento a gran escala que persiguen tratar una cantidad considerable de datos personales a nivel regional, nacional o supranacional y que podrían afectar a un gran número de interesados y entrañen probablemente un alto riesgo, por ejemplo, debido a su sensibilidad, cuando, en función del nivel de conocimientos técnicos alcanzado, se haya utilizado una nueva tecnología a gran escala y a otras operaciones de tratamiento que entrañan un alto riesgo para los derechos y libertades de los interesados, en particular cuando estas operaciones hace más difícil para los interesados el ejercicio de sus derechos. La evaluación de impacto relativa a la protección de datos

debe realizarse también en los casos en los que se tratan datos personales para adoptar decisiones relativas a personas físicas concretas a raíz de una evaluación sistemática y exhaustiva de aspectos personales propios de personas físicas, basada en la elaboración de perfiles de dichos datos o a raíz del tratamiento de categorías especiales de datos personales, datos biométricos o datos sobre condenas e infracciones penales o medidas de seguridad conexas. También es necesaria una evaluación de impacto relativa a la protección de datos para el control de zonas de acceso público a gran escala, en particular cuando se utilicen dispositivos optoelectrónicos o para cualquier otro tipo de operación cuando la autoridad de control competente considere que el tratamiento entrañe probablemente un alto riesgo para los derechos y libertades de los interesados, en particular porque impida a los interesados ejercer un derecho o utilizar un servicio o ejecutar un contrato, o porque se efectúe sistemáticamente a gran escala. El tratamiento de datos personales no debe considerarse a gran escala si lo realiza, respecto de datos personales de pacientes o clientes, un solo médico, otro profesional de la salud o abogado. En estos casos, la evaluación de impacto de la protección de datos no debe ser obligatoria."

Finalmente, el considerando 94 menciona: "Debe consultarse a la autoridad de control antes de iniciar las actividades de tratamiento si una evaluación de impacto relativa a la protección de datos muestra que, en ausencia de garantías, medidas de seguridad y mecanismos destinados a mitigar los riesgos, el tratamiento entrañaría un alto riesgo para los derechos y libertades de las personas físicas, y el responsable del tratamiento considera que el riesgo no puede mitigarse por medios razonables en cuanto a tecnología disponible y costes de aplicación. Existe la probabilidad de que ese alto riesgo se deba a determinados tipos de tratamiento y al alcance y frecuencia de este, lo que también puede ocasionar daños y perjuicios o una injerencia en los derechos y libertades de la persona física. La autoridad de control debe responder a la solicitud de consulta dentro de un plazo determinado. Sin embargo, la ausencia de respuesta de la autoridad de control dentro de dicho plazo

no debe obstar a cualquier intervención de dicha autoridad basada en las funciones y poderes que le atribuye el presente Reglamento, incluido el poder de prohibir operaciones de tratamiento. Como parte de dicho proceso de consulta, se puede presentar a la autoridad de control el resultado de una evaluación de impacto relativa a la protección de datos efectuada en relación con el tratamiento en cuestión, en particular las medidas previstas para mitigar los riesgos para los derechos y libertades de las personas físicas."

Ya en el articulado, el artículo 35 regula con detalle esta cuestión[9], mientras que el artículo 36 lo complementa al referirse al mecanismo

[9] Artículo 35 Evaluación de impacto relativa a la protección de datos

1. Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares.

2. El responsable del tratamiento recabará el asesoramiento del delegado de protección de datos, si ha sido nombrado, al realizar la evaluación de impacto relativa a la protección de datos.

3. La evaluación de impacto relativa a la protección de los datos a que se refiere el apartado 1 se requerirá en particular en caso de: a) evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar; b) tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9, apartado 1, o de los datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10, o c) observación sistemática a gran escala de una zona de acceso público.

4. La autoridad de control establecerá y publicará una lista de los tipos de operaciones de tratamiento que requieran una evaluación de impacto relativa a la protección de datos de conformidad con el apartado 1. La autoridad de control comunicará esas listas al Comité a que se refiere el artículo 68.

5. La autoridad de control podrá asimismo establecer y publicar la lista de los tipos de tratamiento que no requieren evaluaciones de impacto relativas a la protección de datos. La autoridad de control comunicará esas listas al Comité.

6. Antes de adoptar las listas a que se refieren los apartados 4 y 5, la autoridad de control competente aplicará el mecanismo de coherencia contemplado en el artículo 63 si esas listas incluyen actividades de tratamiento que guarden relación con la oferta de bienes o servicios a interesados o con la observación del comportamiento de estos en varios

de consulta previa a la autoridad de control, que incluye las relativas a los estudios de impacto sobre los riesgos de los tratamientos y sobre la consiguiente viabilidad de los tratamientos proyectados.

Los Estándares de la RIPD lo regulan en el numeral 41.

1.1.4. Hábeas data "diseñador"

Los principios de "privacidad por defecto" (*privacy by default*); "privacidad desde el diseño" (*privacy by design*) y "privacidad

Estados miembros, o actividades de tratamiento que puedan afectar sustancialmente a la libre circulación de datos personales en la Unión.

7. La evaluación deberá incluir como mínimo: a) una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento; b) una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad; c) una evaluación de los riesgos para los derechos y libertades de los interesados a que se refiere el apartado 1, y d) las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con el presente Reglamento, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas.

8. El cumplimiento de los códigos de conducta aprobados a que se refiere el artículo 40 por los responsables o encargados correspondientes se tendrá debidamente en cuenta al evaluar las repercusiones de las operaciones de tratamiento realizadas por dichos responsables o encargados, en particular a efectos de la evaluación de impacto relativa a la protección de datos.

9. Cuando proceda, el responsable recabará la opinión de los interesados o de sus representantes en relación con el tratamiento previsto, sin perjuicio de la protección de intereses públicos o comerciales o de la seguridad de las operaciones de tratamiento.

10. Cuando el tratamiento de conformidad con el artículo 6, apartado 1, letras c) o e), tenga su base jurídica en el Derecho de la Unión o en el Derecho del Estado miembro que se aplique al responsable del tratamiento, tal Derecho regule la operación específica de tratamiento o conjunto de operaciones en cuestión, y ya se haya realizado una evaluación de impacto relativa a la protección de datos como parte de una evaluación de impacto general en el contexto de la adopción de dicha base jurídica, los apartados 1 a 7 no serán de aplicación excepto si los Estados miembros consideran necesario proceder a dicha evaluación previa a las actividades de tratamiento.

11. En caso necesario, el responsable examinará si el tratamiento es conforme con la evaluación de impacto relativa a la protección de datos, al menos cuando exista un cambio del riesgo que representen las operaciones de tratamiento.

por rediseño" (*privacy by redesign*) son de reciente factura (también e implican, básicamente, que; a) en cualquier tipo de equipos y aplicaciones informáticas (hardware y software), normas que regulen aspectos del tratamiento de datos personales, contratos, etc., se protejan los datos personales desde el diseño, y b) en la instalación y utilización de programas, aplicaciones, servicios, etc., éstas prevean por defecto, entre varias opciones posibles, la que mejor protege su privacidad.

Los principios de privacidad "por defecto" y "desde el diseño" recién fueron incorporados por el RGPD y de allí fueron tomados en los Estándares de la RIPD.

En el caso del RGPD, éste se encuentra explicado en cuanto a sus alcances en el considerando 78, que indica que "la protección de los derechos y libertades exige la adopción de medidas técnicas y organizativas apropiadas, entre las cuales el responsable del tratamiento debe adoptar políticas internas y aplicar medidas que cumplan en particular con estos principios, las que pueden consistir, entre otras, en "reducir al máximo el tratamiento de datos personales, seudonimizar lo antes posible los datos personales, dar transparencia a las funciones y el tratamiento de datos personales, permitiendo a los interesados supervisar el tratamiento de datos y al responsable del tratamiento crear y mejorar elementos de seguridad". Agrega luego que al desarrollar, diseñar, seleccionar y usar aplicaciones, servicios y productos que están basados en el tratamiento de datos personales o que tratan datos personales para cumplir su función, debe "alentarse a los productores de los productos, servicios y aplicaciones a que tengan en cuenta el derecho a la protección de datos cuando desarrollan y diseñen estos productos, servicios y aplicaciones, y que se aseguren, con la debida atención al estado de la técnica, de que los responsables y los encargados del tratamiento están en condiciones de cumplir sus obligaciones en materia de protección de datos".

Luego, se lo regula en su artículo 25[10], y en el caso de los Estándares de la RIPD, está contenido en el numeral 38.

1.2. Hábeas datas "reparadores" (hábeas data "manipulador" según el TC)

Un hábeas data reparador es aquél que tiene por finalidad específica actuar sobre los datos contenidos en los sistemas de información, sobre los sistemas en sí, o con el objetivo de obtener un resarcimiento económico por los daños causados a partir de un tratamiento ilegal o ilegítimo de datos de carácter personal.

Nos ocuparemos de ellos a continuación.

1.2.1. Hábeas data "aditivo": subtipos "actualizador", "aclaratorio" e "inclusorio" ("aditivo", y "correctivo", según el TC)

El hábeas data aditivo tiene por finalidad agregar al sistema de información datos de carácter personal no asentados en éste.

---

[10] Artículo 25 Protección de datos desde el diseño y por defecto

1. Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados.

2. El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas.

3. Podrá utilizarse un mecanismo de certificación aprobado con arreglo al artículo 42 como elemento que acredite el cumplimiento de las obligaciones establecidas en los apartados 1 y 2 del presente artículo.

En este subtipo confluyen tres subtipos distintos, los dos primeros, destinados a actuar sobre los datos del interesado que ya se encuentran asentados en un banco o base de datos, y el tercero, dirigido a que los datos de aquél sean ingresados a registro en el que fueron omitidos. Así, puede distinguiese entre:

a) el hábeas data **actualizador**, que es el diseñado para actualizar datos vetustos pero ciertos (v.gr., si alguien figura como abogado, pero ha sido designado juez, aunque el título profesional lo sigue teniendo, su perfil de ejercicio –y de identidad– es sustancialmente diferente),

b) el hábeas data **aclaratorio**, que es el destinado a aclarar situaciones ciertas pero que pueden ser incorrectamente interpretadas por quien acceda a los datos contenidos en el registro (v.gr., si bien un banco de datos puede colectar y proporcionar a terceros datos sobre las personas que han obtenido créditos comerciales y registraron atrasos en el pago, quien figure como deudor podría pretender que el banco de datos a coloque que su carácter no era de deudor principal sino de garante de la obligación contraída, o que la misma se encuentra controvertida por el deudor principal y se encuentra inhibido de cancelarla hasta tanto sea determinada su exigibilidad), y

c) el hábeas data **inclusorio**, cuya finalidad es la de operar sobre un registro que ha omitido asentar los datos del interesado, quien se encuentra perjudicado por dicha omisión (v.gr., el titular de un establecimiento hotelero cuyo dato no figura en un banco de datos de la Secretaría de Turismo de la Nación destinada a los turistas en los aeropuertos).

El único subtipo regulado expresamente en el plano constitucional es el hábeas data actualizador, y lo incluyen las cartas de Argentina, Brasil, Colombia, Ecuador, Paraguay y Venezuela. También lo contienen las constituciones de Portugal y las de la ciudad autónoma y de la provincia de Buenos Aires, Córdoba, Chaco, Chubut, San Juan y Tierra del Fuego.

También se refieren a ellos, entre otras, la ley argentina de protección de datos (25.326), artículo 16; la ley chilena sobre protección de la vida privada (19.628), artículos 6 y 9 y la ley peruana de protección de datos (29.733) artículo 20.

El RGPD lo trae regulado en el artículo 16 y los Estándares de la RIPD refieren a este tipo en el numeral 26.

1.2.2. Hábeas data "rectificador" o "correctivo" ("correctivo", según el TC)

Este subtipo está dirigido a corregir no sólo a los datos falsos (aquellos que no se corresponden siquiera mínimamente con la realidad), sino también a los inexactos o imprecisos (v.gr., el dato registrado es incompleto o puede dar lugar a más de una interpretación).

Se encuentra regulado en las constituciones de Argentina, Brasil, Colombia, Ecuador, Guatemala, Paraguay y Venezuela. Lo prevén también expresamente la Constitución de Portugal las de la ciudad autónoma y provincia de Buenos Aires, Córdoba, Chaco, Chubut, Jujuy, San Juan y Tierra del Fuego.

También, en el plano subconstitucional, refieren a ellos, entre otras, la ley argentina de protección de datos (25.326), artículo 16; la ley chilena sobre protección de la vida privada (19.628), artículo 6 y la ley peruana de protección de datos (29.733) artículo 20.

El RGPD lo trae regulado en los artículos 16 y 19 y los Estándares de la RIPD refieren a este tipo en el numeral 26.

1.2.3. Hábeas data "supresorio", "exclutorio" o "cancelatorio" ("supresorio", según el TC)

Este subtipo está diseñado a fin de eliminar total o parcialmente los datos almacenados, cuando por algún motivo no deben mantenerse incluidos en el sistema de información de que se trate, normalmente por derivación de tratamientos ilegales.

Esto puede ocurrir en múltiples supuestos, como en el caso del registro de cualquier tipo de datos que no se correspondan con la finalidad del banco o base de datos, de datos falsos que el registrador se niega a rectificar o actualizar, del tratamiento ilegal de los denominados "datos sensibles" (que en algunos casos no pueden ser objeto de tratamiento, y en otros sólo pueden ser tratados por escasos registros expresamente autorizados legalmente para ello, como los datos de afiliación política, por los partidos políticos), etc.

También puede utilizarse para ejercer el derecho al olvido cuando se trate de datos que deben eliminarse luego de un plazo determinado, es decir que tienen una fecha de caducidad luego de la cual su tratamiento es ilícito (v.gr., los datos de solvencia patrimonial y de crédito llevados por las centrales de riesgo, que en promedio, en las leyes de protección de datos o en las sectoriales, deben ser eliminados a los cinco años).

La figura se encuentra regulada expresamente en las constituciones de Argentina, Ecuador, Paraguay y Venezuela. También lo prevén las cartas de Portugal, ciudad autónoma y provincia de Buenos Aires, Chaco y Chubut.

Refieren a este subtipo, entre otras, la ley argentina de protección de datos de carácter personal (art. 16) y la ley chilena sobre protección de la vida privada (19.628), artículo 6, y la ley peruana de protección de datos (29.733) artículo 20.

El RGPD lo trae regulado en los artículos 17 y 19 y los Estándares de la RIPD refieren a este tipo en el numeral 27.

1.2.4. Hábeas data "esquecedor", "desmemorizador" o "desindexador"

El "derecho al olvido" o "a ser olvidado", es un derecho que suscita mucha controversia cuando se debe ponderar ante un conflicto con la libertad de expresión, esto es, cuando se trata de utilizar respecto de publicaciones realizadas por medios de comunicación, especialmente en Internet.

Se trata de un derecho que funciona respecto de información personal: a) lícitamente publicada; b) cierta; c) carente, por su antigüedad, de interés público actual; y d) que afecta desproporcionada e injustamente a quien es protagonista de ella. Deben así confluir los siguientes criterios: a) la existencia de un dato vetusto que cause un efecto dañino, persecutorio o denigrante; b) el transcurso de un tiempo razonable (no contemporaneidad); c) la ausencia de relevancia histórica de los hechos (historicidad), y d) el agotamiento de la relevancia informativa del evento.

Configurados dichos presupuestos, entre los derechos concedidos a los titulares de los datos en las normas de protección de datos personales (los denominados "derechos ARCO"), los que se vinculan directamente con el derecho al olvido son tres: a) el de acceso a los datos (porque es un límite para quien pretenda acceder a los datos cuyo olvido se dispuso en función de que ya no cumplen con la finalidad para la que fueron recabados, al ofrecer un perfil desactualizado de la persona en cuestión); b) el de supresión o cancelación de los datos (porque quien busca que un dato se olvide solicita su cancelación o la supresión del enlace que lleva a ese dato) y c) el de oposición al tratamiento de los datos (porque el titular de los datos puede oponerse a que determinada información personal vetusta se trate de determinada manera, por ejemplo, exigiendo que los buscadores no encuentren esa información que pretende ser olvidada a partir del nombre de aquél).

El ejercicio de este derecho origina el tipo de hábeas data "desmemorizador" que, a falta de una palabra en nuestro idioma que pueda reflejarlo de otro modo, también podríamos rotular "esquecedor", y que cabe denominar "desindexador" cuando se lo utiliza más específicamente en la modalidad que el TJUE aceptó en 2014 en el célebre caso "Costeja", es decir, limitando el efecto que causan los buscadores de internet de modo que éstos no muestren entre sus resultados de búsqueda una información determinada por el nombre de la persona que ejerce ese derecho.

El RGPD lo trata de manera singular pues asimila a un supuesto de ejercicio del derecho de supresión pues lo menciona sólo en el epígrafe del artículo 17 "Derecho de supresión («el derecho al olvido»)", sin establecer una regulación concreta alrededor de sus contornos.

Más allá de esto, se refiere a él en el considerando 66, al justificar su inserción en el artículo 17: "A fin de reforzar el «derecho al olvido» en el entorno en línea, el derecho de supresión debe ampliarse de tal forma que el responsable del tratamiento que haya hecho públicos datos personales esté obligado a indicar a los responsables del tratamiento que estén tratando tales datos personales que supriman todo enlace a ellos, o las copias o réplicas de tales datos. Al proceder así, dicho responsable debe tomar medidas razonables, teniendo en cuenta la tecnología y los medios a su disposición, incluidas las medidas técnicas, para informar de la solicitud del interesado a los responsables que estén tratando los datos personales".

Esa asimilación al derecho de supresión es incorrecta a nuestro modo de ver pues no abarca todos los supuestos en que el derecho al olvido puede ser ejercido y además puede implicar también una desindexación de un motor de búsqueda de Internet, que se asemeja más a una confidencialización de los datos o a una limitación del tratamiento, debido a que esa información personal no se suprime del sitio en el cual está publicada y por lo tanto puede encontrarse por vía de otros criterios de búsqueda que no incluyan el nombre de la persona en cuestión.

Los Estándares de la RIPD no lo incluyen expresamente debido a que se trata de un derecho más polémico en la región.

1.2.5. Hábeas data "objetor de tratamientos"

Este hábeas data se vincula con el derecho de oposición a los tratamientos y se encuentra regulado, en el RGPD, en diversas normas latinoamericanas, entre ellas en la ley peruana de protección de datos (29.733), que lo reconoce expresamente en su artículo 22.

El RGPD lo trata en su artículo 21[11], donde se reconoce a todo interesado el derecho a oponerse en cualquier momento, por motivos relacionados con su situación particular, a que sus datos personales sean objeto de un tratamiento, incluida la elaboración de perfiles, y si sus datos deben dejar de tratarse si no existen razones de las autorizadas en el propio reglamento (v.gr. motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones), especialmente cuando se esté ante tratamientos de mercadotecnia directa que incluyan elaboración de perfiles.

Los Estándares de la RIPD lo contienen en el numeral 28.

[11] Artículo 21 Derecho de oposición

1. El interesado tendrá derecho a oponerse en cualquier momento, por motivos relacionados con su situación particular, a que datos personales que le conciernan sean objeto de un tratamiento basado en lo dispuesto en el artículo 6, apartado 1, letras e) o f), incluida la elaboración de perfiles sobre la base de dichas disposiciones. El responsable del tratamiento dejará de tratar los datos personales, salvo que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones.

2. Cuando el tratamiento de datos personales tenga por objeto la mercadotecnia directa, el interesado tendrá derecho a oponerse en todo momento al tratamiento de los datos personales que le conciernan, incluida la elaboración de perfiles en la medida en que esté relacionada con la citada mercadotecnia.

3. Cuando el interesado se oponga al tratamiento con fines de mercadotecnia directa, los datos personales dejarán de ser tratados para dichos fines.

4. A más tardar en el momento de la primera comunicación con el interesado, el derecho indicado en los apartados 1 y 2 será mencionado explícitamente al interesado y será presentado claramente y al margen de cualquier otra información.

5. En el contexto de la utilización de servicios de la sociedad de la información, y no obstante lo dispuesto en la Directiva 2002/58/CE, el interesado podrá ejercer su derecho a oponerse por medios automatizados que apliquen especificaciones técnicas.

6. Cuando los datos personales se traten con fines de investigación científica o histórica o fines estadísticos de conformidad con el artículo 89, apartado 1, el interesado tendrá derecho, por motivos relacionados con su situación particular, a oponerse al tratamiento de datos personales que le conciernan, salvo que sea necesario para el cumplimiento de una misión realizada por razones de interés público.

1.2.6. Hábeas data "impugnativo" ("interpretativo", según el TC)

Las normas sobre protección de datos suelen prever el derecho del registrado a impugnar las valoraciones que de sus datos realicen los responsables de tratamiento, como asimismo a que se adopten decisiones judiciales o administrativas con único fundamento en el resultado del tratamiento informatizado de datos de carácter personal que suministren una definición del perfil o personalidad del interesado. Este derecho fue ampliado en el RGPD a las decisiones automatizadas privadas, incluida la posibilidad de impugnar, bajo determinadas circunstancias, la elaboración de perfiles.

Este subtipo presenta cierta similitud con el hábeas data rectificador o correctivo, si por vía de esa impugnación se pretende establecer una conclusión distinta a la que aparece en el registro, y con el excluto-rio, cuando a través de esa impugnación se persigue la eliminación total de dicha valoración o decisión.

Entre otras normas, la ley argentina de protección de datos personales (25.326) prevé el derecho de impugnación de las valoraciones personales en su artículo 20, pero limitándola como lo hacían las leyes de protección de datos de su tiempo, a las decisiones judiciales y administrativas. También lo reconoce la ley peruana de protección de datos (29.733) en su artículo 23.

El RGPD se refiere expresamente a esta posibilidad de impugnación respecto de los tratamientos realizados por el sector privado en el artículo 22[12], donde concede a todo interesado el derecho a no ser

[12] Artículo 22 Decisiones individuales automatizadas, incluida la elaboración de perfiles

1. Todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar.

2. El apartado 1 no se aplicará si la decisión:

objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, cuando ésta produzca efectos jurídicos en él o le afecte significativamente de modo similar, salvo cuando la decisión sea necesaria para la celebración o la ejecución de un contrato, esté autorizada legal o comunitariamente o se base en el consentimiento explícito del interesado.

Los Estándares de la RIPD se refieren a este derecho en el numeral 29.

1.2.7. Hábeas data "restrictivo", "limitador de tratamientos" o "bloqueador" ("cautelar", según el TC)

Muy emparentado al hábeas data reservador y al exclutorio se presenta un subtipo ligeramente distinto, que pretende "trabar" el tratamiento –generalmente en lo relativo a la transmisión o cesión a terceros– de los datos asentados en un registro. Este bloqueo debe ser realizado por el responsable del sistema de información si se dan esas condiciones y una norma lo prevé (en este aspecto, el RGPD lo trata expresamente), pero también puede ocurrir que lo ordene un órgano de control frente a la resistencia del responsable o incluso el juez del hábeas data como medida cautelar mientras se tramita la pretensión de fondo.

a) es necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento;
b) está autorizada por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca asimismo medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, o
c) se basa en el consentimiento explícito del interesado.

3. En los casos a que se refiere el apartado 2, letras a) y c), el responsable del tratamiento adoptará las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, como mínimo el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión.

4. Las decisiones a que se refiere el apartado 2 no se basarán en las categorías especiales de datos personales contempladas en el artículo 9, apartado 1, salvo que se aplique el artículo 9, apartado 2, letra a) o g), y se hayan tomado medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado.

Ese impedimento de comunicación de los datos puede o no ser temporalmente limitado (aunque preponderantemente lo es), según las circunstancias, y es definido por el RGPD como la operación de "marcado" de los datos de carácter personal conservados con el fin de limitar su tratamiento en el futuro.

El bloqueo puede proceder cuando se impugne la exactitud de los datos personales; el tratamiento sea ilícito pero el interesado se oponga a la supresión y solicite en su lugar la limitación de su uso; el interesado necesite datos para ejercer su derecho de defensa que el responsable ya no precise, y cuando el interesado se haya opuesto al tratamiento por motivos relacionados con su situación particular o alegue el tratamiento es ilícito.

Entre otras, la ley argentina de protección de datos personales (25.326) prevé el primero de estos supuestos (art. 38); se refiere a éste la ley chilena sobre protección de la vida privada (19.628), en el artículo 6 y lo incluye la ley peruana de protección de datos (29.733) en su artículo 21.

El RGPD incorporó la limitación de los tratamientos, que es definida en el artículo 4[13] y se desarrolla en el artículo 18[14]. También

[13] Art. 4. Definiciones. A efectos del presente Reglamento se entenderá por: … 3) «limitación del tratamiento»: el marcado de los datos de carácter personal conservados con el fin de limitar su tratamiento en el futuro.

[14] Artículo 18. Derecho a la limitación del tratamiento.

1. El interesado tendrá derecho a obtener del responsable del tratamiento la limitación del tratamiento de los datos cuando se cumpla alguna de las condiciones siguientes:

a) el interesado impugne la exactitud de los datos personales, durante un plazo que permita al responsable verificar la exactitud de los mismos;
b) el tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso;
c) el responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones;
d) el interesado se haya opuesto al tratamiento en virtud del artículo 21, apartado 1, mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado.

refiere a la limitación del tratamientos el considerando 67[15] entre otras normas del mismo reglamento.

Los Estándares de la RIPD lo tratan en el numeral 31.

1.2.8. Hábeas data reservador ("confidencial", según el TC)

Este subtipo tiende a asegurar que un dato correcta y legítimamente almacenado sea mantenido en reserva y en consecuencia sólo se comunique a quienes se encuentran legalmente autorizados y exclusivamente en los supuestos en que tales sujetos han sido habilitados para ello.

En general –pero no exclusivamente– se vincula a los casos de datos "sensibles" (v.gr., si un registro público de antecedentes penales evacuara los informes sobre tales antecedentes fuera de los supuestos autorizados por su ley de creación). También puede utilizárselo para asegurar el deber de secreto profesional típico de quienes tratan datos personales, que por regla están incluidos en las leyes de protección de datos.

Fue incorporado por primera vez de manera expresa en el plano constitucional en la reforma constitucional federal argentina de 1994 y

2. Cuando el tratamiento de datos personales se haya limitado en virtud del apartado 1, dichos datos solo podrán ser objeto de tratamiento, con excepción de su conservación, con el consentimiento del interesado o para la formulación, el ejercicio o la defensa de reclamaciones, o con miras a la protección de los derechos de otra persona física o jurídica o por razones de interés público importante de la Unión o de un determinado Estado miembro.

3. Todo interesado que haya obtenido la limitación del tratamiento con arreglo al apartado 1 será informado por el responsable antes del levantamiento de dicha limitación.

[15] Entre los métodos para limitar el tratamiento de datos personales cabría incluir los consistentes en trasladar temporalmente los datos seleccionados a otro sistema de tratamiento, en impedir el acceso de usuarios a los datos personales seleccionados o en retirar temporalmente los datos publicados de un sitio internet. En los ficheros automatizados la limitación del tratamiento debe realizarse, en principio, por medios técnicos, de forma que los datos personales no sean objeto de operaciones de tratamiento ulterior ni puedan modificarse. El hecho de que el tratamiento de los datos personales esté limitado debe indicarse claramente en el sistema.

ha sido objeto de ciertas críticas, no por su indudable utilidad, sino por la forma de su inclusión. Lo incluye también la Constitución de la República Dominicana, de 2010. También pueden encontrarse previsiones que permiten configurarlo en las constituciones de Perú y Portugal y –ya en el ámbito interno argentino–, en las cartas de la ciudad autónoma y provincia de Buenos Aires, Córdoba, Chaco, Chubut, Jujuy y Tierra del Fuego.

En el plano subconstitucional está regulado por la ley argentina de protección de datos (25.326), artículos 8 y 10; la ley chilena sobre protección de la vida privada (19.628), artículo 7 y la ley peruana de protección de datos (29.733) artículo 17.

El RGPD alude a este principio en el artículo 5, cuando refiere a que entre los principios que rigen los tratamientos de los datos, éstos deben ser "tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»)".

Los Estándares de la RIPD lo regulan en el numeral 23.

1.2.9. Hábeas datas "disociador" o "seudonimizador" ("desvinculador", según el TC)

Ordinariamente, las normas sobre protección de datos de carácter personal (y también otras, como las que regulan el secreto estadístico), prevén la posibilidad de que uno o más datos referidos a una persona determinada pueda ser valorado dentro de determinados parámetros (v.gr., pertenencia grupal, ubicación social, sexo, edad, estado de salud, etc.), pero sin que quien opera sobre los mismos tenga acceso a conocer la identidad de la persona a la cual se refieren esos datos. Esto se hace a partir de un proceso de desvinculación del dato mediante técnicas de disociación, que como regla no deben permitir la identificación de quien fue registrado.

Así, de modo paralelo a la anonimización –que implica que esos datos no pueden asociarse a persona alguna y por lo tanto no son datos personales que estén cubiertos por las normas de protección de datos mientras no cambien de este estado- aparecen la disociación "reasociable", que vendría a ser la seudonimización, que es muy similar dado que, en los términos del RGPD refiere a "el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable" (art. 4, inc. 5).

Es decir, habría, para decirlo de manera gráfica, una disociación "no reasociable", que sería la anonimización, y otra "reasociable" que sería la seudoniminazión.

La falta de cumplimiento de normas de anonimización (v.gr., en el caso de datos estadísticos que pueden asociarse a personas) o de seudonimización, se habilita al perjudicado a plantear un hábeas data disociador, precisamente para que ese dato sea sometido a las técnicas correctas que aseguren el cumplimiento de la finalidad legal.

Este subtipo tiene similitud con los hábeas datas reservador y exclutorio, por cuanto en definitiva apunta a que los datos en cuestión puedan ser valorados dentro de determinados parámetros –aunque sin conocer la identidad del registrado, o sólo conociéndola en los casos en que las normas lo habiliten– y a que se eliminen las referencias de esos datos, pero difiere de ellos en cuanto a que no necesariamente implica la eliminación de un dato del registro ni su confidencialización, sino su transformación en otro respecto del cual no puede predicarse la identidad de su titular.

Entre sus diversas utilidades puede ser eficaz para, por ejemplo, contrarrestar violaciones a las normas que autorizan a recoger datos anónimos con fines epidemiológicos (v.gr., la comunicación de

enfermos de sida en los términos de la ley argentina de lucha contra el sida, 23.798, que debe hacerse de manera codificada).

Se refieren, entre otras, a la disociación de datos la ley de protección de datos argentina (25.326) en sus artículos 11 y 28 y la ley chilena sobre protección de la vida privada (19.628), en su artículo 3.

El RGPD alude a este principio en los artículos 6, 25 y 32.

Los Estándares de la RIPD lo regulan en los numerales 2, 4 y 19.

1.2.10. Hábeas data "encriptador" ("cifrador", según el TC)

Más allá del derecho a que determinados datos sean reservados o disociados, en algunos supuestos, y a fin de brindar mayor seguridad y agilidad a la operación sobre determinados datos, puede ser necesario acudir a técnicas de encriptación, lo que implica en definitiva otra perspectiva, donde el dato está de algún modo oculto, y sólo puede ser conocido por quienes cuenten con la clave para descifrarlos.

Este subtipo entonces está dirigido a que se lleve a cabo tal tarea de encriptación, y no cuenta hasta el momento con reconocimiento legal expreso en el ámbito latinoamericano.

El RGPD trata las técnicas de cifrado como medio de protección de los datos en los artículos 6, 32 y 34, y explica su utilidad en el considerando 83.

1.2.11. Hábeas data "portabilizador"

Este tipo se vincula con el derecho a la portabilidad de los datos personales, que no se encuentra hasta el momento regulado en ninguna de las constituciones latinoamericanas y sólo fue incorporado por México en el artículo 57 de la Ley General de Protección de Datos en Posesión de Sujetos Obligados, que lo tomó del RGPD , extendiéndolo al ámbito público.

En el RGPD se encuentra regulado en el artículo 20[16] y se explica su sentido en el considerando 68, donde indica: "para reforzar aún más el control sobre sus propios datos, cuando el tratamiento de los datos personales se efectúe por medios automatizados, debe permitirse que los interesados que hubieran facilitado datos personales que les conciernan a un responsable del tratamiento los reciban en un formato estructurado, de uso común, de lectura mecánica e interoperable, y los transmitan a otro responsable del tratamiento".

Los Estándares de la RIPD lo contienen en el numeral 30.

1.2.12. Hábeas data "asegurador" ("garantista", según el TC)

Uno de los más importantes principios relativos al tratamiento de datos es el que indica que, para que un tratamiento sea legal, debe garantizarse la seguridad de los datos, pues de nada sirve que se reconozcan los derechos a operar sobre los bancos de datos si los procedimientos técnicos utilizados para dicho tratamiento permiten fugas o alteraciones ilegales de la información almacenada.

[16] Artículo 20. Derecho a la portabilidad de los datos

1. El interesado tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado, cuando:

a) el tratamiento esté basado en el consentimiento con arreglo al artículo 6, apartado 1, letra a), o el artículo 9,

apartado 2, letra a), o en un contrato con arreglo al artículo 6, apartado 1, letra b), y

b) el tratamiento se efectúe por medios automatizados.

2. Al ejercer su derecho a la portabilidad de los datos de acuerdo con el apartado 1, el interesado tendrá derecho a que los datos personales se transmitan directamente de responsable a responsable cuando sea técnicamente posible.

3. El ejercicio del derecho mencionado en el apartado 1 del presente artículo se entenderá sin perjuicio del artículo 17. Tal derecho no se aplicará al tratamiento que sea necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.

4. El derecho mencionado en el apartado 1 no afectará negativamente a los derechos y libertades de otros.

Por tal motivo, cabe la utilización de este subtipo para lograr la constatación judicial de las condiciones en que opera el sistema de información que contiene los datos y —en su caso— la imposición de condiciones técnicas mínimas de seguridad para que se pueda proseguir con el tratamiento de datos de carácter personal, bajo apercibimientos de cancelación del registro o bien de exclusión de los datos en él registrados.

El hábeas data asegurador se asimila al reservador por cuanto ambos persiguen la efectiva vigencia de la confidencialidad y permiten el control técnico de la actividad del registrador, pero es de otro lado más amplio en el sentido de que no opera sólo respecto de datos confidenciales, sino de cualquier tipo de datos.

Entre varias otras, la ley argentina de protección de datos personales (25.326) prevé este supuesto en su artículo 9; la ley chilena sobre protección de la vida privada (19.628), lo trata en su artículo 11 y la ley peruana de protección de datos (29.733) lo incluye en su artículo 16.

El RGPD lo trae regulado en los artículos 32 a 34, con nuevas medidas obligatorias en materia de notificación de los incidentes de seguridad, y los Estándares de la RIPD lo tratan en los numerales 21 y 22.

1.2.13. Hábeas data "resarcitorio" ("indemnizatorio", según el TC)

A este subtipo preferiríamos denominarlo "reparador" –pues se vincula con lo que los iusprivatistas denominan actualmente "derecho a la reparación"–, pero optamos por rotularlo "resarcitorio" a fin de no aportar a la confusión entre hábeas datas preventivos y reparadores.

Su objeto es lograr la satisfacción de las indemnizaciones por los daños y perjuicios sufridos a partir del indebido tratamiento de los datos personales.

En los países que ello es factible –en la mayoría de los ordenamientos que regulan el hábeas data o las acciones procesales constitucionales por las que se vehiculiza el derecho a la protección de datos no pueden

articularse pretensiones resarcitorias–, suele utilizarse conjuntamente con otras pretensiones conexas, como la rectificación o exclusión de los datos.

La Constitución del Ecuador lo prevé de manera expresa al regular el hábeas data, y en Colombia se han admitido regularmente acciones de tutela frente a la violación del "derecho de hábeas data" donde se pretendían indemnizaciones por los perjuicios sufridos por el accionante.

Asimismo, algunas leyes sobre protección de datos también se ocupan de destacar la pertinencia de la reparación de los daños causados por la violación de las normas del derecho a la protección de datos. Así lo prevén, v.gr., la ley argentina de protección de datos personales (25.326), en su artículo 31; la ley chilena sobre protección de la vida privada, en su artículo 11 y la ley peruana de protección de datos (29.733), en su artículo 25.

El RGPD lo trae regulado en el artículo 82 y los Estándares de la RIPD refieren a este tipo en el numeral 44.

2. Hábeas data "impropio" ("impuro", según el TC)

El hábeas data impropio, como se adelantó, no está dirigido a la protección de datos de carácter personal asentados en bases o bancos de datos, sino a otros objetivos, por ejemplo, a obtener información pública que le es indebidamente negada al legitimado activo, a replicar información de carácter personal difundida a través de los medios de difusión tradicionales, y a acceder a historias clínicas no informatizadas.

Puede estar regulado de manera conjunta con reglas sobre protección de datos de carácter personal, como ocurre en las constituciones de Perú y Venezuela, o bien independientemente de ellas, como ocurre en el caso argentino con el "hábeas data clínico".

2.1. Hábeas data "de acceso a información pública"

Como ya fuera expresado inicialmente, algunas constituciones (como las de España y –en el plano interno argentino–, las de las

provincias de Chaco, Formosa, Río Negro, San Luis y San Juan), contienen reglas que garantizan el libre acceso a la información pública (en algunos casos traen también sus excepciones, como cuando hubiera en juego asuntos vitales para la seguridad del Estado, según lo disponen las constituciones de San Juan y Perú). Adicionalmente, algunas constituciones establecen acciones procesales constitucionales específicas para su tutela, dentro de las cuales la del Perú adjudica al hábeas data tal naturaleza protectoria.

Algunos autores rotulan a este tipo de hábeas data impropio como "hábeas data público", pero tal denominación nos parece que puede llevar a confusión por no ser claramente definitoria de sus alcances.

En el caso argentino, la ley de acceso a la información pública (nº 27.275) prevé que las decisiones en materia de acceso a la información pública pueden ser revisadas tanto por vía administrativa como por vía judicial, disponiendo que "son recurribles directamente ante los tribunales de primera instancia en lo contencioso administrativo federal, sin perjuicio de la posibilidad de interponer el reclamo administrativo pertinente ante la Agencia de Acceso a la Información Pública o el órgano que corresponda según el legitimado pasivo", sin que pueda exigirse el agotamiento de la vía administrativa, y que resulta competente "el juez del domicilio del requirente o el del domicilio del ente requerido, a opción del primero". Aclara además que la acción judicial por incumplimiento tramitará por la vía del amparo; habilita un amparo de tipo informativo respecto de cualquier incumplimiento de las disposiciones de la ley, de modo que –como en Argentina el hábeas data es un subtipo de amparo que se rige supletoriamente por sus normas-, bien puede entenderse que se está ante este subtipo de hábeas data.

2.2. Hábeas data replicador

La única Constitución que –acertadamente- previó al hábeas data como una acción articulable como medio de ejercicio del derecho de réplica fue la carta peruana de 1993, que en su artículo 200 inc. 3, segundo párrafo, por remisión al artículo 2, inc. 7, dispuso que la

acción de hábeas data procedía, entre otros supuestos, contra el hecho u omisión por parte de cualquier autoridad, funcionario o persona, que vulnere o amenace los derechos al honor y a la buena reputación, a la intimidad personal y familiar así como a la voz y a la imagen propias, agregando que "Toda persona afectada por informaciones o agraviada en cualquier medio de comunicación social, tiene derecho que éste se rectifique en forma gratuita, inmediata y proporcional, sin perjuicio de las responsabilidades de ley", pero, como se anticipó, esta remisión fue derogada por la reforma constitucional realizada por la ley 26.470, debido a duras críticas de la doctrina y de las entidades periodísticas, por lo que ya no subsiste esta vía para el ejercicio de la réplica, que debe vehiculizarse ahora por la ruta del amparo.

2.3. Hábeas data "clínico"

En Argentina, la ley de derechos del paciente (n° 26.596, modificada por la ley 26.742) trata, entre otros aspectos relevantes para la tutela de aquellos, lo atinente a la historia clínica, que la define como un documento. Durante bastante tiempo se discutió si el hábeas data constituía una vía idónea para acceder a las historias clínicas, esto debido a que no fue concebido como una garantía destinada a operar sobre documentos, aunque éstos acumulen información personal, salvo que estén articulados de forma tal que conformen bases o bancos de datos personales.

El Capítulo IV de la ley, que está expresamente dedicado a la historia clínica, trata tanto a las historias clínicas no informatizadas como a las informatizadas, estableciendo diversos recaudos técnicos respecto de estas últimas y regulando los derechos del paciente en cuanto al tratamiento de sus datos en dicho entorno. Particularmente, en lo que resulta de interés, la ley indica que cuando cualquier sujeto que esté legitimado reclame el acceso a la historia clínica no encuentre satisfecho su derecho por consecuencia de la "negativa, demora o silencio del responsable que tiene a su cargo la guarda de la historia clínica", podrá ejercer "la acción directa de 'hábeas data' a fin de "asegurar el acceso y

obtención" de la historia clínica, y que a "dicha acción se le imprimirá el modo de proceso que en cada jurisdicción resulte más apto y rápido", siendo que en jurisdicción nacional, "esta acción quedará exenta de gastos de justicia" (art. 20). El decreto reglamentario, en sintonía con lo anterior, estipula que vencidos los plazos establecidos en el artículo 14 de la ley sin que se satisfaga el pedido, o en el caso en que, evacuado el informe de la historia clínica éste se estimara insuficiente, "quedará expedita la acción de protección de los datos personales o de hábeas data prevista en la Ley Nº 25.326", sin perjuicio de las sanciones que correspondan al establecimiento de salud respectivo (art. 20).

La norma, desde lo literal, habilita sólo un hábeas data de tipo informativo, es decir, un hábeas data de acceso a la historia clínica, a través del cual se puede obtener una copia de ésta. Sin embargo, nada impide que se puedan ejercer todos los otros "derechos ARCO" emanados de la ley de protección de los datos personales, en tanto se trata de información personal que, además de ser "sensible" y por lo tanto contener "datos especialmente protegidos" (arts. 2, 7 y 8 de la ley 25.326), puede causar efectos negativos sobre la salud del paciente, ya sea por la ausencia o por la inexactitud de información que resulta relevante para su tratamiento.

6. Conclusiones

Como puede verse a lo largo de este trabajo, si bien originalmente existían un puñado de tipos y subtipos de hábeas data, éstos fueron diversificándose en unos casos y ampliándose en cuanto a sus objetivos en otros, pero también surgieron varios nuevos, en especial al calor de las disposiciones emanadas del RGPD y de los Estándares de la RIPD.

La clasificación precedente, seguramente no será perfecta y probablemente seguirán las diversificaciones, ampliaciones y nuevas tipologías, como consecuencia de la evolución incesante de las TICs y del derecho.

Esperamos que este esfuerzo clasificatorio pueda auxiliar a los operadores jurídicos a comprender más acabadamente las posibilidades tutelares que nos brinda una acción tan simple y prometedora como el hábeas data y a aplicarla al máximo de sus posibilidades a fin de que se pueda tutelar lo más eficazmente posible no sólo su bien jurídico protegido principal ("el derecho a la protección de los datos personales") sino también todos los derechos que este derecho permite proteger.

DEL HÁBEAS DATA A LA ACCIÓN DE PROTECCIÓN DE PRIVACIDAD EN BOLIVIA.

Su evolución y desarrollo en la jurisprudencia del Tribunal Constitucional Plurinacional

✍ Alan E. Vargas Lima*

1. Los derechos humanos y fundamentales en el sistema constitucional boliviano

Para comenzar el análisis acerca de la regulación normativa del *Hábeas Data* en Bolivia, y así comprender adecuadamente su actual configuración constitucional como *Acción de Protección de Privacidad*, considero pertinente revisar brevemente el proceso de constitucionalización de los derechos humanos y fundamentales en el sistema constitucional boliviano, sobre la base de los estudios realizados por el jurista boliviano Dr. José Antonio Rivera Santibáñez, para luego hacer énfasis en la naturaleza jurídica, la configuración constitucional y procesal, así como el intenso

* Abogado Especialista en Derecho Constitucional y Procedimientos Constitucionales (UMSA). Miembro de la Academia Boliviana de Estudios Constitucionales; del Instituto Iberoamericano de Derecho Procesal Constitucional - Sección Nacional (Bolivia), del Instituto Latinoamericano de Investigación y Capacitación Jurídica (LATIN IURIS - Bolivia), y de la Asociación Euroamericana de Derechos Fundamentales (ASDEFUN - Bolivia). Miembro Honorario del Consejo Académico de la Sociedad Filosofía y Estado Constitucional APEX IURIS (Perú); Director adjunto del Centro Iberoamericano de Investigaciones Jurídicas y Sociales CIIJUS (México) – Capítulo Bolivia; y Secretario Académico de la Asociación Boliviana de Derecho Procesal Constitucional. Docente invitado a nivel pregrado y posgrado en distintas Universidades bolivianas. Autor de distintos Libros sobre Derecho Constitucional, Derecho Procesal Constitucional y Derechos Humanos. E-mail: alanvargas4784@gmail.com

desarrollo jurisprudencial de la referida Acción de Defensa que ahora prevé la Constitución boliviana de 2009, a través de los casos más relevantes, conocidos y resueltos por el Tribunal Constitucional de Bolivia.

Debemos comenzar señalando que en el sistema constitucional boliviano, el proceso de constitucionalización de los derechos humanos se ha operado de manera gradual; por lo que, atendiendo a razones metodológicas, se podría explicar dicho proceso en cuatro fases (cuya denominación es estrictamente convencional).

1.1. La fase inicial de la constitucionalización: las proclamas formales de derechos

La primera fase del referido proceso se podría denominar convencionalmente como la de "las proclamas formales de los derechos fundamentales"; y comprende el período transcurrido desde 1825 hasta antes de 1931. Se caracteriza por la mera proclamación formal de los derechos fundamentales en la Constitución, carente de todo mecanismo de protección y defensa de los mismos; lo que refleja un proceso inicial de positivación de los derechos humanos sin el componente necesario de la judicialización de los mismos.

En efecto, la Constitución Bolivariana de 1826 no consagró expresamente los derechos fundamentales de la persona, simplemente estableció un régimen de garantías constitucionales de carácter normativo para el ejercicio de los derechos civiles y políticos, que no los consagró sino presumió que eran inherentes a la naturaleza humana. Las garantías estaban previstas para la protección de los derechos a la libertad civil, la seguridad individual, la propiedad, la igualdad de las personas ante la ley, la libertad de expresión, el libre tránsito y el derecho a la privacidad o intimidad.

Posteriormente, y no obstante de haberse reformado la Constitución en los años 1831, 1834, 1839 y 1843, se mantuvo este sistema de tratamiento de los derechos fundamentales en la Ley Fundamental del Estado, es decir, con la sola proclamación formal de las garantías

constitucionales, sin consagrar expresamente los derechos fundamentales para permitir judicializar los derechos humanos.

En la reforma constitucional de 1851, el Constituyente modificó su posición respecto al tratamiento de los derechos humanos en el sistema constitucional boliviano, pasando a consagrar formalmente en la Constitución algunos derechos civiles y políticos. En efecto, en los artículos 1 al 25 de aquella Constitución, con el *nomen juris* "Del derecho público de los bolivianos" se consagraron por primera vez, en forma expresa, algunos derechos civiles, entre ellos el derecho a la libertad física y el libre tránsito, el derecho de petición, la libertad de pensamiento, el derecho a la intimidad o privacidad, la libertad de enseñanza, la libertad de trabajo y de industria, el derecho a la propiedad privada, y la igualdad a la Ley.

En las reformas constitucionales posteriores realizadas en el Siglo XIX, es decir, las efectuadas en los años 1861, 1868, 1871, 1878 y 1880, se mantuvo esa forma de tratamiento, dejando en la fase inicial el proceso de constitucionalización mediante la proclamación formal de los derechos humanos en la Constitución como derechos fundamentales.

2.2. La fase intermedia del proceso: positivación e inicios de judicialización

El segundo momento del proceso se podría denominar convencionalmente como el de "positivación e inicios de judicialización", comprende el período transcurrido desde 1931 hasta 1994.

Este periodo, que transcurre bajo el influjo del constitucionalismo social, se caracteriza por un lado, por la positivación ya sistematizada de los derechos humanos civiles y políticos, así como de una parte de los derechos económicos, sociales y culturales, consagrados como derechos fundamentales en el catálogo previsto por la Constitución; y, por otro, por la adopción de mecanismos para la judicialización de los derechos consagrados.

Con relación al proceso de positivación de los derechos humanos, cabe señalar que en la reforma constitucional de 1938 ya se

estableció un catálogo de derechos fundamentales, consagrando en tal condición a los derechos civiles y políticos; asimismo, se consagró como derechos constitucionales algunos derechos económicos, sociales y culturales; así, en la norma prevista por el artículo 106 de la Constitución, se proclamó que "el régimen económico debe responder esencialmente a principios de justicia social, que tiendan a asegurar para todos los habitantes una existencia digna del ser humano"; y se incorporaron en la Constitución los regímenes social, familiar, cultural y del campesinado.

En la reforma constitucional de 1967, se amplió el catálogo de los derechos fundamentales incorporando algunos derechos sociales como el derecho a la educación, el derecho al trabajo, el derecho a la justa remuneración y el derecho a la seguridad social.

En lo que se refiere al proceso de judicialización, corresponde señalar que en la reforma constitucional efectuada mediante el referéndum popular de 1931 se adoptó el *hábeas corpus* como vía tutelar para la protección del derecho a la libertad física o el de libre tránsito. De ahí que, en la Constitución adoptada en la Convención Nacional Constituyente de 1938, la norma prevista por el artículo 8 instituyó el hábeas corpus como un proceso constitucional sumarísimo para restablecer o restituir el derecho a la libertad física de la personas en los casos en los que sea restringido o suprimido de manera ilegal o indebida, a cuyo efecto estableció el procedimiento para su trámite respectivo.

Posteriormente, a través de la reforma constitucional de 1967 se introdujo al sistema constitucional boliviano, el *amparo constitucional* como una vía tutelar para la protección y restablecimiento inmediato de los derechos fundamentales y garantías constitucionales, con excepción del derecho a la libertad física, en aquellos casos en los que fuesen restringidos, suprimidos o amenazados de restricción o supresión por actos u omisiones de autoridades públicas o particulares. En lo que concierne a los derechos que protegía, el amparo constitucional no tuvo límites, salvo para el derecho a la libertad física que era protegido por

el hábeas corpus; de manera que, mediante el amparo constitucional se podían proteger los derechos civiles y políticos, así como los derechos económicos, sociales y culturales.

A través de la adopción de las vías tutelares referidas, el Constituyente creó las condiciones necesarias para judicializar los derechos humanos[1].

[1] El panorama antes descrito, hizo surgir un gran interés por el estudio de los derechos y sus garantías constitucionales en Bolivia, destacándose entre ellos, un primer ensayo sobre la Doctrina y Práctica del Hábeas Corpus (1950), escrito por el Catedrático universitario y Magistrado de la ciudad de Sucre, Dr. Manuel Durán Padilla, en donde básicamente expone sobre: *la libertad y la seguridad personales en las Constituciones de Bolivia, el Referéndum Popular de 1931 y el Hábeas Corpus, el primer Auto Supremo sobre Hábeas Corpus, el Hábeas Corpus a través de los Informes de los Presidentes del Supremo Tribunal, la Jurisprudencia de la Corte Suprema en los primeros años, la aplicación del Hábeas Corpus durante el estado de sitio, el Hábeas Corpus y la vigencia de la Constitución Política, y algún caso original de Hábeas Corpus en Bolivia*. Cfr. DURÁN PADILLA, Manuel. *Doctrina y Práctica del Hábeas Corpus*. Sucre, Bolivia: Universidad Mayor de San Francisco Xavier de Chuquisaca - Oficina de Publicaciones de la Facultad de Derecho, Ciencias Políticas y Sociales, 1950. Asimismo, el entonces Catedrático de Derecho Constitucional de la Universidad Mayor de San Andrés, Dr. Ciro Félix Trigo, a tiempo de estudiar las garantías de la libertad y seguridad personales en su brillante obra sobre Derecho Constitucional Boliviano, insertó un acápite referido al Recurso de Hábeas Corpus, en donde indaga acerca de sus antecedentes históricos, su desarrollo y su sentido normativo, de acuerdo a lo previsto por el artículo 8º de la Constitución Política de 1938, que hasta ese tiempo (y pese a sus reformas) permanecía vigente e inalterado. Cfr. TRIGO, Ciro Félix. Derecho Constitucional Boliviano. La Paz, Bolivia: Editorial Cruz del Sur, 1952. Págs. 390 - 400. También existe otro ensayo sobre el Recurso de Amparo (1967), en base a una conferencia dictada por el jurista y entonces Ministro de la Corte Suprema de Justicia, Dr. Enrique Oblitas Poblete (con una segunda edición publicada en 1979, que logró recopilar gran parte de la jurisprudencia constitucional producida hasta ese tiempo), en cuyo contenido expone sobre: *los Antecedentes Históricos, el Recurso de Amparo en México, el Amparo en la Argentina, el Amparo en Brasil y en otros países, para luego referirse al Recurso de Amparo en Bolivia, su configuración en el Proyecto de Código de Procedimiento Penal boliviano, y en la Constitución puesta en vigencia en 1967, algunas cuestiones emergentes, el primer caso de jurisprudencia sobre Amparo Constitucional, su tendencia en ese tiempo, incluyendo además como apéndice: fragmentos normativos sobre el procedimiento de Amparo en México, Jurisprudencia boliviana y Jurisprudencia de la Corte Suprema de EE.UU., el Recurso de Amparo en el Anteproyecto de Código de Procedimiento Penal, y Jurisprudencia Argentina sobre este instituto*. Cfr. OBLITAS POBLETE, Enrique. *Recurso de Amparo*. La Paz, Bolivia: Librería Editorial Popular, 1967.

2.3. La fase intensa del proceso: judicialización intensa

El tercer momento del proceso, convencionalmente, se lo podría denominar como el de la "judicialización intensa", que se inicia con la reforma constitucional de 1994. Se caracteriza por la adopción de un nuevo modelo de control de constitucionalidad, como es del modelo europeo o "kelseniano", con la creación del Tribunal Constitucional, entre cuyas funciones se encuentra la de protección de los derechos humanos.

Si bien el proceso de judicialización se inició con la adopción de las vías tutelares del hábeas corpus y el amparo constitucional, es a partir de la creación (1994) y el funcionamiento del Tribunal Constitucional (1999), como órgano encargado del control de constitucionalidad y máximo intérprete de la Constitución, que la judicialización de los derechos humanos se materializa y se hace intensiva. Ello se explica desde diversas perspectivas.

En primer lugar, al conocer y resolver las acciones tutelares de hábeas corpus y amparo constitucional, en grado de revisión, el Tribunal Constitucional dio una funcionalidad práctica a dichas acciones, reivindicándolas como vías idóneas para la protección inmediata y oportuna de los derechos fundamentales y garantías constitucionales. Esto se explica con el incremento del número de acciones tutelares planteadas a partir de 1999, un crecimiento en el orden del 20% anual.

En segundo lugar, el Tribunal Constitucional, asumiendo la posición del activismo judicial, dio fuerza expansiva a los derechos humanos en el sistema constitucional boliviano, pues mediante la interpretación integradora y acudiendo a la cláusula abierta extrajo las normas implícitas de la Constitución para integrar al catálogo de los derechos fundamentales otros derechos no consagrados expresamente y ampliar los núcleos esenciales, así como los alcances de las normas constitucionales respecto a los derechos fundamentales.

En tercer lugar, integró al catálogo de los derechos fundamentales previsto por la Constitución, los derechos humanos consagrados en las declaraciones, tratados o convenciones internacionales a los que se ha adherido o suscrito y ratificado el Estado boliviano, a través de la doctrina jurisprudencial del bloque de constitucionalidad.

Es importante señalar también que en esta última fase, mediante la reforma constitucional de 2004, el Constituyente adoptó el *hábeas data* como una vía jurisdiccional para la protección del derecho a la libre autodeterminación informativa[2].

[2] Cabe señalar que la incorporación del Recurso de Hábeas Data en el sistema constitucional de protección de los derechos fundamentales, resultó muy novedosa en Bolivia; sin embargo, con bastante anterioridad ya se había indagado acerca de la utilidad de insertar este mecanismo de protección en la Constitución. Es así que, una primera aproximación sobre el recurso de Hábeas Data –sin precedentes entre los estudios constitucionales bolivianos–, que explicaba los alcances jurídicos de su aplicación, y la necesidad de su incorporación vía reforma constitucional en Bolivia, fue propuesta inicialmente por el profesor Juan Ramos, Catedrático de Derecho Constitucional de la Facultad de Derecho de la UMSA. Cfr. RAMOS M., Juan. *Nuevo Recurso Constitucional de Hábeas Data en el Derecho Informático*. La Paz, Bolivia: Artes Gráficas Trama Color, 1999. Años más tarde, y una vez puesta en vigencia la reforma constitucional del año 2004, el Recurso de Hábeas Data, aparece por primera vez desarrollado sistemáticamente, en el Capítulo XXII de la segunda edición de la obra sobre Jurisdicción Constitucional, escrita por el entonces Magistrado del Tribunal Constitucional, Dr. José Antonio Rivera Santivañez, en donde expone de manera muy didáctica: *el concepto y antecedentes del Hábeas Data, su naturaleza jurídica, objetivos y fines, clasificación, así como los eventuales conflictos que podrían surgir de la aplicación del Hábeas Data en Bolivia*, para luego examinar su configuración en el sistema constitucional boliviano, sus características y los derechos que protege, explicando además el procedimiento para su interposición y su posterior revisión ante el Tribunal Constitucional, de acuerdo a la normativa constitucional vigente en aquel tiempo. Cfr. RIVERA SANTIVAÑEZ, José Antonio. *Jurisdicción Constitucional. Procesos Constitucionales en Bolivia*. Segunda Edición Actualizada. Cochabamba, Bolivia: Grupo Editorial Kipus, 2004. Págs. 425-456. Las bases doctrinales señaladas en aquel texto, sirvieron de base para estructurar los fundamentos jurídicos del fallo, en la Sentencia Constitucional Nº 0965/2004-R, de 23 de junio (Sentencia fundadora de línea jurisprudencial, como se ha reconocido en los fundamentos de la SC 0431/2005-R, de 28 de abril. Dicho entendimiento jurisprudencial fue reiterado posteriormente en las SSCC 0188/2006-R, de 21 de febrero, 1738/2010-R, de 25 de octubre, 1999/2010-R, de 26 de octubre, entre muchas otras). Luego de aquella importante publicación, un estudio doctrinal y de legislación comparada sobre los derechos tutelados por el hábeas data, su ámbito de aplicación

2.4. La fase de la consolidación del proceso de constitucionalización de los Derechos Humanos

Esta fase se inició con la última reforma constitucional encarada por la Asamblea Constituyente entre agosto de 2006 a diciembre de 2007, dando como resultado la Constitución promulgada el 07 de febrero de 2009. Se caracteriza porque el proceso de constitucionalización de los derechos humanos se consolida con la ampliación del catálogo de los derechos, la definición de la integración de los tratados y convenciones internacionales sobre derechos humanos al Derecho interno, la creación de nuevas acciones constitucionales para la protección de los derechos consagrados en el texto constitucional, y la consolidación del modelo europeo o "kelseniano" de control de constitucionalidad.

Con relación a la positivación de los derechos humanos, en la Constitución se ha ampliado considerablemente el catálogo con la inclusión de un grupo de derechos denominados fundamentales, la ampliación de los derechos civiles, políticos, económicos, sociales y culturales, y la incorporación de los derechos colectivos de las naciones y pueblos indígena originario campesinos.

Respecto a los tratados y convenciones internacionales sobre derechos humanos, la Constitución de manera explícita define el rango con el que se integran al Derecho interno, al establecer expresamente que: *"el bloque de constitucionalidad está integrado por los Tratados y Convenios internacionales en materia de Derechos Humanos y las normas*

y alcances, fue abordado por: DURÁN RIBERA, Willman R. *Contenido y alcances del hábeas data en Bolivia*. En: Anuario de Derecho Constitucional Latinoamericano – 2006. Tomo II. Montevideo, Uruguay: Fundación Konrad Adenauer, 2006. Págs. 903-931. Disponible en: https://bit.ly/2VtCyPg Años más tarde, se publicó una amplia investigación doctrinal sobre el derecho a la intimidad, a la privacidad, y el derecho a la protección de datos personales, incluyendo legislación comparada y una selección de las Sentencias Constitucionales más relevantes sobre el Hábeas Data en Bolivia: OSSIO ONOFRE, Freddy. *Protección de Datos Personales ¿Hábeas Data o Sistema de Data Protection?* Doctrina, Jurisprudencia y Legislación Comparada. La Paz, Bolivia: Editora M.V., 2010.

de Derecho Comunitario, ratificados por el país. (…)" (Artículo 410, parágrafo II constitucional), posicionándose así como un texto constitucional a la vanguardia de la protección de los derechos humanos en Latinoamérica[3].

Con relación a las garantías constitucionales, en la Ley Fundamental están consignadas las garantías normativas que constituyen obligaciones positivas y negativas para el Estado, como una medida efectiva para su goce pleno y ejercicio efectivo; además, se ha cambiado la denominación de los anteriores *Recursos Constitucionales*[4], y se han creado

[3] A nivel latinoamericano, la Constitución Boliviana del año 2009, ciertamente fue la primera que incluyó la voz "bloque de constitucionalidad" en su texto normativo (art. 410). Cfr. FERRER MAC-GREGOR, Eduardo y otros (Coords.). *Diccionario de Derecho Procesal Constitucional y Convencional*. Segunda edición. México: Instituto de Investigaciones Jurídicas de la Universidad Nacional Autónoma de México, 2014. Pág. 123. Disponible en: https://bit.ly/3j3r7rH Éste precepto referido al Bloque de Constitucionalidad, ciertamente constituye una reivindicación de las líneas jurisprudenciales establecidas con bastante anterioridad por la jurisprudencia del Tribunal Constitucional boliviano –en su primera época–; dado que, a partir de la emisión de la Sentencia Constitucional Nº 95/01, de 21 de diciembre de 2001 (cuyo Magistrado Relator fue el Dr. José Antonio Rivera Santivañez), que entre sus fundamentos jurídicos desarrolló los alcances del principio y derecho a la seguridad jurídica que proclamaba la Constitución vigente en ese entonces, el Tribunal Constitucional de Bolivia, asumiendo una posición de activismo judicial respecto a la protección de los derechos humanos, estableció por vez primera, que: *"es deber del Estado proveer seguridad jurídica a los ciudadanos asegurando a todas las personas el efectivo ejercicio de sus derechos fundamentales y garantías constitucionales proclamados por la Constitución, los tratados, convenios y convenciones suscritos y ratificados por el Estado como parte del bloque de constitucionalidad, así como las leyes ordinarias"*.

[4] De acuerdo a la jurisprudencia constitucional establecida en las Sentencias Constitucionales Nº 0040/2011-R de 7 de febrero, y Nº 0100/2011-R de 21 de febrero entre otras, el Tribunal Constitucional Plurinacional manifestó que: *"(…) La garantía jurisdiccional del hábeas corpus fue consagrada por el artículo 18 de la CPEabrg, actualmente, la Constitución Política del Estado vigente también la contempla pero con la denominación de Acción de Libertad artículos 125 al 127 de la (CPE); sin embargo, no se trata de un simple cambio de nomenclatura, sino de una precisión conceptual, pues conforme a la teoría del Derecho Procesal Constitucional, sustituir la denominación de "recurso", por la de "acción" -además de adecuar la legislación boliviana a la evolución de la doctrina de la materia- implica reconocer a esta garantía como "la facultad de demandar la protección de un derecho ante los órganos jurisdiccionales" o sea "poner en marcha el aparato del Estado para la protección de un derecho conculcado", en contraposición a la denominación de "recurso" que implicaba*

dos nuevas *Acciones de Defensa*, para la protección de los derechos de las personas: la Acción Popular para la protección de los derechos e intereses colectivos, y la Acción de Cumplimiento para la protección del derecho al cumplimiento efectivo de la Constitución y las leyes.

Finalmente, con relación al modelo de control de constitucionalidad, se ha consolidado el modelo europeo o "kelseniano" (con resabios del modelo americano o de la revisión judicial, según Rivera), con una modificación de la naturaleza jurídica del órgano encargado del control; ya que, de un lado, es independiente con relación a los órganos del poder constituido, y no forma parte de la estructura orgánica del Órgano Judicial; y de otro, es el Tribunal Constitucional Plurinacional, el que tiene la función de velar por la supremacía de la Constitución y ejercer el control de constitucionalidad sobre el sistema jurídico del Estado y sobre los sistemas jurídicos de las naciones y pueblos indígena originario campesinos; vale decir, sobre su derecho consuetudinario y sobre la impartición de justicia que realiza la jurisdicción indígena; cometido en el que deberá proteger y resguardar los derechos fundamentales[5].

considerarla como la simple impugnación o reclamación que, concedida por ley, efectúa quien se considera perjudicado o agraviado por la providencia de un juez o tribunal para que el superior la reforme o revoque y que por ello supone la existencia previa de un litigio (García Belaunde, Domingo. "El hábeas corpus en el Perú". Universidad Mayor de San Marcos, 1979, p. 108). La precisión conceptual que implica el cambio de denominación, también conlleva que, englobando el ámbito de protección y las características esenciales del hábeas corpus, la acción de libertad adquiera una nueva dimensión; en ese sentido, se constituye en una garantía jurisdiccional esencial, pues su ámbito de protección ahora incorpora al derecho a la vida -bien jurídico primario y fuente de los demás derechos del ser humano- junto a la clásica protección al derecho a la libertad física o personal, la garantía del debido proceso en los supuestos en que exista vinculación directa con el derecho a la libertad física y absoluto estado de indefensión (SC 1865/2004) y el derecho a la libertad de locomoción, cuando exista vinculación de este derecho con la libertad física o personal, el derecho a la vida o a la salud (SC 0023/2010-R). (…)". Cita contenida en la Sentencia Constitucional Plurinacional Nº 0009/2012, de fecha 16 de marzo de 2012 (Sala Primera Especializada). Este entendimiento, podría ser relativamente aplicable para explicar el cambio de nomenclatura del Hábeas Data en Bolivia.

[5] Cfr. RIVERA SANTIVAÑEZ, José Antonio. La protección de los derechos humanos y fundamentales en el Estado Plurinacional de Bolivia. En: CARBONELL, Miguel,

2. El hábeas data en el sistema constitucional boliviano

De acuerdo al criterio de los profesores Ekmekdjian y Pizzolo[6], la acción de Hábeas Data se define como el derecho que asiste a toda persona –identificada o identificable– a solicitar judicialmente la exhibición de los registros –públicos o privados– en los cuales están incluidos sus datos personales o los de su grupo familiar, para tomar conocimiento de su exactitud; a requerir la rectificación, la supresión de datos inexactos u obsoletos, o que impliquen discriminación.

En el caso de Bolivia, el hábeas data, como una vía procesal de carácter instrumental, para la protección del derecho a la autodeterminación informática, fue incorporado al sistema constitucional mediante la Ley Nº 2631 de Reforma a la Constitución Política del Estado, de fecha 20 de febrero de 2004; determinando en su artículo 23, lo siguiente:

> *"I. Toda persona que creyere estar indebida o ilegalmente impedida de conocer, objetar u obtener la eliminación o rectificación de los datos registrados por cualquier medio físico, electrónico, magnético, informático en archivos o bancos de datos públicos o privados que afecten su derecho fundamental a la intimidad y privacidad personal y familiar, a su imagen, honra y reputación reconocidos en esta Constitución, podrá interponer el recurso de Hábeas Data ante la Corte Superior del Distrito o ante cualquier Juez de Partido a elección suya.*
>
> *II. Si el tribunal o juez competente declara procedente el recurso, ordenará la revelación, eliminación o rectificación de los datos personales cuyo registro fue impugnado.*

FIX-FIERRO, Héctor, GONZÁLES PÉREZ, Luis Raúl y VALADÉS, Diego (Coords.). *Estado Constitucional, Derechos Humanos, Justicia y Vida universitaria. Estudios en Homenaje a Jorge Carpizo – Derechos Humanos*. Tomo V. Volumen 2. México: Instituto de Investigaciones Jurídicas de la Universidad Nacional Autónoma de México, 2015. Págs. 311-346. Disponible en: https://bit.ly/2Ye14Fn

[6] Cfr. EKMEKDJIAN, Miguel Angel, y PIZZOLO, Calogero. *Hábeas Data. El derecho a la intimidad frente a la revolución informática*. 2ª Edición. Buenos Aires, Argentina: Ediciones Depalma, 1998.

III. La decisión que se pronuncie se elevará en revisión, de oficio ante el Tribunal Constitucional, en el plazo de veinticuatro horas, sin que por ello se suspenda la ejecución del fallo.

IV. El recurso de Hábeas Data no procederá para levantar el secreto en materia de prensa.

V. El recurso de Hábeas Data se tramitará conforme al procedimiento establecido para el Recurso de Amparo Constitucional previsto en el Artículo 19° de esta Constitución".

Como se puede ver, el texto constitucional reformado en aquel tiempo, contenía normas de carácter sustantivo, porque en su primer parágrafo instituye el hábeas data como una garantía constitucional, determinando su alcance; y, establece normas de carácter procesal dando la configuración básica en cuanto al trámite de esta acción tutelar.

Tomando en cuenta sus fines y objetivos, así como la aplicación supletoria de las normas previstas por el artículo 19 de la Constitución (abrogada), dispuesta por el artículo 23 parágrafo V antes referido, se entiende que *el hábeas data es una acción de carácter subsidiario*, es decir, que solamente puede ser viable en el supuesto que el titular del derecho lesionado haya reclamado ante la entidad pública o privada encargada del banco de datos, la entrega de la información o datos personales obtenidos o almacenados, y en su caso, la actualización, rectificación o supresión de aquella información o datos falsos, incorrectos, o que inducen a discriminaciones, y no obtiene una respuesta positiva o favorable a su requerimiento, o sea que la entidad pública o privada no asume inmediatamente la acción solicitada. Dicho de otro modo, el hábeas data se activa exclusivamente cuando la persona demuestra que ha acudido previamente ante la entidad pública o privada para pedir la restitución de su derecho lesionado y no ha podido lograr la reparación a dicha vulneración[7].

[7] Posteriormente, y siguiendo este entendimiento jurisprudencial, en un caso de hábeas data en que el recurrente solicitó se ordene la rectificación de sus datos personales y de su familia, el Tribunal Constitucional estableció que de acuerdo a la normativa

La legitimación activa del hábeas data recae en la persona natural o jurídica –aunque el precepto constitucional no lo determina de esa manera en forma expresa, se entiende que dentro de la protección de este recurso se puede y debe abarcar tanto a las personas físicas como a las jurídicas, de quienes también se pueden registrar datos e informaciones– respecto de la cual, la entidad pública o privada haya obtenido y tenga registrados datos e informaciones que le interesen a aquella

vigente: "las rectificaciones de los datos asentados en partidas de nacimiento, matrimonio y defunción, sólo pueden ser realizadas a través de las dos vías establecidas en las normas glosadas: la judicial o la administrativa; en consecuencia, si es que previamente no se ha cumplido ese procedimiento, no es posible acudir directamente al hábeas data; pues, conforme a la norma contenida en el artículo 23.V de la Constitución Política del Estado (CPE), que establece que este recurso "…se tramitará conforme al procedimiento establecido para el Recurso de Amparo Constitucional previsto en el Artículo 19° de esta Constitución", al hábeas data le es aplicable la doctrina constitucional sentada para el amparo constitucional, y en consecuencia, se debe aplicar el principio de subsidiariedad, establecido en el artículo 19.IV de la CPE; lo que significa que sólo se activa cuando el recurrente ha agotado los medios o recursos que tenía a su alcance para lograr conocer, objetar u obtener la eliminación, rectificación de los datos públicos o privados que afectan a su derecho a la intimidad y privacidad personal y familiar, a su imagen, honra y reputación" (Cfr. Sentencia Constitucional Nº1511/2004-R, de 21 de septiembre, que reitera la aplicación del principio de subsidiariedad en el recurso de hábeas data). De igual manera, en la Sentencia Constitucional Nº0397/2005-R, de 19 de abril, se estableció lo siguiente: "Entendida la tramitación del recurso de hábeas data se debe expresar que en el caso de autos es aplicable el principio de subsidiariedad antes desarrollado, pues el recurrente denuncia que la lesión a sus derechos a la imagen, honra y reputación, se produce por el registro asentado en el RUAT (…), por tanto pide que tal registro sea eliminado; sin embargo, acude a la jurisdicción constitucional y al recurso de hábeas data sin haber agotado antes las vías ordinarias encargadas de la eliminación del registro que se intenta suprimir, ya que de los datos cursantes en el expediente, se constata que el actor no solicitó a la autoridad recurrida la eliminación del registro señalado anteriormente, sino que en forma directa promovió el presente recurso, sustentando tal hecho en la supuesta inexistencia de mecanismos de atención al administrado en el RUAT; siendo insuficiente afirmar que no existe mecanismo administrativo encargado de dar respuesta a la solicitud de eliminación de los datos que causan agravio, lo que además no es evidente, sino que *se debe demostrar haber solicitado la eliminación de los datos, así como también que la respuesta a dicha solicitud fue negativa, con prueba documental que demuestre que efectivamente se acudió ante las autoridades recurridas, pues caso contrario la jurisdicción constitucional se ve impedida de ingresar a analizar el fondo del recurso*" (Línea jurisprudencial reiterada en la Sentencia Constitucional Nº1999/2010-R, de 26 de octubre).

conocer, aclarar, rectificar, modificar, o eliminar, y que no haya tenido respuesta favorable por la citada entidad para lograr esos extremos.

La legitimación pasiva de esta acción, tomando en consideración que protege a la persona en el ejercicio de su derecho a la autodeterminación informativa contra cualquier manejo impropio de sus datos personales registrados o almacenados en bancos de datos públicos o privados, recae en el personero legal de la entidad pública o privada que tengan los archivos o bancos de datos personales de quien se sienta afectado en el ejercicio del citado derecho (Cfr. Sentencia Constitucional Nº0965/2004-R, de 23 de junio; entendimiento reiterado en la Sentencia Constitucional Nº0488/2005-R, de 9 de mayo).

3. Concepto, naturaleza jurídica y ámbitos de protección[8]

Siguiendo la doctrina del Dr. José Antonio Rivera Santivañez en su obra *"Jurisdicción Constitucional. Procesos Constitucionales en Bolivia"* (2004), el hábeas data se define como el proceso constitucional de carácter tutelar que protege a la persona en el ejercicio de su derecho a la "autodeterminación informática"[9].

[8] Este acápite y los siguientes, corresponden a los fundamentos jurídicos expuestos en la Sentencia Constitucional Nº0965/2004-R, de 23 de junio de 2004 (Sentencia Fundadora de línea jurisprudencial), que desarrolla las bases doctrinales de este instituto y su configuración constitucional, sobre la base de lo expuesto en la citada obra del entonces Magistrado del Tribunal Constitucional de Bolivia, Dr. José Antonio Rivera.

[9] Cfr. RIVERA SANTIVAÑEZ, José Antonio. *Jurisdicción Constitucional. Procesos Constitucionales en Bolivia*. Segunda Edición Actualizada. Cochabamba, Bolivia: Grupo Editorial Kipus, 2004. Por su parte, el profesor Pablo Dermizaky, llegó a establecer en aquel tiempo, que el hábeas data "es un derecho y una garantía de los derechos de intimidad y de identidad personal (…). Habilita a solicitar judicialmente la exhibición de registros públicos y privados para conocer los datos que contiene sobre la persona individual y/o su grupo familiar, a fin de requerir su rectificación, eliminación o complementación, cuando se considere que su inexactitud es perjudicial, discriminatoria, deshonrosa o infamante. La denominación proviene de dos voces, una latina, *hábeas*, que quiere decir tener, haber, y otra inglesa, *data*, que es el plural de datos (obtener los datos)". Cfr. DERMIZAKY PEREDO, Pablo. *Derecho Constitucional*. Séptima Edición (revisada y actualizada). Cochabamba, Bolivia: Editora J & V.,

Es una garantía constitucional que, sin desconocer el derecho a la información, al trabajo y al comercio de las entidades públicas o privadas que mantienen centrales de información o bancos de datos, reivindica el derecho que tiene toda persona a verificar qué información o datos fueron obtenidos y almacenados sobre ella, cuáles de ellos se difunden y con qué objeto, de manera que se corrijan o aclaren la información o datos inexactos, se impida su difusión y, en su caso, se eliminen si se tratan de datos o informaciones sensibles que lesionan su derecho a la vida privada o íntima en su núcleo esencial referido a la honra, buena imagen o el buen nombre.

Partiendo de los conceptos referidos, se puede inferir que el hábeas data es una garantía constitucional por lo mismo se constituye en una acción jurisdiccional de carácter tutelar que forma parte de los procesos constitucionales previstos en el sistema de control de la constitucionalidad. Es una vía procesal de carácter instrumental para la

2004. Pág. 160. Respecto a la doble dimensión del hábeas data, la Corte Constitucional de Colombia, a través de la Sentencia SU-458 de 2012, precisó lo siguiente: "La Corte reafirma esta condición del hábeas data como derecho autónomo y como garantía. Como derecho autónomo, tiene el hábeas data un objeto protegido concreto: el poder de control que el titular de la información puede ejercer sobre quién (y cómo) administra la información que le concierne. En este sentido el hábeas data en su dimensión subjetiva faculta al sujeto concernido a conocer, actualizar, rectificar, autorizar, incluir, excluir, etc., su información personal cuando ésta es objeto de administración en una base de datos. A su vez, como garantía, tiene el hábeas data la función específica de proteger, mediante la vigilancia del cumplimiento de las reglas y principios de la administración de datos, los derechos y libertades que dependen de (o que pueden ser afectados por) una administración de datos personales deficiente. Por vía de ejemplo, el hábeas data opera como garantía del derecho al buen nombre, cuando se emplea para rectificar el tratamiento de información falsa. Opera como garantía del derecho a la seguridad social, cuando se emplea para incluir, en la base de datos, información personal necesaria para la prestación de los servicios de salud y de las prestaciones propias de la seguridad social. Opera como garantía del derecho de locomoción, cuando se solicita para actualizar información relacionada con la vigencia de órdenes de captura, cuando éstas por ejemplo han sido revocadas por la autoridad competente. Y finalmente, puede operar como garantía del derecho al trabajo, cuando se ejerce para suprimir información que funge como una barrera para la consecución de un empleo" (Cfr. Sentencia T-020/14, de 27 de enero de 2014).

defensa de un derecho humano como es el derecho a la autodeterminación informática[10].

Como una acción tutelar, el hábeas data sólo se activa a través de la legitimación activa restringida, la que es reconocida a la persona afectada, que puede ser natural o jurídica. En consecuencia, no admite una activación por la vía de acción popular, es decir, no se reconoce la legitimación activa amplia.

Así, el hábeas data como un proceso constitucional de carácter tutelar, tiene la finalidad de brindar tutela efectiva, inmediata e idónea a la persona en el ejercicio de su derecho a la autodeterminación informática. La protección que brinda el hábeas data abarca los siguientes ámbitos:

a) *Derecho de acceso a la información* o registro de datos personales obtenidos y almacenados en un banco de datos de la entidad pública o privada, para conocer qué es lo que se dice respecto a la persona que plantea el hábeas data, de manera que pueda verificar si la información y los datos obtenidos y almacenados son los correctos y verídicos; si no afectan las áreas calificadas como sensibles para su honor, la honra y la buena imagen personal;

[10] "Esta última (autodeterminación informática) entendida como el derecho de la persona -individual o colectiva- a ser única titular de los datos inherentes a su personalidad, por consiguiente la única facultada a manejarlos o autorizar a que sean difundidos a través de la informática, entendiendo esta denominación como la "información automática", es decir la contracción de ambas. Luego de esta aclaración conceptual y descriptiva del término, acudiendo siempre a la doctrina contemporánea sobre la materia, el hábeas data "busca primordialmente asegurar una protección de tipo jurisdiccional a diversos aspectos de la autodeterminación informativa" (Eloy Espinosa-Saldaña Barrera), posición doctrinal coincidente con la formulada en la SC 965/2004-R." (Cfr. Sentencia Constitucional Nº1572/2004-R, de 4 de octubre, que reitera la aplicación del principio de subsidiariedad en el recurso de hábeas data).

b) *Derecho a la actualización de la información* o los datos personales registrados en el banco de datos, añadiendo los datos omitidos o actualizando los datos atrasados; con la finalidad de evitar el uso o distribución de una información inadecuada, incorrecta o imprecisa que podría ocasionar graves daños y perjuicios a la persona;

c) *Derecho de corrección o modificación de la información* o los datos personales inexactos registrados en el banco de datos público o privado, tiene la finalidad de eliminar los datos falsos que contiene la información, los datos que no se ajustan de manera alguna a la verdad, cuyo uso podría ocasionar graves daños y perjuicios a la persona;

d) *Derecho a la confidencialidad* de cierta información legalmente obtenida, pero que no debería trascender a terceros porque su difusión podría causar daños y perjuicios a la persona;

e) *Derecho de exclusión de la llamada "información sensible"* relacionada al ámbito de la intimidad de la persona, es decir, aquellos datos mediante los cuales se pueden determinar aspectos considerados básicos dentro del desarrollo de la personalidad, tales como las ideas religiosas, políticas o gremiales, comportamiento sexual; información que potencialmente podría generar discriminación o que podría romper la privacidad del registrado[11].

En consecuencia, el hábeas data es una garantía constitucional que tiene por objetivo el contrarrestar los peligros que conlleva el desarrollo de la informática, en lo referido a la distribución o difusión ilimitada de información sobre los datos de la persona; y tiene por finalidad principal el proteger el derecho a la autodeterminación informática,

[11] Estos ámbitos de protección del hábeas data, también fueron reiterados en la Sentencia Constitucional Nº0030/2006-R, de 11 de enero de 2006.

preservando la información sobre los datos personales ante su utilización incontrolada, indebida e ilegal, impidiendo que terceras personas usen datos falsos, erróneos o reservados que podrían causar graves daños y perjuicios a la persona[12].

4. Función esencial, tipología y efectos jurídicos del hábeas data

El hábeas data tiene la función primordial de establecer un equilibrio entre el "poder informático" y la persona titular del derecho a la autodeterminación informática, es decir, entre la entidad pública o privada que tiene la capacidad de obtener, almacenar, usar y distribuir la información sobre datos personales y la persona concernida por la información.

La doctrina ha clasificado los diversos tipos de hábeas data que pueden presentarse, a saber:

a) *Hábeas data informático*, que permite a la persona ejercer su derecho a la autodeterminación informática accediendo a los registros o bancos de datos públicos o privados destinados a proveer información para que pueda recabar toda la información obtenida, almacenada y registrada en torno a su persona. Aquí se tienen las variantes de:

a.a) Hábeas data exhibitorio, para que la persona que lo plantea tome conocimiento de sus datos, almacenados en bancos de datos;

a.b) Hábeas data finalista, para que la persona sepa para qué o para quién se almacenaron sus datos;

[12] Una recopilación muy útil de la normativa sobre protección de datos personales en Bolivia, puede verse en: https://bit.ly/38e7pUY (2019); y una obra colectiva reciente, que recoge en una investigación práctica y comparada, la legislación específica sobre protección de datos de diferentes naciones del mundo, corresponde a: LÓPEZ CARBALLO, Daniel A., y GONZÁLEZ-CALERO MANZANARES, Francisco Ramón (Coords.). *Protección de Datos y Hábeas Data: Una visión desde Iberoamérica*. Madrid, España: Agencia Española de Protección de Datos, 2015. Disponible en: https://bit.ly/2Fycpd2

a.c) Hábeas data autoral, para que la persona conozca quién tuvo, almacenó y registró sus datos.

b) *Hábeas data aditivo*, permite a la persona lograr que se actualice el registro de sus datos, y se adicione un dato personal que no fue inserto en el banco de datos;

c) *Hábeas data rectificador*, a efecto de otorgar la tutela a la persona perjudicada en su derecho a la libertad informática, disponiendo que los encargados del banco de datos procedan a sanear los datos falsos o incorrectos almacenados;

d) *Hábeas data reservador*, es el que permite a la persona conservar el ámbito de su intimidad frente la divulgación de información obtenida y almacenada en los registros públicos o privados, información que en su criterio es sensible y debe mantenerse en reserva;

e) *Hábeas data cancelatorio o exclusorio*, por medio del que se logra se borren los datos conocidos como información sensible.

Dentro de ese marco, a efectos de delimitar el campo de acción de este recurso constitucional, es necesario expresar que para la aplicación del hábeas data existen distintos posibles planteamientos:

1) El primero está referido a la constatación sobre la existencia del registro. Esta cuestión parte de un primer problema relativo a la existencia misma del banco de datos, ya que si él no existiera, no habría solicitud atendible alguna. Acreditada la existencia, y ante la sospecha de la inclusión de datos suyos, la persona podrá solicitar la constatación sobre el contenido del asiento a ella referido, su finalidad y uso concreto;

2) El segundo planteamiento concierne al control del contenido. La persona que accedió al registro realizado respecto suyo, ahora puede controlar y analizar el contenido de los datos. Este control puede materializarse en un actuar concreto dirigido a diferentes acciones, tales como:

a) *Anular el asiento*, cuando el dato no responde a la realidad de los hechos, cuando nunca existió la circunstancia que anota, o si, habiendo existido, desapareció o se extinguió por diferentes causas;

b) *Actualizar el asiento*, cuando en el registro figuran algunos datos ciertos y otros que se han modificado por el tiempo o por alguna acción del titular, por lo que se solicita que toda la información se relacione con las actuales circunstancias del afectado;

c) *Rectificar o modificar*, si en el registro se ha consignado información que es incorrecta, falsa o mendaz;

d) *Aclarar,* si en el registro existe información que, si bien es cierta, está dada en una forma incorrecta o equívoca respecto de la real situación;

e) *Anulación de registros referidos a datos "sensibles",* cuando dichos datos sólo le pertenecen e incumben al titular, y están referidos a temas, circunstancias, y en general a todo lo que, de ser conocido públicamente, puede generar perjuicios o discriminación.

f) *Reserva de datos,* cuando la información resulta correcta, y también lo es su origen, pero no se trata de información susceptible de darse indiscriminadamente o publicarse sin autorización del titular. La acción tiende a preservar que los datos sean revelados, salvo que obedezca a la solicitud de autoridad competente o del interesado, debidamente fundada;

g) *Datos que importen discriminación,* implicarán necesariamente su anulación, por ser ilegítima la posesión de este tipo de información;

5. Etapas de sustanciación del hábeas data, dimensiones de su tutela y límites

La garantía del hábeas data se desarrolla en dos etapas, la prejudicial y la judicial propiamente dicha: **a)** etapa prejudicial, se produce cuando la persona que pretende la exhibición del registro y, si es el caso, la corrección de los datos asentados en él, debe notificar fehacientemente a la empresa titular del banco de datos, su pretensión de que se le exhiban sus datos incluidos en el registro, y pedir, si así estima necesario, sean rectificados, corregidos, modificados o eliminados. Si la entidad requerida consiente en lo solicitado, queda consumado el ejercicio del derecho con esa sola fase prejudicial. Si el interesado no recibe respuesta alguna o se le da una negativa a lo solicitado, puede válidamente pasar a la siguiente fase; **b)** etapa judicial, que se realiza -se reitera- cuando el titular del registro se niega a exhibir los datos, hace caso omiso del requerimiento, o si exhibiéndolos, pretendiera mantener los datos cuestionados, negándose a rectificarlos o a cancelarlos en su caso, entonces es procedente la vía constitucional del hábeas data.

Las dimensiones de la persona que están bajo la tutela del hábeas data pueden sintetizarse en las siguientes:

1) El propio cuerpo, referido a la salud de la persona o de los miembros de su familia;

2) Las ideas y creencias religiosas, filosóficas, políticas;

3) La vida pasada, relacionada con el ámbito que a la persona podría generarle bochorno al estar compuesta por pasajes desagradables o ingratos;

4) La vida doméstica, relacionada con los hechos o situaciones que se producen dentro del hogar;

5) La vida familiar concerniente con el matrimonio y la filiación;

6) La vida amorosa, relaciones de amistad, la vida sexual;

7) El ámbito de las comunicaciones personales que comprende las diferentes vías de comunicación;

8) La situación económica de las personas referidas al nivel de ingreso, patrimonio, inversiones, obligaciones financieras.

En cuanto a los límites del hábeas data[13], es importante remarcar que, como vía procesal instrumental, protege a la persona en su derecho a la autodeterminación informática, activándose contra el poder informático. De manera que cabe advertir que existe un límite en cuanto a los alcances del hábeas data que se establece en el ejercicio de la libertad o derecho de información y libertad de expresión. En efecto, el hábeas data no se activa contra la difusión de información a través de los medios masivos de comunicación social, toda vez que este medio no es el adecuado para viabilizar el derecho de réplica por parte de un medio de prensa con relación a una información difundida que la persona considere inexacta o que agravia su derecho al honor, la honra o la buena imagen, o lesione su vida privada o íntima.

Debe quedar claramente establecido que el hábeas data no es un medio para ejercer control sobre los medios de comunicación social y el ejercicio de la libertad de expresión e información, no es un mecanismo para establecer censura previa ni correctiva (Cfr. Sentencia Constitucional Nº0965/2004-R, de 23 de junio de 2004).

Posteriormente, la jurisprudencia del Tribunal Constitucional boliviano, hizo referencia a la Sentencia T-729 de 2002, de la Corte Constitucional de Colombia, en la cual se había definido que: *"el derecho fundamental de hábeas data es aquel que otorga la facultad al titular de datos personales, de exigir a las administradoras de datos personales el acceso, inclusión, exclusión, corrección adición, actualización y certificación*

[13] Cfr. RIVERA S., José Antonio; JOST, Stefan y otros. *La Constitución Política del Estado: Comentario Crítico*. Tercera Edición, actualizada con las reformas del 2004. Cochabamba, Bolivia: Talleres Gráficos Kipus, 2005. Pág. 123.

de los datos, así como la limitación en las posibilidades de divulgación, publicación o cesión de los mismos, conforme a los principios que informan el proceso de administración de datos personales".

De ahí que, y siguiendo dicha Sentencia, ese derecho, contiene los siguientes **principios:**

a) De Libertad: por el cual las personas pueden autorizar la recolección, conservación, uso y circulación de sus datos existentes en una base de datos pública o privada;

b) De necesidad: Los datos deben ser los estrictamente necesarios para el cumplimiento de los fines de las bases de datos de que se trate;

c) De veracidad: los datos deben ser reales y ciertos;

d) De integridad: los datos deben ser completos;

e) De finalidad: la recopilación de datos debe tener un fundamento lícito;

f) De utilidad: su función debe ser clara y determinable;

g) De circulación restringida: La divulgación y circulación de la información está ligado al objeto de la base de datos, a la finalidad y a la autorización del titular;

h) De incorporación de la bases de datos: cuando de la inclusión de datos personales en determinadas bases deriven situaciones ventajosas para el titular, la entidad administradora de datos estará en la obligación de incorporarlos;

i) De caducidad: La información desfavorable al titular debe ser retirada de las bases de datos siguiendo criterios de razonabilidad y oportunidad;

j) De individualidad: No se permite el cruce de datos a partir de información proveniente de diversas bases de datos.

En Bolivia el derecho de autodeterminación informática no estaba expresamente reconocido en la Constitución (reformada el año 2004); empero, se ha entendido que deriva de la protección del derecho a la vida privada y la intimidad familiar y personal, a la propia imagen, a la honra de la persona y de su familia; derechos que emanan de la dignidad de la persona reconocida y consagrada en el artículo 6 de la Ley Fundamental (Cfr. Sentencia Constitucional Nº 0488/2005-R, de 9 de mayo).

6. Los derechos tutelados por el recurso de hábeas data[14]

El hábeas data ha sido considerado un proceso constitucional especializado en la protección de los derechos de quienes se encuentran registrados en bancos de datos, sean públicos o privados, que pueden contener información desactualizada, falsa, equivocada, o sensible; permitiendo al agraviado, a través de esta acción, lograr el conocimiento, la modificación, eliminación o reserva de los datos existentes, a fin de tutelar la esfera personal de perturbaciones externas no deseadas, garantizando, fundamentalmente, la privacidad o intimidad personal, protegiendo a la persona frente al almacenamiento, registro y utilización indebida de datos.

Tiene como antecedente la definición del derecho a la privacidad como *the right to be let alone*[15], esto es, "el derecho a ser dejado en sole-

[14] Este acápite y el siguiente, corresponden a los fundamentos jurídicos expuestos en la Sentencia Constitucional Nº0188/2006-R, de 21 de febrero.

[15] Aunque, sin duda, la paternidad del derecho a la privacidad en el sistema jurídico norteamericano se atribuye generalmente a los célebres abogados de Boston, Samuel D. Warren y Louis D. Brandeis, quienes reformularon la expresión «the right to be let alone» en un estudio publicado en diciembre de 1890 en la Harvard Law Review con el título «The Right to Privacy», cuando reaccionaban frente a la divulgación indiscriminada por la prensa de información privada y afirmaban que impedir su publicación es solo un ejemplo del derecho más general del individuo a no ser molestado (the more general right of the individual to be let alone), defendiendo un «right to privacy» que le otorga a toda persona plena disponibilidad para decidir en qué medida «pueden ser comunicados a otros sus pensamientos, sentimientos y emociones». Cfr. NIEVES SALDAÑA, María.

dad", que fue elaborada por el Juez Thomas Cooley, y desarrollada por los juristas norteamericanos Samuel D. Warren y Louis D. Brandeis, que intentaron proteger a las personas de aquellos actos o datos personales que eran divulgados sin el consentimiento del afectado, combatiendo las intromisiones ilegítimas en la vida privada[16].

Este derecho a la privacidad primigenio, por el desarrollo tecnológico de los últimos años, que permite el almacenamiento ilimitado de información y su transmisión, tiene actualmente una nueva dimensión: no sólo es el derecho a rechazar la intromisión de terceras personas en la esfera privada, sino también es el derecho de controlar la información y, en su caso, rectificar los datos[17].

Nuestra Ley Fundamental, en armonía con la doctrina y la legislación comparada, ha instituido el hábeas data como una acción tutelar

"El Derecho a la Privacidad en los Estados Unidos: aproximación diacrónica a los intereses constitucionales en juego". En: UNED. Teoría y Realidad Constitucional, núm. 28, 2011, pp. 279-312. Disponible en: https://bit.ly/2QmGK09

[16] El artículo publicado en 1890 por Warren y Brandeis en la Harvard Law Review bajo el título «The Right to Privacy», es considerado el ensayo fundacional de la protección de la privacidad en los Estados Unidos y el artículo doctrinal más influyente de la literatura jurídica norteamericana. Sin duda su influencia ha sido incuestionable, ha originado la preocupación colectiva por el reconocimiento y garantía de la esfera privada, ha generado al menos cuatro acciones civiles para su protección y ha encuadrado y fundamentado el discurso constitucional del derecho a la privacidad en los Estados Unidos durante todo el siglo XX. Sin embargo, en la concepción formulada por Warren y Brandeis en «The Right to Privacy» no cabe reconocer exclusivamente una dimensión individual o subjetiva, antes al contrario, su defensa de la privacidad presenta igualmente una dimensión colectiva y social que coadyuva al mantenimiento y avance del sistema democrático, pues, en última instancia, la privacidad contribuye a establecer los límites del control estatal sobre los individuos y a definir el atributo esencial de la ciudadanía. Cfr. NIEVES SALDAÑA, María. «The right to privacy». La génesis de la protección de la privacidad en el sistema constitucional norteamericano: el centenario legado de Warren y Brandeis. En: UNED. Revista de Derecho Político Nº 85, septiembre-diciembre 2012, págs. 195-240. Disponible en: https://bit.ly/3aQVUEs

[17] Cfr. DURÁN RIBERA, Willman R. *Contenido y alcances del hábeas data en Bolivia*. En: Anuario de Derecho Constitucional Latinoamericano - 2006. Tomo II. Montevideo, Uruguay: Fundación Konrad Adenauer, 2006. Págs. 903-931. Disponible en: https://bit.ly/2VtCyPg

de los *derechos a la intimidad y privacidad personal y familiar, a la imagen, honra y reputación*, derechos que si bien no estaban dentro del catálogo establecido en el artículo 7 de la Constitución (abrogada), sí formaban parte de los derechos fundamentales reconocidos por la misma Constitución, conforme lo ha establecido la jurisprudencia del Tribunal Constitucional en las SSCC 69/2004, 338/2003-R, 1662/2003-R, entre otras, al señalar que: *"En Bolivia, si bien los derechos fundamentales de la personas están consagrados en el artículo 7 de la Constitución, ello no significa que la misma, de manera implícita, no reconozca otros derechos no incluidos en el catálogo del precepto aludido, pero que por su naturaleza y ubicación sistemática, son parte integrante de los derechos fundamentales que establece el orden constitucional boliviano".*

De lo dicho se concluye que a través del recurso de hábeas data sólo era posible proteger los derechos señalados expresamente por el artículo 23 de la Constitución (abrogada); en consecuencia, no es posible, mediante este recurso, tutelar otros derechos, pues para éstos existían otros recursos constitucionales previstos expresamente por la Ley Fundamental (entendimiento reiterado por la Sentencia Constitucional Nº0267/2006-R, de 23 de marzo).

7. Sobre el derecho de acceso a la información

El derecho de acceso a la información pública, está previsto en el artículo 13 de la Convención Americana sobre Derechos Humanos (CADH), *como parte integrante del derecho a la libre expresión* consagrado por ese precepto, que establece:

> *"1. Toda persona tiene derecho a la libertad de pensamiento y de expresión. Este derecho comprende la libertad de buscar, recibir y difundir información 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".

La Corte Interamericana, interpretando el artículo 13 de la CADH, en la Opinión Consultiva sobre *"La Colegiación obligatoria de periodistas"*, señaló que la libertad de pensamiento y expresión "comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole" y, en consecuencia, existe una doble dimensión del derecho: individual y social. Así, en la dimensión individual, nadie puede ser arbitrariamente impedido de manifestar su pensamiento, comprendiendo además, el derecho a utilizar cualquier medio apropiado para difundirlo; en la social, un derecho colectivo a recibir cualquier información y a conocer la expresión del pensamiento ajeno.

En ese orden, el derecho a la información forma parte del derecho a la libre expresión e implica la facultad de toda persona a solicitar información de las instituciones públicas, quienes se encuentran obligadas a proporcionarla, salvo algunos supuestos en los que se determina la confidencialidad de los datos; confidencialidad que debe ser razonable y destinada a la protección de determinados valores.

La doctrina establece que las solicitudes deben estar dirigidas a obtener información pública, entendida por Ernesto Villanueva como: "El conjunto de datos y hechos ordenados que tienen como propósito servir a las personas para la toma de decisiones, de manera que se enriquezca la convivencia y participación democrática". En ese sentido, la información pública tiene una doble perspectiva, pues opera como un "deber del Estado de dar a conocer a la sociedad sus propias decisiones y derecho de los ciudadanos a acceder a dicha información pública".

Como deber, nace de la forma republicana de gobierno, e importa ya no solamente la obligación de publicar aquellos actos trascendentales de los órganos ejecutivo, legislativo y judicial (decretos, leyes y sentencias), que antes permitía una participación y control ciudadano indirecto

y con limitaciones, sino que, dados los requerimientos actuales, es necesario brindar la más amplia información, como muestra de transparencia de las actividades desplegadas por la administración pública, que permita a las personas controlar los actos de gobierno y conocer aquella información de carácter público que pueda tener relevancia no sólo personal, sino también para el grupo social al que pertenece el individuo que solicita los datos, enriqueciendo el sistema democrático representativo.

En Bolivia, si bien este derecho no estaba previsto en la Ley Fundamental en forma independiente, no es menos cierto que el artículo 7 inc. b) de la Constitución abrogada, establecía que toda persona tiene derecho *"A emitir libremente sus ideas y opiniones por cualquier medio de difusión"*, consagrando, entonces, el derecho a la libre expresión que, conforme a la interpretación de la Corte Interamericana de Derechos Humanos antes aludida, comprende la libertad de buscar y recibir información de toda índole; en consecuencia, en virtud del principio de favorabilidad, *"(…) reconocido como básico en toda hermenéutica interpretativa de los derechos y garantías fundamentales, dado que el intérprete está obligado a optar por aquel entendimiento interpretativo que desarrolle de mejor forma y con la mayor efectividad, los derechos, principios y valores que consagran el orden constitucional…."*. (SSCC 144/2003-R, 987/2003-R, 983/2003-R, 651/2003-R, 569/2003-R, 157/2003-R, entre otras) que impide una interpretación restrictiva de derechos, se entiende que el derecho de acceso a la información está comprendido dentro del derecho a la libre expresión.

El ejercicio del derecho al acceso a la información no es absoluto, sino que, de hecho, existen algunas limitaciones en virtud a los intereses superiores que deben ser protegidos. Así, la defensa nacional, la seguridad del Estado, la intimidad de las personas, etc. Este ha sido el criterio seguido por el artículo18 de la Ley Nº 2341 de Procedimiento Administrativo.

En resumen, la jurisprudencia constitucional ha señalado que el derecho al acceso a la información forma parte del contenido del

derecho a la libre expresión, y de acuerdo a la doctrina, implica la facultad de toda persona a solicitar información de las instituciones públicas; consiguientemente, no puede ser considerado como un derecho protegido por el hábeas data; pues, como se ha visto, este recurso sólo protege los derechos expresamente previstos por el artículo 23 de la Constitución (abrogada).

8. Del Hábeas Data a la Acción de Protección de Privacidad en Bolivia

8.1. Naturaleza jurídica y alcances de la Acción de Protección de Privacidad[18]

La Constitución Política del Estado vigente desde 2009, cambia el *nomen juris* del hábeas data a Acción de Protección de Privacidad, pero no así su esencia tutelar, empero contempla algunos cambios

[18] Este acápite, corresponde a uno de los fundamentos jurídicos de la Sentencia Constitucional Nº0127/2010-R, de 10 de mayo. Esta Sentencia, basándose en la jurisprudencia y el texto de la Constitución Política del Estado vigente, concluyó que la Acción de Protección de Privacidad es una acción tutelar que tiene por objeto la protección a la *autodeterminación informativa*, constituyéndose en una vía instrumental que precautela los derechos de la persona para que puedan acceder al conocimiento de los datos e informaciones referidos a su vida privada o íntima, así como de su familia, obtenidos y almacenados en los bancos de datos públicos o privados, como también saber el uso que se le dará a esa información. Si esta información contiene datos errados o falsos, mediante esta acción tutelar se puede exigir la rectificación de los mismos, para evitar su difusión, ya que podrían causar graves daños a la persona registrada en estos bancos de datos. Finalmente, se podrá pedir la eliminación de estos datos en caso de que contengan información sensible, relacionada al ámbito de su intimidad o de su familia; es decir, aspectos considerados básicos dentro del desarrollo de la personalidad, ideas religiosas, orientaciones políticas, ideológicas o sexuales; información que podría generar discriminación o que pueda romper la privacidad del registrado. "Se concluye entonces –dice la *ratio decidendi* de la Sentencia–, que para solicitar, en especial, la rectificación o la eliminación de los datos, se debe tener la certeza de que estos bancos de datos contienen registros falsos o errados, que no están sujetos a discusión, es decir, que no existan dudas sobre la falsedad de los datos que se pretenden rectificar o eliminar, en esos casos el Tribunal Constitucional procederá a tutelar los derechos vulnerados por los contenidos erróneos o falsos de estos registros, rectificando o en su caso eliminando los mismos (…)".

específicos en cuanto a su redacción, en especial el artículo 130.I, en el que se refiere a los casos de legitimación activa que, si bien es muy similar al texto del artículo 23.I de la Constitución abrogada (CPEabrg), tiene una diferencia notoria cuando afirma; *"… Toda persona individual* ***o colectiva*** *que crea estar indebida o ilegalmente impedida de conocer, objetar u obtener la eliminación o rectificación de los datos registrados por cualquier medio físico, electrónico, magnético o informático, en archivos o bancos de datos públicos o privados,* ***o que afecten a su derecho fundamental a la intimidad y privacidad personal o familiar, o a su propia imagen, honra y reputación, podrá interponer la Acción de Protección de Privacidad****"* (las negrillas son nuestras).

Observamos en primer lugar que se añaden a las personas colectivas como posibles legitimados activos, o futuros accionantes, concibiendo que las personas colectivas también tienen acceso a los derechos reconocidos por el artículo 21.2 de la CPE, los cuales son: derecho a la intimidad, a la privacidad, honra, propia imagen y dignidad. Se entiende que el texto del artículo 130.I al reconocer como posibles accionantes a personas colectivas, se refiere a aquellas de orden público como privado, pero con algunas diferencias en cuanto a los derechos tutelados para estas, es decir, *que las personas colectivas no podrán aducir la vulneración de su derecho a la intimidad personal y familiar, que son derechos fundamentales de índole personal, pero sí podrían denunciar la vulneración de sus derechos a la imagen; y reputación.*

Corresponde aclarar que si bien el derecho a la imagen, a la honra y a la reputación, parecieran estar dentro del mismo grupo de derechos tutelados por la acción de protección de privacidad, en el caso de las persona colectivas, que es el objeto del presente análisis, sólo podrían denunciar la vulneración de los derechos a la imagen y la reputación, pero no así de la honra, debido a que el derecho a la honra es de índole estrictamente personal, es decir, entra dentro de la esfera de la personalidad y es concebido doctrinalmente como la pretensión de respeto que corresponde a cada persona como reconocimiento de su dignidad frente a la sociedad.

Es así que la Corte Constitucional de Colombia en su Sentencia T-412, al referirse al derecho a la honra, estableció lo siguiente:

> *"El concepto de honra se debe construir desde puntos de vista valorativos y, en consecuencia, con relación a la dignidad de la persona. Desde dicha perspectiva la honra es un derecho de la esfera personal y se expresa en la pretensión de respeto que corresponde a cada persona como consecuencia del reconocimiento de su dignidad".*
>
> *"…El artículo 21 de la C.P. consagra específicamente la protección del derecho a la honra, entendiendo por ella, la estimación o deferencia con la que cada persona debe ser tenida por los demás miembros de la colectividad que le conocen y le tratan, en razón a su dignidad humana. Es por consiguiente, un derecho que debe ser protegido con el fin de no menoscabar el valor intrínseco de los individuos frente a la sociedad y frente a sí mismos, y garantizar la adecuada consideración y valoración de las personas dentro de la colectividad".*
>
> *"Tradicionalmente esta Corte ha sostenido, que los derechos al buen nombre y a la honra son derechos que se ganan de acuerdo a las acciones realizadas por el individuo, sea que en virtud de ellas pueda gozar del respeto y admiración de la colectividad como consecuencia de su conducta intachable…".*

Criterio que es compartido por la jurisprudencia del Tribunal Constitucional de Bolivia, que en su SC 0686/2004-R, de 6 de mayo estableció que:

> *"Según la doctrina del Derecho Constitucional el derecho a la honra, es la estimación o deferencia con la que cada persona debe ser tenida y tratada por los demás miembros de la colectividad que le conocen; es el derecho que tiene toda persona a que el Estado y las demás personas reconozcan y respeten la trascendencia social de su honor. Es un derecho que se gana de acuerdo a las acciones realizadas por cada persona, de manera que en virtud de ellas pueda gozar del respeto y admiración de la colectividad como consecuencia de su conducta correcta e intachable acorde con valores de la ética y la moral, o, por el contrario, carezca de tal imagen y prestigio, en razón a su indebido comportamiento social; cabe advertir que la honra, se constituye en una valoración externa de la manera como cada persona proyecta y presenta su imagen; de manera que las actuaciones buenas o malas,*

son el termómetro positivo o negativo que la persona irradia para que la comunidad se forme un criterio objetivo respecto de la honorabilidad de cada ser; pues las buenas acciones acrecientan la honra, las malas decrecen su valoración. En este último caso se entiende que no se puede considerar vulnerado el derecho a la honra de una persona, cuando es ella misma quien ha impuesto el desvalor a sus conductas y ha perturbado su imagen ante la colectividad.

Este derecho, si bien no está expresamente proclamado en el catálogo previsto por el artículo 7 de la Constitución, sí lo está en los artículos 12 de la Declaración Universal de Derechos Humanos; 5 de la Declaración Americana de Derechos y Deberes del Hombre; 17 del Pacto Internacional de Derechos Civiles y Políticos; y 11 de la Convención Americana sobre Derechos Humanos o Pacto de San José de Costa Rica."

La segunda diferencia consiste en la inclusión de la letra "o" en las siguiente frases: *"Toda persona individual o colectiva que crea estar indebida o ilegalmente impedida de conocer, objetar u obtener la eliminación o rectificación de los datos registrados por cualquier medio físico, electrónico, magnético o informático, en archivos o bancos de datos públicos o privados, o que afecten a su derecho fundamental a la intimidad y privacidad personal o familiar, o a su propia imagen, honra y reputación, podrá interponer la Acción de Protección de Privacidad"*; la letra "o", según el Diccionario de la Real Academia de la Lengua Española, tiene tres diferentes significados:

En primer lugar puede denotar diferencia, separación o alternativa entre dos o más personas, cosas o ideas, cuando es utilizada como una conjunción disyuntiva (Antonio o Francisco); en su segundo significado puede ser utilizado ante cada uno de dos o más términos contrapuestos (blanco o negro); en su tercera acepción denota equivalencia significando "o sea, o lo que es lo mismo", acepción que el Tribunal Constitucional boliviano adoptará para interpretar la parte final del artículo 130.I, debido a que el sentido en esta última frase tiene como objetivo el definir una idea común y no denotar diferencias o ideas contrapuestas; por lo que el objeto de este artículo no cambia en

cuanto a lo que estaba prescrito en la Constitución abrogada (entendimiento reiterado por la Sentencia Constitucional Nº1999/2010-R, de 26 de octubre)[19].

8.2. El resguardo al derecho a la "autotutela informativa" y el recurso de hábeas data[20]

En derecho comparado contemporáneo, el Estado Social y Democrático de Derecho, es entendido como aquella organización jurídica y política articulada y cimentada sobre ejes o pilares estructurales de carácter esencial entre los cuales se encuentran la protección de derechos fundamentales y el reconocimiento de mecanismos idóneos y efectivos para su real resguardo.

En ese orden, cabe precisar que la teoría general de los Derechos Humanos, en su clasificación, reconoce dos categorías concretas de derechos a saber: En primer orden se encuentran los derechos fundantes, como ser el derecho a la vida o la libertad de tránsito entre otros y en segundo lugar, se tienen los derechos fundamentales derivados, entre los cuales inequívocamente se encuentra el llamado derecho de "autotutela informativa".

En efecto, el derecho a la "autotutela informativa", deriva directamente del derecho fundamental a la dignidad, a partir del cual, toda persona tiene el derecho de acceder, conocer, pedir rectificación, modificación o eliminación de datos que le conciernan y que le afecten o puedan atentar a sus derechos a la intimidad, privacidad personal o familiar, a la imagen, honra y reputación; generando para el administrador de estos datos contenidos cursantes en archivos públicos o privados,

---

[19] Cfr. SANTIAGO SALAME, Soraya. *La Acción de Protección de Privacidad*. En: Anuario de la Revista Boliviana de Estudios Constitucionales. Tomo I - Año 2017, Págs. 249-290. Ciudad Autónoma de Buenos Aires: IJ Editores, 2018.

[20] Este acápite y los siguientes, corresponden a los fundamentos jurídicos expuestos en la Sentencia Constitucional Nº0189/2010-R, de 24 de mayo.

la obligación de garantizar este derecho fundamental, siempre y cuando no exista una norma expresa que prohíba dicho acceso, conocimiento, modificación o eliminación, ya sea por afectación a terceros, a la seguridad colectiva o por encontrarse sometidos al secreto o reserva.

En ese contexto, se establece que la génesis constitucional del derecho a la autotutela informativa, encuentra cauce jurídico en el bloque de constitucionalidad boliviano, específicamente en el artículo 21.6 de la Constitución vigente; asimismo, su contenido se encuentra sustentado por los artículos 13 del Pacto de San José de Costa Rica, 19 de la DUDH y 19.2 del Pacto Internacional de Derechos Civiles, adoptado por la Asamblea General de la Organización de Naciones Unidas; además, es importante señalar también, que este derecho, encuentra fundamento en la Resolución AG/RES. 1932 (XXXIII-O/03), ACCESO A LA INFORMACIÓN PÚBLICA: FORTALECIMIENTO DE LA DEMOCRACIA[21], de la Organización de Estados Americanos, adoptada en su cuarta sesión plenaria de 10 de junio de 2003, que por su naturaleza, en el marco del artículo 410 de la CPE, forma parte del Bloque de Constitucionalidad y que garantiza el libre acceso a la información de todo Estado Democrático.

De lo expresado precedentemente, a partir del marco normativo descrito, se colige que el derecho a la "autotutela informativa" al margen de ser un derecho derivado, es también un derecho sustantivo, por tanto, en un Estado Social y Democrático de Derecho debe ser defendido por medios jurídicos idóneos, que logren su respeto efectivo.

21 Esta disposición, principalmente resuelve: "1. Reafirmar que toda persona tiene la libertad de buscar, recibir, acceder y difundir informaciones y que el acceso a la información pública es un requisito indispensable para el funcionamiento mismo de la democracia. 2. Reiterar que los Estados tienen la obligación de respetar y hacer respetar el acceso a la información pública a todas las personas y promover la adopción de disposiciones legislativas o de otro carácter que fueren necesarias para asegurar su reconocimiento y aplicación efectiva. (…)".

8.3. La defensa al derecho a la "autotutela informativa"

Siguiendo un orden coherente con lo expresado precedentemente, se tiene que los derechos fundamentales sustantivos, como es el caso del derecho a la autotutela informativa, para su defensa necesitan medios o mecanismos idóneos para su protección. En efecto, en el contexto del Estado Social y Democrático de Derecho, máxime cuando se trate de la protección de datos administrados por entidades públicas, el Estado tiene la obligación de garantizar ya sea por la vía administrativa o jurisdiccional, el resguardo pleno y eficaz de este derecho.

Por tanto, es evidente que el control de constitucionalidad a través de la garantía procesal-constitucional del hábeas data regulado por el artículo 23 de la CPEabrg y denominado ahora acción de protección de privacidad protegida por los artículos 130 y 131 de la CPE, no puede sustituir a estos mecanismos administrativos y jurisdiccionales, y solamente debe ser activado en tanto y cuanto los mismos una vez agotados no restituyan el derecho a la "autotutela informativa" afectado.

A partir del postulado antes señalado, considerando que la naturaleza o esencia procesal constitucional de este instituto no ha cambiado con la entrada en vigor de la Constitución vigente, es pertinente señalar en principio que el hábeas data (ahora acción de protección de privacidad), es una garantía constitucional de naturaleza tutelar destinada a proteger el derecho a la "autotutela informativa" en tanto y cuanto, no exista o no haya sido eficaz otro medio jurídico establecido para garantizar este derecho sustantivo, razón por la cual, se establece que la activación del control de constitucionalidad a través de este mecanismo de defensa, de ninguna manera puede sustituir o ser alternativo a los mecanismos administrativos o jurisdiccionales establecidos para su protección, posición además sustentada por las SSCC 1572/2004-R, 1511/2004-R y 965/2004-R, entre otras.

8.4. Ingeniería constitucional y normativa vigente para proteger el Derecho a la autotutela informativa

En el contexto de los postulados precedentemente citados, en principio es pertinente analizar la normativa legal que protege y garantiza el derecho a la autotutela informativa, en ese orden y a la luz del caso concreto, se tiene que en el marco jurídico imperante, se encuentra vigente el Decreto Supremo Nº 28168 de 17 de mayo de 2005, que tiene por objeto garantizar el acceso a la información, como derecho fundamental de toda persona y la transparencia en la gestión del Poder Ejecutivo, cuyo alcance abarca también al espectro del derecho a la autotutela informativa para datos administrados por entidades públicas. En este contexto, el artículo 19 de esta disposición, de forma expresa regula la institución jurídica del hábeas data en sede administrativa, como mecanismo previo y diferente a la garantía constitucional del hábeas data regulado por los artículos 23 de la CPEabrg y 130 de la CPE.

En efecto, el reclamo en sede administrativa para la protección de datos administrados por una entidad pública, se encuentra disciplinado por el artículo 19.1 del Decreto Supremo 28168, disposición que de forma expresa señala lo siguiente: *"Toda persona, en la vía administrativa, podrá solicitar ante la autoridad encargada de los archivos o registros la actualización, complementación, eliminación o rectificación de sus datos registrados por cualquier medio físico, electrónico, magnético o informático, relativos a sus derechos fundamentales a la identidad, intimidad, imagen y privacidad. En la misma vía podrá solicitar a la autoridad superior competente el acceso a la información en caso de negativa injustificada por la autoridad encargada del registro o archivo público"*.

Del contenido de esta disposición y a la luz del caso concreto, se establece que la normativa boliviana contempla la petición en sede administrativa para la eliminación de datos registrados en archivos públicos que puedan afectar los derechos fundamentales a la identidad, intimidad, imagen y privacidad, garantizando la obligación de la entidad pública administradora de los datos, a responder a la petición realizada

en ejercicio del derecho a la autotutela informativa, reforzando además el resguardo a los derechos del peticionante con la doble instancia establecida para la esfera administrativa.

Además y en la perspectiva de la problemática concreta, es imperante precisar que el artículo 19.2 del citado Decreto Supremo, establece de forma concreta los plazos para que las autoridades públicas a las cuales se solicite la modificación de datos que puedan afectar los derechos de los peticionantes, garantice una respuesta pronta y oportuna, razón por la cual, la norma concede un plazo de cinco días hábiles para la resolución de la petición de "*hábeas data en sede administrativa*". Asimismo, señala que en caso de negativa injustificada, la autoridad jerárquica competente, tendrá un plazo de quince días hábiles para proporcionar la información solicitada.

Ahora bien, la solicitud de eliminación de datos, que puedan afectar derechos a la identidad, intimidad, imagen, privacidad u honra, en sede administrativa debe regirse por las disposiciones citadas, las mismas que para el planteamiento de recursos administrativos y para la aplicación del silencio administrativo que en caso de ausencia de respuesta expresa hace expedita la interposición del recurso jerárquico, debe además contemplar las previsiones establecidas en la Ley de Procedimiento Administrativo.

Por tanto, se establece que únicamente en caso de ser agotado el procedimiento antes descrito, siempre y cuando no se restituya el derecho a la autotutela informativa -dentro del cual se encuentra el derecho de toda persona a pedir eliminación de datos-, puede operar el control de constitucionalidad a través del recurso de hábeas data regulado por los artículos 23 de la Constitución abrogada y 130 y 131 de la Constitución vigente.

Finalmente, para brindar seguridad jurídica a los justiciables, con la finalidad de aclarar los alcances de la institución jurídica del *"hábeas data en sede administrativa"* en relación a la garantía constitucional del

"hábeas data" regulada por el artículo 23 de la Constitución abrogada, y configurada como una acción de defensa por los artículos 130 y 131 de la Constitución vigente, es imperante establecer los alcances del artículo 19.III del Decreto Supremo 28168.

Al respecto, la teoría constitucional ha establecido criterios de interpretación para el ejercicio del control de constitucionalidad, entre los cuales se encuentra el de "interpretación de y desde la Constitución", parámetro en virtud del cual el entendimiento de la normativa infra-constitucional debe ser determinado en el marco de los alcances y contenido de la norma suprema, por tanto, cuando la primera parte del artículo 19.III del Decreto Supremo 28168, señala que *"La petición de hábeas data no reemplaza ni sustituye el recurso constitucional establecido en el artículo 23 de la Constitución Política del Estado …"*, debe entenderse que el hábeas data regulado por este artículo es un mecanismo administrativo idóneo para garantizar el derecho a la "autotutela informativa", diferente al de la garantía constitucional regulada por los artículos 23 de la CPEabrg, 130 y 131 de la CPE, mecanismo procesal que se activa siempre y cuando se haya agotado el hábeas data activado en sede administrativa, en ese contexto, se tiene que efectivamente este mecanismo administrativo de defensa no "sustituye" a la citada garantía constitucional.

Asimismo, cuando el parágrafo tercero del artículo 19 del Decreto Supremo 28168, establece que *"…el interesado podrá acudir, alternativamente, a la vía administrativa sin que su ejercicio conlleve renuncia o pérdida de la vía judicial…"*; y cuando establece también que *"… el acceso a la vía judicial no estará condicionado a la previa utilización ni agotamiento de esta vía administrativa…"*; siguiendo el criterio de interpretación antes señalado y utilizando además un criterio de interpretación referente a la "unidad del ordenamiento jurídico", no puede interpretarse esta disposición como una alternatividad entre el "hábeas data administrativo" y la garantía constitucional del hábeas data, ya que tal como se dijo, para activar el control de constitucionalidad a través de este medio procesal-constitucional de defensa, previamente deben agotarse los mecanismos idóneos establecidos por ley, en ese contexto, el

ejercicio del derecho a la "autotutela informativa", puede hacerse valer en la esfera administrativa y también en la esfera jurisdiccional ordinaria, a la cual el afectado puede acudir sin necesidad de agotar previamente la vía administrativa, aspectos que de ninguna manera alteran la esencia de la garantía constitucional del hábeas data, ahora acción de protección de privacidad, que reiteramos, solo puede ser activada cuando se haya agotado la vía administrativa o judicial pertinente, toda vez que le es aplicable el principio de subsidiaridad (tal como lo establecen las SSCC 1572/2004-R, 1511/2004-R y 965/2004-R, entre otras). Por lo expresado, se tiene que esta es precisamente la interpretación acorde a la Constitución que debe atribuírsele al artículo 19.III del Decreto Supremo 28168 (según el entendimiento establecido en la Sentencia Constitucional Nº0189/2010-R, de 24 de mayo).

9. La configuración constitucional de la Acción de Protección de Privacidad[22]

9.1. Naturaleza jurídica

Actualmente en la doctrina existen numerosas reflexiones sobre la necesidad de modificar los esquemas jurídicos con la intención de dar protección legal a los derechos que puedan ser dañados a partir de los nuevos inventos de reproducción de la imagen y la voz, y la creciente posibilidad de comunicación de los mismos, por lo que es de imperiosa necesidad la protección de los datos que revelen la personalidad del individuo; es así, que en nuestro país el artículo 130.I y II de la Constitución Política del Estado vigente (CPE) –antes artículo 23 de la CPEabrg, protegiendo los derechos personalísimos estableció que: *"Toda persona individual o colectiva que crea estar indebida o ilegalmente*

[22] Este acápite y los siguientes, corresponden a los fundamentos jurídicos expuestos en la Sentencia Constitucional Nº1738/2010-R, de 25 de octubre. Cfr. ASOCIACIÓN BOLIVIANA DE DERECHO PROCESAL CONSTITUCIONAL. *Código Procesal Constitucional de Bolivia. Doctrina, Jurisprudencia Constitucional y Legislación Comparada.* Cochabamba, Bolivia: Grupo Editorial Kipus, 2014. Pág. 310.

impedida de conocer, objetar u obtener la eliminación o rectificación de los datos registrados por cualquier medio físico, electrónico, magnético o información, en archivos o banco de datos públicos o privados, o que afecten a su derecho fundamental a la intimidad y privacidad personal o familiar, o a su propia imagen, honra y reputación, podrá interponer la Acción de Protección de Privacidad" señalando además que no procede para levantar el secreto en materia de prensa.

De lo que se tiene que, la acción de protección de privacidad, protege los derechos relativos a la personalidad del individuo como son la intimidad, privacidad personal o familiar, la propia imagen, honra y reputación, contra el manejo de datos o informaciones obtenidas y almacenadas en los bancos de datos públicos o privados, por esta misma razón la doctrina señala que esta acción en realidad protege el derecho a la autodeterminación informática, entendido como la facultad de una persona para conocer, actualizar, rectificar o cancelar la información existente en una base de datos pública o privada, y que hubiesen obtenido, almacenado y distribuido.

9.2. Los derechos a la intimidad y privacidad como base de la protección de datos personales

Del artículo 130 de la CPE, se concibe que tanto las personas naturales y jurídicas tienen acceso a los derechos a la privacidad, intimidad, honra, honor, propia imagen y dignidad reconocido en el artículo 21.1 de la CPE, entre uno de esos derechos esta la intimidad, que sin duda es uno de los bienes más susceptibles de ser lesionados o puesto en peligro por el uso de las nuevas tecnologías, por lo que se hace necesario colocar un límite a la utilización de la informática y las comunicaciones ante la posibilidad de que se pueda agredir a la intimidad de los ciudadanos y con ello se pueda coartar el ejercicio de sus derechos (Conde Ortíz Concepción, "La protección de datos personales: un derecho autónomo en base a los conceptos de intimidad y privacidad"), por lo mismo, este autor citando a Albaladejo, señaló que la intimidad consiste en *"el poder concebido a la persona sobre el conjunto de actividades*

que forman un círculo íntimo, personal y familiar, poder que le permite excluir a los extraños de entrometerse en él y de darle un publicidad que no desee el interesado"; así también la jurisprudencia de España en su STC 134/1999 de 15 de julio, señaló que: *"El derecho a la intimidad garantiza el individuo un poder jurídico sobre la información relativa a una persona o a su familia, pudiendo imponer a terceros, sean éstos simples particulares o poderes públicos, su voluntad de no dar a conocer dicha información o prohibiendo su difusión no consentida"*.

Ahora bien en lo que respecta a la privacidad personal o familiar, el mismo autor citando a Ruano Albertos, señaló que es "el poder de ejercer un control sobre las informaciones que le atañen a uno, teoría que viene a considerar la intimidad como el derecho a poder participar y controlar las informaciones que concierne a cada persona", de igual forma hace una distinción entre intimidad y privacidad, señalando que la intimidad es "el conjunto de sentimientos, pensamientos e inclinaciones más internos, como la ideología, religión o creencias, las tendencias personales que afectan a la vida sexual, problemas de salud que deseamos mantener en secreto y otras inclinaciones"; mientras que, privacidad hace referencia "al ámbito de la persona formado por su vida familiar, aficiones, bienes particulares y actividades personales".

De todo lo anterior se tiene que tanto la intimidad como la privacidad son la base fundamental para la protección de todos los datos personales de las personas, que sólo le atingen a él o a ella, por lo mismo se encuentra facultado para determinar cuándo y dentro de qué límites pueden revelarse situaciones referentes a su propia vida, entendiéndose en consecuencia de que la acción de protección de privacidad, entre otros protege la intromisión por parte de personas particulares y/o jurídicas a la vida íntima del ser humano que le corresponde como consecuencia del reconocimiento a su dignidad, por lo que la vulneración de estos derechos afectan directamente a su imagen, honra y reputación (entendimiento reiterado por las Sentencias Constitucionales Plurinacionales Nº 1283/2016-S3, de 22 de noviembre, y Nº 0345/2018-S1 de 23 de julio).

9.3. Alcances de esta acción tutelar

Al estar ligado con los derechos señalados precedentemente, la jurisprudencia constitucional a través de la SC 0965/2004-R de 23 de junio, señaló los siguientes alcances:

1. *Conocer la información* o "registro de datos personales obtenidos y almacenados en un banco de datos de la entidad pública o privada, para conocer qué es lo que se dice respecto a la persona que plantea el hábeas data, de manera que pueda verificar si la información y los datos obtenidos y almacenados son los correctos y verídicos; si no afectan las áreas calificadas como sensibles para su honor, la honra y la buena imagen personal"; asimismo, conocer los fines y objetivo de la obtención y almacenamiento; es decir, qué uso le darán a esa información.

2. *Actualizar los datos existentes*, este es "el derecho a la actualización de la información o los datos personales registrados en el banco de datos, añadiendo los datos omitidos o actualizando los datos atrasados; con la finalidad de evitar el uso o distribución de una información inadecuada, incorrecta o imprecisa que podría ocasionar graves daños y perjuicios a la persona ".

3. *Modificar o corregir la información existente en el banco de datos*, cuando son incorrectos o ajenos a la verdad, en otros términos es "el derecho corrección o modificación de la información o los datos personales inexactos registrados en el banco de datos público o privado, tiene la finalidad de eliminar los datos falsos que contiene la información, los datos que no se ajustan de manera alguna a la verdad, cuyo uso podría ocasionar graves daños y perjuicios a la persona".

4. *Preservar la confidencialidad de la información* que si bien es correcta y obtenida legalmente, no se la puede otorgar en

forma indiscriminada; esta acción se funda en el derecho a la "confidencialidad de cierta información legalmente obtenida, pero que no debería trascender a terceros porque su difusión podría causar daños y perjuicios a la persona".

5. *Excluir la información sensible*, es decir, aquella información que sólo importa al titular, como las ideas políticas, religiosas, orientación sexual, enfermedades, etc.; así la citada Sentencia Constitucional señaló que es el "Derecho de exclusión de la llamada `información sensible` relacionada al ámbito de la intimidad de la persona, es decir, aquellos datos mediante los cuales se pueden determinar aspectos considerados básicos dentro del desarrollo de la personalidad, tales como las ideas religiosas, políticas o gremiales, comportamiento sexual; información que potencialmente podría generar discriminación o que podría romper la privacidad del registrado" (entendimiento reiterado por las Sentencias Constitucionales Plurinacionales Nº1300/2012, de 19 de septiembre, y Nº1445/2013, de 19 de agosto).

9.4. Presupuestos indispensables de procedencia

Conforme lo establece la misma Constitución, para su procedencia se requiere de dos presupuestos esenciales:

a) La existencia de un banco de datos, que puede ser público o privado, físico, electrónico, magnético, informático, que tengan como finalidad proveer informes, dado que como ha señalado la SC 0965/2004-R de 23 de junio: "…la acción del hábeas data es una modalidad de amparo que permite a toda persona interesada acceder al conocimiento de los datos que consten en registros o bancos de datos públicos o privados destinados a proveer informes, y a exigir su supresión, rectificación, confidencialidad o actualización, en caso de falsedad o discriminación".

Esta cuestión, ciertamente parte de un primer problema relativo a la existencia misma del banco de datos, ya que si él no existiera, no habría solicitud atendible alguna. Entonces, acreditada la existencia, y ante la sospecha de la inclusión de datos suyos, la persona podrá solicitar la constatación sobre el contenido del asiento a ella referido, su finalidad y uso concreto.

b) Que el banco de datos contenga información vinculada a los derechos protegidos por la acción de protección de privacidad.

Esto significa que la persona que accedió al registro realizado respecto suyo, ahora puede controlar y analizar el contenido de los datos. Este control puede materializarse en un actuar concreto dirigido a diferentes acciones, tales como: a) *Anular el asiento*, cuando el dato no responde a la realidad de los hechos, cuando nunca existió la circunstancia que anota, o si, habiendo existido, desapareció o se extinguió por diferentes causas; b) *Actualizar el asiento*, cuando en el registro figuran algunos datos ciertos y otros que se han modificado por el tiempo o por alguna acción del titular, por lo que se solicita que toda la información se relacione con las actuales circunstancias del afectado; c) *Rectificar o modificar*, si en el registro se ha consignado información que es incorrecta, falsa o mendaz; d) *Aclarar,* si en el registro existe información que, si bien es cierta, está dada en una forma incorrecta o equívoca respecto de la real situación; e) *Anulación de registros referidos a datos "sensibles",* cuando dichos datos sólo le pertenecen e incumben al titular, y están referidos a temas, circunstancias, y en general a todo lo que, de ser conocido públicamente, puede generar perjuicios o discriminación; f) *Reserva de datos,* cuando la información resulta correcta, y también lo es su origen, pero no se trata de información susceptible de darse indiscriminadamente o publicarse sin autorización del titular. La acción tiende a preservar que los datos sean revelados, salvo que obedezca a la solicitud de autoridad competente

o del interesado, debidamente fundada; g) *Datos que importen discriminación,* implicarán necesariamente su anulación, por ser ilegítima la posesión de este tipo de información (SC 0965/2004-R de 23 de junio)[23].

9.5. Legitimación

a) Activa, de acuerdo al artículo 130 de la CPE, esta acción puede ser interpuesta por toda persona individual o colectiva, que crea estar indebida o ilegalmente impedida de conocer, objetar u obtener la eliminación o rectificación de los datos registrados por cualquier medio físico, electrónico, magnético o informático; sin embargo, no se descarta que también pueda ser presentado por un miembro del grupo familiar pues uno de los derechos protegidos es la privacidad familiar.

b) Pasiva, siendo presupuesto indispensable para la procedencia de esta acción la existencia de archivos o bancos de datos tiene legitimación pasiva la persona individual o colectiva, pública o privada, que tiene o administra los archivos o bancos de datos.

Sobre este último aspecto, la Sentencia Constitucional Nº1978/2011-R, de 7 de diciembre, ha establecido qué debe entenderse por banco de datos y cuáles serán los que pueden ser objeto de protección por esta acción tutelar; a cuyo efecto señala que la legitimación activa corresponde a toda persona, natural o jurídica, nacional o extranjera, que actúa por sí, o mediante su representante; de quienes se pueden registrar datos e informaciones acumulables en distintos soportes, entonces, por simple lógica, la legitimación pasiva corresponderá a las entidades públicas o privadas (y sus representantes) que hayan obtenido y tengan registrados tales datos e informaciones, sobre cuyo contenido, los accionantes tengan el interés de conocer, aclarar, rectificar,

[23] Cfr. ASOCIACIÓN BOLIVIANA DE DERECHO PROCESAL CONSTITUCIONAL. Obra citada. Pág. 316.

modificar o eliminar, y que no haya obtenido la respuesta favorable por la citada entidad para lograr tales extremos.

> *"Tenemos entonces que la legitimación pasiva recae precisamente sobre los bancos de datos (sean públicos o privados), que consisten en centros de acopio e intercambio de información, o de documentación, destinados a rubros específicos y a la prestación de determinados servicios (bancarios; policiales; comunicacionales; servicios web; compra y venta de distintos bienes; agencias matrimoniales; etc.), que estén expresamente destinados a brindar información a terceros.*
>
> *Por lo anteriormente descrito* –concluye la Sentencia–, *los bancos de datos no comparten características similares a aquella información de carácter personal que una persona pueda tener en registros privados (computadoras, celulares, correos electrónicos, e-mails, y otros), debido a que son archivos que no tienen por objeto el de la publicidad del contenido de los mismos, es decir que no tienen por objeto el brindar información a terceros, por lo que no pueden ser objeto de tutela mediante la acción de protección de privacidad, en mérito a la naturaleza jurídica distinta a la de los bancos de datos y a que gozan de su protección constitucional propia, establecida como la inviolabilidad del secreto de las comunicaciones privadas y los documentos y manifestaciones privadas contenidas en cualquier soporte (así lo establece el artículo 25.I y II de la CPE), por lo que la acción destinada a proteger este tipo de derechos no es la acción de protección de privacidad, sino la acción de amparo constitucional…"* (Entendimiento reiterado por la Sentencia Constitucional Plurinacional Nº1300/2012, de 19 de septiembre).

9.6. Procedimiento y la excepción a la regla de la subsidiariedad

En lo que respecta a su procedimiento el artículo 131.I de la CPE, establece que esta acción tendrá lugar de acuerdo con el procedimiento previsto para la acción de amparo constitucional, de ahí que, le son aplicables todos los requisitos de admisión y las causales de improcedencia del amparo constitucional, así como los principios de subsidiariedad e inmediatez.

En lo que respecta específicamente a la subsidiariedad, la SC 0965/2004-R, señaló:

> *"Tomando en cuenta sus fines y objetivos, así como la aplicación supletoria de las normas previstas por el artículo 19 de la CPE, dispuesta por el artículo 23 parágrafo V antes referido, se entiende que el hábeas data es una acción de carácter subsidiario, es decir que solamente puede ser viable en el supuesto que el titular del derecho lesionado haya reclamado ante la entidad pública o privada encargada del banco de datos, la entrega de la información o datos personales obtenidos o almacenados, y en su caso, la actualización, rectificación o supresión de aquella información o datos falsos, incorrectos, o que induce a discriminaciones, y no obtiene una respuesta positiva o favorable a su requerimiento, o sea que la entidad pública o privada no asume inmediatamente la acción solicitada. Dicho de otra manera, el hábeas data se activa exclusivamente cuando la persona demuestra que ha acudido previamente ante la entidad pública o privada para pedir la restitución de su derecho lesionado y no ha podido lograr la reparación a dicha vulneración".*

En el mismo sentido, la SC 1572/2004-R de 4 de octubre, señaló que le eran aplicables al hábeas data los principios de subsidiariedad e inmediatez. De igual forma la SC 0188/2006-R de 21 de febrero, establece el carácter subsidiario del hábeas data en los siguientes términos: *"El artículo 23.V de la CPE, determina que el recurso de hábeas data '…se tramitará conforme al procedimiento establecido para el Recurso de Amparo Constitucional previsto en el artículo 19° de esta Constitución'; consiguientemente, al hábeas data le es aplicable la doctrina constitucional sentada para el amparo constitucional, por lo que se debe aplicar el principio de subsidiariedad, establecido en el artículo 19.IV de la CPE; lo que significa que sólo se activa cuando el recurrente ha agotado los medios o recursos que tenía a su alcance para lograr conocer, objetar u obtener la eliminación, rectificación de los datos públicos o privados que afectan a su derecho a la intimidad y privacidad personal y familiar, a su imagen, honra y reputación".*

De lo anterior se tiene que la acción de protección a la privacidad sólo será procedente si se han agotado los recursos existentes y, además, se ha presentado la acción dentro del plazo de seis meses.

No obstante, la misma jurisprudencia constitucional, ha establecido que es posible aplicar la excepción a la regla de la subsidiaridad

en situaciones en las que los hechos ilegales o indebidos denunciados en una acción de protección de privacidad podrían producir efectos *irreparables* o *irremediables*; de manera que, a pesar de existir vías legales ordinarias para que los accionantes puedan lograr la restitución de sus derechos fundamentales restringidos o suprimidos es posible activar inmediatamente esta vía tutelar para que, compulsando los antecedentes y verificando que los hechos ilegales o indebidos denunciados lesionaron los derechos fundamentales, cuyos efectos podrían ser irreparables o irremediables, se otorgue una tutela provisional o directa.

Para ese efecto, el Tribunal Constitucional Plurinacional, a través de su jurisprudencia, ha establecido las respectivas subreglas que permitan determinar de manera objetiva el peligro del perjuicio irreparable o irremediable; así, en su SC 1743/2003-R de 1 de diciembre, ha señalado que:

> *"Para determinar la irremediabilidad del perjuicio hay que tener en cuenta la presencia concurrente de varios elementos que configuran su estructura, como la inminencia, que exige medidas inmediatas, la urgencia que tiene el sujeto de derecho por salir de ese perjuicio inminente, y la gravedad de los hechos, que hace evidente la impostergabilidad de la tutela como mecanismo necesario para la protección inmediata de los derechos constitucionales fundamentales. La concurrencia de los elementos mencionados pone de relieve la necesidad de considerar la situación fáctica que legitima la acción de tutela, como mecanismo transitorio y como medida precautelativa para garantizar la protección de los derechos fundamentales que se lesionan o que se encuentran amenazados. Con respecto al término `amenaza' es conveniente manifestar que no se trata de la simple posibilidad de lesión, sino de la probabilidad de sufrir un mal irreparable y grave de manera injustificada. La amenaza requiere un mínimo de evidencia fáctica, de suerte que sea razonable pensar en la realización del daño o menoscabo material o moral. De acuerdo con lo que se ha esbozado sobre el perjuicio irremediable, se deduce que hay ocasiones en que de continuar las circunstancias de hecho en que se encuentra una persona, es inminente e inevitable la destrucción grave de un bien jurídicamente protegido, de manera que urge la protección inmediata e impostergable por parte del Estado ya en forma directa o como mecanismo transitorio".*

Ahora bien, expuesta la naturaleza subsidiaria del amparo constitucional y también la excepción a dicho principio, en la Sentencia Constitucional Nº1738/2010-R, de 25 de octubre, el Tribunal Constitucional estableció que el caso concreto trataba de una menor de edad, cuyos derechos debían ser analizados tomando en cuenta su interés superior, que comprende la preeminencia en sus derechos y prioridad en el acceso a la administración de justicia, tal cual lo señala el artículo 60 del CPE cuando establece: *"Es deber del Estado, la sociedad y la familia garantizar la prioridad del interés superior de la niña, niño y adolescente, que comprende la preeminencia de sus derechos, la primacía en recibir protección y socorro en cualquier circunstancia, la prioridad en la atención de los servicios públicos y privados, y el acceso a una administración de justicia pronta, oportuna y con asistencia de personal especializado"*, lo que significa que cuando se trata de una denuncia que afecte o vulnere los derechos de menores de edad, éstos deben ser analizados con preferencia a los derechos que pudiera pertenecer a terceros; más, cuando se trata de actos que atentan los derechos de su personalidad, como es la intimidad y privacidad, y que de ser ciertos dañarían su imagen, honra y reputación.

> *"Por lo anteriormente señalado* –indica la Sentencia–, *la situación descrita configura un escenario en el cual la hija de la accionante se encuentra en una situación inminente de verse afectada en sus intereses, pues la aplicación tardía de la tutela podría provocar que esa filmación del acto sexual, se siga expandiendo por los diferentes medios electrónicos como son la página web y el bluetooth, generando un desprestigio de su persona hacia la sociedad, dañando su imagen, honra y reputación, por lo que precisa de medidas inmediatas, pues existe urgencia de evitar ese perjuicio inminente, que además configura una situación grave, que puede ocasionar un mal irreparable a la hija de la recurrente, de forma injustificada (…); por tanto, concurren los elementos necesarios para que se aplique excepcionalmente la subsidiariedad en el presente caso, debiendo por ello ingresarse al análisis de fondo de la problemática planteada*[24].

[24] Para concluir con esta parte y hacer más sustentable esta determinación, el Tribunal hizo referencia a que en otras legislaciones se viene aplicando ésta excepción; así,

(…)

En el presente caso al no haberse respetado la vida íntima y privacidad de la representada de la accionante que dicho sea de paso es menor de edad, el demandado vulneró los derechos denunciados por la accionante en representación de su hija menor de edad, ya que ésta jamás otorgó su consentimiento para que esas imágenes que forman parte de su vida íntima sean divulgadas a través de los medios electrónicos como es la página web y el bluetooth, afectándola directamente a su imagen, honra y reputación, es más le ocasionó un desprestigio al interior de la sociedad, a tal punto que tuvo que abandonar sus estudios en la universidad; por lo que se hace imperiosa la necesidad de que esos datos sean eliminados de forma inmediata de los medios electrónicos señalados, a objeto de que no se siga causando mayores daños irreparables a la menor; con mayor razón cuando en un Estado Democrático Social, se respeta la vida íntima y privacidad de las personas, pero no solamente eso, sino también su derecho a tener una honra y reputación acordes con los valores y principios imperantes en un país pluricultural como es el nuestro; consecuentemente corresponde otorgar la tutela solicitada".

10. Jurisprudencia emitida por el Tribunal Constitucional Plurinacional en Acciones de Protección de Privacidad, en las que se denunció la omisión en la cancelación de antecedentes policiales[25]

En ocasión de resolver la problemática planteada por una persona (como accionante) que cuestionó la omisión de las autoridades ju-

el Código Procesal Constitucional del Perú, en el artículo 62 determina que *"para la procedencia del hábeas data se requerirá que el demandante previamente haya reclamado, por documento de fecha cierta, el respeto de los derechos a que se refiere el artículo anterior, y que el demandado se haya ratificado en su incumplimiento o no haya contestado dentro de los diez días útiles siguientes a la presentación de la solicitud tratándose del derecho reconocido por el artículo 2 incs 5) de la Constitución, o dentro de los dos días si se trata del derecho reconocido por el artículo 2 incs 6) de la Constitución. Excepcionalmente se podrá prescindir de este requisito cuando su exigencia genere el inminente peligro de sufrir un daño irreparable, el que deberá ser acreditado por el demandante. Aparte de dicho requisito, no será necesario agotar la vía administrativa que pudiera existir"*.

[25] Este acápite, corresponde a uno de los fundamentos jurídicos expuestos en la Sentencia Constitucional Plurinacional Nº0090/2014-S1, de 24 de noviembre, misma que

dicial, fiscal y policial, en la cancelación de sus antecedentes policiales, impetrado en cada una de las instancias indicadas; le correspondió al TCP referirse a casos resueltos mediante el conocimiento de Acciones

definió que: *"...la acción de protección de privacidad, constituye un medio procesal constitucional de protección de los datos personales, dirigido a la protección efectiva, inmediata y oportuna del derecho a la autodeterminación informática, en los supuestos en que éste sea transgredido por acciones u omisiones ilegales o indebidas. En ese sentido, por intermedio de ella, toda persona natural o jurídica, puede acudir a la jurisdicción constitucional, para demandar a los bancos de datos y archivos de entidades públicas o privadas, persiguiendo el conocimiento, actualización, rectificación o supresión de las informaciones o datos contenidos en éste, que se hubiesen obtenido, almacenado o distribuido en los mismos"*. Asimismo, cabe señalar que la Acción de Protección de Privacidad, de acuerdo a la reiterada jurisprudencia constitucional citada a través de las SC 1738/2010-R y las SSCCPP 1445/2013 y 0089/2014-S2, entre otras, tiene los siguientes presupuestos indispensables de procedencia: a) La existencia de un banco de datos público o privado, físico, electrónico, magnético, informático, cuya finalidad sea la de proveer informes, y; b) Que ese banco de datos contenga información vinculada a los derechos protegidos por la acción de protección de privacidad. Bajo ese contexto, la SCP Nº0572/2018-S3, de 31 de octubre, a tiempo de resolver el caso concreto, hizo hincapié en que la Acción de Protección de Privacidad, se activa necesariamente frente a la existencia de un archivo o banco de datos público o privado, que contenga información sensible del accionante y que hubiese sido obtenida, almacenada o distribuida, en afectación a los derechos fundamentales anteriormente señalados, permitiendo a su titular acceder al conocimiento, actualización, rectificación o eliminación de dicha información, en el ejercicio de su derecho a la autodeterminación informática; archivos y/o banco o base de datos, que pueden ser físicos, electrónicos, magnéticos o informáticos. Finalmente, llegó a establecer el siguiente entendimiento: "En ese marco, se tiene que en el caso en revisión, los impetrantes de tutela denuncian que fueron objeto de vulneración de sus derechos que invocan, debido a que el ahora demandado a través de un medio informático como es el *whatsapp* y un boletín informativo de la FRUTCAS, se hubiera dado a la tarea de propalar una serie de adjetivos calificativos en relación a sus personas, los cuales aseveran son completamente falsos y alejados de la verdad, entrometiéndose así en su vida íntima; por lo que al respecto cabe señalar, que los medios de difusión que aluden y a través de los cuales se hubiese efectuado dicha divulgación que busca dañar su imagen, no constituyen propiamente un archivo o banco de datos público o privado que contenga información susceptible de ser utilizada ilegal o indebidamente y que se encuentre vinculada a los derechos que se tutelan por vía de la acción de protección de privacidad; así el *whatsapp* es simplemente una aplicación de mensajería, a través de la cual se envían y reciben mensajes vía internet, no recopila, acumula ni clasifica información, mientras que el boletín informativo que se cita, como tal, se encuentra dentro del género periodístico, sin que tampoco se haga acopio de información; consiguientemente, en la especie, no se cumplen los presupuestos que hacen a la activación de la presente acción de defensa, circunstancia que determina se deba denegar la tutela solicitada".

de Protección de Privacidad, cuyas temáticas versaban precisamente, en relación a solicitudes de anulación de los antecedentes aludidos, que iban en desmedro de los derechos de los entonces accionantes protegidos por esta garantía jurisdiccional constitucional. Ello bajo los siguientes argumentos:

En forma previa, concierne referir que la Policía Nacional, cuenta con un sistema computarizado de registro de antecedentes policiales, en el que se mantienen, archivan y registran los antecedentes penales de las personas. Debiendo considerarse que, dicho registro, según la SC 0379/2002-R de 9 de abril, se halla compuesto por: *"…hechos comprobados durante la investigación y elaboración de Diligencias de Policía Judicial. (…) el registro de antecedentes policiales, constituye un problema grave, para quien realmente lo merece, por cuanto puede generar consecuencias adversas, cuando se trata de valorar en un proceso penal la buena conducta anterior (arts. 37 y 38 - a) del Código Penal), consecuencias que también se encuentran vinculadas al buen nombre y honra de las personas o aquellas situaciones en las que se deben valorar los antecedentes de una persona, para obtener un puesto de trabajo; situaciones expuestas y otras que no han sido mencionadas, que pueden llegar a tener un efecto negativo para la persona que tiene ese registro"*.

En ese orden de ideas, la SC 1972/2011-R de 7 de diciembre, en un asunto en el que la entonces impetrante de tutela, recurrió contra el Director Departamental de la FELCN de Santa Cruz, por no haber procedido a la eliminación de sus antecedentes, precisó que: *"…la cancelación de antecedentes en actividades de narcotráfico, debe ser mediante orden judicial, adjuntando certificado de antecedentes de la FELCN y del REJAP. Sin embargo, la accionante en vez de proceder de esa manera; es decir, acudir a la jurisdicción ordinaria para que mediante orden judicial se ordene a la FELCN, la eliminación de los antecedentes que considera lesionan sus derechos a la imagen, honra y reputación; por cuanto, la autoridad demandada no negó la solicitud, sino indicó el procedimiento a seguir, y que sería mediante orden judicial; ello no fue tomado en cuenta*

por la accionante, que en vez de agotar esa vía, ignorando el carácter subsidiario de la acción de protección a la privacidad, interpuso directamente la presente acción de tutela…".

Por su parte, la SC 1976/2011-R de 7 de diciembre, que resolvió un caso, en el que constaba el registro de antecedentes policiales en relación al accionante, por una denuncia sentada en su contra, producto de la que no se inició investigación alguna y por ende, tampoco proceso penal; determinó que: *"Con las certificaciones emitidas,* -el impetrante de tutela- *solicitó al Fiscal de Distrito y al Director de la FELCC el levantamiento de antecedentes penales, misma que fue denegada por ambas autoridades, motivando que acuda ante el Juez de Instrucción de Turno en lo Penal, autoridad judicial que mediante Decreto de 22 de mayo de 2010, no dio curso a lo solicitado señalando no constar ningún proceso contra el impetrante, menos que estuviere radicado en ese Juzgado, lo que evidencia que con esas negativas se ha vulnerado el derecho a la privacidad, la imagen y reputación del accionante, pues no obstante de reconocer que si bien existió una denuncia en su contra no se inició la investigación ni tampoco proceso penal, por lo cual debieron dar curso a lo solicitado y ordenar el levantamiento de antecedentes policiales de la base de datos de archivo, además, del sistema de ingreso y seguimiento de causas, lo que evidencia vulneraron los derechos a la dignidad, imagen, honra y reputación, determinando ello se conceda la tutela solicitada".*

De los fallos constitucionales plurinacionales citados, se llega al siguiente entendimiento:

> En el caso de antecedentes policiales, en los que conste denuncia, que no hubiera derivado en el inicio de un proceso penal ni investigación alguna respecto a la misma, resulta procedente la cancelación de éstos, sin orden judicial previa alguna, toda vez que se entiende que, la causa no estuvo sometida a control jurisdiccional alguno, por las razones indicadas; no obstante, en el supuesto en que, se hubiera dado apertura a la acción penal, extinguiéndose ésta por algún criterio de

oportunidad reglada, aplicada en el marco de los artículos 21 y 22 del CPP, es necesaria una orden judicial expresa, que establezca aquello, acompañando la Resolución ejecutoriada pertinente, que hubiere emitido dicha determinación.

En ese sentido, ante la negativa de una autoridad judicial cautelar, en expedir la orden aludida, a efecto que la Policía Nacional, a través de la instancia respectiva, proceda a la cancelación de antecedentes policiales, por estar extinguida la acción penal, ante la admisión de un criterio de oportunidad reglada aceptado en instancia jurisdiccional, con el consiguiente archivo de obrados del proceso penal -criterios de oportunidad que se hallan instituidos en el ordenamiento jurídico procesal penal, que buscan simplificar, economizar y concentrar los recursos y esfuerzos de la justicia penal, hacia los asuntos graves que requieran de mayor conocimiento y contradicción, sin que ello implique menoscabar las garantías procesales de los sujetos intervinientes; propendiendo además con ello al descongestionamiento del sistema de administración de justicia penal, prescindiendo de la instalación del juicio oral público y contradictorio-; el agraviado, se halla facultado a activar la acción de protección de privacidad, que se halla destinada a lograr el conocimiento, actualización, rectificación o supresión de las informaciones o datos contenidos en bases de datos públicos o privados, logrando así una tutela efectiva, respecto al derecho a la autodeterminación informática, y la protección derivada de los derechos que tutela esta garantía constitucional.

Debiendo precisarse en este punto que, si bien la autoridad judicial, no es el representante de la entidad titular del banco de datos, la omisión ilegal que acarrea la vulneración de los derechos amparados por esta acción constitucional, emerge de la ausencia de una orden expresa dictada a fin que la

instancia pertinente, materialice y concretice la cancelación y eliminación de los datos contenidos en aquella. Lo que en definitiva, lo hace pasible a ser demandado, en pro de una tutela efectiva, inmediata y oportuna del justiciable.

11. Un caso polémico de vulneración de la privacidad e intimidad de la vida sexual

En un caso polémico y difundido ampliamente a nivel nacional, la accionante (conductora de televisión) presentó Acción de Protección de Privacidad alegando la vulneración de sus derechos a la privacidad e intimidad, a la honra y honor, a la propia imagen, a la dignidad y a la autodeterminación informática, toda vez que el demandado, sin su autorización ni consentimiento, filmó una relación íntima que mantuvo con él, procediendo posteriormente a extorsionarla y amenazarla con difundirla, lo que en efecto se produjo el 1 de noviembre de 2013, siendo publicada por veintiún páginas webs.

En consecuencia, a tiempo de resolver el caso, le correspondió al Tribunal Constitucional Plurinacional determinar si los extremos demandados eran evidentes a efectos de conceder o denegar la tutela solicitada, exponiendo entre los fundamentos jurídicos de la Sentencia Constitucional Plurinacional Nº0819/2015-S3, de 10 de agosto, aspectos referentes al deber del Estado de garantizar la protección de los derechos y la red de informática, así como también hizo referencia al Ministerio Público y su rol de protección a las víctimas en un proceso penal.

Posteriormente, y pese a que el Tribunal de garantías denegó la tutela impetrada, el Tribunal Constitucional Plurinacional consideró pertinente establecer medidas correspondientes a una tutela inmediata y efectiva a razón de que la protección procesal ofrecida por el Estado boliviano, específicamente por la Fiscalía General del Estado, relacionada con la protección a víctimas de delito, no se acreditó como efectiva para el restablecimiento de los derechos y garantías invocados por la

parte accionante, así como para garantizar la no revictimización y la no vulneración continua de derechos fundamentales.

Por la trascendencia del caso, considero pertinente reproducir *in extenso* los fundamentos jurídicos y las razones de la decisión de la citada Sentencia Constitucional Plurinacional Nº0819/2015-S3:

11.1. Naturaleza procesal de la acción de protección de privacidad

La acción de protección de privacidad se encuentra instituida en los artículos 130 y 131 de la CPE, en ese entendido el artículo 131 determina el aspecto procesal de la misma, al señalar que: "La Acción de Protección de Privacidad tendrá lugar de acuerdo al procedimiento previsto para la Acción de Amparo Constitucional", por lo que en base a ese razonamiento el artículo 128 de la CPE, sobre la acción de amparo constitucional refiere que: "La Acción de Amparo Constitucional tendrá lugar contra actos u omisiones ilegales o indebidos de los servidores públicos, o de persona de persona individual o colectiva, que restrinjan, supriman o amenacen restringir o suprimir los derechos reconocidos por la Constitución y la ley"; además, el legislador ha previsto la interposición directa de la acción de protección de privacidad, así se tiene el artículo 61 del CPCo, que determina: "La Acción de Protección de Privacidad podrá interponerse de forma directa, **sin necesidad de reclamo administrativo previo, por la inminencia de la violación del derecho tutelado y la acción tenga un sentido eminentemente cautelar**" (las negrillas agregadas en la Sentencia).

En ese sentido y dada la naturaleza procesal que el constituyente dio a la acción de protección de privacidad cabe establecer la relación armónica entre subsidiariedad e inmediatez, sobre ese aspecto la SC 1337/2003-R de 15 de septiembre, estableció las siguientes reglas y sub reglas de improcedencia del amparo por subsidiariedad, estas se aplicarán cuando:

> "*1) las autoridades judiciales o administrativas no han tenido la posibilidad de pronunciarse sobre un asunto porque la parte no ha utilizado*

un medio de defensa ni ha planteado recurso alguno, así: a) cuando en su oportunidad y en plazo legal no se planteó un recurso o medio de impugnación y b) cuando no se utilizó un medio de defensa previsto en el ordenamiento jurídico; y 2) las autoridades judiciales o administrativas pudieron haber tenido o tienen la posibilidad de pronunciarse, porque la parte utilizó recursos y medios de defensa, así: a) cuando se planteó el recurso pero de manera incorrecta, que se daría en casos de planteamientos extemporáneos o equivocados y b) cuando se utilizó un medio de defensa útil y procedente para la defensa de un derecho, pero en su trámite el mismo no se agotó, estando al momento de la interposición y tramitación del amparo, pendiente de resolución. Ambos casos, ***se excluyen de la excepción al principio de subsidiaridad, que se da cuando la restricción o supresión de los derechos y garantías constitucionales denunciados, ocasionen perjuicio irremediable e irreparable, en cuya situación y de manera excepcional, procede la tutela demandada, aún existan otros medios de defensa y recursos pendientes de resolución***" (las negrillas corresponden a la Sentencia). Así también lo entendió la SCP 1445/2013 de 19 de agosto[26].

[26] "No obstante lo glosado, el artículo 61 del CPC establece una excepción al principio de subsidiariedad de esta acción tutelar, cuando señala que la acción de protección de privacidad podrá interponerse de forma directa, sin necesidad de reclamo administrativo previo, por la inminencia de la violación del derecho tutelado y la acción tenga un sentido eminentemente cautelar. De donde se concluye que previo a acudir ante la jurisdicción constitucional, de manera general se debe actuar conforme dispone la jurisprudencia, es decir, reclamar ante la entidad pública o privada encargada del resguardo y administración de la información, la entrega, actualización, rectificación o supresión de la información o datos falsos, incorrectos o que induce a discriminaciones; y en caso de no obtener una respuesta positiva favorable a su petitorio, y por ende, la reparación de sus derechos, entonces recién quedará expedita la vía constitucional; sin embargo, de acuerdo al texto contenido en el precitado artículo 61 del CPCo, podrá hacerse abstracción de la aplicación del principio de subsidiariedad, en virtud a lo cual, no se exigirá el reclamo administrativo previo, por la inminencia de la violación del derecho tutelado y la acción tenga un sentido eminentemente cautelar. No se debe perder de vista que para que sea viable la excepción alegada, se deben cumplir de manera simultánea ambos requisitos, dado que se encuentran unidos por la conjunción copulativa "y", que denota el vínculo o nexo entre ambas, e implica que deben darse a la vez, es decir, se evidencia la inminente de la violación al derecho a la autotutela informativa, lo que se traduce en que exista una extrema proximidad de una lesión o vulneración, y el mecanismo de defensa, pretenda evitar daños y perjuicio irreparables, como una medida preventiva".

Ahora bien cabe referirnos al artículo 61 del CPCo, que prevé que la acción de protección de privacidad podrá interponerse ante la "…inminencia de la violación del derecho tutelado…" denotando además su sentido estrictamente cautelar, no obstante y en base a lo referido previamente, cabe diferenciar entre *tutela transitoria* y *tutela inmediata*, siendo que la primera procederá en caso que exista otro mecanismo para la protección del derecho, pero que ante la gravedad e inminencia de la vulneración será necesario acudir a la misma, requisito que no es atendible en nuestro caso al constatar que no existe mecanismo alguno con el que la víctima pueda contar en un proceso penal como el que nos ocupa en el presente, por su parte la tutela inmediata responde a la inminencia de vulneración del hecho tutelado, lo cual se evidencia en el caso concreto, por lo que corresponde aplicar de manera directa la tutela inmediata en base al fundamento ut supra referido. Sin embargo, cabe aclarar que la aplicación de la tutela transitoria e inmediata de la acción de protección de privacidad, dependerá siempre de cada caso concreto y responderá a la evaluación de los antecedentes y supuestos fácticos para determinar si procede o no la interposición directa (entendimiento reiterado por la Sentencia Constitucional Plurinacional Nº0345/2018-S1, de 23 de julio).

11.2. De la legitimación pasiva en el caso concreto

A través de la presente acción de protección de privacidad esta Sala no puede declarar que el demandado fue quien lesionó los derechos de la accionante pues ello implicaría vulnerar la garantía de presunción de inocencia y el debido proceso, toda vez que ello debe determinarse por la autoridad penal competente, de ahí que el mismo no cuenta con legitimación pasiva en la presente acción, aspecto que impide la concesión de la acción de protección de privacidad bajo los términos demandados por la accionante, pues solo se podría determinar la supuesta responsabilidad que tuviere el hoy demandado sobre la distribución y difusión de dicho material en un proceso ordinario, es decir "…*la facultad de valoración de la prueba aportada en cualesquier proceso*

corresponde privativamente a los órganos jurisdiccionales ordinarios, por lo que el Tribunal Constitucional no puede pronunciarse sobre cuestiones que son de exclusiva competencia de aquellos, y menos atribuirse la facultad de revisar la valoración de la prueba que hubieran efectuado las autoridades judiciales competentes…" (SC 1461/2003-R de 6 de octubre); por lo tanto este Tribunal se encuentra impedido de determinar responsabilidad penal alguna, porque si bien el demandado está siendo investigado, el mismo goza de la garantía constitucional de presunción de inocencia (art. 116.I de la CPE), por lo mismo, no puede imponerse medidas de manera directa a favor de la accionante, en ese mismo entendimiento se refiere la jurisprudencia constitucional en la SC 1449/2002-R de 28 de noviembre.

Pese a lo antes referido cabe resaltar que el video con contenido sexual de la accionante afecta de sobremanera su derecho a la privacidad, intimidad, honra, honor, propia imagen y dignidad lo que alcanza a su familia, en la medida en la que, al encontrarse el archivo aún disponible en banco de datos de servidores privados, además de ser comercializado en La Paz y El Alto (conforme se desprende de la documentación aparejada al expediente -fs. 253-) se vulnera de manera particularmente intensa, constante y repetitiva los derechos ya referidos reconocidos tanto en Tratados Internacionales, como por la Constitución Política del Estado; en ese sentido, esta Sala no puede ignorar que el error en la interposición de la acción respecto a la legitimación pasiva puede agravar el daño irreparable generado.

Así pues, este Tribunal mediante la SCP 0033/2013 de 4 de enero, estableció que: "***La falta de legitimación pasiva no necesariamente provoca la denegatoria de una tutela sino debe atenderse a la urgencia y tipo de la tutela y si no se provoca indefensión****, en este sentido, se otorgó tutela de manera excepcional por ejemplo respecto vías de hecho y la concurrencia de legitimación pasiva parcial (SSCC 0953/2006-R y 0537/2007-R), cuando el colegiado se compone de muchos miembros también se admitió la legitimación pasiva parcial (SC 0447/2010-R de 28*

de junio), la posibilidad de plantear contra el cargo (SCP 0402/2012 de 22 de junio) o la no necesidad de plantear contra todos los responsables de los actos denunciados por las circunstancias del caso concreto ante vías de hecho (SCP 998/2012 de 5 de septiembre) todo ello bajo la idea de que la acción de amparo constitucional busca la protección de derechos fundamentales y no el cumplimiento de formalidades de forma que una tutela inoportuna por la exigencia de un nuevo planteamiento de demanda podría provocar un daño irreparable" (las negrillas corresponden a la Sentencia).

Así pues, ignorar la tutela de los derechos vulnerados en la presente acción de defensa, implicaría dejar en un estado de absoluta indefensión a la accionante y por lo mismo una revictimización, manteniendo de esa manera lesionados sus derechos fundamentales, de ahí que de forma excepcional, en el presente caso corresponde a esta justicia constitucional, actuando bajo los principios de *pro actione* y *pro homine*, tutelar los referidos derechos en los términos que serán infra expuestos.

Aclarado lo anterior, corresponde realizar el respectivo análisis de fondo de la problemática venida en revisión, siendo pertinente verter un examen acerca de los derechos presuntamente vulnerados.

Al respecto, la evolución de internet hizo que algunos derechos personales se vean amenazados, como el derecho a la privacidad, intimidad y al honor, por lo que cabe referirnos a los derechos vulnerados en el presente caso.

a) El derecho a la privacidad e intimidad

Al derecho a la intimidad se lo tiene como el derecho más clásico de esta índole, es así que el artículo 12 de la Declaración Universal de Derechos Humanos refiere que: "Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques".

Por su parte, nuestra Norma Suprema lo reconoce como derecho fundamental dentro del acápite de derechos civiles y políticos en su artículo 21.2 señalando que las bolivianas y los bolivianos tienen derecho: "A la privacidad, intimidad, honra, honor, propia imagen y dignidad", en ese sentido concebimos el derecho a la intimidad como esa esfera que protege la vida más privada del individuo frente a injerencias ajenas, salvo excepciones muy concretas contenidas en la Ley, por lo tanto dicha esfera protege elementos físicos e instrumentales (art. 25 de la CPE) como elementos sustanciales que suponen determinados datos sensibles sobre la persona (ideología, religión creencias, **vida sexual** o salud).

Bajo ese contexto la diferenciación con el derecho a la privacidad radica principalmente en la amplitud y alcance del mismo, es así que el derecho a la privacidad es mucho más amplio que el de la propia intimidad, que contiene datos vinculados a la persona, sean estos sensibles o no, que deben ser protegidos a razón del mal uso que se le pueda dar.

En ese sentido en el caso concreto, se evidenció (Conclusiones II.3 y II.4) la vulneración de los derechos de privacidad e intimidad de la accionante, al comprobarse que se encuentran datos sensibles de la misma dentro del tráfico de internet sin su consentimiento, por lo que su esfera de la privacidad fue vulnerada, pues dichos datos personales de la accionante involucran una relación íntima, por lo que al tratarse de elementos sustanciales del derecho de privacidad, la vulneración se amplía a su derecho a la intimidad por tratarse de datos sensibles, en específico de su vida sexual; por lo que, tanto su derecho a la privacidad, al ingresar, distribuir y difundir sus datos personales, como su derecho a la intimidad, al considerarse referidos datos como sensibles, fueron vulnerados; además, por su naturaleza y el poder de acceso a diferentes medios en los cuales se puede reproducir dicho material, se convierte en actos flagrantes vulneratorios a los indicados derechos, por lo que más allá de tratar de determinar una responsabilidad penal dentro de un proceso ordinario (Conclusión II.5) son derechos fundamentales que

deben garantizarse de manera inmediata y efectiva e incluso de oficio por parte del Estado.

b) Derecho a la propia imagen y dignidad

La Convención Americana sobre Derechos Humanos en su artículo 11 refiere que: "1. Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad; 2. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación; 3. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques"; en ese sentido la Corte Interamericana de Derechos Humanos trata el derecho a la honra y dignidad como aspectos con interconexión directa con los derechos a la privacidad e intimidad, es así como lo desarrolló en el caso de los hermanos Gómez Paquiyauri *Vs* Perú: *"En lo que respecta al artículo 11 de la Convención, está probado que las presuntas víctimas fueron tratadas como 'terroristas', sometiéndolas a ellas y a su familia al odio, desprecio público, persecución y a la discriminación, por lo cual se ha conformado una violación del artículo 11 de la Convención Americana, en relación con el artículo 1.1 de la misma, en perjuicio de los miembros de la familia mencionados en los párrafos 67.t y 67.u de la presente Sentencia*".

En el caso concreto se evidenció que en las plataformas de las páginas webs referidas (Conclusiones II.3 y II.4) y a raíz de la publicación de datos sensibles inherentes a la vida sexual de la accionante se vertieron todo tipo de comentarios, de índole sexual, siendo violentos y denigrantes no solo contra la accionante, sino también contra su familia y a su condición de mujer, demostrando además una violencia psicológica ejercida a la accionante y a su entorno, vulnerando así su derecho a la dignidad como persona inherente además al uso que ella puede hacer de su imagen personal.

En ese entendido igualmente cabe hacer referencia al artículo 17 de la Convención Americana sobre Derechos Humanos que evoca a la

protección a la familia, puesto que la vulneración a la honra de la accionante, también significó un ataque a la familia de la misma por evidenciarse que los comentarios no solo iban hacia su persona sino además a su esposo, en ese sentido debe considerarse incluso que la tutela viene a proteger derechos inherentes a la familia por haberse demostrado, que la accionante cuenta con una familia en la cual existe un niño, por lo que todo tipo de comentario ofensivo del que ella no pueda tener un control, involucra un atentado contra su núcleo familiar.

c) El derecho a la autodeterminación informática

La protección de datos personales se concreta jurídicamente a través de la acción de protección de privacidad, en ese sentido, cabe referirnos al derecho de autodeterminación informática como la prerrogativa que toda persona posee frente a cualquier entidad pública o privada, por la cual nadie debe introducirse, sin autorización expresa (de él mismo o por mandato de la ley), en aspectos que no sean públicos y se refieran a su vida personal y familiar, para que pueda procesarlos y/o difundirlos como vea conveniente, independientemente de la existencia o no de daño alguno.

En ese entendido, la autodeterminación informática constituye la dimensión positiva del ejercicio del derecho fundamental a la intimidad y la privacidad, es decir que dicha dimensión positiva implica el derecho que tiene la persona de acceder a los bancos de datos públicos y privados con el fin de tener conocimiento de cuanta información se ha almacenado, hacia donde fluyó la información o datos de la misma y para que fines, por lo que, sin una autorización expresa, tan solo el titular de ese derecho tiene la potestad de disponer la información concerniente a sus datos de carácter personal, de preservar la propia identidad informática, o lo que es igual, de consentir, controlar, o incluso el de rectificar los datos informáticos de carácter personal.

En el caso concreto, la accionante refiere que nunca autorizó, mucho menos consintió una grabación o video filmación de una

relación íntima, accediendo recién a ese material audiovisual el 1 de noviembre de 2013, a través de dos sitios webs, por lo que tampoco consintió una distribución del mismo de manera expresa, evidenciándose una flagrante vulneración a su derecho a la privacidad, intimidad, honra y dignidad que invoca la misma al ser constante la reproducción del material audiovisual y aun disponible, puesto que no existe un control directo sobre ese material, es decir que se encuentra indebida o ilegalmente impedida de conocer, objetar u obtener la eliminación o rectificación de los datos registrados y hecho público por veintiún páginas webs (Conclusión II.3).

Incluso, después de haber advertido la publicación de datos que van contra su privacidad, intimidad, honra y dignidad, su esposo planteó a través de un correo electrónico directo ante uno de los que maneja una de las páginas webs (Conclusión II.4) la eliminación de todo material que atentaba contra su persona y la ley, pese a eso la respuesta fue negativa, aduciendo el controlador de la referida página web que sería contraproducente la eliminación de ese material por que provocaría más morbo en la gente.

Desarrollado lo anterior e identificadas las flagrantes vulneraciones de los derechos de la accionante, es imperante aclarar dos aspectos, primero, que esta justicia constitucional mal podría atribuir como perpetrador de tales vulneraciones a la parte demandada (O. M. R.) pues, ello, significaría una intromisión directa al proceso penal que inclusive ya cuenta con una imputación formal, obviando la garantía de la presunción de inocencia y el debido proceso del antes nombrado; es decir, de actuar en tal sentido, esta justicia constitucional incurriría en un prejuzgamiento y una condena anticipada contra quien se encuentra siendo investigado por la justicia ordinaria, así, este Tribunal mal podría vulnerar los derechos del ahora demandado a título de "tutelar" derechos de la accionante; segundo, si bien es cierto que este Tribunal no puede de forma alguna actuar del modo supra señalado, no es menos cierto que en el caso concreto las vulneraciones a los derechos de la parte accionante son particularmente intensas, constantes y repetitivas,

lo que además afectan a su núcleo familiar el cual está integrado por un menor de edad que resulta ser hijo de ésta; ello es evidente y de conocimiento público, siendo fehacientemente comprobado a través de las diferentes documentales aparejadas al expediente (Conclusiones II.3 y II.4), es decir el material videográfico que afecta a los derechos de la accionante se encuentra siendo difundido en diferentes páginas webs e inclusive comercializado en las calles de La Paz y El Alto (fs. 253) y es precisamente dicha difusión la que origina en la accionante un profundo daño psicológico, pues a partir de lo anterior es que se genera el "repudio" de la sociedad contra ella y su núcleo familiar, ocasionándole como ella refiere una "muerte civil".

De ahí que este Tribunal, ante las particularidades del caso concreto descritas en el párrafo que antecede, se encuentra impelido de manifestar su profundo rechazo a las actitudes perpetradas por la sociedad boliviana contra la ahora accionante y que tienen su origen en la difusión del material que denigra tanto a ella como a su familia; y, es justamente a partir de lo anterior que, aplicando los principios *pro actione* y *pro homine,* esta justicia constitucional se encuentra impelida a conceder la tutela en los términos que se expondrán a continuación.

Así, las particularidades del caso concreto develaron una omisión por parte del Estado, a través del Ministerio Público, y es que la Fiscalía General del Estado es la institución que no solo debe ejercer la acción penal pública sino que, entre otras cosas, debe velar por los derechos de las víctimas evitando que lesiones constantes y repetitivas, como ocurrió en el presente caso, vayan en desmedro de la integridad de las mismas (Fundamento Jurídico III.2).

En ese sentido y a objeto de tener mayores luces a la hora de resolver la presente acción tutelar esta Sala solicitó documentación complementaria a la institución antes referida; así, obtuvo como respuesta la nota FGE/RJGP 104/2015, por la cual, el Fiscal General del Estado remitió a este Tribunal Constitucional Plurinacional, el informe FGE/STRIA. GRAL./1/2015 (Conclusión II.8), mediante el cual se

evidenció que el Ministerio Público omitió su deber de garantizar los derechos de la víctima, ello bajo el argumento de "…**tratarse de un delito que no está relacionado con imágenes de contenido sexual**" (negrillas agregadas en la Sentencia). Al respecto, la justicia constitucional manifiesta su más profunda preocupación pues, primero, las vulneraciones constantes y repetitivas que devienen del repudio social contra la hoy accionante eran de conocimiento público (basta dar una mirada a los diferentes medios de prensa para comprobar tal afirmación), más aún del Ministerio Público (Conclusión II.5); y, segundo, de la revisión de la imputación formal presentada por el Ministerio Público contra O. M. R. (demandado en la presente acción) se tiene que la misma se basó en que el antes mencionado adecuó su conducta en los delitos de violencia familiar o doméstica y extorsión, bajo el argumento que: "De la publicación y difusión de imágenes en las diferentes redes sociales de internet **sobre la intimidad de la víctima P. B. G., habiendo afectado de sobremanera la violencia psicológica y sexual sobre todo el entorno familiar**" (sic) (las negrillas corresponden a la Sentencia).

En ese sentido, lo alegado por el Fiscal General del Estado en sentido de justificar la falta de protección de los derechos de la víctima (P. B. G.) no resulta ser lógica ni razonable; pues con tales antecedentes y particularidades del caso concreto debió actuar proactivamente a efectos de evitar la constante y repetitiva vulneración de derechos de la hoy accionante.

Así también corresponde destacar que del referido informe remitido por el Fiscal General del Estado, se tiene que dicha institución puede aperturar casos por hechos descritos en el tipo penal de pornografía, adoptando medidas de protección necesarias para la víctima, como las previstas en el artículo 7 de la Ley de Protección de Denunciantes y Testigos, cuando la víctima se constituye en denunciante; corresponde aquí hacer un paréntesis y verificar cuáles son esas medidas a las que se refiere el Fiscal General del Estado, así la referida norma prevé las siguientes:

> *"I. Las medidas de protección destinadas a las personas que hayan realizado o se dispongan a realizar una actividad protegida y hayan sufrido o estén en riesgo de sufrir una represalia en los términos del Artículo 4 de la presente Ley, son las siguientes: 1. Preservación de la identidad y la confidencialidad de los datos personales; 2. Preservación de sus derechos laborales; 3. Protección policial para el traslado a fin de cumplir diligencias administrativas y/o judiciales; 4. Custodia policial en el domicilio de la persona; 5. Uso de sistemas tecnológicos que impidan que la identidad de la persona sea conocida; 6. Métodos de distorsión del aspecto físico o de la voz; 7. Alojamiento temporal en albergues destinados a protección de víctimas y testigos; cuya ubicación debe ser reservada y con custodia policial; 8. Atención psicológica; 9. Separación del resto de la población carcelaria o su traslado, bajo reserva, a otro recinto penitenciario, donde se le brinde mayor seguridad en el caso de persona protegida que se encuentre privada de libertad; 10. Otras que se puedan adoptar para preservar la seguridad de la persona protegida".*

Con lo anterior se evidencia otra omisión por parte de la Fiscalía General del Estado y es que de las medidas que, en su caso se adoptarían a favor de la víctima, no serían idóneas para evitar vulneraciones constantes y repetitivas como las perpetradas contra la ahora accionante. De ahí que esta Sala, ante tales omisiones que son contrarias con los deberes internacionalmente asumidos por el Estado boliviano (art. 2 de la Convención Americana sobre Derechos Humanos) se encuentra impelida de conceder la tutela impetrada, pero no contra O. M. R., sino contra la Fiscalía General del Estado por las razones ampliamente expuestas y sin responsabilidad por no haber sido demandado.

Así como efecto de la concesión de la tutela, esta Sala se encuentra impelida de exhortar a la Fiscalía General del Estado a que en su posición de garantes en razón a sus competencias gestionen y coordinen con las instancias gubernamentales pertinentes las medidas necesarias para la implementación de programas de protección a las víctimas surgidas de plataformas virtuales y de internet, así como la propagación de material que denigre al ser humano; tomando en

cuenta el deber de garantía hacia las víctimas, rol que constitucionalmente le está asignado como representante de la sociedad ante los órganos jurisdiccionales para velar por el respeto de los derechos y las garantías constitucionales, lo contrario sería no obedecer a su propósito como institución, e ir contra las normas constitucionales, siendo en ese caso responsable de nuevas vulneraciones a los derechos referidos en este fallo constitucional.

12. Conclusiones preliminares

La jurisprudencia constitucional boliviana, ha puesto de manifiesto que a lo largo de toda su vida, una persona es objeto de innumerables formas de identificación o individualización que se registran en otros tantos bancos de datos; desde el registro del nacimiento hasta el mismo momento de la defunción se realiza un sinfín de actividades en ese sentido. La individualización y anotación con un nombre, el otorgamiento de un documento de identidad numerado, la extracción de fichas dactiloscópicas, la obtención del pasaporte, la elaboración de la ficha de ingreso laboral, la apertura de cuentas corrientes o cajas de ahorro bancarias, las fichas de ingreso a un club deportivo, el registro en una entidad de salud, la historia clínica y tantas otras más, implican la existencia de una serie de datos personales que, merced al avance tecnológico, se encuentran interconectados, pudiendo establecerse una posible difusión o complementación o conocimiento de los datos, sin autorización expresa ni consentimiento por parte de la persona a la cual están referidos.

Por ello, y para resguardar los derechos del titular de dichos datos, se ha instituido la acción del *hábeas data*, que es una modalidad de amparo que permite a toda persona interesada acceder al conocimiento de los datos que consten en registros o bancos de datos públicos o privados destinados a proveer informes, y a exigir su supresión, rectificación, confidencialidad o actualización, en caso de falsedad o discriminación; y esta información debe referirse a cuestiones relacionadas con la intimidad, no pudiendo utilizarse por terceros sin derecho a hacerlo,

conforme lo ha precisado en su momento la jurisprudencia argentina sobre esta temática[27].

A su tiempo, el Informe Anual de la Relatoría para la Libertad de Expresión (2001)[28], estableció que la acción de *hábeas data* se erige sobre la base de tres premisas: 1) el derecho de cada persona a no ser perturbado en su privacidad (art. 11 CADH), 2) el derecho de toda persona a acceder a información sobre sí misma en bases de datos públicos y privados para modificar, anular o rectificar información sobre su persona por tratarse de datos sensibles (entendida como toda aquella información relacionada con la vida íntima de la persona), falsos, tendenciosos o discriminatorios, y 3) el derecho de las personas a utilizar la acción de hábeas data como mecanismo de fiscalización.

Este derecho de acceso y control de datos personales constituye un derecho fundamental en muchos ámbitos de la vida, pues la falta de mecanismos judiciales que permitan la rectificación, actualización o anulación de datos, afectaría directamente el derecho a la privacidad, el honor, la identidad personal, la propiedad y la fiscalización sobre la recopilación de datos obtenidos.

Asimismo, esta acción adquiere mayor importancia con el avance de las nuevas tecnologías de información y comunicación; dado que con la expansión en el uso de la computación e Internet, tanto el Estado como el sector privado tienen a su disposición en forma rápida una gran cantidad de información sobre las personas. Por lo tanto, es necesario garantizar la existencia de canales concretos de acceso rápido a la información para modificar información incorrecta o desactualizada

---

[27] (Cont. adm. Córdoba, "Flores, M. c/Provincia de Córdoba", LLC, 1996-316), citado por: PIERINI, Alicia, LORENCES, Valentín y TORNABENE, María Inés. *Hábeas data. Derecho a la intimidad*, Buenos Aires, Argentina: Editorial Universidad, 1999.

[28] Informe Anual de la Relatoría para la Libertad de Expresión 2001, disponible en: https://bit.ly/3lkFHvU

contenida en las bases de datos electrónicas protegiendo el derecho a la intimidad de los individuos, que precisamente es uno de los derechos que se relacionan más directamente con los límites del ejercicio de la libertad de expresión y la libertad de información.

En este contexto, la introducción del *hábeas data* en el sistema constitucional boliviano (2004), como una vía procesal de carácter instrumental, para la protección del derecho a la autodeterminación informática, ha significado un avance normativo importante en el proceso de judicialización de los derechos humanos y fundamentales en Bolivia, dado que se ha configurado como una acción jurisdiccional de carácter tutelar que forma parte de los procesos constitucionales previstos en el sistema de control de la constitucionalidad; a cuyo efecto, el texto constitucional reformado en aquel tiempo, contenía normas de carácter sustantivo, instituyendo el hábeas data como una garantía constitucional, determinando su alcance; y, establecía normas de carácter procesal dando la configuración básica en cuanto al trámite de esta acción tutelar.

Actualmente, la Constitución Política del Estado aprobada el año 2009, si bien cambia el *nomen juris* del hábeas data, con el nombre de Acción de Protección de Privacidad, ello no ha afectado su esencia tutelar, aunque también es cierto que contempla algunos cambios específicos en lo que se refiere a los casos de legitimación activa; no obstante, se mantiene la regla de la subsidiariedad, cuyas excepciones han sido fijadas oportunamente en cada caso por la jurisprudencia constitucional, siendo que además, actualmente se ha establecido la posibilidad de interposición directa de la Acción, de acuerdo a lo previsto en el Código Procesal Constitucional vigente en Bolivia.

AYER Y HOY DEL HÁBEAS DATA FINANCIERO.

El caso colombiano

✍ Martha C. Paz*

1. Introducción

El derecho fundamental al hábeas data se encuentra consagrado en el artículo 15 de la Constitución Política Colombiana, según el cual, todas las personas tienen derecho a la intimidad personal, al buen nombre, a conocer, actualizar y rectificar la información que se haya recogido sobre ellas en los diferentes bancos de datos y en los archivos de entidades públicas y privadas. Adicionalmente, establece la obligación que tiene el Estado de hacer respetar tales derechos. Asimismo, de conformidad con el artículo 152 de la Constitución Política, corresponde al Congreso de la República regular los derechos

* La Doctora Martha Cecilia Paz es ex Magistrada Auxiliar de la Corte Constitucional Colombiana. Master en Derechos Fundamentales de la Universidad Carlos III de Madrid (España); Especialista en Gestión Pública de la Universidad de los Andes en Bogotá; Egresada del Programa P.I.L. de la Universidad de Harvard en Derecho Constitucional y Jurisprudencia, con estudios de Maestría en Filosofía de la Universidad Javeriana de Bogotá; Diplomada en Argumentación jurídica en perspectiva de género del Instituto Flacso de México; Especialista en Justicia Constitucional de la Universidad Salamanca (España) y de la Universidad de Pisa (It.); Diplomada en derecho comparado de la Universidad de Bologna (It.) Ha sido Docente en la Universidad del Rosario en Bogotá en el área de interpretación constitucional y líneas jurisprudenciales. Autora de numerables artículos y obras en derecho constitucional y filosofía del derecho. Actualmente árbitro y abogada en ejercicio.

fundamentales de las personas, los procedimientos y recursos para su protección a través de la expedición de leyes estatutarias.

No obstante, ante el vacío generado por la falta de regulación inicial para el ejercicio del derecho fundamental al hábeas data, la Corte Constitucional se ocupó de caracterizarlo y determinar su alcance mediante sentencias de revisión de amparos.

2. La jurisprudencia que interpretó el artículo 15 de la Constitución Colombiana

El iter de la jurisprudencia efectivamente, puede refundirse en decisiones del período que se ha llamado "de la primera Corte", donde se advierten de manera tímida, los primeros lineamientos sobre el contenido esencial del hábeas data, sosteniendo que el derecho a la protección de los datos personales se encuentra directamente relacionado con la eficacia del derecho a la intimidad, toda vez que, el individuo es quien tiene la potestad de divulgar la información de su vida privada. Al respecto, la sentencia **T. 414 de 1992**, estableció que toda persona, *"(…) es titular a priori de este derecho y el único legitimado para permitir la divulgación de datos concernientes a su vida privada. Su finalidad es la de asegurar la protección de intereses morales; su titular no puede renunciar total o definitivamente a la intimidad pues dicho acto estaría viciado de nulidad absoluta."*

Desarrollos siguientes del mismo período, fueron ampliando el radio de acción del derecho y en las **sentencias T-444 de 1992**, **T-525 de 1992** y **T-022 de 1993** la Corte Constitucional consideró que la intimidad personal ciertamente comprendía varias dimensiones, dentro de las cuales se encuentra el hábeas data, que comporta el derecho de las personas a obtener la información personal que se encuentre en archivos o bases de datos, la posibilidad de ser informado acerca de los datos registrados sobre sí mismo, la facultad de corregirlos, la divulgación de datos ciertos y la proscripción de manejar tal información cuando existe una prohibición para hacerlo. En este orden de ideas,

estimó que *"(…) tanto el hábeas data como la intimidad encuentran su razón de ser y 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 su personalidad y en homenaje justiciero a su dignidad".*

Seguida la **sentencia SU-082 de 1995**, donde la Corte escinde para su análisis las categorías ius fundamentales del artículo 15 referido, diferencia los derechos a la intimidad y al hábeas data y, en particular, distingue tres derechos fundamentales derivados del artículo 15, a saber: la intimidad, el buen nombre y el hábeas data. Desde esa oportunidad, determinó que el *hábeas data* era un derecho fundamental autónomo que comprendía tres facultades concretas: (i) el derecho a conocer las informaciones que a su titular se refieren; (ii) el derecho a actualizar tales informaciones; y (iii) el derecho a rectificar las informaciones que no correspondan a la verdad.

En el año 2000, ya con una nueva integración de magistrados, en la **sentencia T-527 de 2000**, la Corte Constitucional reconoció que el titular de la información que reposa en una base de datos cuenta con dos mecanismos de protección: (i) la rectificación, que implica la concordancia del dato con la realidad, y (ii) la actualización, que hace referencia a la vigencia del dato, de tal manera que no se muestren situaciones ajenas a una situación actual.

Posteriormente, en la **sentencia T-729 de 2002**, definió el derecho al hábeas data como la facultad que tiene el titular de información personal de exigir a las administradoras de bases de datos el acceso, la inclusión, la exclusión, la corrección, la adición, la actualización, la certificación de la información y la posibilidad de limitar su divulgación, publicación o cesión. Se trata de una sentencia hito en el tema, puesto que la Corte intenta ambientar y contextualizar el escenario eventual de aplicación del derecho al hábeas data, aduciendo que éste depende del entorno en el cual se desarrollan los procesos de administración de bases de datos personales. En consecuencia, el

contexto material de dicho derecho, está integrado por "*el objeto o la actividad de las entidades administradoras de bases de datos, las regulaciones internas, los mecanismos técnicos para la recopilación, procesamiento, almacenamiento, seguridad y divulgación de los datos personales y la reglamentación sobre usuarios de los servicios de las administradoras de las bases de datos*". Igualmente sintetizó los principios que la jurisprudencia había desarrollado al conocer de tutelas relacionadas con el derecho al hábeas data. En particular, determinó que el proceso de administración de los datos personales se basa en los principios de *libertad*, *necesidad*, *veracidad*, *integridad*, *incorporación*, *finalidad*, *utilidad*, *circulación restringida*, *caducidad* e *individualidad*.

3. Ley Estatutaria 1266 de 2008. Principios rectores

A fuerza de pronunciamientos constitucionales y en cumplimiento del deber de regular el derecho fundamental al hábeas data a cargo del Congreso de la República, se expidió en el año 2008 la **Ley Estatuaria 1266** , por la cual se dictaron las disposiciones generales del hábeas data y se reguló el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países. Se trató de una normativa sectorizada que regulaba especialmente el derecho al hábeas data circunscrito al dato financiero. En la **sentencia C-1011 de 2008,** la Corte efectuó el análisis de constitucionalidad previo del proyecto de ley y efectivamente determinó, que se trataba de una Ley de carácter sectorial, dirigida a la regulación de la administración de datos personales de contenido comercial, financiero y crediticio.

No obstante su carácter parcial, la Ley 1266 de 2008 reiteró los principios que había esbozado la jurisprudencia como rectores del derecho al hábeas data en general. Específicamente, estableció que las actividades de recolección, procesamiento y circulación de datos personales contenidos en bases de datos de carácter financiero, deben regirse por los siguientes principios: veracidad, temporalidad, integridad, seguridad, confidencialidad, circulación restringida y finalidad. El principio

de veracidad o calidad tiene dos funciones, la primera, es exigir que la información contenida en los bancos de datos regidos por la Ley 1266 de 2008, sea veraz, completa, exacta, actualizada, comprobable y comprensible. El segundo objetivo, es prohibir el registro y divulgación de datos parciales, incompletos, fraccionados o que conduzcan a error. La temporalidad del dato hace referencia a que la información registrada debe dejar de ser suministrada a los usuarios, cuando deje de servir para la finalidad del banco de datos. La interpretación integral de los derechos constitucionales establece que la norma estatutaria, debe ser interpretada en el sentido de que se dé la máxima eficacia posible a los derechos constitucionales, en particular, al hábeas data, el buen nombre, la honra, la intimidad y de acceso a la información. Asimismo, dispone que los derechos de los titulares de los datos personales se deben interpretar conforme lo establecido en el artículo 20 de la Constitución.

El principio de seguridad está relacionado con la obligación que tienen los administradores de las bases de datos de incorporar las medidas técnicas necesarias para garantizar la seguridad de la información al momento de transmitirla, a fin de evitar su adulteración, pérdida, consulta o usos no autorizados. La confidencialidad se refiere a la obligación que tienen todas las personas naturales o jurídicas que intervengan en la administración de datos personales que no sean públicos, de garantizar la reserva de la información, incluso después de que ha terminado su labor en la cadena de administración de datos y limitándose a suministrar o comunicar la información cuando se relacione con el desarrollo de las actividades autorizadas en la ley.

La circulación restringida de la información busca ceñir la administración de los datos personales a los límites que se deriven de su naturaleza, de la norma estatutaria, de los principios propios que le son aplicables a dicha actividad, en particular la temporalidad de la información y la finalidad del banco de datos. Con fundamento en lo anterior, se prohíbe acceder a datos personales por internet o por otros medios de divulgación de información masiva, excepto que sea información pública, o que los datos tengan un acceso técnicamente

controlable para brindar un conocimiento restringido, limitándose a los titulares o usuarios autorizados para tener dicho acceso. El principio de finalidad, implica que la administración y divulgación de datos personales debe tener una finalidad legítima conforme a la Constitución Política y la ley. Adicionalmente, dispone que el objetivo de registrar un dato debe ser informado al titular del mismo, antes o durante el otorgamiento de la autorización para su uso, en los casos en que esta fuera necesaria y en general cuando el titular solicita información al respecto.

Con la expedición de la Ley 1266 de 2008, se dio un gran paso en la materialización del derecho al hábeas data y la protección de los datos personales, abriendo la puerta a que Colombia estuviera a la vanguardia de países con buen nivel en protección de datos y haciéndolo más atractivo para la inversión extranjera como se ha comprobado en los años posteriores a la expedición de esa normatividad. La Ley del Hábeas Data financiero hoy es considerada en Colombia como el principal sustrato normativo para el tratamiento de la información financiera y comercial de los ciudadanos. Su promulgación fue el alivio para millones de colombianos reportados en centrales de riesgo financiero.

Nadie duda que el desarrollo de este derecho fundamental que otorga la Carta Política a los ciudadanos colombianos, sobre la información que acerca de ellos repose en bases de datos, ha tenido una serie de efectos positivos, particularmente económicos. Una de las aristas más relevantes de la Ley 1266 de 2008 radica, en que estableció responsabilidades puntuales a las fuentes, a los operadores y a los usuarios de la información. Esto es importante, pues significó otorgar y precisar los roles concretos a cada uno de los actores involucrados, con el fin de garantizar el derecho fundamental al Hábeas Data. Del mismo modo, le permitió al ciudadano hacer efectivo su derecho, consagrado constitucionalmente, mediante peticiones, consultas o reclamos. Así, es de destacar igualmente, que ésta ley ha permitido que las prácticas y los usos de la información financiera de millones de colombianos, que hacen el

sector público y privado, se ciñan de manera estricta a los principios de veracidad, finalidad, circulación restringida, temporalidad de la información, interpretación integral de derechos constitucionales, seguridad y confidencialidad. También, dio la potestad a la Superintendencia de Industria y Comercio y a la Superintendencia Financiera, de imponer sanciones a los operadores, fuentes o usuarios, que le den un trato ilegal a la información financiera personal.

4. La nueva ley Estatutaria sobre hábeas data. Un proyecto en discusión

Desde la vigencia de la mencionada norma, y gracias a un trabajo mancomunado entre la academia, la jurisprudencia y el cuerpo legislativo, se ha logrado determinar cuáles son las necesidades más urgentes de los colombianos en relación con la protección de datos personales en el sector financiero, y se han detectado las falencias más urgentes de corregir y en qué sentido se debe fortalecer la Ley de Hábeas Data en este sector, por ello, un nuevo proyecto de Ley Estatutaria que actualmente cursa su proceso de revisión constitucional, busca fortalecer la protección al derecho de Hábeas Data brindando más y mejores herramientas que permitan a los titulares ejercer su derecho a la autodeterminación informática, efectivizando los actos de conocer, actualizar y rectificar las informaciones que sobre ellos esté en los bancos de datos del sector financiero, comercial y crediticio.

Para el Legislador colombiano, es actualmente imperioso, contar con una normativa adecuada a las transformaciones tecnológicas más recientes, que garantice a los ciudadanos que los nuevos contextos de interacción entre los distintos agentes involucrados en dinámicas económicas particulares, no vulneren sus derechos. Ello, porque el trasfondo de la garantía del Hábeas Data es en últimas, el reconocimiento del individuo como núcleo de la sociedad y la apertura de los esquemas legales a las nuevas realidades internacionales, con el fin de evitar que las personas se encuentren en situaciones de vulnerabilidad por el uso inadecuado de su información personal.

Las necesidades propias de la vida moderna han privilegiado la necesidad de que todos los ciudadanos tengan acceso al sector financiero, pues éste se ha convertido en la columna vertebral de la economía de los demás sectores, factores como el crédito dinamizan la sociedad y activan la economía del país, los bancos tienen la facultad de recaudar el ahorro de la sociedad, para luego poder redistribuirlo entre empresas y familias que a su vez demandan créditos y fondos que les permitan desarrollar actividades económicas, que a su vez se convierten muchas de ellas en la materialización de derechos que dignifican el nivel de vida como los créditos para vivienda, e impulsan el desarrollo social con créditos en educación y para la conformación de empresas, de allí la necesidad de facilitar el acceso al crédito como piñón esencial de ese engranaje llamado economía y como parte de la denominada d*emocratización del crédito.*

La Constitución colombiana en su artículo 335 describe la actividad financiera como una actividad de interés público, es decir, que el Estado está en la obligación de regular y establecer los límites de su ejercicio, al tiempo que la Constitución reconoce también la libertad contractual y la autonomía privada en materia de contratación. El artículo 333 indica, que la actividad económica y la iniciativa privada son libres, dentro de los límites del bien común. Sin embargo, según el artículo 335 las actividades financieras, bursátil, aseguradora y cualquier otra relacionada con el manejo, aprovechamiento e inversión de los recursos de captación a las que se refiere el literal d) del numeral 19 del artículo 150, son de interés público y sólo pueden ser ejercidas previa autorización del Estado, conforme a la ley, la cual regulará la forma de intervención del Gobierno en estas materias y promoverá la democratización del crédito.

En consecuencia, el desarrollo de ayudas, alternativas y recursos jurídicos que contribuyan a la democratización del crédito permitiendo que más personas puedan acceder de una manera rápida y efectiva al sector financiero y comercial para suplir necesidades y mejorar su nivel

de vida, es uno de los propósitos principales de la nueva ley estatutaria sobre hábeas data, pues al actualizarse de manera más rápida la información de los titulares, se dinamizan las relaciones comerciales, cumpliendo así el Estado con las obligaciones de democratizar del crédito.

5. Conclusión. Los cambios que propone la nueva ley de hábeas data. Bondades y críticas

- Los cambios más relevantes de la nueva ley, (que actualmente se encuentra en control constitucional previo en la Corte Constitucional) o el cambio que más impacta es el de la caducidad del dato negativo. Se disminuye (de 4 a 2 años) el tiempo de permanencia de la información de carácter negativo (reportes financieros negativos), que actualmente es del doble del tiempo de la mora no sobrepasando 4 años.

  En la actualidad y gracias al seguimiento que se le ha venido haciendo a la Ley 1266, se ha logrado determinar que las necesidades propias del mercado financiero, comercial y la dinámica del crédito hacen necesario que el tiempo de permanencia del dato negativo se ajuste a las necesidades que tienen los ciudadanos. Saber que el tiempo de permanencia del dato luego de la extinción de la obligación es prudencial, permite a los deudores tener una motivación para la cultura del pago pues simplemente sabrán que el tiempo de permanencia no excede al hecho mismo que la generó.

  A mi juicio el término de 2 años no es arbitrario ni carente de rigor. Por el contrario, es serio y preserva la función de gestión del riesgo de los intermediadores financieros, y retoma una muy clara línea jurisprudencial de la Corte Constitucional que a través de fallos de tutela estableció como límite razonable para los reportes negativos el término de 2 años. La sentencia SU 082/1995 indicó que *"el término para la caducidad del dato lo debe fijar, razonablemente, el legislador. Pero,*

mientras no lo haya fijado, hay que considerar que es razonable el término que evite el abuso del poder informático y preserve las sanas prácticas crediticias, defendiendo así el interés general (...) cuando el pago se ha producido una vez presentada la demanda, con la sola notificación del mandamiento de pago, el término de caducidad será solamente de dos (2) años, es decir, se seguirá la regla general del pago voluntario". Lo propio se dijo en la sentencia T-565/2004.

Disminuir el tiempo máximo de permanencia del reporte cuando la obligación es extinguida, está de acuerdo también con el derecho al olvido en el que se fundamenta la no perennidad de las informaciones en las bases de datos, además de dinamizar el acceso al crédito y respetar los derechos conexos al buen nombre y la dignidad; sin embargo albergo también dudas, porque esta disposición podría afectar los avances alcanzados en materia de inclusión financiera, por cuanto la reducción del término de permanencia de la información de 4 a 2 años puede restringir el acceso al crédito por falta de información.

2. Se propone una amnistía para todo aquel que se ponga al día en sus deudas, consistente en la eliminación de los reportes negativos.

   Sugiero que eliminar la información negativa de las centrales de riesgo impide una valoración real del comportamiento crediticio del cliente y contamina posiblemente un alto porcentaje de la información positiva, castigando a quienes honran a tiempo sus obligaciones. Podría presentarse igualmente una discriminación, que afecta gravemente la democratización del crédito y la inclusión financiera; si el mercado crediticio no cuenta con la información histórica de los deudores, preferirá obviamente, prestarle a clientes conocidos y de mayores recursos, marginando a aquellos de menores recursos cuya

única carta de presentación era su historia de crédito. Creo que puede haber un efecto perverso en la norma pues se obligará a las personas a que continúen expuestas a prácticas abusivas e ilegales buscando fondos en los mercados informales con tasas de interés irracionales y con financiación solo a corto plazo. Pienso igualmente, que se trata de una medida que afecta primordialmente al microcrédito pues la experiencia demuestra que las amnistías en materia de información, se traducen en restricción del crédito para los segmentos menos favorecidos de la población y promueven eivdentemente la cultura del no pago.

3. La nueva ley propone la eliminación del reporte de deudas inferiores a un salario mínimo legal vigente.

   Parecería una norma en apariencia favorable, pero estimo que en el fondo y en la práctica, disminuiría de manera considerable la cobertura y calidad de la información crediticia en los sectores menos favorecidos y, por lo tanto, se les restringiría el acceso al crédito. El 68% del total de las obligaciones existentes en buros de crédito podrían ser obligaciones inferiores a ese monto, que actualmente en Colombia es de $877.803 pesos.

4. Finalmente, otras disposiciones como las siguientes creo que son bienvenidas y no ofrecen grandes dudas: (i) consultar la información crediticia será en todo caso y por todos los medios gratuita para el titular de la información y no disminuirá su calificación; (ii) el Gobierno nacional deberá promover la firma de convenios internacionales de cooperación para que la información crediticia de los colombianos radicados en el exterior pueda ser homologada en Colombia y (iii) se crea un procedimiento especial para que las víctimas de suplantación personal puedan ejercer el derecho al hábeas data y mantener su buen nombre.

Bibliogafía

- Grupo del Banco Mundial. (2010). Doing business (No. 3). Recuperado de http://espanol.doingbusiness.org/~/media/GIAWB/Doing%20Business/Documents/Subnational-Reports/DB13-ColombiaSpanish.pdf.

- Escobar, Andrés F.; Pajarito, Mónica P. (2014) Alcance e implicaciones del derecho al Hábeas Data en el comercio colombiano. (Tesis) Bogotá: Pontificia Universidad Javeriana.

- Ramírez Prado, Juliana, (9 de marzo de 2015) La violación de Hábeas Data La República. Recuperado de: http://www.larepublica.co/la-violaci%C3%B3nde-hábeas-data-dej%C3%B3-multas-por1892-millones-durante-ela%C3%B1opasado_228696)

www.corteconstitucional.gov.co para consulta de las sentencias citadas

www.senado.gov.co para los proyectos de ley consultados.

- Estudios Constitucionales, Año 3 N° 2, ISSN 0718-0195, Universidad de Talca, 2005 El hábeas data y el derecho de autodeterminación informativa en perspectiva de derecho comparado Víctor Bazán; páginas 85 a 139.

HÁBEAS DATA EN MATERIA TRIBUTARIA Y REPERCUSIÓN ANTE LOS CONTRIBUYENTES

✍ Artur Ricardo Ratc*

1. Introducción

En los países subdesarrollados, es común que los contribuyentes no tengan acceso a la información de datos públicos, especialmente los datos personales por pagos de tributos de personas físicas y jurídicas. Es una situación constante que un contribuyente, persona física o jurídica, tenga la necesidad de contar con informaciones acerca de pagos de tributos o débitos controlados por el Ministerio de Hacienda o la Secretaría de Hacienda correspondiente que hace ese encuentro de cuentas entre pagos y débitos de contribuyentes en general.

* Doctor en Ciencias Jurídicas y Sociales UMSA - Universidad Museo Social Argentino; Doctorando en Derecho Constitucional UBA - Universidad de Buenos Aires; Posgrado en Derecho Administrativo PUC/SP – Pontifícia Universidade Católica de São Paulo; Especialista en Derecho Tributário UNISUL/SP – Universidade do Sul de Santa Catarina Especialista; en Derecho Constitucional UNISUL/SP – Universidade do Sul de Santa Catarina Especialista; en Ciências Procesuales UNAMA/SP – Universidade da Amazônia Especialista; en Derecho Procesual Civil UNISUL/SP – Universidade do Sul de Santa Catarina; Abogado Internacional Tributarista en Sudamerica y Europa con registro en la Orden de los Abogados de Brasil y Portugal. Profesor en Derecho Constitucional y Derecho Tributario.

Actualmente, con la COVID-19[1], es normal que las personas no puedan hacer sus pagos de tributos porque estamos viviendo una gran recesión y perdiendo empleos, al tiempo que la mayoría de las empresas del mundo están pasando por serios problemas financieros –consecuencia lógica– con el pago de tributos. Sin embargo, existen contribuyentes que están al día con sus cuentas y otros que necesitan acceder a los datos del Fisco para regularizar las deudas pendientes y controlar los pagos efectuados. En estos casos, el contribuyente necesita sus propios datos ante los registros del ente gubernamental y el acceso a la información que, muchas veces, es increíblemente negado.

En Brasil, se utilizan algunos instrumentos constitucionales a favor de los contribuyentes con la idea de que la Constitución garantice derechos fundamentales, especialmente con la idea de compensar tributos con créditos en contra del Estado (en la hipótesis de las ejecuciones de sentencias contra el Estado), así como con la imposibilidad de acceso a informaciones del contribuyente de la base de datos del Estado que impide el regular ejercicio del derecho a la información.

El cobro de tributos, en algunas ocasiones, en los países de Sudamérica, es un medio de aumentar la caja del Estado ilegalmente para después responder en la vía judicial si el pago fue ilegal o no. La mayoría de las veces es ilegal. Sin embargo, pocas personas tienen la posibilidad de hacer su descargo frente a este cobro ilegal porque es costosa la contratación de un abogado posteriormente al cobro ilegal de tributos para reivindicar sus derechos. Resultado: El Estado durante décadas recauda valores ilegales para mantener su estructura costosa y grava a los contribuyentes de manera injusta.

[1] Es un virus que surgió en Wuhan - China de una fuente animal y propagado de persona a persona a través de gotas salivales que se producen, al tiempo que crea una afección respiratoria que se puede propagar entre las personas, principalmente con el contacto cercano. La previsión de los mercados es que llevará a la peor recesión global desde 1929 ante la imposibilidad de actuación de las empresas que están en cuarentena y a "puertas cerradas".

Independientemente del concepto de justicia o injusticia[2], es cierto que en países subdesarrollados tenemos problemas con el acceso a la justicia, así como a los datos de los propios contribuyentes que a veces tienen deudas ya alcanzadas por la caducidad o prescripción, pero el Estado no se manifiesta sobre la extinción del crédito tributario y espera que el contribuyente desinformado pague una deuda que está extinguida. En otras ocasiones, inclusive con la extinción de la deuda, el Estado mantiene los registros desactualizados del contribuyente con la indicación de una deuda indebida.

A veces, la única solución es accionar ante el poder judicial para tener acceso a las propias informaciones a través de un instrumento constitucional que garantiza el derecho de acceso a las informaciones.

La cuestión que surge es: ¿Qué hacer cuando el contribuyente necesita su propio dato frente al ente público que mantiene el control de las informaciones fiscales, y, se mantiene inerte al suministro de datos solicitados por el contribuyente?

2. La constitución y el hábeas data

En la actual constitución de Brasil (1988), esta acción constitucional está garantizada por medio del *hábeas data*, acción constitucional que tiene como objetivo garantizar el acceso a los bancos de datos de los entes públicos para que la persona tenga informaciones propias, como forma de garantizar el acceso irrestricto a las informaciones que son obstaculizadas por el Estado.

La Constitucional Federal de Brasil crea, en el artículo 5º, los derechos fundamentales a los nacionales y extranjeros, que reza: *"Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza,*

[2] Entendemos que la justicia es un valor del Derecho, de acuerdo con la doctrina trialista (MIGUEL REALE) que busca la resolución de conflictos en situaciones concretas.

garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: (...) LXXII - Conceder-se-á hábeas data: a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público; b) b) para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo;"[3].

Es de nivel constitucional fundamental, por lo tanto, el derecho irrestricto a las informaciones de las personas para garantizar el conocimiento de datos propios que están registrados o en un banco de datos de entidades gubernamentales o en alguna entidad de carácter público.

En Perú, así como en Brasil, el tema es de nivel constitucional[4] y la acción procede contra todo hecho u omisión de cualquier autoridad (incluso el Fisco) que vulnera o amenaza derechos fundamentales.

El inicio de la constitucionalización del tema, creemos que fue con la constitución estadunidense en 1974 con el "*Freedom of Information Act*" que tenía como esencia la posibilidad de que las personas obtengan sus datos en registros y bancos de datos públicos de manera transparente y de acceso por el ciudadano. La tratativa del hábeas data como derecho constitucional fundamental en los dos países referidos (Brasil y Perú) tiene origen en el derecho europeo, especialmente, la constitución española de 1978 y la constitución portuguesa de 1976

[3] Constitución Federal - Art. 5: www.planalto.gov.br

[4] Artículo 200.- Acciones de Garantía Constitucional: Son garantías constitucionales: 3. La Acción de Hábeas Data, que procede contra el hecho u omisión, por parte de cualquier autoridad, funcionario o persona, que vulnera o amenaza los derechos a que se refiere el artículo 2, incisos 5, 6 y 7 de la Constitución. (*) (*) Inciso modificado por el Artículo Único de la Ley Nº 26470, publicada el 12 junio 1995, cuyo texto es el siguiente: "3. La Acción de Hábeas Data, que procede contra el hecho u omisión, por parte de cualquier autoridad, funcionario o persona, que vulnera o amenaza los derechos a que se refiere el artículo 2, incisos 5 y 6 de la Constitución."

que ofrecen un remedio constitucional[5] similar que garantiza a la persona el derecho a la información y a la transmisión de datos.

Al tratar el derecho constitucional de acceso a la información y datos, debemos entender que el término *"datos"* debe ser considerado con una interpretación extensiva, o sea, todos los datos necesarios de la persona física o jurídica que de manera directa o indirecta puede causar algún perjuicio al derecho de privacidad. En la esfera tributaria, todos los entes gubernamentales que mantienen los datos de los contribuyentes tienen el deber de presentar informaciones acerca de pagos de tributos, competencias, cuotas, compensación, débitos y cualquier otra información del propio interesado que puede ser perjudicado con la omisión o la falta de información solicitada.

Otra cuestión importante es que tal derecho es protegido siempre que el Estado se haya negado a suministrar las informaciones, es decir, el contribuyente primero necesita solicitar las informaciones al órgano competente para después pensar en un juicio vía *hábeas data*.

A propósito, el Supremo Tribunal Federal tiene una *súmula*, es decir, una consolidación de la jurisprudencia que dicta el siguiente entendimiento: Súmula 2 del STF *"não cabe o hábeas data (CF, artículo 5º LXXII, letra a) se não houve recusa de informações por parte da autoridade administrativa"*. En este sentido, por lo tanto, determina un requisito indispensable para la acción de *hábeas data* que es la prueba de denegación de la solicitud de información o la omisión de la autoridad en atender la solicitud.

---

[5] *"(...) O hábeas data é considerado como um writ, uma garantia, um remédio constitucional à disposição dos cidadãos para que eles possam implementar direitos subjetivos que estão sendo obstaculados, assegurando o liame entre a normatividade e a normalidade. Como uma das espécies de remédios constitucional, ocupa um papel de relevo na teorética constitucional porque auspicia a garantia de direitos constitucionais, possibilitando sua concretização normativa. Sua inspiração adveio da Constituição portuguesa de 1976 e da Constituição espanhola de 1978, que previram instituto semelhante para resguardar o direito à informação e à transmissão de dados (...) (Jose Joaquim Gomes Canotilho, Gilmar Ferreira Mendes, Ingo Wolfgang Sarlet e Lenio Luiz Streck, Comentários à Constituição. Editora Saraiva, 1ª Edição, 2013, p.487)".*

3. La reglamentación del hábeas data en Brasil - Ley 9.507/97 - La importancia de la prueba

A continuación, la ley 9.507/97 en Brasil reglamentó el instituto del hábeas data ante la necesidad de saber el procedimiento de la acción que tenía previsión constitucional, pero no tenía una aplicación efectiva por falta de reglamentación.

Con la promulgación de la ley del hábeas data, quedaron más claras y objetivas algunas cuestiones, como por ejemplo los requisitos para la acción judicial, plazos para que el órgano público se pronuncie, recurso al Tribunal en casos de no aceptación del juicio, entre otros.

Nuestro entendimiento está dirigido, especialmente, al artículo octavo de la referida ley, toda vez que en el tema tributario los contribuyentes tienen muchos problemas de acceso a la información, ya sea por la omisión del Fisco o por la falta de actos de rectificación necesarios para mantener íntegramente el derecho de privacidad.

Pasamos al estudio, especialmente del artículo octavo[6] de la ley 9.507/97, que reza: *"Art. 8° A petição inicial, que deverá preencher os requisitos dos artículos 282 a 285 do Código de Processo Civil, será apresentada em duas vias, e os documentos que instruírem a primeira serão reproduzidos por cópia na segunda. Parágrafo único. A petição inicial deverá ser instruída com prova."*. Esta primera parte del artículo se refiere a los requisitos básicos de la acción, es decir, la constitución de la prueba de ofensa al derecho de información, así como, el juez o tribunal competente, nombre de las partes, hechos y fundamentos jurídicos y valor de la causa.

---

[6] *Lei 9.507/97 - Art. 8° A petição inicial, que deverá preencher os requisitos dos artículos 282 a 285 do Código de Processo Civil, será apresentada em duas vias, e os documentos que instruírem a primeira serão reproduzidos por cópia na segunda.*

Parágrafo único. A petição inicial deverá ser instruída com prova:

I . da recusa ao acesso às informações ou do decurso de mais de dez dias sem decisão;

II. da recusa em fazer-se a retificação ou do decurso de mais de quinze dias, sem decisão; ou

III. da recusa em fazer-se a anotação a que se refere o § 2° do artículo 4° ou do decurso de mais de quinze dias sem decisão.

El tema que más nos preocupa, principalmente en materia tributaria, son los incisos del párrafo único del artículo octavo también referido a las pruebas, que establece: *"I - da recusa ao acesso às informações ou do decurso de mais de dez dias sem decisão;"*. Este dispositivo de la ley reglamentaria prevé que el contribuyente necesita probar que no fue posible acceder a los datos por negativa del órgano o atendida la solicitud en el órgano gubernamental, este, no decidió acerca del pedido de informaciones luego de más de diez días.

Por otro lado, aún en la etapa de las pruebas, es interesante el otro inciso del artículo octavo, que prevé: *"II - da recusa em fazer-se a retificação ou do decurso de mais de quinze dias, sem decisão; ou"*. En esta situación específica, el contribuyente solicitó una rectificación de la base de datos del fisco y este órgano se negó a hacer la rectificación o transcurrieron más de quince días sin pronunciarse sobre el tema. En estos casos, el contribuyente necesita comprobar el transcurso del plazo de quince días o la falta de rectificación.

Por último y no menos importante, el artículo octavo párrafo único inciso III, trata sobre la negativa del fisco en hacer la anotación de explicaciones del contribuyente en documentos que necesitan rectificación[7], o el hecho de solicitar el agregado de documentos con explicaciones para la rectificación sin que el órgano se manifieste en los quince días posteriores a la solicitud, al decir: *"III - da recusa em fazer-se a anotação a que se refere o § 2° do artículo 4° ou do decurso de mais de quinze dias sem decisão"*.

Es cierto que el contribuyente, cuando tratamos materia tributaria, necesita comprobar los hechos desfavorables en la búsqueda de informaciones fiscales, cuando el Estado - directa o indirectamente - mantiene

[7] *Lei 9.507/97 - Art. 4° Constatada a inexatidão de qualquer dado a seu respeito, o interessado, em petição acompanhada de documentos comprobatórios, poderá requerer sua retificação.*
(...)
§ 2° Ainda que não se constate a inexatidão do dado, se o interessado apresentar explicação ou contestação sobre o mesmo, justificando possível pendência sobre o fato objeto do dado, tal explicação será anotada no cadastro do interessado.

registros o banco de datos (permanentes o temporarios) con las informaciones de los contribuyentes y una vez solicitado omite atender la solicitud o no cumple con la posibilidad de un amplio acceso a la información.

4. Recurso con repercusión general en el supremo tribunal federal y hábeas data en materia tributaria

El Supremo Tribunal Federal, incluso bajo el sistema de ofrecer celeridad a los pronunciamientos y disminuir el número de procesos con carácter solamente dilatorio que no discutían materias constitucionales o, si las discutían, eran de interés de las partes involucradas y no de una colectividad, pasó a adoptar la regla de la repercusión general de temas políticos, económicos, sociales o jurídicos en la admisión de los recursos extraordinarios[8]. La repercusión general es una cuestión preliminar que debe ser suscitada en el recurso extraordinario, con el objeto de demostrar que la cuestión debatida se revela de interés político, social, económico o jurídico para un gran número de personas y no, solamente, respecto de intereses subjetivos. Ésta, en tal sentido, es la esencia de la Corte Suprema, es decir, analizar el interés de la colectividad al juzgar las causas constitucionales de su competencia y someter la decisión de los recursos con repercusión general a los tribunales inferiores.

En materia de hábeas data, esencialmente, el entendimiento del Supremo Tribunal Federal brasileño en el Recurso Extraordinario N.º 673707 del relator Ministro Luiz Fux con reconocimiento de

[8] Constitución Brasileña: Art. 102. *Compete ao Supremo Tribunal Federal, precipuamente, a guarda da Constituição, cabendo-lhe: (...)* § 3º No recurso extraordinário o recorrente deverá demonstrar a repercussão geral das questões constitucionais discutidas no caso, nos termos da lei, a fim de que o Tribunal examine a admissão do recurso, somente podendo recusá-lo pela manifestação de dois terços de seus membros. Código Processual Civil: *Art. 543-A. O Supremo Tribunal Federal, em decisão irrecorrível, não conhecerá do recurso extraordinário, quando a questão constitucional nele versada não oferecer repercussão geral, nos termos deste artigo. § 1º Para efeito da repercussão geral, será considerada a existência, ou não, de questões relevantes do ponto de vista econômico, político, social ou jurídico, que ultrapassem os interesses subjetivos da causa.*

repercusión general (sirve para todos los demás órganos judiciales con las mismas acciones de falta de acceso a informaciones tributarias) creó la siguiente tesis[9]: El *hábeas data* es la garantía constitucional adecuada

[9] STF - www.stf.jus.br: *Ementa: DIREITO CONSTITUCIONAL. DIREITO TRIBUTÁRIO. Hábeas DATA. ARTIGO 5º, LXXII, CRFB/88. LEI Nº 9.507/97. ACESSO ÀS INFORMAÇÕES CONSTANTES DE SISTEMAS INFORMATIZADOS DE CONTROLE DE PAGAMENTOS DE TRIBUTOS. SISTEMA DE CONTA CORRENTE DA SECRETARIA DA RECEITA FEDERAL DO BRASIL-SINCOR. DIREITO SUBJETIVO DO CONTRIBUINTE. RECURSO A QUE SE DÁ PROVIMENTO. 1. O hábeas data, posto instrumento de tutela de direitos fundamentais, encerra amplo espectro, rejeitando-se visão reducionista da garantia constitucional inaugurada pela carta pós-positivista de 1988. 2. A tese fixada na presente repercussão geral é a seguinte: "O Hábeas Data é garantia constitucional adequada para a obtenção dos dados concernentes ao pagamento de tributos do próprio contribuinte constantes dos sistemas informatizados de apoio à arrecadação dos órgãos da administração fazendária dos entes estatais." 3. O Sistema de Conta Corrente da Secretaria da Receita Federal do Brasil, conhecido também como SINCOR, registra os dados de apoio à arrecadação federal ao armazenar os débitos e créditos tributários existentes acerca dos contribuintes. 4. O caráter público de todo registro ou banco de dados contendo informações que sejam ou que possam ser transmitidas a terceiros ou que não sejam de uso privativo do órgão ou entidade produtora ou depositária das informações é inequívoco (art. 1º, Lei nº 9.507/97). 5. O registro de dados deve ser entendido em seu sentido mais amplo, abrangendo tudo que diga respeito ao interessado, seja de modo direto ou indireto. (…) Registro de dados deve ser entendido em seu sentido mais amplo, abrangendo tudo que diga respeito ao interessado, seja de modo direto ou indireto, causando-lhe dano ao seu direito de privacidade.(...) in José Joaquim Gomes Canotilho, Gilmar Ferreira Mendes, Ingo Wolfgang Sarlet e Lenio Luiz Streck. Comentários à Constituição. Editora Saraiva,* 1ª Edição, 2013, p.487. 6. A *legitimatio ad causam para interpretação de Hábeas Data estende-se às pessoas físicas e jurídicas, nacionais e estrangeiras, porquanto garantia constitucional aos direitos individuais ou coletivas. 7. Aos contribuintes foi assegurado constitucionalmente o direito de conhecer as informações que lhes digam respeito em bancos de dados públicos ou de caráter público, em razão da necessidade de preservar o status de seu nome, planejamento empresarial, estratégia de investimento e, em especial, a recuperação de tributos pagos indevidamente, verbis: Art. 5º. …LXXII. Conceder-se-á hábeas data para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público, considerado como um writ, uma garantia, um remédio constitucional à disposição dos cidadãos para que possam implementar direitos subjetivos que estão sendo obstaculados. 8. As informações fiscais conexas ao próprio contribuinte, se forem sigilosas, não importa em que grau, devem ser protegidas da sociedade em geral, segundo os termos da lei ou da constituição, mas não de quem a elas se referem, por força da consagração do direito à informação do artículo 5º, inciso XXXIII, da Carta Magna, que traz como única ressalva o sigilo imprescindível à segurança da sociedade e do Estado, o que não se aplica no caso sub examine, verbis: Art. 5º.… XXXIII - todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade,*

para la obtención, por el propio contribuyente, de los datos que involucran el pago de tributos del sistema de apoyo de recaudación de los órganos de la administración de la hacienda de los entes estatales.

Con esa tesis del STF, tenemos seguridad jurídica que el contribuyente tendrá acceso a los datos propios amplios solicitados a todos los entes estatales de control fiscal, es decir, las entidades gubernamentales deben ser entendidas como entes públicos o personas jurídicas de derecho privado que administran datos públicos (hacen las veces del Estado). Por lo tanto, las entidades gubernamentales que administran las informaciones fiscales son las de la administración directa e indirecta, o sea, todas las instituciones públicas y personas jurídicas privadas que prestan el trabajo de interés público de registro o sistema de datos, sea permanente o temporario, que es de interés del contribuyente.

En materia tributaria, es común que el fisco reciba un determinado pago, pero no vincule el pago a un débito específico y en esas ocasiones puede tener lugar una falta de regularidad fiscal y, como consecuencia, que el contribuyente no pueda participar de licitaciones por ausencia de presentación de documentos obligatorios. Asimismo, existen situaciones que el débito, mismo con el pago en mora, consta pendiente en los datos del fisco *ad eternum,* así como situaciones de pagos en cuotas del tributo o de extinción del crédito tributario por caducidad o prescripción del crédito tributario. Estos últimos casos,

---

ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado. 9. In casu, o recorrente requereu à Secretaria da Receita Federal do Brasil os extratos atinentes às anotações constantes do Sistema de Conta-Corrente de Pessoa Jurídica-SINCOR, o Sistema Conta-Corrente de Pessoa Jurídica-CONTACORPJ, como de quaisquer dos sistemas informatizados de apoio à arrecadação federal, no que tange aos pagamentos de tributos federais, informações que não estão acobertadas pelo sigilo legal ou constitucional, posto que requerida pelo próprio contribuinte, sobre dados próprios. 10. Ex positis, DOU PROVIMENTO ao recurso extraordinário. (RE 673707, Relator(a): LUIZ FUX, Tribunal Pleno, julgado em 17/06/2015, ACÓRDÃO ELETRÔNICO REPERCUSSÁO GERAL - MÉRITO DJe-195 DIVULG 29-09-2015 PUBLIC 30-09-2015)

sabemos que pueden ocurrir de manera substancial ante la actual crisis de la COVID-19 que imposibilitó a muchas empresas mantener la regularidad fiscal y si el fisco no avanza con una moratoria, o un incentivo de pagos, estos débitos no serán pagados y pueden ser alcanzados por caducidad (extinción por la falta de anotación del crédito tributario en 5 años) o prescripción (extinción por la falta de actos constrictivos del patrimonio del deudor por el plazo de 5 años).

El *hábeas data,* así, es el remedio constitucional para tener un amplio acceso a las informaciones tributarias administradas por los entes vinculados al fisco, ante el supuesto de falta de análisis de la solicitud del contribuyente por el transcurso del plazo (10 o 15 días, dependiendo del pedido) u omisión del análisis en contra del contribuyente.

De otra manera, es importante resaltar que el STF también se manifestó en otra oportunidad sobre el amplio acceso a las informaciones al momento de la apreciación de la acción directa de inconstitucionalidad N.º 4.815 de la relatora, Ministra Cármen Lúcia, cuando el Tribunal dictó una decisión que relaciona la información al derecho de libertad y como tal no puede ser censurada, es decir, es un derecho fundamental que involucra el acceso, búsqueda, recibimiento, y exposición general de datos del interesado.

No podemos olvidar, que uno de los principios basilares de la administración pública es el principio de publicidad, o sea, principio de carácter fundamental que normativiza los actos de las personas que tratan la cosa pública y, como tal, todo lo que pasa en los entes gubernamentales, debe tener la mayor transparencia posible, principalmente cuando tratamos el derecho de los administrados.

5. Conclusión

El *hábeas data*, después de pasar por dictaduras y actos de déspotas del siglo anterior, continúa siendo un instrumento o remedio de efectividad de derechos constitucionales fundamentales en pleno siglo

XXI. Es verdad que vamos en camino al proceso digital, al fácil acceso a las informaciones de manera simple y transparente. No obstante, aunque tengamos herramientas nuevas con la ayuda de *big datas* e *internet,* el control de informaciones es realizado por personas que controlan las máquinas. Como tal, el acceso irrestricto de informaciones es fundamental para una democracia, e instrumentos que viabilicen tal acceso son fundamentales.

El *hábeas data,* diferentemente de lo que algunos doctrinarios sustentaban en el siglo anterior, nunca, a nuestro sentir, va a caer en desuso. Por el contrario, con el registro y bancos de datos controlados por entes y "robos" es fundamental una acción constitucional que permita el amplio acceso a las informaciones.

El derecho a la privacidad está siempre caracterizado como un derecho fundamental, y, como tal, necesita de protección especial y amplio control por el propio interesado. No es razonable pensar en un mundo que está interconectado, interdependiente y globalizado donde los datos son almacenados por los entes gubernamentales y la persona no tiene un amplio acceso a la información.

Actualmente, tenemos varios bloques que comparten informaciones como el Mercosur en Sudamérica y la Unión Europea en Europa y sin dudas necesitamos pensar en un *hábeas data* del futuro, es decir, que va proteger derechos fundamentales de las personas a nivel mundial para facilitar el libre acceso a las informaciones.

En Brasil, datos del Instituto Brasileño de Planeamiento y Tributación (IBPT) demuestran que los contribuyentes comprometen sus propios recursos financieros en el 41,47% con pagos de tributos. Además, las empresas gastan 1.958 horas anuales para mantener sistemas burocráticos del fisco (*Receita Federal*), lo que llamamos "custo Brasil", es decir, un país muy costoso para producir porque la exigencia del fisco con obligaciones accesorias es extravagante. Mismo con estos controles de datos, el fisco de Brasil se niega, en algunas ocasiones, a suministrar

datos detallados del propio contribuyente, lo que es ofensivo a la Constitución que garantiza el acceso irrestricto a las informaciones.

Con esas consideraciones y analizando este caso específico de restricción del fisco de Brasil a suministrar los datos del propio contribuyente, no tenemos dudas que en tiempos actuales y futuros, el *hábeas data* continuará resguardando derechos fundamentales, siendo un instrumento procesal que garantiza el amplio acceso a datos tributarios como pagos, compensaciones, caducidad, prescripción y otras informaciones de la situación de regularidad fiscal del contribuyente.

Por último, el derecho fundamental de la privacidad debe ser sopesado en situaciones que involucran un estado democrático de derecho que tiene como uno de los principios fundamentales de la administración pública el principio de la publicidad. No dejemos que los robos controlen y confisquen datos de los humanos. A través de remedios constitucionales que garantizan derechos fundamentales pensemos igual que Heródoto: "*Pensar en el pasado para comprender el presente e idealizar el futuro".*

Bibliografía

- Aristóteles, "De Anima", 2ª ed., trad. Alberto Llanos, Buenos Aires: Leviatán, 2008.
- Barbarosch, Eduardo, *"Teoría de la Justicia y la Metaética Contemporánea"*, 1ª ed., Buenos Aires: La Ley – Facultad de Derecho, UBA, 2007.
- Barroso, Luís Roberto, "*A dignidade da pessoa humana no direito constitucional: a construção de um conceito jurídico à luz da jurisprudência mundial*". Trad. Humberto Laport de Mello. 2ª reimp., Belo Horizonte: Editora Fórum, 2013.

  _____, "*Interpretação e Aplicação da Constituição*", 7ª ed. rev., São Paulo: Saraiva, 2009.

- Bidart Campos, Germán José, *"La Corte Suprema: El tribunal de las garantías constitucionales"*, colaboración de Pablo Luis Manili, 1ª ed., Buenos Aires: Ediar, 2010.

  _____, "*Manual de la Constitución Reformada*", Tomos I, II, III, 6ª reimp., Buenos Aires, Ediar, 2009.

- Cammarosano, Márcio *"O princípio constitucional da moralidade e o exercício da função administrativa"*, Belo Horizonte: Fórum, 2006.

- Cícero, "*Dos Deveres",* Trad. Alex Marins, 2ª reimp, São Paulo: Editora Martin Claret, 2011.

- Gordillo, Agustín. *"Tratado de Derecho Administrativo"*, Tomo I. 8ª ed., Buenos Aires: Fundación de Derecho Administrativo, 2003.

- Jose Joaquim Gomes Canotilho, Gilmar Ferreira Mendes, Ingo Wolfgang Sarlet e Lenio Luiz Streck. *"Comentários à Constituição"*, São Paulo, Editora Saraiva, 1ª Edição, 2013.

- Mendes, Gilmar Ferreira,"*Curso de Direito Constitucional",* 7ª ed., rev. e atual. São Paulo: Editora Saraiva, 2012.

  _____, "*Direitos Fundamentais e Controle de Constitucionalidade: estudos de direito constitucional",* 3ª ed., rev. e amplia. São Paulo: Editora Saraiva, 2004.

- Muscari, Marco Antonio Botto, *"Súmula Vinculante",* São Paulo: Editora Juarez de Oliveira,1999.

- Ratc, Artur Ricardo, *"Precatórios: A Compensação de Tributos Federais com o Advento da Lei 12.431/2011*", Revista Tributária e de Finanças Públicas, Ano 19, Vol. 100, Set-Out/2011, São Paulo: Editora Revista dos Tribunais.

_____, *"Saídas tributárias para enfrentar o coronavírus"*, site migalhas.com.br

- Reale, Miguel, "*Teoria Tridimensional do Direito"*, 5ª ed., São Paulo: Saraiva, 1994.
- Sandel, Michael J., *"Justiça: O que é fazer a coisa certa"*, trad. Heloisa Matias e Maria Alice Máximo, 10ª. ed., Rio de Janeiro: Civilização Brasileira, 2013.
- Sola, Juan Vicente, "*La Corte Suprema de Justicia*. El nuevo proceso constitucional", 1ª ed. Ciudad Autónoma de Buenos Aires: La Ley. 2015.

Otras fuentes:

- Sitio - Supremo Tribunal Federal: www.stf.jus.br
- Sitio - Corte Suprema de Justicia de la Nación: www.csjn.gov.ar
- Sitio - Suprema Corte Estados Unidos: www.supreme.justia.com
- Sitio - Migalhas: www.migalhas.com.br
- Sitio - Presidência da República: www2.planalto.gov.br
- Sitio - Organización Mundial de la Salud: www.oms.org
- Constitución de Brasil
- Constitución del España
- Constitución de Perú
- Constitución de Portugal

ORÍGENES Y EVOLUCIÓN DEL PROCESO DE *HÁBEAS DATA*

✍ Milushka Carrasco Gallardo*

La garantía constitucional recaída sobre el *hábeas data* es concebida como el mecanismo especializado de protección de los datos de la persona que "procede contra el hecho u omisión, por parte de cualquier autoridad, funcionario o persona, que vulnera o amenaza [de manera cierta e inminente] los derechos a los que se refiere el Artículo 2°, incisos 5 y 6 de la Constitución"[1]: acceso a la información pública y autodeterminación informativa, respectivamente.

Aunque esta definición contenida en nuestra Constitución resulte poco novedosa, el proceso evolutivo sobre el que recae este mecanismo de garantía constitucional sí que lo es. Y es precisamente sobre dicho proceso sobre el que recae el objeto del presente artículo. Aquí, por tanto, se apreciarán las disquisiciones en torno a los orígenes del *hábeas data* y su evolución tanto en sede constitucional como legislativa.

Con este propósito, en el plano constitucional se reseñan a las constituciones más recientes y a la vez más emblemáticas, por ejemplo, a las constituciones de España (1978) y Brasil (1988); y en el plano legislativo, a las leyes de Alemania (1970), Suecia (1973), Austria (1978) y España (1992).

* Abogada por la Universidad Femenina del Sagrado Corazón. Asesora de Despacho en el Tribunal Constitucional.

[1] Artículo 200, inciso 3, de la Constitución.

Como no podía ser de otra manera, se hace también una breve descripción de los antecedentes del *hábeas data* en el Perú. Su constitucionalización en el año 1993 y su posterior regulación en el Código Procesal Constitucional de 2004 y en la Ley de Protección de Datos Personales y su Reglamento.

1. Un panorama general: orígenes históricos

El primer antecedente constitucional latinoamericano que se tiene del proceso de *hábeas data*, y del cual tomó la figura el Constituyente peruano, lo encontramos en el Derecho brasilero, específicamente en su Constitución de 1988, en donde se incorporó por vez primera una disposición que regulaba este proceso con una denominación y características similares a los aquí adoptados (artículo 5, numeral LXXII), bajo los siguientes términos:

> "(…) se concede el hábeas data:
>
> a. Para asegurar el conocimiento de informaciones relativas a la persona del solicitante contenidas en registros o bancos de datos, de entidades gubernamentales o de carácter público;
>
> b. Para la rectificación de datos, cuando no se prefiera hacerlo por procedimiento secreto de carácter judicial o administrativo".

Al respecto, resulta válido señalar que aún cuando el Constituyente peruano no consideró esta legislación al momento de incorporar el *hábeas data* en nuestro ordenamiento jurídico, cabe indicar que la Constitución colombiana de 1991 incorporó en su artículo 15 el siguiente texto (aún cuando este era tutelado en aquel entonces por la acción de tutela o proceso de amparo):

> "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 tiene 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 correspondencia y demás formas de comunicación privada son inviolables. Solo pueden ser interceptadas o registradas mediante orden judicial, en los casos y con las formalidades que establezca la ley.
>
> Para efectos tributarios o judiciales y para los casos de inspección, vigilancia e intervención del Estado podrá exigirse la presentación de libros de contabilidad y demás documentos privados en los términos que señale la ley".

Por su parte, la Constitución paraguaya de 1992 ya también regulaba esta garantía constitucional en su Capítulo XII, artículo 135, bajo el siguiente tenor:

> "Toda persona puede acceder a la información y a los datos que sobre sí misma, o sobre sus bienes, obren en registros oficiales o privados de carácter público, así como conocer el uso que se haga de los mismos y de su finalidad. Podrá solicitar ante el magistrado competente la actualización, rectificación o la destrucción de aquellos, si fuesen erróneos o afectaran ilegítimamente sus derechos".

No obstante lo anterior, resulta conveniente señalar que la Asamblea General de las Naciones Unidas proclamó la Declaración Universal de los Derechos Humanos (1948), introduciendo, en su artículo 12, el primer antecedente histórico/normativo *hábeas data*:

> "Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o as su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques".

Dos años después, la Asamblea Parlamentaria del Consejo de Europa aprobó el Convenio Europeo para la Protección de los Derechos

Humanos y de las Libertades Fundamentales, en cuyo artículo 8 se reconoce el derecho a la vida privada y familiar. En ese mismo sentido, se expresa el artículo 17, numeral 1, del Pacto Internacional de Derechos Civiles y Políticos, adoptado por la Asamblea General de las Naciones Unidas, en Nueva York, el 16 de diciembre de 1966.

Esta universalización de protección de derechos humanos tuvo repercusión en las normas europeas, que son precursoras en la materia y de las que, finalmente, adoptamos sus notas esenciales casi en su integridad.

En las legislaciones europeas este proceso tuvo acogida en distintas legislaciones desde el año 1960, fecha a partir de la cual el avance tecnológico abrió paso con fuerza a una serie de vulneraciones de la intimidad personal debido al mal uso de la información personal contenida en bancos de datos automatizados.

En Alemania, por ejemplo, el desarrollo del *hábeas data* estuvo vinculado con el derecho a controlar la información de índole personal –o lo que sería el derecho a la protección de datos personales–, que tiene sus orígenes en 1919 con la Constitución de Weimar, que otorgó a los funcionarios públicos la facultad de examinar su expediente personal. Es recién en enero de 1970 cuando el *Land de Hesse* aprueba la primera ley federal (vigente solo en el *Land*) para la protección contra el abuso de datos sobre las personas, *Datenschutz*, con motivo del tratamiento informático que se le daba a estos. La peculiaridad de esta norma está en que se basaba de manera exclusiva en la disposición constitucional, fundamentada en el *allgemeines Persönlichkeisrecht* contemplado en los artículos 1 y 2 de su Constitución. Posteriormente, en 1977, el Parlamento Federal alemán aprobó la Ley Federal *Bundesdatenschutzgesetz*, que establecía como su objetivo la protección de los datos personales de cualquier posible abuso en su almacenamiento, transmisión, modificación y destrucción. Esta ley excluyó de su ámbito de aplicación aquellos datos que se traten por empresas, incluyendo las vinculadas a algún tipo de medio de comunicación, siempre y cuando adopte las medidas

técnicas y organizativas necesarias. Aquí se consideró datos personales a aquellos que se vinculan a las circunstancias personales y objetivas de personas naturales y no jurídicas.

La norma alemana reconocía a los interesados los derechos a recibir información sobre los datos almacenados sobre ellos, a la corrección de los datos almacenados si son inexactos, a la inaccesibilidad de los datos almacenados cuando no se puede determinar si son exactos o no, o si es que hubiesen desaparecido los presupuestos que generaron el almacenamiento, a la destrucción de los datos almacenados si es que el almacenamiento fue ilícito, la obligación del secreto por quienes almacenen modifiquen, destruyan o transmitan la información, entre otros derechos.

En la misma década otros países europeos también empezaron a regular la protección de datos personales. Así, Suecia expidió la *Data Lag* en 1973 –primera norma de alcance nacional– que creó un registro público específico que estaba obligado a registrar todos los datos personales públicos o privados.

Por su parte, Francia siguió la misma línea en enero de 1978, con la dación de la *Loi relative à l'informatique, aux fichiers et aux libertés*, que creó una Comisión Nacional de Informática y Libertades que contaba con facultades reglamentarias de regulación y protección de la información personal. Esta ley tuvo una fuerte influencia de la ley sueca y se inspiró en algunas directrices incorporadas en la legislación alemana y en el *Privacy Act* estadounidense, y consideró como uno de sus principios rectores que la informática debe estar al servicio del ciudadano y de su desarrollo, por lo que no podrá atentar contra ella.

Uno de los principales aspectos que aborda esta norma fue la prohibición de actuar sobre datos sensibles sin previa autorización de su titular; igualmente, se previó la posibilidad de solicitar ante la referida Comisión la información personal pública o sensible, así como la de impugnarla en caso se incurriera en errores. Igualmente, se contempla

que ninguna decisión judicial, administrativa o privada que implique alguna apreciación de la conducta de las personas podrá fundarse en operaciones automatizadas que exploten ficheros o bases de datos que contengan información que permita realizar un perfil de estas. Un aporte interesante de esta ley está vinculado no solo con la protección de la vida privada de los titulares de la información, sino también con posibles actos de discriminación, pues se prohíbe la conservación de información relacionada, directa o indirectamente, con el origen racial, las opiniones públicas, filosóficas o religiosas, o incluso su filiación sindical, entre otros aspectos.

Dinamarca reguló el tema mediante su *Public and Private Authorities Registers Act* en junio de 1978. Dicha norma regulaba en dos apartados distintos los registros del sector público y los del sector privado. En agosto del mismo año, Austria introdujo la *Federal Data Act*, norma que concedió el derecho a la protección de datos tanto de las personas naturales como de las jurídicas, frente a registros públicos y privados. También creó una Comisión de Protección de Datos con facultades administrativas y judiciales.

Por su parte, Inglaterra emitió la *Data Protection Act* en julio de 1984; mientras que Portugal ya regulaba a nivel constitucional el derecho a la autodeterminación informativa. Igualmente, a nivel reglamentario en la Ley 10/91 de la protección de datos personales frente a la informática. Esta legislación creó una Comisión Nacional de Protección de Datos Personales Informatizados, creada como una autoridad encargada de la adecuada aplicación de la normativa mencionada.

Como no podía ser de otra manera, España no fue ajena a esta ola regulatoria, pues también garantizó a nivel constitucional (artículo 18.4) la tutela de la información personal y familiar, limitando por la ley el uso de la informática. Y en octubre de 1992 vio la luz la Ley Orgánica de Regulación del Tratamiento Automatizado de Datos, en donde se estableció medidas para cautelar posibles violaciones al derecho a la privacidad que estuviesen vinculadas a información personal. En esta

norma también se creó una entidad encargada de la aplicación de esta normativa: la Agencia de Protección de Datos.

En la legislación norteamericana, la de Estados Unidos resulta ilustrativa. Las primeras ideas del derecho a la privacidad provienen de la definición hecha por Brandeis y Warren en 1891 en su famoso trabajo *The right of privacy* publicado en Harvard Law Review. En dicho país existe una tradición de protección del derecho a la privacidad (*right of privacy*) que data de 1966 con la *Freedom Information Act (FOIA)*. Esta norma consagra el principio de publicidad de la información –el derecho a saber– contenida en los documentos públicos, es decir, que todos los ciudadanos sin excepción tienen la posibilidad de acceder a dicha información. Asimismo, esta ley dispuso la publicidad de cuatro categorías de actos administrativos en el *Federal Register*: (i) La descripción del organigrama de entes, lugares y oficinas en los cuales el interesado solicite información; (ii) las funciones, modos y métodos de actividad de las agencias, (iii) las normas expedidas por delegación del Parlamento y las enmiendas; y (iv) otras formas de publicación de los actos que permiten a los ciudadanos conocer las decisiones de las agencias, así como sus normas administrativas.

Algunos años después, en 1970, se aprobó la *Fair Reporting Act*, cuya finalidad era tutelar a los clientes de entidades financieras de posibles violaciones a su privacidad por instituciones encargadas de brindar esta información. Cuatro años más tarde, en 1974, se expidió la *Privacy Act* norma cuya finalidad era tutelar los derechos de personas físicas cuyos nombres están registrados en la base de datos del gobierno federal, de este modo las entidades gubernamentales solo podrán solicitar aquella información de los registros públicos que esté directamente vinculada con los fines para los cuales estas han sido creadas. Adicionalmente, las dependencias gubernamentales deberán obtener la información directamente de sus titulares quienes deberán prestar su consentimiento para la difusión de sus datos personales; y finalmente, tienen, además, la obligación de mantenerla actualizada y de conceder al titular el derecho de acceder a esta información.

Me parece interesante destacar dos criterios que la *Privacy Act* tomó en cuenta al referirse a la recolección de información: (i) el nexo que debe existir entre el tipo de información y la finalidad de la agencia; y el (ii) está referido al contenido de la información, pues se prohibió la recolección de información personal de los ciudadanos. No obstante, esta norma también tenía algunas falencias entre las que cuenta que no se haya previsto que las agencias informen acerca de la identidad que no se haya previsto que las agencias informen acerca de la identidad de terceros que hayan brindado información sobre los administrados; ni la de aquellos que hayan solicitado esta información a la agencia respectiva.

Una vez desarrollados los orígenes históricos del *hábeas data* en el mundo, a través de los principales textos que consagraron este proceso, y que sirvieron de antecedentes de nuestra legislación, pasaremos a analizar el proceso evolutivo del *hábeas data* a nivel constitucional y legal en la legislación interna.

2. El *hábeas data* en el Perú: evolución constitucional

El primer antecedente constitucional que se tiene en el Perú de la tutela de derechos constitucionales –entre los que se cuenta alguno garantizado actualmente por el *hábeas data*– es el *hábeas corpus*. En efecto, este era el proceso encargado por excelencia de garantizar todos los derechos constitucionales. Más adelante se diferenció entre el "*hábeas corpus* penal" (dirigido a la defensa de la libertad personal) y el "*hábeas corpus* civil" (dirigido a la tutela de los demás derechos fundamentales); hasta que con la entrada en vigencia de la Constitución de 1979 el último de estos se convierte en lo que hoy conocemos como el proceso de amparo.

Ahora bien, a nivel constitucional el proceso de *hábeas data* fue recogido por primera vez en la Constitución Política de 1993 (artículo 200, numeral 3). Para nadie es un secreto que la introducción de esta garantía constitucional generó gran polémica en la doctrina nacional. Las críticas a su incorporación se sustentaban básicamente en

la pertinencia de contar con un proceso autónomo dirigido a tutelar derechos que bien podrían ser garantizados a través del proceso de amparo.

Y es que si bien el *hábeas data* es un proceso pensado para tutelar los derechos fundamentales lesionados por un uso extralimitado del poder informático, entonces, en puridad, estaríamos frente a afectaciones de los derechos a la intimidad, el honor, la buena reputación y/o la imagen.

Siendo así, ¿acaso su adecuada protección no estaría en manos del proceso de amparo? ¿Es el *hábeas data* un mecanismo procesal eficaz para lograr la tutela de estos derechos? Múltiples han sido las respuestas a estas preguntas.

Por un lado, algunos autores nacionales son detractores de esta institución pues consideran que "resultaba innecesaria su incorporación en la nueva Constitución pues para proteger este derecho bastaba con regular adecuadamente al proceso de amparo"[2], pues "importa una pieza del Derecho Procesal Constitucional configurativa de un amparo especializado, con finalidades específicas"[3]; mientras que otros la han defendido advirtiendo que "[hoy] día el manejo de la información, máxime si esta se encuentra en bancos de datos informatizados, va progresivamente consolidándose como la fuente de acumulación de poder económico y político a nivel mundial. Y lamentablemente, como suele ocurrir con toda fuente de poder que no esté sometida a controles eficientes, la inexistencia de mecanismos específicos y expeditivos al respecto puede originar una impune comisión de abusos, con el consiguiente resquebrajamiento de las pautas de convivencia pacífica

[2] ABAD YUPANQUI, Samuel. "Hábeas data y conflicto entre órganos constitucionales: dos nuevos procesos constitucionales". En: AA.VV. *La Constitución de 1993. Análisis y comentarios*. Comisión Andina de Juristas, Lima, 1994, p. 268.

[3] SAGUES, Néstor Pedro. "Amparo informativo". En: *La Ley. Revista argentina*. Argentina, 1991, p. 1035.

que deben caracterizar a todo Estado de Derecho. El carecer de un mecanismo destinado específicamente a la protección de aquel derecho que unos llaman 'autodeterminación informativa' y otros 'libertad informática' pareciera ser algo manifiestamente inconveniente, pues dicha carencia solamente acentuaría una situación de indefensión ciudadana frente a una cada vez más dinámica e incontrolable concentración de poder, circunstancia sumamente nociva para la subsistencia de cualquier Estado Democrático"[4].

Por su parte, el profesor Castillo Córdova, quien se ha mostrado favorable a la existencia del *hábeas data* como un proceso autónomo, esboza algunas razones interesantes para sustentar su posición. Así, considera que la principal diferencia entre el proceso de amparo y el *hábeas data*, y que permite escoger cuál de los dos resulta eficaz en la tutela de los derechos mencionados, es el tipo de acto agresor. Si bien en ambos casos se garantizan los mismos derechos, en el caso del *hábeas data* los actos lesivos provienen de un especialísimo ámbito de cosas: la técnica informática (computarizada o no); y "[e]n la medida que las agresiones del derecho constitucional son de una naturaleza tal que las singulariza y diferencia del resto de agresiones, y en la medida que esa singularidad tiene entidad propia al estar referida a un ámbito de la técnica que requiere especialización, es que queda justificada la entidad propia y consecuentemente [la] autonomía del hábeas dará como garantía constitucional"[5].

La propuesta de regulación constitucional fue presentada por el congresista Carlos Torres y Torres Lara quien, como se señaló anteriormente, tomó como referencia la legislación brasilera, encargándole

[4] ESPINOSA-SALDAÑA BARRERA, Eloy. "El hábeas data en el Derecho Comparado y el Perú, y algunas notas sobre su real viabilidad y la pertinencia en nuestro país". En: *Jurisdicción constitucional, impartición de justicia y debido proceso*. Ara, Lima, 2003, pp. 331 y 332.

[5] CASTILLO CÓRDOVA, Luis. "Proceso de hábeas data". En AA.VV. *La Constitución Comentada. Análisis artículo por artículo*. Tomo II. Gaceta Jurídica, Lima, 2006, p. 1087.

la protección de tres derechos fundamentales: a) Solicitar y obtener información de entidades públicas (artículo 2, numeral 5); b) Que los servicios informáticos, sean públicos o privados, no suministren información que afecte la intimidad personal y familiar (artículo 2, numeral 6); y c) Al honor y a la buena reputación, a la intimidad personal y familiar, a la voz y a la imagen propias, y a la rectificación (artículo 2, numeral 7).

Con posterioridad a esta inicial regulación, en el año 1995 se produjo una reforma constitucional mediante la Ley N.° 26470 del 12 de junio, que eliminó del ámbito de protección de este proceso al derecho a la rectificación de afirmaciones inexactas o agraviantes difundidas por los medios de comunicación social regulado en el numeral 7 del artículo 2 de la Norma Fundamental. Ocurriría lo propio en aquellos casos en los cuales se lesione los derechos al honor, la buena reputación, la intimidad, la voz e imagen propias por medios de comunicación social. Y, como es de público conocimiento, a partir de esta reforma constitucional, estos derechos pasaron a ser tutelados por el amparo.

Por su parte, en julio de 2002, la Comisión de Constitución presentó al Congreso de la República el Proyecto de Reforma Constitucional parcial, texto que fue aprobado parcialmente, y que introdujo diversas modificaciones. Entre ellas está comprendida el artículo 57 que señala que el *hábeas data* para tutelar el derecho de acceso a la información pública y el derecho a la autodeterminación informativa (frente a aquella información contenida en bancos de datos, registros informáticos, teniendo la facultad de acceder a ella, cancelarla o corregirla si es que existiese datos inexactos o indebidamente procesados, así como decidir sobre su transmisión).

En esa línea, el Proyecto de Reforma Constitucional también corrige el problema que plantea el numeral 6 del artículo 2 de la Constitución respecto al derecho a la autodeterminación informativa, aún cuando en su literalidad continúa circunscribiéndose al derecho a la intimidad a pesar de tratarse de un derecho autónomo.

3. El *hábeas data* en el Perú: evolución legislativa

El primer desarrollo a nivel legal del *hábeas data* se plasmó en la Ley N.° 26301 del 3 de mayo de 1994. Esta norma de desarrollo constitucional contenía una serie de precisiones y pautas procesales que permitían ejercer adecuadamente este derecho, entre las que se hallaban cuál era el órgano competente para su conocimiento, la regulación de la denominada vía previa en estos casos en estos casos (el requerimiento por conducto notarial), entre otros aspectos de orden procesal.

Tras la necesidad advertida por el Constituyente de sistematizar en un solo cuerpo normativo la regulación de todos los procesos constitucionales. En diciembre de 2004 entró en vigencia el Código Procesal Constitucional, norma que reemplazó a la Ley N.° 26470, en donde se reguló de manera integral todos los procesos constitucionales. Siendo así, el proceso de *hábeas data* fue regulado de manera específica en su Título IV (artículos 61 al 65). Asimismo, el Código establece pautas generales aplicables a todos los procesos de tutela de derechos fundamentales en el Título I (artículos 1 al 24), por lo que le son aplicables al *hábeas data* también.

No obstante, la práctica ha puesto al juez constitucional frente a situaciones no reguladas por el legislador, evidenciando la insuficiencia de la regulación del Código. Así, han quedado desfasados muchos aspectos a los cuales los órganos jurisdiccionales, en especial el Tribunal Constitucional, han debido darle respuesta jurisprudencialmente.

Sin perjuicio de ello, y con una fecha un tanto más reciente, encontramos dos normas, que son normas de desarrollo constitucional, que tratan con detenimiento los derechos tutelados por esta garantía constitucional.

Nos referimos, en primer lugar, al Texto Único Ordenado de la Ley N.° 27806, Ley de Transparencia y Acceso a la Información Pública, Decreto Supremo N.° 043-2003-PCM, publicada en el diario Oficial

el Peruano el 22 de abril de 2003; así como a su Reglamento, con el objeto de promover la transparencia de los actos del Estado y regular el derecho fundamental del acceso a la información pública consagrado en el numeral 5 del artículo 2 de la Constitución; y en segundo lugar, a la Ley de Protección de Datos Personales, Ley N.° 29733, publicada en el diario oficial *el Peruano* el 3 de julio de 2011 y su Reglamento, con el objeto de garantizar el derecho fundamental a la protección de los datos personales, previsto en el artículo 2 numeral 6 de la Constitución, a través de su adecuado tratamiento, en un marco de respeto de los demás derechos fundamentales que en ella se reconocen.

4. Reflexiones finales

Primera reflexión: el primer antecedente constitucional latinoamericano que se tiene del proceso de *hábeas data*, y del cual tomó la figura el Constituyente peruano, lo encontramos en el Derecho brasilero, específicamente en su Constitución de 1988.

Segunda reflexión: el primer antecedente histórico y normativo del *hábeas data* fue consagrado en el artículo 12 de la Declaración Universal de los Derechos Humanos. Esta universalización de protección de derechos humanos tuvo repercusión en las normas europeas, que son precursoras en la materia y de las que, finalmente, adoptamos sus notas esenciales casi en su integridad.

Tercera reflexión: a nivel constitucional el proceso de *hábeas data* fue recogido por primera vez en la Constitución Política de 1993 (artículo 200, numeral 3).

Cuarta reflexión: En diciembre de 2004 entró en vigencia el Código Procesal Constitucional en donde se reguló de manera integral todos los procesos constitucionales. Siendo así, el proceso de *hábeas data* fue regulado de manera específica en su Título IV (artículos 61 al 65). No obstante, la práctica ha puesto al juez constitucional frente a situaciones no reguladas por el legislador, evidenciando la insuficiencia

de la regulación del Código. Así, han quedado desfasados muchos aspectos a los cuales los órganos jurisdiccionales, en especial el Tribunal Constitucional, han debido darle respuesta jurisprudencialmente.

Quinta reflexión: Sin perjuicio de ello, y con una fecha un tanto más reciente, encontramos dos normas, que son normas de desarrollo constitucional: el Texto Único Ordenado de la Ley N.° 27806, Ley de Transparencia y Acceso a la Información Pública; y la Ley de Protección de Datos Personales, ambos con sus respectivos reglamentos.

EL AMBITO DE PROTECCIÓN DEL PROCESO CONSTITUCIONAL DE HÁBEAS DATA

Reflexiones sobre los derechos cuya tutela se le encomienda

✍ Luis R. Sáenz Dávalos*

1. Consideraciones preliminares

Con el nacimiento de la Constitución Peruana de 1993, aparecieron varios derechos nuevos, algunos de los cuales no sólo no habían sido reconocidos en la Constitución precedente de 1979, sino en general, carecían de todo tipo de antecedente por lo menos en lo que respecta a nuestro constitucionalismo histórico o tradicional.

Entre esos nuevos derechos, dos de ellos nos merecen especial atención, no sólo por la indudable importancia que poseen, sino porque el propio constituyente optó por conferirles una protección especializada, al habilitar el proceso constitucional de hábeas data para dicho objetivo. Estamos hablando en concreto del derecho de acceso a la información pública y del derecho a la autodeterminación informativa.

---

* Director de Publicaciones y Documentación en el Centro de Estudios Constitucionales del Tribunal Constitucional. Profesor de los cursos de Derecho Constitucional y Derecho Procesal Constitucional en la Academia de la Magistratura. Secretario de la Asociación Peruana de Derecho Constitucional.

Interrogarse sobre los alcances de ambos derechos y porque se les otorga una protección procesal atípica es lo que motiva estas breves líneas, en las que evidentemente no se pretende realizar una explicación extensa o detallada, sino dejar sentadas algunas pautas sobre los lineamientos generales que, a partir de lo dispuesto en la Constitución Política de nuestro país, caracterizarían su contenido esencial, dejando en claro que varios de estos aspectos han venido siendo abordados por la jurisprudencia constitucional e incluso, por sendas normas de desarrollo, mientras que otros aún se encuentran pendientes de serlo, lo que en buena cuenta representa todo un reto para los operadores jurídicos.

También se pretende explicar las razones por las que se habría optado por establecer una vía procesal especial, a contrario de aquellas voces que en su momento consideraron, que ello no era rigurosamente necesario, tras existir como en efecto ocurría, la correspondiente al amparo constitucional.

Finalmente y aunque con una perspectiva relativamente distinta, se intentara evaluar los motivos que en su momento justificaron el que se sustrajeran ciertos derechos del ámbito de protección del proceso de hábeas data.

Veamos a renglón seguido cada uno de estos extremos.

2. El derecho de acceso a la información pública

Una de las maneras de fortalecer el Estado Democrático de Derecho, en los tiempos modernos, reside sin duda en garantizar los diversos niveles de participación ciudadana.

A fin de hacer ello posible, no debe entenderse que la referida participación, solo radica en habilitar las vertientes políticas ofrecidas por los procesos electorales y su periódica concretización, sino que existen otras maneras de asegurar el concurso de las personas en el correcto y democrático manejo del Estado.

En este contexto, se acepta pacíficamente que un adecuado instrumento promotor de la intervención ciudadana, se materializa en tanto y en cuanto se le permite fiscalizar lo que hace el Estado y para hacerlo, nada mejor que facilitarle el acceso a todo tipo de información que por una u otra razón se encuentre bajo su esfera de dominio.

De esta forma, el ideal de una democracia semidirecta[1], que permite al pueblo delegar su poder pero sin renunciar a específicos ámbitos de interacción permanente, encuentra una de sus expresiones en el derecho de acceso a la información pública.

De acuerdo con lo señalado por el artículo 2, inciso 5 de la Constitución Política del Perú queda meridianamente establecido que:

> *Toda persona tiene derecho:*
>
> *(…)*
>
> *A solicitar sin expresión de causa la información que requiera y a recibirla de cualquier entidad pública, en el plazo legal, con el costo que suponga el pedido. Se exceptúan informaciones que afectan la intimidad personal y las que expresamente se excluyan por ley o por razones de seguridad nacional.*
>
> *El secreto bancario y la reserva tributaria pueden levantarse a pedido del juez, del Fiscal de la Nación o de una Comisión investigadora del Congreso con arreglo a ley y siempre que se refieran al caso investigado.*

[1] Desde el punto de vista de la forma como participa el pueblo, cabe recordar que existen tres tipos de democracia; la directa o pura, donde el pueblo toma por sí mismo sus decisiones y que si bien se dio en el pasado (Esparta y Atenas así lo demuestran) hoy es prácticamente imposible materializarla debido al crecimiento y masificación de las sociedades; la indirecta o representativa, donde el pueblo delega su soberanía sin sujetar al gobernante a mandato imperativo alguno y la semidirecta o semirepresentativa, donde el pueblo delega el poder pero se reserva específicos ámbitos de control o fiscalización sobre el gobernante a través de mecanismos de participación. Sobre el tema: Quispe Correa, Alfredo.- *Derecho Constitucional e Instituciones Políticas*; Gráfica Yovera S.A.; Lima 2004; Págs. 62 y ss.

Lo primero que al respecto corresponde aclarar es que lo que la Constitución denomina derecho de acceso a la información pública, no es igual al tradicional y mucho más antiguo derecho a la información (artículo 2 inciso 4). Este último es el atributo por el cual toda persona puede conocer o dar a conocer a través de la existencia de medios de comunicación o de quienes hagan sus veces[2], todo tipo de suceso noticioso, sin que para tal efecto se requiera de autorización previa y sin que se justifique eventuales comportamientos de censura o impedimento alguno, dentro de las responsabilidades de ley.

Distinto es lo que se denomina como acceso a la información pública, que en rigor se nos presenta como un derecho que recae sobre cualquier persona[3] o ciudadano y que le permite obtener toda información que, independientemente de su trascendencia o no, se encuentre en poder del Estado en cualquiera de sus dependencias o reparticiones y que por principio sea de exclusivo interés o preocupación de quien la solicita.

Conforme lo señalado por la Constitución, existen algunas notas esenciales que caracterizan dicho atributo. Por un lado su no motivación y su autofinanciamiento, ambas de carácter material y que recaen sobre el directo titular del derecho. A las mismas se agrega otra de carácter más bien instrumental concerniente con el plazo y cuya concretización depende del directamente obligado, es decir, del Estado.

---

[2] La idea de medios de comunicación hoy en día trasciende lo tradicional y abarca el amplio circuito del mundo virtual y en particular de las redes sociales, lo que implica que la información y la forma como esta se transmite desborda lo que en su momento pudo entender el legislador.

[3] Cabe advertir que la jurisprudencia constitucional ha señalado desde muy temprano que el acceso a la información pública no sólo es un derecho que recae sobre el ciudadano o persona natural, sino que también puede ser ejercitado por las personas jurídicas. Cfr. Al respecto revisar los fundamentos 2 y 3 de la sentencia recaída en el Exp. N° 0644-2004-HD/TC, Caso: Inmobiliaria las Lomas de Monterrico S.A., publicada con fecha 11.11.2005.

Sobre lo primero está claro que quien peticiona la información no requiere justificar las razones de su solicitud. Esta, en otras palabras, resulta de su entera discreción o libertad, pero también de su reserva, no justificándose ningún tipo de condicionamiento a partir de argumentos sustentados en el interés o relevancia que la información invocada pueda representar para el solicitante. Simplemente se pide y correlato de dicha petición, se entrega obligatoriamente por parte del Estado o de sus dependencias, la información requerida.

Sobre lo segundo, se deja establecido que con independencia de la trascendencia que reviste el citado atributo, el mismo resulta de interés fundamentalmente para su titular, por lo que es éste quien se encuentra obligado a sufragar el monto que suponga el pedido. De esta forma, la inversión que pueda implicar el soporte en el que la información deba ser proporcionada, debe correr a cargo del directo interesado. El Estado, si bien tiene la obligación de dispensar la información, no puede verse afectado por lo que implica una petición cuyo solvento o sufragio no pudo en concreto prever. La única obligación individualizable para el Estado, será la exigir un monto plenamente compatible con los estándares del mercado, lo que como es obvio deslegitimará cualquier intento de imponer sumas por encima de lo objetivamente razonable.

En cuanto al tercer elemento que también se contempla se pone de manifiesto que quien se encuentra obligado a entregar la información, debe hacerlo en el plazo que la ley disponga, lo que evidentemente estará muy asociado al tipo y cantidad al igual que al soporte en el que la misma habrá de ser dispensada[4]. En este contexto y de acuerdo con la

[4] En cuanto al tipo o características de la información, la jurisprudencia ha hecho hincapié en que la misma no debe adolecer de determinados defectos, como los de ser dispensada en forma fragmentaria, desactualizada, incompleta, imprecisa, falsa, no oportuna o errada. Cfr. Al respecto lo señalado en el fundamento 16 de la ejecutoria recaída en el Exp. N° 1797-2002-HD/TC, Caso: Wilo Rodriguez Gutierrez, publicada con fecha 30.09.2003.

previsión contenida en el artículo 62 del Código Procesal Constitucional, se deja establecido que el periodo legal que se ha convenido como razonable a los efectos de entregar la información no debe exceder de los 10 días hábiles contabilizados desde el momento de formulada la solicitud respectiva.

Siendo importante el derecho de acceso a la información pública, tampoco es un derecho con características absolutas. La propia Constitución se ha encargado de establecer determinadas variantes de limitación, de las cuales dos pueden considerarse taxativas mientras que la otra de alcances más bien genéricos, aunque no por ello indeterminados.

Las limitaciones que pueden considerarse taxativas se encuentran asociadas a los supuestos en los que la información requerida pueda generar incidencias o afectar determinados bienes de relevancia como lo son la intimidad personal y la seguridad o defensa nacional.

Si bien ambos supuestos restrictivos, tiene base perfectamente razonable, debe especificarse que ello no significa ni debe interpretarse como que a nombre de cualquiera de los mismos se pretenda involucrar informaciones que no tengan relación o vínculo directo con lo que es materia de la limitación. Dicho en otras palabras, que por intimidad personal o seguridad y defensa nacional pueda entenderse lo que cualquier entidad pública o repartición del Estado pueda discrecionalmente considerar.

Desde tal perspectiva, será a todas luces cuestionable que por intimidad se asuma, no el tradicional concepto de lo estrictamente concerniente a la vida personal, afectiva o sexual, sino lo que se le antoje por capricho al Estado, como podría ser por ejemplo, lo concerniente con las conductas o comportamiento de interés más bien general. Lo mismo se sigue en el caso de la seguridad y defensa nacional, pues aunque existen datos o informaciones que efectivamente tienen que ver o son parte integrante de lo que por estrategia de defensa o seguridad deben mantenerse en reserva, hay otros que escapan por completo o

simplemente nada tienen que ver con dicho bien jurídico[5]. Y mal se haría con apelar a los membretes establecidos para so pretexto de los mismos desnaturalizar la verdadera razón de dichas limitaciones[6].

La restricción de naturaleza genérica, de acuerdo con el mandato constitucional, se encuentra reconducida a lo que el legislador disponga, lo cual si bien se entiende como perfectamente legítimo en un modelo donde se habilita la opción de desarrollos en aquello que no haya podido prever el constituyente, no significa tampoco que por tal motivo el legislador ordinario pueda aprovecharse de su capacidad normativa para sustraer del escenario de la información pública, datos que en lugar de garantizar la facultad fiscalizadora del ciudadano tiendan a fomentar el denominado secretismo estatal[7].

En el contexto de esta tercera variante de limitación, está claro que justificadamente puede incluirse al secreto bancario y a la reserva tributaria, los mismos que se encuentran muy asociados al concepto privacidad (los aspectos propios de la vida laboral, profesional, etc.).

[5] El Tribunal Constitucional ha dejado en claro que *"…el solo hecho de que una norma o un acto administrativo… atribuya o reconozca la condición de seguridad nacional a una información determinada, no es razón suficiente, en términos constitucionales, para denegar el acceso a la misma; por el contrario, es siempre indispensable examinar si la información calificada de reservada reviste realmente o no tal carácter, acudiendo para tal efecto al principio constitucional de razonabilidad".* Cfr. Fundamento 6, de la sentencia recaída en el Exp. N° 0950-2000-HD/TC, Caso: Asociación de Pensionistas de la Fuerza Armada y Policía Nacional, publicada con fecha 10.09.2001.

[6] Coincidimos con Alfredo Quispe Correa en la conveniencia de reglamentar adecuadamente la norma constitucional en este extremo *"…para determinar que casos se consideran propios de la intimidad personal o de la seguridad nacional, no vaya a ser que la persona obligada a dar la información la invoque como pretexto sin fundamentar su negativa. O apele a una respuesta trivial para bloquear la información".* Cfr. Las Garantías Constitucionales; Gráfica Horizonte S.A.; Lima 2003; Págs. 93-94.

[7] En igual sentido: Quispe Correa, Alfredo.- *Las Garantías Constitucionales*; Págs. 94-95. A lo que habría agregar, como lo advierte autorizada doctrina, que esta excepción representa un típico supuesto de reserva legal, que no autoriza que sea el Poder ejecutivo, a través de su facultad normativa, quien incorpore los supuestos de limitación. Cfr. Borea Odria, Alberto.- *Evolución de las Garantías Constitucionales;* Editorial Fe de Erratas; Segunda Edición Actualizada; Lima 2000; Pág. 454.

Podrían eventualmente, aventurarse otro tipo de espacios, pero siempre que con los mismos se auspiciara lo eminentemente individual.

Ahora bien, un tema poco explorado pero que es conveniente ponerlo de manifiesto, es el relativo al eventual y atípico escenario de la relatividad implícita en las propias reglas e incluso en las excepciones. Por estas últimas, entendemos aquellos supuestos, en los que a pesar de auspiciarse la garantía de bienes como los que a título de reglas o de limitaciones aquí se ha mencionado, puedan sin embargo habilitarse legítimas restricciones no previstas en específicos escenarios de conflicto de derechos o de bienes jurídicos de relevancia.

Tales hipótesis se producirían, por ejemplo, si tratándose de las reglas a las que ya nos hemos referido, se auspiciara sin ningún tipo de ponderación, que una persona carente de medios económicos, tuviese que sufragar un alto costo respecto de información pública previamente solicitada. O también podría suceder en el caso de las limitaciones, si a pesar de encontrarnos frente a informaciones que incidan sobre la intimidad o seguridad y defensa nacional, existieran bienes constitucionales que justificaran relativizar las premisas constitucionales establecidas. En el primer supuesto y por excepción debidamente respaldada, podría optarse, por un solvento excepcional desde el propio Estado, en el segundo supuesto, evidentemente mucho más opinable, podría legitimarse la entrega de información que aún a sabiendas de encontrarse protegida, fuese indispensable para garantizar determinados bienes constitucionales, forzando la regla de la no motivación por una directamente alentadora de lo contrario[8].

[8] Nuestra jurisprudencia constitucional, ha contemplado tal posibilidad como se desprende del fundamento 8 de la sentencia recaída en el Exp. N° 1133-2012-PHD/TC donde señala que *"…aunque los presupuestos del acceso a la información pública que aquí se indican son normas de alcance general estos podrían atenuarse en casos de naturaleza especial. Es lo que sucedería, por ejemplo… si la entrega de información afectase otros bienes constitucionales (incluso las típicas excepciones referidas a la intimidad, a la defensa nacional u otros casos exceptuados por ley) y donde la única forma de ponderar el conflicto sería conociendo la razón de la petición formulada. Es también… lo que acontecería si quien requiere*

Ahora bien, aunque las consideraciones explicadas en torno del citado atributo fundamental, se desprenden específicamente de la Constitución del Estado en sus lineamientos generales, sería oportuno contrastar lo señalado con la ley encargada de regularlo, esto es, con Ley N° 27806 o Ley de transparencia y Acceso a la Información Pública, debiendo precisarle al respecto que aunque dicha norma, en sus aspectos esenciales regula de manera bastante adecuada su ejercicio, cualquier eventual oposición entre dicha norma y lo señalado por la Carta Fundamental e incluso por lo desarrollado por la propia jurisprudencia, debe ser resuelto con miras a la mejor eficacia de los objetivos constitucionales, a lo que cabe establecer, concordante con una correcta teoría de la interpretación que toda norma (y dentro de ellas evidentemente las de desarrollo) se interpretan de conformidad con lo previsto en la Constitución, no al revés como a veces y de manera equivocada, parece entenderse.

El derecho de acceso a la información pública, en suma, se nos aparece pues con una fisonomía muy especial pero también plantea retos importantes en cuanto a su desarrollo. Con el mismo se busca consolidar de manera plena el Estado Democrático y romper la llamada cultura del secreto, lamentablemente tan arraigada en realidades como la nuestra[9].

3. El derecho a la autodeterminacion informativa

Con independencia de lo que algunos estudiosos suelen opinar sobre la autodeterminación informativa, vinculándolo decididamente con una suerte de protección reforzada de la intimidad personal, el citado atributo fundamental, además de ser un derecho también novedoso,

---

información, en principio necesaria de costear, careciera de capacidad económica suficiente para cumplir con dicho requisito. En este último supuesto, no cabe duda de que el juez constitucional se encontrara en la necesidad de distinguir y por supuesto decidir, caso por caso". Cfr. Caso: Jesús Barboza Cruz. Sentencia publicada con fecha 11.09.2012.

[9] Cfr. Al Respecto el Informe Defensorial N° 60; *El acceso a la Información pública y la cultura del secreto;* Serie Informes Defensoriales; Defensoría del Pueblo; Lima 2001.

involucra un contenido mucho más amplio que dicha noción. Técnicamente hablando es el derecho que tiene toda persona de disponer de los propios datos que le conciernen o pertenecen, se encuentren o no vinculados a su intimidad y cuya posesión o almacenamiento se verifique en poder de terceros, sea que estos últimos resulten sujetos públicos sea que se trate de sujetos privados.

En la sociedad moderna absolutamente informatizada y en la que los datos y referencias de cada persona han pasado a ser un asunto divulgable a gran escala, la información ha terminado por convertirse en un producto de espectro difuso, donde nadie sabe a ciencia cierta que tanto de lo que le pertenece o ha contribuido a generar a partir de su propia existencia se encuentra en poder de terceros. Comprobarlo es tan sencillo, como abrir un buscador en internet y colocar el dato personal más elemental como es el nombre. A renglón seguido saldrá consignada tal cantidad de información que el directo interesado ni siquiera y en sus más amplias expectativas de hallazgo, podía intuir que existía.

El problema en todo caso, no es que la información individual pueda existir y que eventualmente se encuentre esparcida a escala ecuménica, sino que la misma pueda eventualmente perjudicar. Es allí donde cobra importancia el derecho del que venimos hablando.

De acuerdo con lo previsto en el artículo 2 inciso 6) de la Constitución Política de 1993, se ha establecido que:

> *Toda persona tiene derecho:*
>
> *(…)*
>
> *A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar*.

Aunque la primera impresión que se podría aventurar, ciertamente sería la de que los datos que puedan circular, se encuentren vinculados a la esfera íntima, no parece ser ese el camino seguido ni

por la ley que prima facie regula dicho atributo, ni tampoco por la jurisprudencia.

En efecto, el Código Procesal Constitucional, que a estos efectos debe ser entendido como una norma integrante del bloque de constitucionalidad, establece en su artículo 61, inciso 2, que el derecho al cual protege el hábeas data, cuando se trata del mandato constitucional reconocido en el artículo 2, inciso 6 ya glosados, es un atributo que permite:

> *Conocer, actualizar, incluir y suprimir o rectificar la información o datos referidos a su persona que se encuentren almacenados o registrados en forma manual, mecánica o informática, en archivos, bancos de datos o registros de entidades públicas o de instituciones privadas que brinden servicio o acceso a terceros. Asimismo, a hacer suprimir o impedir que se suministren datos o informaciones de carácter sensible o privado que afecten derechos constitucionales*.

Si efectuamos un simple y elemental cotejo entre lo proclamado por la Constitución y lo reconocido por el Código Procesal Constitucional, por referencia al derecho a la autodeterminación informativa, saltan a la vista diversas y muy notorias diferencias.

La primera de las mencionadas diferencias radica en que la información o datos almacenados o registrados tienen que ver con todo aquello referido a una persona, no únicamente con lo estrictamente íntimo. Con lo cual y como ya lo habíamos adelantado, no es este un derecho que sólo se refiera, como lo dijimos en otro momento a las situaciones propias de la vida personal, sexual o afectiva, sino a todo lo que le pertenece a un individuo en su condición de tal[10].

[10] Carlos Mesía Ramírez indica que *"No se trata solo de controlar la difusión o uso de los datos que pueden afectar la intimidad personal, familiar o la imagen personal, sino también se hace necesario proteger los datos personalizados; es decir, aquellos sobre los cuales una persona ejerce un derecho de propiedad reservada, por cuanto está dentro de su posesión personal"*; Cfr. *Derechos de la persona. Dogmática Constitucional*; Fondo Editorial del Congreso de la República; Lima 2004; Pág. 129.

Incluso el párrafo que permite la supresión o impedimento de los llamados datos sensibles (que tienen que ver con la esfera de lo íntimo) se ve complementado por lo privado que como también lo hemos adelantado, es un concepto similar (aunque no exactamente igual) a lo rigurosamente íntimo[11]. Añadiéndose a ello, que todo lo que pueda afectar derechos constitucionales (en plural) da lugar a un reclamo por la infracción o desconocimiento de tal derecho.

En una perspectiva más clara, lo que ha hecho el Código es posicionar a la autodeterminación informativa en lo que representa su real esencia, la de ser un atributo de disposición de todos los datos que le conciernen a una persona en cuanto fuente de origen o generación de los mismos.

Desde tal óptica y siendo el individuo quien produjo los datos, se explica perfectamente que pueda este decidir lo que finalmente ocurra con los mismos y por consiguiente disponer, cuando de alguna manera se sienta afectado. Con tal propósito, el Código Procesal Constitucional brinda un repertorio bastante amplio de opciones que van desde conocer los datos que existen almacenados sobre su persona, hasta decidir la situación en la que se encuentran, para lo cual puede actualizarlos, incluir aspectos que no tengan, suprimir aquellos que lo perjudiquen, rectificar lo que no se ajuste a la verdad o incluso solicitar su prohibición o libre circulación, cuando evidentemente y de alguna manera le generen consecuencias no favorables[12].

[11] Es curioso que en nuestro medio no se hayan realizado mayores esfuerzos por delimitar o distinguir los conceptos de intimidad y privacidad que aunque entendemos son muy similares, apuntan hacía ámbitos materiales diferenciados. La propia jurisprudencia de nuestro Tribunal Constitucional ha sido más bien algo imprecisa sobre dicha temática, pues suele utilizarlos frecuentemente como figuras equivalentes. Una excepción a la regla, en todo caso, se aprecia en los fundamentos 37, 38 y 39 de la ejecutoria recaída en el Exp. N° 6712-2005-HC/TC. Caso: Magaly Medina Vela y Ney Guerrero Orellana, publicada con fecha 20.01.2006.

[12] El tema de las consecuencias no favorables puede ser sujeto a cierta discusión a partir de la frase que utiliza el Código en torno a los archivos, banco de datos o registros

Por otra parte y acorde con señalado desde la propia Constitución, la autodeterminación informativa podrá tener como destinatario a todo tipo de registro, sea que este le pertenezca al Estado o sea que se encuentre en manos de privados y procederá cualquiera que sea la variante o modalidad en la que hayan resultado almacenados los datos de tipo personal, independientemente de que la misma sea meramente manual, sofisticadamente mecánica, o tecnológicamente virtual.

Al igual como lo sostuvimos en relación al derecho de acceso a la información pública, en el caso de la autodeterminación informativa, también existe una norma de desarrollo detallado que es en concreto la Ley N° 29733 o Ley de Protección de Datos Personales. La citada norma, si bien en sus lineamientos esenciales efectúa un adecuado tratamiento del referido atributo fundamental, la misma exige ser interpretada de conformidad con la Constitución y con lo desarrollado por vía de la jurisprudencia constitucional.

Por último debe considerarse que aunque la Constitución ni el Código Procesal Constitucional hayan desarrollado un esquema taxativo o expreso de límites a considerar sobre dicho derecho fundamental, ello no supone que no puedan existir o deducirse los mismos a partir de una interpretación sistemática y concordante con otros bienes constitucionales. Por lo demás a ello apunta lo dispuesto en el artículo 13,

---

"que brinden servicio a terceros"; Cfr. Sáenz Dávalos, Luis.- "Panorama general de los procesos constitucionales y su ámbito de protección en el Código Procesal Constitucional"; en: Sáenz Dávalos, Luis & Meléndez Sáenz, Jorge.- *El ámbito de protección de los procesos constitucionales y el Hábeas Corpus*; Cuadernos de Trabajo N° 1; Centro de Estudios Constitucionales. Tribunal Constitucional; Lima 2004; Pág. 24. En nuestra opinión, pueden haber casos en los que sin otorgarse ese servicio al que se refiere la norma podría estar afectándose la autodeterminación personal. Es lo que sucedería si datos sensibles de una persona pudiesen estar siendo colectados por cualquier persona aprovechando la vulneración a espacios propiamente íntimos o también privados que por diversas razones no desea su titular que sean conocidos por nadie. Naturalmente, acreditar este supuesto requeriría de prueba sólidamente construida. Cfr. Borea Odría, Alberto.- *Evolución de las Garantías Constitucionales*; Pág. 457.

inciso 13.2 de la antes citada Ley de Protección de Datos Personales[13], debiendo en todo caso precisarse que no siempre es la ley la que puede definir las eventuales restricciones cuando estas bien pueden ser individualizadas dentro de un típico escenario de conflicto a nivel casuístico y donde el juzgador debe decidir en clave constitucional exista o no fuente legal de directa referencia.

Prueba de lo dicho es por lo demás, lo establecido en el artículo 27 de la misma norma reguladora de este derecho que de manera enfática y dejando abierto un amplio espectro interpretativo, reconoce que:

> *Los titulares y encargados de los bancos de datos personales de administración pública pueden denegar el ejercicio de los derechos de acceso, supresión y oposición por razones fundadas en la protección de derechos e intereses de terceros o cuando ello pueda obstaculizar actuaciones judiciales o administrativas en curso vinculadas a la investigación sobre el cumplimiento de obligaciones tributarias o previsionales, a las investigaciones penales sobre la comisión de faltas o delitos, al desarrollo de funciones de control de la salud y del medio ambiente, a la verificación de infracciones administrativas, o cuando así lo disponga la ley.*

Si evidentemente la autoridad administrativa ostenta capacidades de merituación sobre este tipo de contextos, con mayor razón, el juez constitucional en su tarea de salvaguarda o preservación de la totalidad de bienes reconocidos por la norma fundamental, puede arribar, caso por caso a similar conclusión, debiendo volverse a reiterar que un escenario de tal naturaleza será la ley la que se interpretara de conformidad con la norma fundamental, descartándose a su vez que sea esa misma ley la que pueda colocarse en todos los supuestos de hipotéticos conflictos.

[13] De acuerdo con la citada previsión *"Las limitaciones al ejercicio del derecho fundamental a la protección de datos personales solo pueden ser establecidas por ley, respetando su contenido esencial y estar justificadas en razón del respeto de otros derechos fundamentales o bienes constitucionalmente protegidos".*

4. Porque el hábeas data y no el amparo

Cuando se aprobó la Constitución de 1993, no falto quienes consideraron que la irrupción en el escenario de un proceso como el hábeas data resultaba injustificada habida cuenta que derechos como el acceso a la información pública y la autodeterminación informativa bien podrían haber sido objeto de protección mediante el amparo ordinario[14].

Se decía por entonces, que si todos los derechos especiales dieran lugar a procesos atípicos, correríamos el riesgo de llenarnos de vías adicionales en sede constitucional y no es esa una lógica muy recomendable a seguir, cuando se cuenta, como en efecto se contaba, con un amparo con finalidades harto tutelares[15].

Sin embargo, la idea de que estos derechos demandaban un trámite rápido de reclamo preliminar a nivel administrativo, no necesariamente igual al que se presenta respecto de otros derechos fundamentales puede que haya influido en la necesidad de reconocer una protección especial en sede constitucional que sin ser exactamente igual a la del hábeas corpus o al propio amparo, resulte compatible con la naturaleza y características de los atributos involucrados.

En todo caso el factor determinante a la hora de optarse por el citado instrumento, puede que haya resultado a la postre su por entonces notoria expansión a nivel del derecho comparado[16] y su paulatino y cada vez más evidente desarrollo jurisprudencial. Y si a eso se añade la

[14] Esta posición fue asumida por algún sector importante de nuestra doctrina. Cfr. Abad Yupanqui, Samuel.- Hábeas Data y conflicto entre órganos constitucionales: Dos nuevos procesos constitucionales; *Lecturas sobre Temas Constitucionales;* N° 10; Comisión Andina de Juristas; Lima 1994; Págs. 268-270.

[15] Cabe recordar que por aquella época nuestro modelo de amparo era más bien alternativo u opcional y no precisamente como lo empezó a ser años después y tras la vigencia del Código Procesal Constitucional, esto es subsidiario o residual.

[16] Cfr. Abad Yupanqui, Samuel.- Hábeas Data y conflicto entre órganos constitucionales…"; *Lecturas sobre Temas Constitucionales*; Pág. 267.- Eguiguren Praeli, Francisco.-

necesidad de perfeccionar una protección de unos derechos particularmente especialísimos a la par que vitales para hacer frente al crecimiento desmesurado del poder informático[17], se comprenderá el porqué, a la larga, el instituto fue terminando por ser aceptado.

Desde entonces la figura encontró receptividad aunque no sin estar exenta, por lo menos en sus orígenes, de ciertas polémicas sobre la manera como se le reconocía o los alcances con los que se le configuraba.

5. El abandono de un ambito de proteccion mas expansivo

Aunque el reconocimiento del hábeas data como mecanismo de protección específica de los derechos de acceso a la información pública y de autodeterminación informativa, es lo que hoy en día aparece con nitidez de nuestro ordenamiento constitucional, conviene recordar que en sus orígenes las cosas fueron algo diferentes, pues junto con tales atributos, el constituyente también reconoció a las libertades personalísimas (honor, buena reputación, intimidad e imagen) así como al derecho de rectificación como susceptibles de protección mediante la citada vía especial.

Esta toma de posición, inicialmente adoptada, origino sin embargo severas críticas provenientes de algunos sectores que entendieron que tal opción anticipaba un peligroso escenario principalmente en relación con los medios de prensa[18], en una época en la que como se sabe,

"El Hábeas Data y su desarrollo en el Perú"; *Derecho. Revista de la Facultad de Derecho de la Pontificia Universidad Católica del Perú*; N° 51; Lima, diciembre de 1997; Págs. 293-296.

[17] Apunta Luis Castillo Córdova que *"…la decisión del constituyente peruano de prever un mecanismo procesal constitucional distinto para cuando se trate de proteger derechos constitucionales por agresiones provenientes del poder informático, tiene justificación plena. Ha sido una decisión con sustento debido a la especialidad que significa el campo en el que está destinada la garantía a actuar".- Cfr. Comentarios al Código Procesal Constitucional*; Tomo II; Segunda edición, corregida y aumentada; Lima 2006; Pág. 983.

[18] Cfr. García Belaunde, Domingo.- "Garantías Constitucionales en la Constitución Peruana de 1993"; *Lecturas sobre Temas Constitucionales*; N° 10; Comisión Andina de Juristas; Lima 1994; Págs. 259-260.

existían notorias y quien sabe si justificadas dudas sobre las intenciones de un gobierno nacido de un escenario no del todo democrático. Basta con recordar al respecto el polémico origen de la Constitución de 1993 y su nunca del todo comprobada necesidad de instauración[19].

El hecho es que desde diversos ámbitos especializados se argumentó que el dotar al hábeas data de unos alcances tan excesivamente amplios bien podría repercutir negativamente o ser mal utilizado, lo que dio lugar a que no bien puesta en vigor la Constitución de 1993, se produjera prácticamente de inmediato una reforma constitucional a través de la Ley N° 26470, suprimiendo parte del artículo 200 inciso 3 cuyo texto originalmente contemplaba que el hábeas data también podía ser utilizado para recabar tutela de los derechos reconocidos en el inciso 7 del artículo 2 de la Carta.

Consecuencia de tal proceder fueron sustraídos del ámbito de protección del hábeas data una buena cantidad de derechos, naturalmente no en la lógica de dejarlos carentes de tutela efectiva en sede constitucional, sino reconduciendo está última hacía el específico escenario del amparo.

Probablemente este suceso tenga una explicación, más que en razones jurídicas, en el contexto político que por entonces se vivía y que alertaba de ciertos riesgos de adoptarse en ese momento dicho temperamento. Hoy en día sin embargo y visto en perspectiva, no necesariamente creemos que argumentos como los entonces utilizados puedan ser del todo exactos para todas las épocas o en todos los momentos. Naturalmente, siempre cabe la opción de considerar que la discusión de libertades como las informativas y el propio derecho de rectificación debe darse en una vía procesal un poco mas abierta como la correspondiente al amparo, pero de ello no se sigue necesariamente que sea tan polémico implementar un hábeas data como aquel que se proyectó

[19] Cfr. García Belaunde, Domingo & Planas Silva, Pedro.- *La Constitución Traicionada. Páginas de historia reciente*; Seglusa Editores; Lima 1993.

en sus orígenes. Ya tuvimos alguna vez un hábeas corpus abiertamente genérico[20] y nadie que sepamos se escandalizo por dicha realidad, sino que la acepto como parte del pasivo de una época en la que aún no se contaba con un mecanismo que permitiera la tutela de derechos distintos a la libertad individual.

En todo caso, nuestro legislador opto por lo que a su parecer resultaba más razonable, vista la manera como el hábeas data venía siendo incorporado en el resto de modelos constitucionales y sobre todo tomando en cuenta que lo que se procura cuando del hábeas data se trata es a la larga la protección adecuada de los datos. Siendo las cosas de este modo, el hábeas data tiene pues unos roles más específicos o concretos y es hacía los mismos que se ha encaminado el desarrollo jurisprudencial de los últimos años.

En la lógica descrita y con independencia de las decisiones que en su momento haya tomado el constituyente, somos de la idea que si el hábeas data existe con el perfil que hoy en día le hemos otorgado, es pues porque su proceso de maduración, de menos a más, nos fue encaminando en dicha dirección.

6. A manera de conclusión

La legitimidad de un proceso como el hábeas data, definitivamente responde a la naturaleza de los derechos a cuya protección se encuentra encaminado.

Tales derechos, no son simples novedades teóricas, sino resultado directo de los cambios y transformaciones en la sociedad moderna decididamente trastocada como resultado de la tecnología y su impacto en el manejo de la información y de los datos personales.

[20] Nos referimos naturalmente al hábeas corpus de la Constitución de 1933 y al desarrollo que por entonces se le otorgó. Un inventario del mismo lo encontramos en García Belaunde, Domingo.- *El Hábeas Corpus en el Perú*; Universidad Nacional Mayor de San Marcos; Lima 1979.

Bajo circunstancias como las descritas y así como su tratamiento tutelar debe resultar lo más depurado y efectivo posible, con igual intensidad se imponen desarrollos adecuados respecto de los alcances y límites que caracterizan tanto al derecho de acceso a la información pública como al derecho a la autodeterminación informativa.

Si bien la Constitución dio un buen paso desde el momento inicial de su reconocimiento, estamos convencidos que los mejores aportes han de esperarse tanto desde el ámbito de la jurisprudencia como desde el que corresponde a las leyes de desarrollo. Sin una adecuada comprensión de las finalidades a las que apuntan ambos derechos su importancia quedaría seriamente mermada a la par que comprometida.

Es obligación de los operadores jurídicos y por supuesto de los legisladores evitar que ello suceda.

De acuerdo a lo observado hasta la fecha y sin ser excesivamente triunfalistas, estamos convencidos que andamos por buen camino.

EL HÁBEAS DATA EN EL PERÚ

Derechos protegidos, alcances y límites a la luz de la jurisprudencia constitucional

✍ Leny Palma Encalada*

1. Preliminares

En principio cabe anotar que el proceso constitucional de hábeas data surge como reacción al denominado "poder informático", el cual viene ganado cada vez mayor posicionamiento mundial a consecuencia de la constante evolución tecnológica e informática y, en mérito al cual se puede tener la capacidad de "influir" en decisiones políticas, económicas, sociales y en cualquier aspecto donde tenga efectos el manejo del contenido de la información almacenada en registros o bancos de datos.

El hábeas data encuentra sus orígenes de regulación en el derecho norteamericano con la promulgación de la Freedom of Information Act (libertad de información) de 1966 y la Privacy Act (ley de privacidad) de 1974 así como en el derecho británico con la Data Protecction Act (Ley de Protección de Datos) de 1984. A partir de estas regulaciones, poco a poco se fueron sumando más países en la incorporación de

* Abogada con estudios concluidos de maestrías en Derecho Constitucional y en Gestión Pública. Post Título en Derecho Procesal Constitucional y estudios de especialización en Derecho Administrativo y Derecho Parlamentario. Miembro de la Asociación Peruana de Derecho Constitucional.

normas, por un lado, de protección del derecho a la privacidad y, por otro, de acceso a la información pública.

A nivel de nuestro ordenamiento nacional, el hábeas data ha ido buscando su propio espacio y posicionándose con carácter autónomo como un proceso de garantía constitucional, lo cual se alcanzó con la dación de la Constitución Política del Perú de 1993.

En sus inicios, se cuestionó la naturaleza del hábeas data como proceso constitucional autónomo, generándose a nivel doctrinario diversos debates y posiciones al respecto. Un sector defiende la tesis de que los derechos tutelados por el hábeas data deberían pasar al ámbito de protección del amparo, justificado tal razonamiento en el hecho de que este proceso no resulta siendo otra cosa que un amparo especializado y que sus instituciones cumplen funciones similares a las de dicho proceso constitucional; contrario sensu, otro sector justifica la pertinencia del hábeas data en las finalidades específicas que le corresponden a este proceso, el cual evidentemente protege al individuo ante el inmenso y potencial riesgo en la vulneración de sus derechos a raíz del mal uso del llamado "poder informático" o ante la denominada "cultura del secreto" en las entidades públicas.

Han transcurrido más de dos décadas desde la regulación constitucional del hábeas data y lo que podemos advertir es que la corriente orientada a su regulación autónoma es la que ha ido ganando más espacio, lo cual se traduce con la dación de leyes de desarrollo constitucional como son la Nº 28237 – Código Procesal Constitucional, N° 27806 - Ley de Transparencia y Acceso a la Información Pública y N° 29733 – Ley de Protección de Datos Personales.

Compartiendo, el criterio adoptado tendiente a reforzar la autonomía del hábeas data, podemos afirmar que la diferencia sustancial con el amparo radica en el origen de la afectación de los derechos, en mérito al cual, serán derechos protegidos por el proceso de hábeas data, todos aquellos que, inclusive siendo susceptibles de protección por el amparo, tengan como origen de afectación una base de datos o registro informático.

Anotada dichas premisas, a continuación, desarrollaremos el contenido, alcances y límites de los derechos que protege el proceso constitucional de hábeas data a la luz de los criterios jurisprudenciales que ha ido estableciendo el Tribunal Constitucional y de los precedentes vinculantes del Tribunal de Transparencia y de Acceso a la Información Pública, así como los retos y desafíos que viene enfrentando en el devenir de los años; para lo cual, partiremos de un estudio que sobre la materia realizamos en el año 2005[1].

2. Derechos protegidos

El ámbito de protección constitucional del hábeas data se encuentra regulado en el artículo 200° inciso 3) de la Constitución Política de 1993, del cual se deprende que los derechos que se tutela con este proceso son concretamente los relativos al derecho de acceso a la información pública y al derecho a la autodeterminación informativa, los cuales se encuentran detallados en los numerales 5 y 6 del artículo 2 de la Carta Magna.

Cabe recordar que, la redacción original del referido artículo 200° inciso 3) de la Constitución, incluía como derechos susceptibles de protección por el hábeas data los reconocidos en el numeral 7 del citado artículo 2° del Texto Constitucional[2]; sin embargo, frente a los cuestionamientos que se dieron en torno a que pondría en peligro básicamente la libertad de expresión, se excluyó del ámbito de protección del hábeas data los derechos al honor, buena reputación, intimidad personal y familiar y el derecho de rectificación, los mismos que luego de la dación de

---

1 En la Revista Derecho & Cambio Social. Número 05 - Año II - 2005.

2 "Artículo 2°. Toda persona tiene derecho:
(…)
7. Al honor y a la buena reputación, a la intimidad personal y familiar así como a la voz y a la imagen propias. Toda persona afectada por afirmaciones inexactas o agraviada en cualquier medio de comunicación social tiene derecho a que éste se rectifique en forma gratuita, inmediata y proporcional, sin perjuicio de las responsabilidades de ley.
(…)".

la ley de reforma constitucional N° 26470[3], pasaron a formar parte de la enumeración de derechos que tutela el proceso de amparo.

Al respecto, vale la pena anotar lo que manifestó el doctor Carlos Torres y Torres Lara en su condición de presidente de la Comisión de Constitución y Reglamento cuando, en su momento, le tocó sustentar ante el Pleno del Congreso Constituyente Democrático – CCD la reforma a dicha norma constitucional:

> *"(…) En ese sentido, señor Presidente, creemos haber encontrado un amplio consenso. Hay un sector que se opone todavía a la acción del Hábeas Data en su totalidad; sin embargo, hemos obtenido de diversos grupos políticos un consenso en la Comisión de Constitución para proponer aquí la modificación del Artículo 200º a fin de que se suprima la referencia sólo al inciso 7) del Artículo 2º de la Constitución. De esta manera, señor, hoy aprobaríamos esta modificación con el propósito de perfeccionar la norma. Para unos, esta modificación será satisfactoria porque entenderán que con ella se ha rectificado lo que creen que es un peligro; para nosotros, no. Para nosotros la rectificación significará que seguimos en el mismo camino del respeto a la libertad de expresión porque estamos llanos a perfeccionar el texto de la Constitución para dejar absolutamente claro este concepto, particularmente, cuando se avecina un proceso electoral. (…)"*[4].

En tal sentido, a partir de la referida reforma[5], la regulación del artículo 200 numeral 3 de la Constitución Política quedó aprobada y redactada de la siguiente manera:

---

[3] Publicada en el Diario Oficial El Peruano el 12 de junio de 1995.

[4] Extraído del Diario de Debates de la 5ta sesión vespertina de la Primera Legislatura Ordinaria llevada a cabo en fecha 17 de agosto de 1994 (página 4).
http://www4.congreso.gob.pe/dgp/constitucion/Const93DD/reforconst/Ley26470.pdf

[5] Conforme lo dispone el artículo 206 de la Constitución Política, los constituyentes del Congreso Constituyente Democrático - CCD, aprobaron la reforma constitucional en dos legislaturas ordinarias sucesivas. La primera se realizó el 17 de agosto de 1994 donde se obtuve 56 votos a favor (aprobación por mayoría) y la segunda el 18 de abril de 1995 donde la aprobación se dio por unanimidad.
http://www4.congreso.gob.pe/dgp/constitucion/Const93DD/reforconst/Ley26470.pdf

"Artículo 200°. Son garantías constitucionales:

(…)

3. La Acción de Hábeas Data, que procede contra el hecho u omisión, por parte de cualquier autoridad, funcionario o persona, que vulnera o amenaza los derechos a que se refiere el artículo 2º, incisos 5 y 6 de la Constitución.

(…)".

A partir de este enunciado constitucional, podemos advertir, los siguientes elementos constitutivos del proceso de hábeas data:

1. Procedencia: contra acciones u omisiones.
2. Sujetos obligados: cualquier autoridad, funcionario o persona.
3. Medio de afectación: vulneración o amenaza.
4. Derechos protegidos: los contenidos en los incisos 5 y 6 del artículo 2° de la Constitución.
5. Titular del derecho protegido: cualquier persona (natural o jurídica).

Ahora bien, a efectos del presente artículo, vamos a focalizar nuestro estudio en lo señalado en el numeral 4.

Contenido constitucional de los derechos protegidos

El contenido, alcances y límites constitucionales de los derechos de acceso a la información pública y a la autodeterminación informativa han sido ampliamente desarrollados en la sentencia del Tribunal Constitucional recaída en el Exp. N° 1797-2002-HD/TC (Wilo Rodríguez Gutiérrez) y, en adelante, consolidada en reiterada jurisprudencia que han venido ratificando la autonomía del proceso de hábeas data en la protección de dichos derechos.

1. Derecho de acceso a la información pública

1.1. Contenido esencial, naturaleza jurídica, dimensiones y ámbito de aplicación

Este derecho está consagrado en el numeral 5 del artículo 2 de la Constitución Política y encuentra su desarrollo constitucional en la Ley 27806, Ley de Transparencia y Acceso a la Información Pública.

El contenido esencial del derecho de acceso a la información, conforme lo ha señalado el Tribunal Constitucional en el Fundamento 5 de su sentencia recaída en el Exp. N° 9050-2000-HD/TC, "reside en el reconocimiento de la facultad de toda persona de solicitar y recibir información de cualquier entidad pública (...) no existiendo, en tal sentido, entidad del Estado o entidad con personería jurídica de derecho público que resulte excluida de la obligación de proveer la información solicitada."

En mérito a dicho enunciado, el derecho de acceso a la información pública tiene una doble dimensión: individual y colectiva, los que han sido desarrollados en la STC N° 1797-2002-HD/TC.

En su dimensión individual "garantiza que nadie sea arbitrariamente impedido de acceder a la información que guarden, mantengan o elaboren las diversas instancias y organismos que pertenezcan al Estado, sin más limitaciones que aquellas que se han previsto como constitucionalmente legítimas. A través de este derecho se posibilita que los individuos, aisladamente considerados, puedan trazar, de manera libre, su proyecto de vida, pero también el pleno ejercicio y disfrute de otros derechos fundamentales. Desde esta perspectiva, en su dimensión individual, el derecho de acceso a la información se presenta como un presupuesto o medio para el ejercicio de otras libertades fundamentales, como puede ser la libertad de investigación, de opinión o de expresión, por mencionar alguna."[6]

[6] Fundamento 10 de la sentencia del Tribunal Constitucional recaída en el Exp. N° 1797-2002-HD/TC.

En su dimensión colectiva "garantiza el derecho de todas las personas de recibir la información necesaria y oportuna, a fin de que pueda formarse una opinión pública, libre e informada, presupuesto de una sociedad auténticamente democrática. Desde este punto de vista, la información sobre la manera como se maneja la res pública termina convirtiéndose en un auténtico bien público o colectivo, que ha de estar al alcance de cualquier individuo, no sólo con el fin de posibilitar la plena eficacia de los principios de publicidad y transparencia de la Administración pública, en los que se funda el régimen republicano, sino también como un medio de control institucional sobre los representantes de la sociedad; y también, desde luego, para instar el control sobre aquellos particulares que se encuentran en la capacidad de poder inducir o determinar las conductas de otros particulares o, 10 que es más grave en una sociedad como la que nos toca vivir, su misma subordinación."[7]

A la luz de ambas dimensiones podemos advertir que el ejercicio de esta prerrogativa constitucional implica una relación de derecho-deber entre las personas y la administración pública. Por un lado, supone el derecho de toda persona, sea natural o jurídica, de conocer la información considerada disponible, dentro del contexto de lo que se entiende por información pública y fuera de las excepciones razonablemente establecidas en el texto constitucional (intimidad personal, seguridad nacional, materias sometidas a reserva legal) y; por otro, la obligación de las entidades públicas de proporcionar la información solicitada.

En ese orden de ideas, conforme lo ha subrayado del Tribunal Constitucional en el Fundamento 5 de su sentencia recaída en el Exp. N° 4865-2013-PHD/TC, "La protección del derecho fundamental de acceso a la información pública no solo es de interés para el titular del derecho, sino también para el propio Estado y para la colectividad en general. Por ello, los pedidos de información pública no deben

[7] Fundamento 11 de la sentencia del Tribunal Constitucional recaída en el Exp. N° 1797-2002-HD/TC.

entenderse vinculados únicamente al interés de cada persona requirente, sino valorados además como manifestación del principio de transparencia en la actividad pública. Este principio de transparencia es, de modo enunciativo, garantía de no arbitrariedad, de actuación lícita y eficiente por parte del Estado, y sirve como mecanismo idóneo de control en manos de los ciudadanos."

En dicho sentido, la trascendencia de este derecho radica en establecer una regla general de publicidad y transparencia en la actuación de los poderes públicos como un elemento consustancial a un régimen democrático que contribuya a la formación de una opinión pública, libre, informada y participativa, procurando eliminar a la par, la cultura del secreto en la gestión pública o cualquier elemento generador de corrupción a partir del ocultamiento o renuencia a la entrega de la información pública. Es decir, la publicidad de la información pública debe ser siempre la regla general; mientras que, el secreto la excepción.

Lo señalado en la parte final del párrafo anterior se encuentra consagrado expresamente en el artículo 3° de la Ley N° 27806, el cual establece: "Toda información que posea el Estado se presume pública, salvo las excepciones expresamente previstas por el artículo 15 de la presente Ley."

Ahora bien, en cuanto al ámbito de aplicación sobre quienes recae la obligación de brindar la información pública, se tiene lo dispuesto en el artículo 2 de la Ley N° 27806, en mérito al cual todas las entidades de la Administración Pública señaladas en el Artículo I del Título Preliminar de la Ley Nº 27444, Ley del Procedimiento Administrativo General, deben de aplicar el principio de publicidad y transparencia de la información, así como proporcionarla a quienes la soliciten. Estas entidades son:

1. El Poder Ejecutivo, incluyendo Ministerios y Organismos Públicos;

2. El Poder Legislativo;

3. El Poder Judicial;
4. Los Gobiernos Regionales;
5. Los Gobiernos Locales;
6. Los Organismos a los que la Constitución Política del Perú y las leyes confieren autonomía.
7. Las demás entidades, organismos, proyectos especiales, y programas estatales, cuyas actividades se realizan en virtud de potestades administrativas y, por tanto, se consideran sujetas a las normas comunes de derecho público, salvo mandato expreso de ley que las refiera a otro régimen; y,
8. Las personas jurídicas bajo el régimen privado que prestan servicios públicos o ejercen función administrativa, en virtud de concesión, delegación o autorización del Estado, conforme a la normativa de la materia.

Al respecto, es de resaltar lo establecido en el numeral 8, en mérito a lo cual las personas jurídicas de derecho privado que brindan servicios públicos o que ejercen función administrativa también se encuentran obligadas a entregar información siempre que, conforme lo dispone el artículo 9º[8] del Texto Único Ordenado de la Ley N° 27806 (Decreto Supremo N° 021-2019-JUS) y lo precisado por el Tribunal Constitucional en su sentencia recaída en el Exp. N° 00390-2007-PHD/TC[9], la información solicitada este referida a:

[8] **"Artículo 9.- Personas jurídicas sujetas al régimen privado que prestan servicios públicos**

Las personas jurídicas sujetas al régimen privado descritas en el inciso 8) del Artículo I del Título Preliminar de la Ley Nº 27444 que gestionen servicios públicos o ejerzan funciones administrativas del sector público bajo cualquier modalidad están obligadas a informar sobre las características de los servicios públicos que presta, sus tarifas y sobre las funciones administrativas que ejerce."

[9] Fundamento 7: "Ahora bien de conformidad con lo dispuesto en el artículo 9° de la Ley de Transparencia y Acceso a la Información Pública, las personas jurídicas privadas

- Las características de los servicios públicos que prestan;
- Sus tarifas; y
- Las funciones administrativas que ejercen bajo concesión, delegación o autorización del Estado.

En este sentido, la referida información también tiene naturaleza pública.

Asimismo, conforme lo señala el artículo 10 de la Ley 27806, se considera como información pública cualquier tipo de documentación financiada por el presupuesto público que sirva de base a una decisión de naturaleza administrativa (por ejemplo, informes realizados a través de consultorías), así como las actas de reuniones oficiales. No obstante, de modo asertivo el Tribunal Constitucional ha interpretado en sentido más amplio este enunciado afirmando que "Lo realmente trascendental, a efectos de que pueda considerarse como "información pública", no es su financiación, sino la posesión y el uso que le imponen los órganos públicos en la adopción de decisiones administrativas, salvo, claro está, que la información haya sido declarada por ley como sujeta a reserva."[10]

Finalmente, respecto a la naturaleza jurídica de este derecho, cabe señalar que tiene la condición de libertad preferida cuando su ejercicio está destinado a contribuir con la formación de una opinión pública, libre e informada. Así lo ha establecido el Supremo Intérprete de la Constitución en el fundamento 11 de la STC N° 1797-2002-HD/TC: "(…) a juicio del Tribunal, cuando el ejercicio del derecho de acceso a la información pública contribuye a la formación de una opinión pública, libre e informada, éste tiene la condición de libertad preferida.

- que efectúan servicios públicos o efectúan funciones administrativas- "están obligadas a informar sobre las características de los servicios públicos que presta, sus tarifas y sobre las funciones administrativas que ejerce" (énfasis agregado). En consecuencia, la información accesible debe referirse a alguno de estos tres aspectos, siendo este el ámbito de información que puede solicitarse a una persona jurídica de derecho privado."

[10] Fundamento 12 de la STC N° 2579-2003-HD/TC

Esta condición del derecho de acceso a la información no quiere decir que al interior de la Constitución exista un orden jerárquico entre los derechos fundamentales que ella reconoce, en la cúspide del cual se encuentre o pueda encontrarse el derecho de acceso a la información u otros derechos que cuentan igualmente con idéntica condición. Y, en ese sentido, que una colisión de éste con otros derechos fundamentales se resuelva en abstracto, haciendo prevalecer al que tiene la condición de libertad preferida. Evidentemente ello no es así. Todos los derechos constitucionales tienen, formalmente, la misma jerarquía, por ser derechos constitucionales. De ahí que ante una colisión entre ellos, la solución del problema no consiste en hacer prevalecer unos sobre otros, sino en resolverlos mediante la técnica de la ponderación y el principio de concordancia práctica."

1.2. Características de la información pública

La sola entrega de la información pública solicitada no necesariamente supone el cumplimiento efectivo de dicho derecho. A efectos de que se cumpla con los estándares constitucionales, la información que se proporciona debe ser cierta, completa, clara, precisa, actualizada y oportuna. Así lo ha afirmado el Tribunal Constitucional en el Fundamento 16 de la acotada STC N° 1797-2002-HD/TC:

> "(…) el contenido constitucionalmente garantizado por el derecho de acceso a la información pública no sólo comprende la mera posibilidad de acceder a la información solicitada y, correlativamente, la obligación de dispensarla de parte de los organismos públicos. Si tal fuese sólo su contenido protegido constitucionalmente, se correría el riesgo de que este derecho y los fines que con su reconocimiento se persiguen, resultaran burlados cuando, p.ej . los organismos públicos entregasen cualquier tipo de información, independientemente de su veracidad o no. A criterio del Tribunal, no sólo se afecta el derecho de acceso a la información cuando se niega su suministro, sin existir razones constitucionalmente legítimas para ello, sino también cuando la información que se proporciona es fragmentaria, desactualizada, incompleta, imprecisa, falsa, no oportuna o errada. De ahí que, si en su faz positiva

> el derecho de acceso a la información impone a los órganos de la Administración pública el deber de informar, en su faz negativa, exige que la información que se proporcione no sea falsa, incompleta, fragmentaria, indiciaria o confusa."

En mérito a ello, se desprende los siguientes atributos que debe tener la información pública:

- Cierta; implica que las entidades públicas proporcionen información auténtica, confiable, seria y veraz para el ciudadano.
- Completa; mediante la cual la información que se entrega debe contener todos los aspectos que permitan su adecuada comprensión y no limitarse solamente a parte o fragmentos de ella.
- Clara; supone que la información debe ser entendible para el ciudadano, en lenguaje sencillo y comprensible, evitándose la indeterminación y la abstracción de su contenido.
- Precisa; la información debe estar referida a lo que concretamente se solicita, de relevancia para quien lo necesita.
- Actualizada; está referida a la necesidad de proporcionar información que se encuentre al día, es decir ajustada a la última versión de su elaboración o procesamiento.
- Oportuna; significa que la información debe ser entregada u obtenida cuando se necesita, lo cual supone el cumplimiento del plazo legal.

Cabe precisar que, la solicitud de la información no requiere expresión de causa, es decir, no necesita ser justificada por su requirente. Su fundamento radica en que la información que producen o poseen las entidades públicas se considera un bien público, es decir, pertenece a la población. Además, porque supone el ejercicio de otros derechos, como por ejemplo la libertad de información.

Dentro de este contexto, resulta necesario enfatizar que la entidad pública no puede negarse a proporcionar la información con el argumento que no ha sido creada o procesada por ésta, puesto que también se considera como información pasible de entrega aquellas que, aún cuando no hayan sido creadas por ellas, se encuentran en su posesión.

Al respecto, es de resaltar la Resolución N° 010300772020 del Tribunal de Transparencia y Acceso a la Información Pública[11], mediante la cual establece como precedente administrativo de observancia obligatoria para toda la administración pública que "(…) cuando las entidades denieguen el acceso a la información pública en virtud a la inexistencia de la documentación requerida, deberán previamente verificar mediante los requerimientos a las unidades orgánicas que resulten pertinentes si la información: i) fue generada por la entidad; y, II) si ha sido obtenida, se encuentre en su posesión o bajo su control; asimismo, luego de descartar ambos supuestos, deberán comunicar de manera clara y precisa dicha circunstancia al solicitante"; lo cual se considera positivo en la medida que obliga a los servidores y funcionarios públicos a agotar todos los medios de búsqueda de la información antes de emitir una respuesta denegatoria al ciudadano.

A mayor abundamiento, se anota lo dispuesto por el numeral 1 del artículo 61 del Código Procesal Constitucional, el cual ha dispuesto de manera categórica que la información pasible de entrega alcanza a toda aquella que se genere, produzca, procese o posea la entidad pública, incluida la que obra en expedientes terminados o en trámite, estudios, dictámenes, opiniones, datos estadísticos, informes técnicos y cualquier otro documento que tenga en su poder, cualquiera que sea la forma de expresión, ya sea gráfica, sonora, visual, electromagnética o que obre en cualquier otro tipo de soporte materia. Es decir, se hace extensivo a toda cuanta información se encuentre en el ámbito de la administración.

[11] Exp. N° 00038-2020-JUS/TTAIP. Resolución de fecha 28 de enero de 2020.

1.3. Diferencia con otros derechos

El derecho bajo comentario, suele confundirse con otros dos derechos constitucionales: derecho de petición (Art. 2.20) y derecho a la libertad de información (Art. 2.4). Sin embargo, a la luz de lo desarrollado en la antes referida STC N° 1797-2002-HD/TC, se ha precisado claramente sus diferencias:

- Con el derecho de petición
  - El derecho de petición no se encuentra vinculado con la existencia en sí de un derecho subjetivo o de un interés legítimo al que tenga derecho acceder; mientras que, a través del derecho de acceso a la información pública sí se tiene derecho a exigir el otorgamiento de lo solicitado.
  - El derecho de petición no supone necesariamente la existencia de un dato o información que disponga la entidad, sino puede referirse a otros contenidos o materias como, por ejemplo, que se otorgue una licencia ambiental, de construcción o de funcionamiento; en cambio, por el acceso a la información pública, se busca obtener necesariamente datos o información que se encuentra en poder de la administración.
  - El derecho de petición no obliga a la administración a acceder a lo solicitado, sino tan solo a dar una respuesta positiva o negativa a la solicitud; por lo que, como dice la doctrina, constituye una decisión graciable sujeta a consideración discrecional. En tal sentido, este derecho se agota con su solo ejercicio (pedir), estando la autoridad pública obligada únicamente a acusar recibo y dar respuesta de las solicitudes. En cambio, por el derecho al acceso de información pública, la entidad pública sí está obligada a entregar la información que se le está solicitando, claro está, siempre que se trate de información

disponible y que no se encuentre exceptuada; por lo que el derecho no se agota en el sólo pedir, sino en la entrega de lo solicitado.

- El derecho de petición se ejerce tanto ante la administración pública como ante una entidad privada; en cambio, el acceso a la información opera únicamente frente a aquellas que tienen la naturaleza de entidades públicas. De ahí que, el primero es considerado dentro del conjunto de los derechos civiles que pertenecen al ser humano; y el segundo, dentro de los derechos políticos que le corresponden a la persona en su condición de ciudadano.

- El derecho de petición supone expresión de causa para justificar lo que se desea alcanzar o acceder; en cambio, el acceso a la información, no.

- Con el derecho a la libertad de información:

Este derecho garantiza el acceso, la búsqueda y la difusión de hechos noticiosos o de información veraz, que permita por un lado acceder a fuentes de información y, por otro, de recibirla a efectos de formarse una opinión propia o la opinión pública; por lo que, su objeto es la *comunicación libre*, tanto de hechos como de opiniones que contribuyan a la construcción, mantenimiento y fortalecimiento de la democracia. En cambio, el derecho al acceso a la información pública garantiza que cada persona pueda conocer lo que acontece al interior de la actividad estatal, sin necesidad de que el ánimo sea la difusión de dicha información. Sin embargo, podrá advertirse que para ejercer el derecho a la libertad de información se podrá hacer uso del derecho de acceso a la información pública, por lo que su relación es evidente. Ambos derechos tienen la condición de libertades preferidas en tanto permiten la plena

realización del sistema democrático y contribuyen al debate sobre la cosa pública.

1.4. Límites al derecho de acceso a la información pública

Partiendo de la premisa que ningún derecho es absoluto, todos son relativos; se conoce que los derechos presentan excepciones en su ejercicio constitucional, los cuales se fundamentan en el respeto de otros derechos o principios constitucionales.

Respecto del derecho bajo análisis, el Tribunal Constitucional en la STC N° 01219-2003-HD/TC ha sostenido lo siguiente: "(…) el ejercicio del derecho fundamental de acceso a la información pública no es absoluto, sino que está sujeto a límites o restricciones que se pueden derivar, ya sea de la necesidad de armonizar su ejercicio con otros derechos de la misma clase (v. gr. derecho a la intimidad personal), o bien por la necesidad de salvaguardar bienes constitucionalmente relevantes (v. gr. la seguridad nacional), y siempre que éstas hayan sido expresamente previstas por ley."

De la lectura del numeral 5 del artículo 2 del Texto Constitucional, se desprende que los límites a la información pública son:

- La intimidad personal
- La seguridad nacional
- El secreto bancario
- La reserva tributaria
- Otros por reserva legal

Por principio constitucional las excepciones deben ser interpretadas de manera restrictiva por tratarse de limitaciones a derechos fundamentales y su regulación debe estar desarrollada a nivel legal, que para el caso de la información pública se encuentran en los artículos 15, 16 y 17 del TUO de la Ley de Transparencia y Acceso a la Información

Pública, donde se ha clasificado la naturaleza excepcional del derecho como secreta, reservada o confidencial.

En el fundamento 32 de la STC N° 0005-2013-PI/TC, el Supremo Intérprete de la Constitución ha dejado sentado que los casos establecidos en los referidos artículos 15, 16 y 17 son los únicos en los que se puede limitar el derecho al acceso a la información pública; por los que, acotando a lo anterior, ha señalado que "el artículo 2, inciso 5, de la Constitución, junto a la Ley de Transparencia y Acceso a la Información Pública, conforman el parámetro de constitucionalidad que debe servir para identificar las exigencias constitucionales que se derivan de este derecho, así como las estrictas y únicas excepciones que pueden justificar la limitación del acceso a la información pública".

Ahora bien, en cuanto a las excepciones por reserva legal, en la jurisprudencia constitucional anotada líneas arriba, se ha establecido las condiciones que se deben cumplir para que las excepciones reguladas por el legislador sean consideradas válidas. A saber:

i) Deben estar previstas en la ley de forma expresa y estricta, no pudiendo quedar al libre arbitrio de cada entidad de la Administración Pública;

ii) Deben perseguir objetivos legítimos que estén indesligablemente unidos a la protección de un fin constitucional;

iii) Deben ser estrictamente necesarias, lo que implica además elegir la medida menos restrictiva posible;

iv) Deben ser proporcionales con el grado de restricción del derecho de acceso a la información pública, de modo que el grado de ventajas o satisfacción del fin constitucional que se quiere proteger con la excepción sea, por lo menos, mayor que el grado de desventajas o restricción del derecho de acceso a la información pública.

En la misma línea de pensamiento, se deber tener presente que la sola nominación formal de una determinada información como secreta, reservada o confidencial no le da el atributo de información exceptuada, sino que, debe ir acompañada de la debida justificación y motivación en el marco de lo señalado en el párrafo precedente.

2. Derecho a la autodeterminación informativa

2.1. Contenido, naturaleza jurídica y ámbito de aplicación

Este otro derecho materia de protección del hábeas data, también denominado derecho a la protección de datos personales, se encuentra consagrado en el numeral 6 del artículo 2 de la Carta Magna y a nivel legal desarrollado en la Ley N° 29733, Ley de Protección de Datos Personales y en el numeral 2 del artículo 61 del Código Procesal Constitucional, mediante el cual toda persona puede *conocer, actualizar, incluir y suprimir o rectificar la información o datos referidos a su persona que se encuentren almacenados o registrados en forma manual, mecánica o informática, en archivos, bancos de datos o registros de entidades públicas o de instituciones privadas que brinden servicio o acceso a terceros. Asimismo, a hacer suprimir o impedir que se suministren datos o informaciones de carácter sensible o privado que afecten derechos constitucionales.*

Conforme se desprende de dicho enunciado, su objeto es proteger la intimidad, personal o familiar, la imagen y la identidad de las personas frente al riesgo de que la información almacenada en servicios informáticos, computarizados o no, pueda ser utilizada y/o manipulada por terceros afectando la esfera íntima de la persona y el ámbito del desenvolvimiento de su personalidad.

Es de precisar que el ámbito de aplicación sobre quienes recae este derecho son tanto las entidades del sector público como privado, exceptuándose según lo dispone el artículo 3 de la Ley N° 29733, los datos personales que estén contenidos o destinados a ser contenidos en:

- Bancos de datos personales creados por personas naturales para fines exclusivamente relacionados con su vida privada o familiar.

- Bancos de datos de administración pública, solo en tanto su tratamiento resulte necesario para el estricto cumplimiento de las competencias asignadas por ley a las respectivas entidades públicas, para la defensa nacional, seguridad pública, y para el desarrollo de actividades en materia penal para la investigación y represión del delito

Dentro de dicho contexto y a la luz de lo que dispone la precitada ley, el contenido de este derecho está compuesto por la facultad que tiene toda persona de:

- Ser informado en forma detallada, sencilla, expresa, inequívoca y de manera previa a su recopilación, sobre la finalidad para la que sus datos personales serán tratados.

- Obtener la información que sobre sí mismo sea objeto de tratamiento en bancos de datos de administración pública o privada, la forma en que sus datos fueron recopilados, las razones que motivaron su recopilación y a solicitud de quién se realizó la recopilación, así como las transferencias realizadas o que se prevén hacer de ellos.

- Derecho a la actualización, inclusión, rectificación y supresión de sus datos personales materia de tratamiento, cuando estos sean parcial o totalmente inexactos, incompletos, cuando se hubiere advertido omisión, error o falsedad, cuando hayan dejado de ser necesarios o pertinentes a la finalidad para la cual hayan sido recopilados o cuando hubiera vencido el plazo establecido para su tratamiento.

- Derecho a impedir el suministro de sus datos personales, especialmente cuando ello afecte sus derechos fundamentales.

- Derecho de oposición al tratamiento de sus datos personales, siempre que, por ley, no se disponga lo contrario y cuando no hubiera prestado su consentimiento.
- Derecho al tratamiento objetivo de sus datos personales.
- Derecho a la tutela, mediante el cual el titular del derecho afectado puede recurrir ante la Autoridad Nacional de Protección de Datos Personales en vía de reclamación o al Poder Judicial a través de la acción de hábeas data.
- Derecho a ser indemnizado.

Atendiendo a lo hasta aquí señalado, podemos colegir que a partir de este derecho toda persona tiene derecho a decidir cómo, cuándo, dónde y por quién se tratan sus datos, con lo cual se le otorga la facultad de controlar el uso de los mismos a efectos que pueda construir y cautelar su esfera privada frente a los actos que manifiesta en su desenvolvimiento social.

Al respecto, en concordancia con lo referido en el párrafo precedente, el Tribunal Constitucional en la sentencia recaída en el Exp. N° 4739-2007-PHD/TC ha sostenido: "El derecho a la autodeterminación informativa consiste en la serie de facultades que tiene toda persona para ejercer control sobre la información personal que le concierne, contenida en registros ya sean públicos, privados o informáticos, a fin de enfrentar las posibles extralimitaciones de los mismos. Se encuentra estrechamente ligado a un control sobre la información, como una autodeterminación de la vida íntima, de la esfera personal."

Ahora bien, en cuanto a su naturaleza, el derecho bajo comentario, al estar vinculado con la protección de otros derechos fundamentales, tiene naturaleza relacional. Así lo ha dejado sentado el Tribunal en la ya conocida STC N° 1797-2002-HD/TC, en cuyo fundamento jurídico 3, último párrafo, estableció lo siguiente: "En ese sentido, por

su propia naturaleza, el derecho a la autodeterminación informativa, siendo un derecho subjetivo tiene la característica de ser, prima jade y de modo general, un derecho de naturaleza relacional, pues las exigencias que demandan su respeto, se encuentran muchas veces vinculadas a la protección de otros derechos constitucionales."

2.2. Diferencia con otros derechos

Atendiendo a la naturaleza relacional anotada en el ítem anterior y a la luz de lo establecido por el Supremo Intérprete de la Constitución en la célebre STC N° 1797-2002-HD/TC que, es la que marca el derrotero de los derechos protegidos por el hábeas data, se tiene las siguientes diferencias:

- Con el derecho a la intimidad. Este derecho está orientado a proteger la *vida* privada de las personas, otorgándoles el poder jurídico de rechazar intromisiones ilegítimas en su esfera íntima o familiar; mientras que, el derecho a la autodeterminación informativa garantiza la facultad de todo individuo de poder preservarla controlando el registro, uso y revelación de los datos que les conciernen.

- Con el derecho a la imagen. Mediante éste se protege esencialmente la imagen del ser humano derivada de la dignidad de la que se encuentra investido; mientras que el derecho a la autodeterminación informativa, en este extremo, garantiza que el individuo sea capaz de disponer y controlar el tipo de datos que sobre él se hayan registrado a efectos de preservar su imagen derivada de su inserción en la vida en sociedad.

- Con el derecho a la identidad. La diferencia radica en la protección a que la proyección social de la propia personalidad no sufra distorsiones a consecuencia de la atribución de ideas, opiniones o comportamientos diferentes de aquellos que el individuo manifiesta en su vida en sociedad.

En consecuencia, el derecho de autodeterminación informativa constituye uno de naturaleza autónoma cuya protección parte de la existencia de bases de datos, computarizados o no, frente a la posibilidad de afectación de la esfera personal y familiar del individuo por el uso y/o manipulación del tratamiento de sus datos, sobre todo en contextos actuales donde la tecnología y el poder informático van en constante aumento.

2.3. Principios rectores

Con la finalidad de orientar la actuación de la administración pública y privada en el tratamiento de los datos personales que tengan en su poder, la Ley N° 29733 ha establecido ocho principios rectores de naturaleza enunciativa:

- Principio de legalidad; mediante el cual el tratamiento de los datos personales se debe realizar conforme a lo dispuesto en la ley, prohibiéndose, además, la recopilación de los datos personales por medios fraudulentos, desleales o ilícitos.

- Principio de consentimiento; en mérito al cual se exige que para el tratamiento de los datos personales debe mediar el consentimiento de su titular, el cual deber ser libre, directo, previo, expreso, claro, informado e inequívoco.

- Principio de finalidad; a partir del cual los datos personales deben ser recopilados para una finalidad determinada, explícita y lícita. Tratándose de banco de datos personales que contengan datos sensibles, su creación solo puede justificarse si su finalidad además de ser legítima, es concreta y acorde con las actividades o fines explícitos del titular del banco de datos personales.

- Principio de proporcionalidad; exige que el tratamiento de datos personales debe ser adecuado, relevante y no excesivo a la finalidad para la que estos hubiesen sido recopilados.

- Principio de calidad; implica que los datos personales que vayan a ser tratados deben ser veraces, exactos y, en la medida de lo posible, actualizados, necesarios, pertinentes y adecuados respecto de la finalidad para la que fueron recopilados.

- Principio de seguridad; obliga al titular del banco de datos personales y al encargado de su tratamiento a adoptar todas las medidas técnicas, organizativas y legales necesarias para garantizar la seguridad de los datos personales.

- Principio de disposición de recurso; a través del cual todo titular de datos personales debe contar con las vías administrativas o jurisdiccionales necesarias para reclamar y hacer valer sus derechos, cuando estos sean vulnerados por el tratamiento de sus datos personales.

- Principio de nivel de protección adecuado; aplicable para los casos de transferencia internacional de datos personales, a partir del cual se debe garantizar un nivel suficiente de protección para su tratamiento transfronterizo.

Cabe precisar que, los referidos principios sirven también de criterio interpretativo para resolver las controversias que puedan generarse entorno a la aplicación de la Ley de Protección de Datos Personales Ley y de su reglamento, así como de parámetro para la elaboración de otras disposiciones y para suplir vacíos en la legislación sobre la materia. Seguramente, será la doctrina y principalmente la jurisprudencia quienes vayan dotando de mayor contenido a estos principios y a la finalidad que persiguen.

2.4. Límites al ejercicio del derecho

El derecho a la autodeterminación informativa, al igual que todos los demás derechos, también presenta excepciones en cuanto a su ejercicio; los cuales, conforme lo señala el artículo 27 de la antes referida Ley 29733, encuentran justificación cuando se encuentre de por medio la protección

de derechos e intereses de terceros o cuando ello pueda obstaculizar actuaciones judiciales o administrativas en curso vinculadas a la investigación sobre el cumplimiento de obligaciones tributarias o previsionales, a las investigaciones penales sobre la comisión de faltas o delitos, al desarrollo de funciones de control de la salud y del medio ambiente, a la verificación de infracciones administrativas, o cuando así lo disponga la ley.

En dichas situaciones los titulares y los encargados de tratamiento de datos personales pueden denegar el ejercicio de los derechos de acceso, supresión y oposición a los datos personales.

De otra parte, encontramos otras limitaciones al derecho en lo dispuesto en el artículo 14 de la precitada ley, donde se ha establecido supuestos en los cuales no se requiere el consentimiento del titular de datos personales, para los efectos de su tratamiento, en casos referidos al ejercicio de las funciones de las entidades públicas, solvencia patrimonial y de crédito, relaciones contractuales en la que el titular del derecho sea parte, prevención, diagnóstico y tratamientos médicos del titular, prevención de lavado de activos y financiamiento del terrorismo, entre otros.

La jurisprudencia emitida al respecto aún es escueta; sin embargo, con ocasión del caso analizado en el Exp. N° 04227-2009-PHD/TC, el Tribunal Constitucional ha tenido la oportunidad de precisar que, en el caso de la información financiera destinada al cálculo del riesgo crediticio, la limitación temporal del almacenamiento de la misma debe estar directamente relacionada con la facultad de que los datos que se conserven en un registro informático sean actuales y veraces. De esto, se puede colegir que, el derecho a la autodeterminación informativa puede restringirse cuando se trate de difundir datos referidos a obligaciones crediticias siempre que la información se encuentre actualizada y, en el caso de datos negativos o adversos siempre que se expresen límites temporales de registro y publicidad.

A mayor abundamiento, señalamos lo que al respecto ha manifestado el Tribunal:

> "La limitación temporal del almacenamiento de la información financiera destinada al cálculo del riesgo crediticio está directamente relacionada con la facultad de que los datos que se conserven en un registro informático sean actuales y veraces. A juicio del Tribunal, la única manera de que a través de los datos se pueda proyectar una imagen real del comportamiento de una persona en el sistema bancario y financiero es que estos sean constantemente actualizados. Tal actualización presupone, *in nuce*, una prohibición de almacenamiento ad aeternum de los datos. En particular, de los denominados "datos negativos", es decir, de los que registran una mala práctica en el mercado, pues también las malas historias crediticias se pueden revertir por la adopción de hábitos de honramiento de las obligaciones contraídas o, llegado el caso, incluso por efectos legales del transcurso del tiempo. (…) La información de que una obligación patrimonial se ha extinguido por su pago oportuno es tan valiosa como la información de que dicha obligación se ha extinguido fuera del plazo (…) cualquiera que fuera el caso de información adversa que se pueda haber registrado en un banco de datos, el deber que tienen de proporcionar información veraz exige que estos sean actualizados constantemente, y reparar que ella no puede mantenerse registrada eternamente. Ello vale incluso para el caso de las obligaciones insolutas, en particular, cuando su exigibilidad haya superado el término de prescripción legal para poder reclamar su satisfacción."

Frente a lo expuesto, se tendrá que determinar caso por caso y a la luz de los principios rectores, en qué casos opera o no la aplicación de las limitaciones a este derecho.

3. Retos y desafíos

Atendiendo al incesante avance de los medios tecnológicos y de la formación de sociedades informatizadas, el mayor reto que le toca

afrontar al hábeas data es sin duda su adecuación y constante actualización normativa para proteger los derechos que tutela frente a la velocidad con que se producen, transmiten y almacenan los datos sin límites fronterizos. Y es que, a partir de la digitalización de la información, de la comunicación por internet, del uso de las redes sociales, de la generación del *big data* y del tratamiento automatizado de los mismos, los derechos se vuelven más vulnerables y por lo mismo necesitan de mejores y mayores mecanismos de protección que estén a la altura de dichos desafíos tecnológicos.

La persona, muchas veces sin darse cuenta; por ejemplo, cuando llena fichas médicas, laborales, comerciales, educativas, encuestas, formatos de solicitud de créditos, de contratación de servicios profesionales, turísticos o de servicios básicos como luz, agua, teléfono, celular, cable; o, cuando de manera casi automática acepta términos y condiciones cuando descarga apps o aplicativos móviles, va dejando por todas partes, tanto a nivel del sector público como privado, sus datos personales y; si a ello le sumamos, todas las publicaciones que hace por redes sociales, nos damos cuenta de la alta vulnerabilidad con que se encuentra expuesta su identidad, privacidad y hasta su libertad y seguridad personales. El control de sus datos va saliendo de su esfera individual y de pronto éstos se encuentran compartiéndose o difundiéndose a nivel global.

En este sentido, el mayor desafío del derecho en general y del hábeas data en particular, es adecuar mecanismos más céleres y efectivos que permitan prevenir y actuar frente a dichos riesgos. Pero, ¿cómo hacerlo? Como punto de partida consideramos que la primera acción debe recaer en la educación a la población sobre la importancia del control de sus datos personales. La información nace del individuo y si éste es capaz de entender la relevancia sobre el manejo de sus datos, podrá entonces estar en condiciones de actuar y decidir con solvencia respecto de su preservación o difusión de los mismos, estando a la par en la capacitad de activar los mecanismos procesales para su defensa y protección.

Resulta, asimismo importante que el Estado fortalezca los sistemas de regulación y fiscalización en el tratamiento de la información pública y privada, que permitan identificar y determinar responsabilidades así como sanciones a los infractores de las normas que garantizan, por un lado, el acceso a la información pública; y, por otro, la protección de la privacidad personal.

Finalmente, consideramos necesario que a nivel global todos los Estados sumen esfuerzos a efectos de generar lazos de cooperación y colaboración internacional a través de convenios o tratados que permita generar una uniformidad normativa vinculante para garantizar el flujo y el tratamiento transfronterizo de los datos con todas las medidas de seguridad para la efectiva protección a los derechos y libertades fundamentales, en particular del derecho a la intimidad personal.

Si bien es cierto, a la fecha existen recomendaciones para la protección de datos personales emitidas a nivel de la Organización de Estados Americanos- OEA[12], de la Organización para la Cooperación y el Desarrollo Económico - OCDE y del Foro de Cooperación Económica Asia- Pacífico – APEC, éstas no tienen carácter vinculante; no obstante, suponen un significativo avance que junto con el Convenio 108 del Consejo de Europa[13] y su Protocolo adicional, conocido como el Convenio 108+[14], sirven de una valiosa base para ir avanzando hacia un instrumento normativo universal.

[12] AG/RES. 2811 (XLIII-O/13) sobre Acceso a la Información Pública y Protección de Datos Personales, aprobado en la cuarta sesión plenaria de la OEA, celebrada el 6 de junio de 2013.

[13] Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal, hecho en Estrasburgo, Francia, el veintiocho de enero de 1981. Constituye el primer instrumento internacional vinculante adoptado en el ámbito de la protección de datos. Se encuentra abierto a la adhesión de cualquier Estado no miembro del Consejo de Europa. A la fecha, el Perú aún no se ha adherido a este Convenio.

[14] Adoptado el 10 de octubre de 2018.

En consecuencia, antes que enfrentarse al vertiginoso e innegable avance de la ciencia y de la tecnología, se trata de ir encontrando los límites a su aplicabilidad a fin de conciliar el interés público que persiguen con el respeto a la espera personal de los individuos.

Ahora bien, en cuanto al derecho de acceso a la información pública, el reto supone en mejorar los niveles de transparencia y acceso a la información que se genera, procesa o almacena en las entidades públicas a través de una política de datos abiertos, de promoción de mecanismos de participación ciudadana, de rendición de cuentas y de ética e integridad pública. Se debe desterrar la cultura del secreto y minimizar la burocracia en los trámites para que los ciudadanos accedan a la información estatal con facilidad y celeridad. Lo deseable sería que toda la información pública se cuelgue en formato de datos abiertos en la web y se avance hacia la implementación de una ventanilla única digital para todo el aparato público tanto a nivel nacional, regional y local. De esta manera el ciudadano ya no tendría que verse obligado a recurrir a una determinada entidad pública para solicitar la entrega de una u otra información, sino, únicamente tendría que descargarlo del portal web. Solo así iremos construyendo una sociedad más democrática y participativa donde el ciudadano sea el protagonista de la gestión pública y el respeto de sus derechos el referente esencial para la toma de decisiones.

LA SALVAGUARDA DE LOS DERECHOS FUNDAMENTALES DE ACCESO A LA INFORMACIÓN PÚBLICA Y A LA AUTODETERMINACIÓN INFORMATIVA EN EL PERÚ EN LA JURISPRUDENCIA DEL TRIBUNAL CONSTITUCIONAL

Repaso de las líneas jurisprudenciales

✍ Gonzalo Carlos Muñoz Hernández*

1. La Constitución como norma jurídica

Como sabiamente lo señala Böckenförde (2000), lo que determina el fundamento y la cohesión del orden político y social ya no es un orden divino o natural; las bases de la ordenación política de la vida en común corresponden al pueblo[1]. En esa misma línea de pensamiento, De Otto (1995), señala ni la moral ni la historia prefiguran normativamente el contenido del ordenamiento jurídico; en las actuales circunstancias, esa función la cumple la norma suprema

* Asesor del Tribunal Constitucional. Abogado por la Pontificia Universidad Católica del Perú. Egresado de las maestrías de Derecho Constitucional y Derechos Humanos de la Universidad Nacional Mayor de San Marcos y de la maestría en Enseñanza del Derecho en la Universidad de San Martín de Porres. Ex docente del curso Derecho Procesal Constitucional y del curso Derecho Constitucional Económico en la Universidad de San Martín de Porres.

[1] Böckenförde, E. (2000). *Estudios sobre el Estado de Derecho y la democracia*. (p. 51) Madrid: Trotta.

del mismo: la Constitución[2], que es definida por Böckenförde (2000) como el orden jurídico fundamental de la comunidad, razón por la cual, le atribuye, por un lado, una posición jerárquica suprema, y, de otro lado, un efecto irradiación sobre el resto de normas que se encuentran por debajo suyo.[3]

Por su parte, el Tribunal Constitucional (2003) en el fundamento 2 de la sentencia emitida en el Exp. 14-2003-AI/TC ha indicado lo siguiente:

> La Constitución es una norma jurídico-política *sui generis*. El origen de dicha peculiaridad, desde luego, no sólo dimana de su posición en el ordenamiento jurídico, sino también del significado que tiene, y de la función que está llamada a cumplir.[4]

Así, en lo concerniente a su innegable carácter normativo, coincidimos con García de Enterría (1985) quien sostiene torna en inválidas a las normas inferiores que la contradigan[5]. De allí que, según él, la Constitución se ha convertido en un documento plenamente jurídico; ha dejado de ser un mero concepto ideal parecido a un catálogo de recetas políticas de carácter vagamente obligatorio en el cual la ciencia política tenía más importancia que el Derecho.[6]

Por ende, si la Constitución es *lex legis* –norma de mayor jerarquía en el Ordenamiento Jurídico– y, al mismo tiempo, *norma normarum* –principal fuente del Derecho que, a su vez, delimita el sistema de

---

[2] De Otto, I. (1995) *Derecho constitucional. Sistema de fuentes* (p 22). Barcelona: Ariel.

[3] Böckenförde, E. (2000). *Estudios sobre el Estado de Derecho y la democracia*. (p. 159)

[4] Tribunal Constitucional (2003). Fundamento 2 de la sentencia emitida en el Exp. 14-2003-AI/TC. Recuperado de: https://tc.gob.pe/jurisprudencia/2003/00014-2003-AI.html.

[5] García de Enterría, E. (1985). *La Constitución como norma y el Tribunal constitucional* (p. 61) Madrid: Civitas.

[6] García de Enterría, E. (1985). *La Constitución como norma y el Tribunal constitucional.* (p. 30-31). Madrid: Civitas SA.

fuentes del Derecho–; la validez formal y material del Derecho *infra-constitucional* se encuentra subordinada al respeto del contenido material y axiológico de la misma.

De este modo, lo constitucional entra, como lo piensa Ferrajoli (2014), en la *"esfera de lo no decidible: esto es, lo que ninguna mayoría puede válidamente decidir"*[7]. Precisamente por ello, coincidimos plenamente con el maestro Zagrebelsky (1995), quien manifiesta que *"la ley, por primera vez en la época moderna, viene sometida a una relación de adecuación, y por tanto de subordinación, a un estrato más alto de derecho establecido por la Constitución"* (Zagrebelsky, G., 1995, p. 34)[8]. Ello, en propias palabras de Zagrebelsky, es una auténtica *"variación genética"*[9]; o, como lo califica Aguiló (2004): es un *"cambio de paradigma dentro de la cultura jurídica"*[10]. De este modo, como lo señala Comanducci (2016), el legicentrismo propio del modelo de Estado decimonónico es reemplazado por la omnipresencia de la Constitución, que informa por sí misma a todo el sistema.[11]

2. Los derechos fundamentales

De acuerdo con Peces-Barba (1999), los derechos fundamentales son las normas básicas del ordenamiento jurídico, en la medida en que permiten al titular de los mismos desarrollar autónomamente todas sus potencialidades en sociedad; en consecuencia, están conformados por una moralidad elemental que emerge de la dignidad humana, y, al mismo tiempo, por una juridicidad básica. Consecuentemente,

---

[7] Ferrajoli, L. (2014). *La democracia a través de los derechos.* (p.9) Madrid, Trotta, trad. *Perfecto Andrés Ibáñez*.

[8] Zagrebelsky, G. (2016). *El derecho dúctil. Ley, derechos, justicia*. (p.34) Madrid: Trotta.

[9] Zagrebelsky, G. (1995). p. 33.

[10] AGUILÓ. J. (2004). *La Constitución del Estado Constitucional* (p. 9). Lima-Bogotá: Palestra-Temis,

[11] Comanducci, P. (2016). *Estudios sobre Constitución y derechos fundamentales*. (p. 32) México: Instituto de Estudios Constitucionales del Estado de Querétaro.

tienen un presupuesto ético basado en la dignidad humana y, a la vez, un componente jurídico, los cuales son inescindibles[12]. Nuestro Tribunal Constitucional (2005) en la sentencia emitida en el Exp. 1417-2005-PA/TC ha hecho suya esa definición, la misma que también hacemos nuestra.

En un momento posterior, el Tribunal Constitucional (2006) complementó dicha idea en el fundamento 30 de la sentencia emitida en el Exp. 30-2005-AI/TC en los siguientes términos:

> Los derechos fundamentales son la materialización del principio democrático en su faz fundacional al interior del Estado social y democrático de derecho, queda evidenciado cuando, sin perjuicio del reconocimiento expreso de una amplia gama de derechos fundamentales, el artículo 3° de la Constitución, además de la dignidad humana, reconoce a la soberanía popular y al Estado democrático como sus fuentes legitimadoras.[13]

Siendo ello así,

> la Constitución (es) la expresión jurídica de la soberanía popular, ésta otorga a aquélla su fundamento y razón de existencia, por lo que una Constitución sólo es identificable como tal en la medida de que se encuentre al servicio de los derechos fundamentales del pueblo.[14]

A pesar de suscribir lo antes expuesto, consideramos necesario añadir lo señalado por el profesor Pérez Luño (1991), quien, al respecto, manifiesta que los derechos fundamentales son la evolución más

---

[12] Peces-Barba, G (1999). *Curso de Derechos Fundamentales. Teoría General.* Madrid: Universidad Carlos III de Madrid. (p. 37).

[13] Tribunal Constitucional (2006). Fundamento jurídico 30 de la sentencia emitida en el Exp. 30-2005-AI/TC. Recuperado de: https://www.tc.gob.pe/jurisprudencia/2006/00030-2005-AI.pdf.

[14] Tribunal Constitucional (2006). Fundamento jurídico 30 de la sentencia emitida en el Exp. 30-2005-AI/TC. Recuperado de: https://www.tc.gob.pe/jurisprudencia/2006/00030-2005-AI.pdf.

avanzada de los derechos naturales[15], en la medida en que se fundan en un orden objetivo y universal de una axiología ontológica que es anterior a los mismos[16]. En todo caso, más allá de cualquier conceptualización, convergemos plenamente con Bobbio (1991) y Comanducci (2016), quienes, en líneas generales, indicaron que, en la actualidad, más debe importarnos cómo garantizarlos que cómo fundamentarlos[17] [18].

3. Los procesos constitucionales como herramientas para la salvaguarda de la supremacía constitucional

Como bien lo describe el profesor Pérez Royo (2012):

> Si los hombres, como escribió Madison en *El Federalista,* fueran ángeles y no hubiera enfrentamientos entre ellos, el Derecho no existiría. Habría paz "sin sujeción", como dijo Hobbes en el *Leviathan.* El Derecho es, por tanto y al mismo tiempo, el resultado de un profundo conocimiento y de una profunda desconfianza en la condición humana. No se trata de algo natural y espontáneo, sino de todo lo contrario. Es lo más antinatural y antiespontáneo que existe en las sociedades humanas. Es un artificio diseñado por la sociedad para neutralizar los impulsos naturales ("el ansia de poder y más poder que solo cesa con la muerte", del que hablaba Hobbes), que conducen a enfrentamientos de unos contra los otros. Natural es, pues, la aspiración humana a la justicia. Pero artificial el instrumento a través del cual se hace efectiva en la vida en sociedad.[19]

Precisamente por lo antes glosado, convergemos con Guastini (2001), quien ha indicado lo siguiente: *"hay que disponer los mecanismos*

---

[15] Pérez Luño, A. (1991). *Los Derechos Fundamentales.* (p. 43) Madrid: Tecnos.

[16] Pérez Luño, A. (1991). *Los Derechos Fundamentales.* (p. 51)

[17] Bobbio, N. (1991). (p. 63).

[18] Comanducci, P. (2016). *Estudios sobre Constitución y derechos fundamentales.* (p. 83) México DF: Instituto de Estudios Constitucionales del Estado de Querétaro.

[19] Pérez Royo, J. (2012). *Curso de Derecho constitucional* (p. 13). Madrid: Marcial Pons.

necesarios para hacer valer esa supremacía en los hechos, pues de otra manera la supremacía se queda como un elemento simplemente retórico"[20] y con Castillo Córdova (2007) quien refiere, con justa razón, que si la Constitución no viene acompañada de mecanismos que vigilen su vigencia efectiva; es una Constitución herida de muerte.[21]

En ese orden de ideas, consideramos los procesos constitucionales no son otra cosa que mecanismos establecidos en la propia Constitución destinados a garantizar, en la práctica, la pregonada supremacía constitucional. De lo contrario, las cláusulas constitucionales serían netamente nominales, esto es, se quedarían en el papel. Y es que, como en su momento lo señaló Siéyes (1993), si la Constitución no es un cuerpo de normas de carácter obligatorio; simple y llanamente no es nada".[22]

En esa lógica, el Tribunal Constitucional (2006), en el fundamento 8 de la sentencia emitida en el Exp. 23-2005-PI/TC, ha señalado lo siguiente:

> Los "derechos fundamentales " y los "procesos para su protección" se han instituido como institutos que no pueden entenderse de modo aislado, pues tales derechos sólo podrían "realizarse" en la medida en que cuenten con mecanismos " rápidos", "adecuados" y "eficaces" para su protección. Así, a los derechos fundamentales, además de su condición de derechos subjetivos del más alto nivel y, al mismo tiempo, de valores materiales de nuestro ordenamiento jurídico, les es consustancial el establecimiento de mecanismos encargados de tutelarlos, pues es

[20] Guastini,R. (2001). *Estudios de Teoría Constitucional* (p.18) México DF: Fontamara.

[21] Castillo Córdova, L. (2007). *La inexistencia de ámbitos exentos de vinculación a la Constitución*. (p.20). Recuperado de: https://pirhua.udep.edu.pe/bitstream/handle/11042/2071/Inexistencia_ambito_extentos_vinculacion_constitucion.pdf?sequence=1&isAllowed=y

[22] Sieyès, Enmanuel (1993). *"Opinión de Sieyès sobre las atribuciones y la organización de la Jury Constitutionnaire propuesta el 2 del termidor",* en Escritos Políticos de Sieyès. Introducción, estudio preliminar y compilación de David Pantoja Morán, Fondo de Cultura Económica, México, 1993, p. 258.

> evidente que derechos sin garantías no son sino afirmaciones programáticas, desprovistas de valor normativo. Así, los derechos fundamentales y los procesos que los tutelan se constituyen en el presupuesto indispensable para un adecuado funcionamiento del sistema democrático y en el instrumento concretizador de los valores, principios y derechos constitucionales.[23]

Atendiendo a ello, consideramos que el Derecho constitucional y, más concretamente, la Constitución es necesario el punto de partida del Derecho Procesal Constitucional. Aquella idea, en nuestra opinión, nos obliga a distanciarlo del Derecho procesal. Y, a su vez, exige que la interpretación del Código Procesal Constitucional se efectúe *desde* de la Constitución, a fin de que los procesos constitucionales cumplan su razón de ser. En relación a esto último, somos de la opinión que su finalidad es netamente instrumental: salvaguardar la supremacía normativa.

En consecuencia, la lógica del Derecho procesal –cimentada en la idea de igualdad de armas entre litigantes que discuten pretensiones disponibles de acuerdo con su propia autodeterminación personal– no puede ser aplicada sin matices a los procesos constitucionales, pues la aplicación de las disposiciones del Código Procesal Constitucional no puede realizarse prescindiendo del informalismo, pues, como bien lo indicó el Tribunal Constitucional (2005), en el fundamento 7 de la sentencia emitida en el Exp. 5-2005-PCC/TC, *"en ningún caso, la supremacía de la Constitución y la vigencia efectiva de los derechos constitucionales (artículo II del Título Preliminar del CPConst) quede subordinada al respeto de las formas por las formas"*[24]. Asimismo, el referido código tampoco puede ser aplicado al margen del principio de socialización,

[23] Tribunal Constitucional (2006). Fundamento jurídico 8 de la sentencia emitida en el Exp. 23-2005-PI/TC. Recuperado de: https://www.tc.gob.pe/jurisprudencia/2006/00023-2005-AI.html

[24] Tribunal Constitucional (2005). Fundamento jurídico 7 de la sentencia emitida en el Exp. 5-2005-CC/TC. Recuperado de: https://www.tc.gob.pe/tc/private/adjuntos/cec/gaceta/gaceta/jurisprudencia/00005-2005-CC.html

que obliga al juez constitucional a desmarcarse de una posición equidistante de las partes cuando, al evaluar lo que efectivamente acaece en la realidad, advierte una manifiesta desigualdad que, en los hechos, materialice una transgresión constitucional.

Así las cosas, cabe concluir, en concordancia con lo previamente expuesto, que la supremacía constitucional se reduce a unas lindas palabras si no va de la mano con los procesos constitucionales encargados de garantizar por, un lado, el carácter normativo de la misma, y, de otro lado, la salvaguarda de los derechos fundamentales. Tal clasificación acogida por la doctrina nacional a partir de lo expresamente previsto en el artículo II del Título Preliminar del Código Procesal Constitucional que dispone lo siguiente:

> Artículo II.- Fines de los Procesos Constitucionales
>
> Son fines esenciales de los procesos constitucionales garantizar la primacía de la Constitución y la vigencia efectiva de los derechos constitucionales.

Empero, tal clasificación no deja de ser relativa, porque en el marco de un proceso de control de constitucionalidad abstracto resulta viable salvaguardar derechos fundamentales. Y, al revés, en un proceso de *hábeas data,* por ejemplo, es posible enmendar una violación objetiva a la Constitución, lo que sucede cuando es declarada fundada y, como consecuencia de esa estimación, se orden la entrega de la documentación requerida, pues aquella inicial negativa afecta a la comunidad en su conjunto.

4. El ámbito de protección del proceso de *hábeas data*

El *hábeas data* es un proceso constitucional regulado en el numeral 3 del artículo 200 de la Constitución. De acuerdo con el texto constitucional, tiene por objeto la salvaguarda, por un lado, del derecho fundamental de acceso a la información pública que ha sido contemplado en el inciso 5 del artículo 2 de la Constitución, y, de otro lado, del derecho fundamental a la autodeterminación informativa que ha

sido previsto en el inciso 6 del artículo 2 de la Constitución. Por ende, la procedencia del mismo se encuentra subordinada a que el demandante se sustente su reclamo en una posición *iusfundamental* amparada por el contenido constitucionalmente tutelado de cualquiera de los mencionados derechos fundamentales. Sobre el particular, el Tribunal Constitucional (2014) el numeral 2 del fundamento 6 del auto expedido en el Exp. 2988-2013-PA/TC ha indicado lo siguiente:

> (…) luego de analizado el ámbito protegido del derecho, debe determinarse si lo alegado en la demanda (en la pretensión, en los hechos descritos) resulta subsumible en el ámbito normativo del derecho invocado, describiéndose a estos efectos quién es el titular de dicho derecho (sujeto activo), el obligado (sujeto pasivo) y la concreta obligación iusfundamental.[25]

En ese sentido, consideramos importante delimitar los contornos del contenido constitucionalmente protegido de ambos derechos fundamentales.

4.1. El Derecho de acceso a la Información Pública.

De conformidad con lo indicado en el fundamento 7 de la sentencia dictada en el Exp. 01797-2002-HD/TC, el Tribunal Constitucional (2003) ha sido explícito en reconocer que dicho derecho fundamental constituye *"una modalidad o concreción del derecho de petición"*[26]. Sin embargo, no puede soslayarse que en fundamento 4 de la sentencia recaída en el Exp. 1071-1998-HD/TC, el Tribunal Constitucional (1999) precisó que *"la Constitución le ha querido brindar un tratamiento particularizado y también un medio de tutela distinto, como en efecto se*

[25] Tribunal Constitucional (2014). Fundamento jurídico 6 de la resolución emitida en el Exp. 2988-2013-P/TC. Recuperado de: https://www.tc.gob.pe/jurisprudencia/2014/02988-2013-AA.html

[26] Tribunal Constitucional (2003). Fundamento jurídico 7 de la resolución emitida en el Exp. 1797-2002-HD/TC. Recuperado de: https://www.tc.gob.pe/jurisprudencia/2003/01797-2002-HD.html

ha previsto al incorporar como uno de los derechos protegidos mediante el hábeas data".[27]

En nuestra opinión, dicho derecho fundamental garantiza el derecho de cualquier persona a exigir sin expresión de causa la entrega oportuna de toda aquella información que califique como pública, previo pago del costo que suponga la absolución de tal requerimiento, salvo que la misma comprometa otro derecho fundamental o algún otro bien jurídico de relevancia constitucional, o, se encuentre en alguna de las restricciones excepcionales contempladas en el Texto Único Ordenado de la Ley 27806, Ley de Transparencia y Acceso a la Información Pública aprobado por Decreto Supremo 21-2019-JUS, las que básicamente se circunscriben a las que califican como: (i) secreta –artículo 15–; (ii) reservada –artículo 16–; o, (iii) confidencial –artículo 17–, pues, al igual que el resto de derechos fundamentales, no es absoluto.

En todo caso, lo realmente trascendente para determinar si califica como información pública es examinar su verdadera naturaleza –la que debe encontrarse ligada al manejo de *res publica*–, no evaluar dónde ella se encuentra ni tampoco quién la ha financiado. Ciertamente, existen escenarios en los que, por ejemplo, determinados particulares deber ser reputados como sujetos pasivos del mencionado derecho, como ocurre cuando se requiere a una empresa privada que brinda un servicio público información relacionada a las tarifas de lo que cobra a los usuarios, pues aquella documentación es trascendente para encontrarse informado sobre el manejo de la *res publica.* En relación a esto último, el Tribunal Constitucional (2009) ha señalado en el fundamento 3 de la sentencia proferida en el Exp. 4912-2018-PHD/TC, que la misma *"resulta esencial para que exista una opinión pública verdaderamente libre que pueda*

[27] Tribunal Constitucional (1999). Fundamento jurídico 4 de la resolución emitida en el Exp. 1071-1998-HD/TC. Recuperado de https://www.tc.gob.pe/jurisprudencia/1999/01071-1998-HD.html

fiscalizar adecuadamente la conducta de los gobernantes"[28]. Del mismo modo, el Tribunal Constitucional (2006) en el fundamento 3 de la sentencia emitida en el Exp. 7440-2005-PHD/TC, ha señalado que, en la práctica, dicho derecho fundamental *"permite monitorear y controlar la gestión pública"*[29]. De este modo, la difusión de esa información permite una verdadera participación ciudadana, la que es necesaria para la consolidación de la democracia en el marco de una sociedad abierta.

Precisamente por ello, el principio de máxima divulgación impone la presunción de que la información pública es de acceso libre, restringiendo las excepciones a lo estrictamente indispensable, razón por la cual, la destrucción de tal presunción se encuentra supeditada a la existencia de una motivación cualificada. Al respecto, el fundamento 6 de la sentencia dictada en el Expediente 3035-2012-PHD/TC, indicó lo siguiente: *"la destrucción de tal presunción requiere de una motivación cualificada en atención al carácter restrictivo con que dichas excepciones deben ser interpretadas"*.[30]

No obstante, debe tenerse presente que el Tribunal Constitucional (2009), en el fundamento 4 de la resolución dictada en el expediente 2893-2008-PHD/TC ha precisado que la entrega de la información requerida se encuentra subordinada a que exista o se halle en poder del emplazado, quien tiene la obligación de "proveerla de manera oportuna, incondicional y completa"[31], porque de nada sirve que la

[28] Tribunal Constitucional (2009). Fundamento jurídico 3 de la resolución emitida en el Exp. 4912-2008-PHD/TC. Recuperado de: https://tc.gob.pe/jurisprudencia/2009/04912-2008-HD.pdf

[29] Tribunal Constitucional (2006). Fundamento jurídico 3 de la resolución emitida en el Expediente 7440-2005-PHD/TC. Recuperado de https://tc.gob.pe/jurisprudencia/2006/07440-2005-HD.pdf

[30] Tribunal Constitucional (2013). Fundamento jurídico 6 de la resolución emitida en el Expediente 3035-2012-PHD/TC. Recuperado de: https://www.tc.gob.pe/jurisprudencia/2013/03035-2012-HD.pdf

[31] Tribunal Constitucional (2009). Fundamento jurídico 4 de la resolución emitida en el Exp. 2893-2008-PHD/TC. Recuperado de: https://www.tc.gob.pe/jurisprudencia/2009/02893-2008-HD%20Resolucion.html

documentación brindada no cumpla con tales características. Empero, a fin de evitar que las entidades demandadas se excusen en la pérdida de la misma, el Tribunal Constitucional (2006) en el fundamento 7 de la sentencia recaída en el Exp. 07440-2005-PHD/TC también obliga a entregar toda aquella información "*que, sin poseerla físicamente, le es atribuible por razón del desempeño propio de sus funciones o de su posición privilegiada frente al requerimiento que se le hace*"[32]. De lo contrario, sería muy fácil que, de mala fe, algunas las entidades puedan eximirse de cumplir con divulgar esa información apelando precisamente a su falta de diligencia o a la mera renuencia a ser transparentes, lo cual es inaceptable debido a que su propia desidia o mala fe no puede relevarla del cumplimiento de esa obligación.

Sin embargo, no ocurre lo mismo con la posición del Tribunal Constitucional (2010) plasmada en el fundamento 4 de la resolución expedida en el Exp. 2512-2009-PHD/TC, que, al delimitar el contenido constitucionalmente protegido del derecho fundamental de acceso a la información pública, ha excluido del ámbito normativo del mismo a *"la obligación por parte de la entidad pública de producir información, sino solo de poner al alcance del ciudadano información preexistente a la solicitud"*[33], dado que algunas entidades han tratado de desligarse de la obligación de acopiar la información que se les exige, excusándose en que lo exigido es conlleva la producción, cuando ello no es así. Al respecto, consideramos que estos casos, basta con brindar información relativa a lo objetivamente obrante en sus bases de datos.

Resulta inadmisible, entonces, que el mero traslado al requirente de aquello que consta en sus archivos sea improcedente. En realidad,

[32] Tribunal Constitucional (2006). Fundamento jurídico 7 de la resolución emitida en el Exp. 7440-2005-PHD/TC. Recuperado de https://tc.gob.pe/jurisprudencia/2006/07440-2005-HD.pdf

[33] Tribunal Constitucional (2010). Fundamento jurídico 4 de la resolución emitida en el Exp. 2512-2009-PHD/TC. Recuperado de: https://www.tc.gob.pe/jurisprudencia/2010/02512-2009-HD%20Resolucion.html.

lo que resulta improcedente es requerir la emisión de un juicio de valor sobre aquella información, no que el acopia de la misma no sea sencillo. También resulta inviable, conforme a lo indicado por el Tribunal Constitucional (2014) en el fundamento 7 de la sentencia emitida en el Exp. 4203-2012-PHD/TC, exigir que la emplazada produzca *"descargos ante determinados cuestionamientos de los particulares"*.[34]

Lo antes expuesto, además, es congruente con la dimensión objetiva del citado derecho fundamental que exige, entre otras cosas, que el Estado promueva el goce efectivo del mismo. De ahí que todas aquellas prácticas tendientes a desincentivar el efectivo ejercicio del mismo se encuentran vedadas. Por ejemplo, en el fundamento 8 de la sentencia emitida en el Exp. 2512-2013-PHD/TC, el Tribunal Constitucional (2014) consideró que exigir al solicitante residente en el interior del país formular su pedido en la capital constituye una conculcación subrepticia del mencionado derecho[35]. Otra práctica vedad es la advertida por el Tribunal Constitucional (2014) en el fundamento 6 de la sentencia emitida en el Exp. 4203-2012-PHD/TC, consistente en requerir al ciudadano que *"especifique, puntual y concretamente, qué documentos son los que peticiona de antemano, resulta a todas luces irrazonable por una cuestión de asimetría informativa"*.[36]

Igualmente, en el fundamento 10 de la sentencia emitida en el Exp. 5216-2015-PHD, este Tribunal Constitucional (2018) señaló que, conforme a la regulación expresa del derecho fundamental de acceso a la información pública, el costo de reproducción es un tributo

[34] Tribunal Constitucional (2014). Fundamento jurídico 7 de la sentencia emitida en el Exp. 4203-2012-PHD/TC. Recuperado de: https://tc.gob.pe/jurisprudencia/2014/04203-2012-HD.pdf

[35] Tribunal Constitucional (2014). Fundamento jurídico 8 de la sentencia emitida en el Exp. 2512-2013-PHD/TC. Recuperado de https://www.tc.gob.pe/jurisprudencia/2014/02512-2013-HD.html

[36] Tribunal Constitucional (2014). Fundamento jurídico 6 de la sentencia emitida en el Exp. 4203-2012-PHD/TC. Recuperado de: https://tc.gob.pe/jurisprudencia/2014/04203-2012-HD.pdf

de la subespecie tasa[37]; por lo tanto, no puede ser superior al costo efectivo del mismo. Precisamente por ello, en el fundamento 6 de la sentencia dictada en el Exp. 4859-2012-PHD/TC, el Tribunal Constitucional (2014) ha sido concluyente en señalar que la entidad emplazada se encuentra *"impedida de lucrar con las reproducciones que proporciona"*.[38]

4.2. El derecho a la autodeterminación informativa

En opinión del Tribunal Constitucional (2008), el derecho fundamental a la autodeterminación informativa básicamente

> protege al titular del mismo frente a posibles abusos o riesgos derivados de la utilización de los datos, brindando al titular afectado la posibilidad de lograr la exclusión de los datos que considera "sensibles" y que no deben ser objeto de difusión ni de registro; así como le otorga la facultad de poder oponerse a la transmisión y difusión de los mismos.

En otras palabras: busca aminorar el innegable riesgo de los bancos de datos utilicen su información personal –no solamente la personalísima, por lo que se distancia de los derechos fundamentales a la intimidad y privacidad– con fines subalternos. Para tal efecto, faculta a su titular controlar aquella información que le es propia, razón por la cual, es necesario que el titular del mismo demuestre, aunque sea mínimamente, tal titularidad. No se aplican, como resulta lógico, las reglas del derecho fundamental de acceso a la información pública ni mucho menos el principio de máxima divulgación.

---

[37] Tribunal Constitucional (2018). Fundamento jurídico 10 de la sentencia emitida en el Exp. 5216-2015-PHD/TC. Recuperado de: https://www.tc.gob.pe/jurisprudencia/2018/05216-2015-HD.pdf

[38] Tribunal Constitucional (2014). Fundamento jurídico 6 de la sentencia emitida en el Exp. 4759-2012-PHD/TC. Recuperado de: https://tc.gob.pe/jurisprudencia/2014/04759-2012-HD.pdf

De ahí que, en palabras de Castillo Córdova (2012), dicho derecho fundamental tiene por objeto neutralizar ese riesgo[39]. Para tal efecto, se faculta al titular de los mismos a tener un control real sobre sus datos personales. En ese entendido, el Tribunal Constitucional (2003) ha delimitado al derecho fundamental a la autodeterminación informativa en el fundamento 4 de la sentencia proferida en el Exp. 1797-2002-HD/TC de la siguiente manera:

> comprende, en primer lugar, la capacidad de exigir jurisdiccionalmente la posibilidad de acceder a los registros de información, computarizados o no, cualquiera que sea su naturaleza, en los que se encuentren almacenados los datos de una persona. Tal acceso puede tener por objeto que se permita conocer qué es lo que se encuentra registrado, para qué y para quién se realizó el registro de información así como la (o las) persona(s) que recabaron dicha información. En segundo lugar, el hábeas data puede tener la finalidad de agregar datos al registro que se tenga, ya sea por la necesidad de que se actualicen los que se encuentran registrados, o bien con el fin de que se incluyan aquellos no registrados, pero que son necesarios para que se tenga una cabal referencia sobre la imagen e identidad de la persona afectada. Asimismo, con el derecho en referencia, y en defecto de él, mediante el hábeas data, un individuo puede rectificar la información, personal o familiar, que se haya registrado; impedir que esta se difunda para fines distintos de aquellos que justificaron su registro o, incluso, tiene la potestad de cancelar aquellos que razonablemente no debieran encontrarse almacenados.[40]

En un momento posterior, en el fundamento 5 de la sentencia emitida en el Exp. 1623-2016-PHD/TC, el Tribunal Constitucional (2018) amplió el ámbito de aplicación del citado derecho fundamental,

[39] Castillo Córdova, L (2012). La finalidad del derecho de autodeterminación informativa y su afianzamiento a través de hábeas data. Recuperado de: https://sumaciudadana.wordpress.com/2012/07/31/la-finalidad-del-derecho-deautodeterminacion-informativa-y-su-afianzamiento-a-traves-del-hábeas-data/

[40] Tribunal Constitucional (2003). Fundamento jurídico 4 de la sentencia emitida en el Exp. 1797-2002-HD/TC. Recuperado de: https://tc.gob.pe/jurisprudencia/2003/01797-2002-HD.pdf

al entender que garantiza a su titular hacer uso de la información que existe sobre él o ella, ya sea que la información se encuentre almacenada o en disposición de entidades públicas, o sea de carácter privado[41]. Así pues, a diferencia del derecho fundamental de acceso a la información pública, el titular del derecho a la autodeterminación informativa tiene un control pleno de la información que le pertenece, tanto es así que en determinados escenarios tiene el derecho a fiscalizar tanto el acopio como el mantenimiento de dichos datos personales, lo que no resulta procedente tratándose del derecho fundamental de acceso a la información pública.

Finalmente, cabe precisar que si bien a nivel constitucional, no existe una regulación expresa sobre cómo calcular el costo que debe asumir el solicitante; el Tribunal Constitucional (2018) en el fundamento 12 de la sentencia emitida en el Exp. 5216-2015-PHD/TC ha señalado que tratándose del Estado, ese pago tiene la calidad de tasa[42]; por ende, debe limitarse al costo efectivo incurrido en su atención. Empero, no ocurre lo mismo cuando el sujeto pasivo de la posición *iusfundamental* es un particular, pues el artículo 26 de la Ley 29733, Ley de Protección de Datos Personales, alude a una contraprestación que se sujeta a las normas que se expidan al respecto, lo que abre la puerta que pueda cobrarse un valor de mercado, pues precisamente los bancos de datos son negocios particulares, que en virtud de su derecho fundamental a la libertad de empresa tienen la potestad, en principio, de fijar sus propias tarifas, lo cual, eventualmente puede ser objeto de control en sede constitucional.

[41] Tribunal Constitucional (2018). Fundamento jurídico 5 de la sentencia emitida en el Exp. 1623-2016-PHD/TC. Recuperado de: https://tc.gob.pe/jurisprudencia/2018/01623-2016-HD.pdf

[42] Tribunal Constitucional (2018). Fundamento jurídico 12 de la sentencia emitida en el Exp. 5216-2015-PHD/TC. Recuperado de: https://www.tc.gob.pe/jurisprudencia/2018/05216-2015-HD.pdf

5. Consideraciones Finales

A diferencia del resto de procesos constitucionales destinados a la salvaguarda de derechos fundamentales, los procesos de hábeas data tienen el más alto índice de pronunciamientos de fondo, lo cual se debe, entre otras cosas, a las líneas jurisprudenciales claras que el Tribunal Constitucional ha expedido. Pero, sobre todo, tratándose del derecho de acceso a la información pública, a la enquistada idea en la Administración Pública de que la entrega de lo requerido es, en cierta medida, discrecional, cuando ello no es así.

Aunque la Constitución ha plasmado, a grandes rasgos, los alcances del derecho fundamental al acceso a la información pública, no ha ocurrido lo mismo con el derecho fundamental a la autodeterminación informativa, que básicamente ha sido regulado por el Código Procesal Constitucional (cfr. numeral 2 de su artículo 61), el cual ha positivizado los contornos que la jurisprudencia del Tribunal Constitucional ha delimitado. No obstante, en relación a este último aún queda mucho por desarrollar. En todo caso, la presente entrega tiene por finalidad mapear, en líneas generales, cómo el Tribunal Constitucional ha venido trabajando estos derechos fundamentales.

EL DERECHO DE ACCESO A LA INFORMACIÓN PÚBLICA.

Alcances y límites

✍ Heidi Soraya Cárdenas Arce*

1. Definición y alcances

El derecho de acceso a la información pública es un derecho fundamental que permite ejercer la vigilancia ciudadana de tal manera que todo acto de gobierno se transparente y se encuentre sometido a escrutinio público.

A través de este derecho se puede acceder a toda información contenida en documentos escritos, fotografías, grabaciones o cualquier otro formato que haya sido creado o se encuentre en posesión de una entidad pues se presume pública, así pues, el derecho de acceso a la información pública se basa en el principio de máxima publicidad y solo puede denegarse, con la debida fundamentación, la información calificada como secreta, reservada o confidencial que son las excepciones establecidas por ley y cuya aplicación se realiza de manera restrictiva.

* Abogada por la Unifé, Magister en Administración y Doctora en Derecho y Ciencias Políticas de la Universidad Nacional Mayor de San Marcos. Ha sido miembro del Consejo Directivo de la Superintendencia Nacional de Fiscalización Laboral – SUNAFIL y Secretaria General encargada del Seguro Social de Salud – Essalud. Actualmente se desempeña como Jefe de la Oficina de Servicios de la Información de la Secretaría General del Seguro Social de Salud - Essalud.

A decir del Tribunal Constitucional, la información pública es "un auténtico bien público o colectivo que ha de estar al alcance de cualquier individuo, no sólo con el fin de posibilitar la plena eficacia de los principios de publicidad y transparencia de la Administración Pública, en los que se funda el régimen republicano, sino también como un medio de control institucional sobre los representantes de la sociedad" (Sentencia recaída en el Exp. N° 04912-2008-PHD/TC).

El derecho a la información es reconocido por organismos internacionales como parte integrante del derecho a la libertad de expresión. En ese sentido, se han desarrollado cuerpos normativos de alcance internacional como la "Declaración de Derechos del Hombre y del Ciudadano" de 1789, la "Declaración Universal de Derechos Humanos" en 1948, el "Pacto Internacional de Derechos Civiles y Políticos" de 1966, la "Convención Americana sobre Derechos Humanos" de 1969 y en el 2010 por la Ley Modelo de acceso a la información pública expedida por la organización de Estados Americanos. En América Latina son varios los países que han desarrollado normas para que los ciudadanos puedan acceder a la información y en el 2006 la "sentencia de la Corte Interamericana de Derechos Humanos recaída en el Caso Claude Reyes y otros Vs. Chile" marcó un hito para el derecho de acceso a la información pública, debido a que, no solo determinó que se habían violado derechos fundamentales como el derecho al acceso a la información y el derecho a la libertad de expresión, sino que también reconoció que el derecho a la información es un derecho fundamental.

En el Perú, el derecho de acceso a la información pública se encuentra regulado en el inciso 5° del artículo 2° de la Constitución Política del Perú que señala que toda persona tiene derecho a solicitar sin expresión de causa la información que requiera de cualquier entidad pública en el plazo legal y con el costo que suponga el pedido. Pero, la solicitud de información no implica la obligación de las entidades de la Administración Pública de crear o producir información con la que no cuenten o no tengan obligación de contar al momento de efectuarse el pedido, tampoco permite que los solicitantes exijan a las entidades que efectúen evaluaciones o análisis de la información que posean.

En ese sentido, el deber de las entidades públicas comprende la obligación de brindar la información que obra en su poder de manera *«cierta, actual, precisa y completa»*, es decir, una entrega parcial y falsa no satisface las exigencias constitucionales del derecho de acceso a la información pública.

Así pues, se trata de un *«derecho instrumental»,* pues a través de su ejercicio se permite satisfacer otros derechos de las personas porque permite a los ciudadanos definir ciertas circunstancias que pueden afectar su vida cotidiana y desarrollar la capacidad para tomar decisiones informadas y acciones concretas con el fin de mejorar sus condiciones de vida. A través de la información adecuada y oportuna se pueden mitigar riesgos de manera efectiva y promover mejoras en los servicios públicos básicos tales como la salud, la educación, la seguridad pública (OEA, 2009, pág. 10)

El acceso a la información pública es un elemento clave de la gestión pública, ha sido considerado una herramienta fundamental para el control ciudadano del funcionamiento del Estado y la gestión pública (OEA, 2009, pág. 13).

El pleno ejercicio del derecho de acceso a la información es una garantía indispensable para evitar abusos de los funcionarios públicos, promover la rendición de cuentas y la transparencia en la gestión estatal y prevenir la corrupción (Rivera, 2008).

En esa línea, el máximo intérprete de la Constitución ha señalado que *«el derecho de acceso a la información pública es consustancial a un régimen democrático»*. Por ello, su ejercicio *«contribuye a la formación de una opinión pública, libre e informada, éste tiene la condición de libertad preferida»* (Caso Wilo Rodríguez Gutierrez, 2003)

2. Dimensiones del Derecho de acceso a la información pública

Es preciso señalar que las mismas no han surgido de la legislación de la materia sino que provienen de la jurisprudencia vinculante publicada por el Tribunal Constitucional. Así, se puede mencionar lo siguiente:

2.1. Dimensión Individual

El Tribunal Constitucional, toma la postura de que el derecho ahora estudiado, posee una doble dimensión, así se hizo referencia en el expediente 1797-2002-HD/TC, caso Wilo Rodríguez (Fj. 10), donde se señaló lo siguiente:

> *"(...) se trata de un derecho individual, en el sentido que garantiza que nadie sea arbitrariamente impedido de acceder a la información que guarden, mantengan o elaboren las diversas instancias y organismos que pertenezcan al Estado, sin más limitaciones que aquellas que se han previsto como constitucionalmente legítimas. A través de este derecho se posibilita que los individuos, aisladamente considerados, puedan trazar, de manera libre, su proyecto de vida, pero también el pleno ejercicio y disfrute de otros derechos fundamentales. Desde esta perspectiva, (...) el derecho de acceso a la información se presenta como un presupuesto o medio para el ejercicio de otras libertades fundamentales, como puede ser la libertad de investigación, de opinión o de expresión, por mencionar alguna (...)".*

En el referido caso, se hace notoria la relevancia en el plano individual de este derecho, lo cual otorga al mismo una calidad de alta incidencia en aspectos no solo sociales, sino personales, protegiendo y garantizando el derecho de libre desarrollo de la persona.

2.2. Dimensión Colectiva

Sobre la dimensión colectiva, cabe mencionar la sentencia del Caso Wilo Rodríguez que obra en el expediente 1797-2002-HD/TC y que a fojas 11 señala que la dimensión colectiva permite que las personas puedan recibir la información pertinente, de manera completa y veraz en el marco de una sociedad democrática.

También es importante citar la sentencia del caso "*Julia Eleyza Arellano Serquén*" recaída en el Exp. 2579-2003-PDH/TC (Lambayeque), debido a que el máximo intérprete de la Constitución expresó que: "*el derecho de acceso a la información pública es consustancial a un régimen democrático*".

En la dimensión colectiva, se resalta este derecho como una herramienta legal, con la cual se otorga mayor seguridad jurídica de que las entidades públicas cumplan adecuadamente con sus funciones encomendadas, sin aprovecharse de su posición de poder, para cometer actos que contravengan la legalidad de sus funciones.

En suma, según esta jurisprudencia del Tribunal Constitucional, la información es un bien público y colectivo.

3. ¿Qué "no es acceso a la información pública"?

Toda solicitud de información formulada por un ciudadano se considera como una "solicitud de acceso a la información pública" y se atiende de acuerdo al procedimiento contemplado en la Ley 27806, pero existen algunos pedidos que no están contemplados en los alcances de esta Ley y son los siguientes:

- Las solicitudes de información formuladas por los Congresistas de la República que se rigen por el artículo 96 de la Constitución Política del Perú.
- Las solicitudes formuladas de información entre entidades públicas.
- Las solicitudes en el marco de un procedimiento TUPA.
- Las solicitudes vinculadas con el derecho que tienen las personas de acceder a información contenida en expedientes administrativos del que forman parte.

4. Desarrollo normativo nacional

El derecho de acceso a la información pública cuenta con una protección nacional que ha ido evolucionando con el pasar de los años:

- **La Constitución de 1979** no reguló de manera expresa el derecho de acceso a la información pública. Este derecho se encontraba tácitamente dentro del contenido del inciso 4 del artículo 2º.

- **La Constitución Política de 1993**, en su artículo 2°, inciso 5, fue la primera en incluir el derecho al acceso a la información pública dentro de la lista de derechos fundamentales. Establece que toda persona tiene derecho a solicitar sin expresión de causa la información que requiera y a recibirla de cualquier entidad pública, en el plazo legal, con el costo que suponga el pedido. Se exceptúan las informaciones que afectan la intimidad personal y las que expresamente se excluyan por ley o por razones de seguridad nacional.

- **La Ley N° 27806, modificada por la Ley N° 27927, y por la Ley N° 30934** que regulan las obligaciones, procedimientos, plazos, y todo lo vinculado con el ejercicio de este derecho fundamental incluidas las excepciones.

- **El Texto Único Ordenado de la Ley N° 27806 aprobado por Decreto Supremo N° 021-2019-JUS que deroga el Decreto Supremo N° 043-2003-PCM.**

- **El Reglamento de la Ley N° 27806 aprobado por Decreto Supremo N° 072-2003-PCM modificado por el Decreto Supremo N° 070-2013-PCM**, tiene por finalidad promover la transparencia de los actos del estado y garantizar el ejercicio del derecho fundamental de acceso a la información pública.

- **El Decreto Legislativo N° 1353, modificado por el Decreto legislativo N° 1416,** que crea la Autoridad Nacional de Transparencia y Acceso a la Información Pública.

- **El Decreto Supremo N° 019-2017-PCM,** que aprueba el Reglamento del Decreto Legislativo N° 1353, modificado por Decreto Supremo N° 007-2018-JUS y Decreto Supremo N° 011-2018-JUS.

5. Desarrollo normativo supranacional

La información, desde los inicios de la humanidad, ha sido determinante en el desarrollo humano tanto individual como en su desarrollo social. Los gobernantes en el transcurrir de la historia, han poseído poder en favor de contener información, debido a que, la información confiere, en cierto modo, un poder a la persona que la posea. Es por esa razón que la información, antiguamente, era considerada como un bien reservado al cual solamente algunos privilegiados tenían acceso.

Este derecho fundamental fue reconocido por primera vez en el mundo, mediante la Ley de Prensa de 1766 de Suecia, en la cual se incluye el derecho de acceso a la información. Esta ley, que forma parte de la constitución de Suecia, incluye la libertad de imprimir y difundir materiales sobre el gobierno, los tribunales y el parlamento, así como también reconoce que la libertad de prensa está supeditada al acceso a la información y establece que, para tal fin, "se debe permitir el libre acceso a todos los archivos".

También, este derecho fundamental fue de cierta manera reconocido en la "Declaración de Derechos del Hombre y del Ciudadano" de 1789, ya que, en esta se establece "que *Todos los Ciudadanos tienen el derecho de comprobar, por sí mismos o a través de sus representantes, la necesidad de la contribución pública, de aceptarla libremente, de vigilar su empleo y de determinar su prorrata, su base, su recaudación y su duración*", lo cual, proporciona de cierto modo un derecho a saber sobre el gasto de impuestos públicos, lo cual sin lugar a duda forma parte de la información que todo ciudadano tiene derecho de solicitar a las entidades públicas.

En 1946, la "Asamblea General de las Naciones Unidas", durante su primer período de sesiones, aprobó por unanimidad la Resolución N° 59, en la cual establece que la "Libertad de información es un derecho humano fundamental y es la piedra angular de todas las libertades a las que se consagran las Naciones Unidas".

En 1948, en el artículo 19 de la "Declaración Universal de Derechos Humanos" se estableció que "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".

Asimismo, el artículo 19 del "Pacto Internacional de Derechos Civiles y Políticos", adoptado por la Asamblea General de las Naciones Unidas reconoce el derecho de acceso a la información pública y dispone que toda persona tiene derecho a la libertad de expresión: "este derecho comprende la libertad de buscar, recibir y difundir informaciones toda índole".

La "Convención Americana sobre Derechos Humanos (Pacto de San José)" aprobada por Decreto Ley Nº 22231, entró en vigor en el Perú el 28 de julio de 1978 y establece en su artículo 13° que "toda persona tiene derecho a la libertad de pensamiento y de expresión".

En 1981, la Recomendación 81 del Comité de Ministros del Consejo Europeo estableció que "Toda persona que se encuentre dentro de la jurisdicción de un Estado miembro tendrá derecho a obtener, previa solicitud, información en poder de las autoridades públicas distintas de los órganos legislativos y judiciales; se deben proporcionar medios efectivos y apropiados para garantizar el acceso a la información; el acceso a la información no debe ser denegado debido a que la persona solicitante no tiene un interés en el asunto; el acceso a la información se proporcionará sobre la base de la igualdad; una autoridad pública que niegue el acceso a la información, deberá explicar las razones en que se basa la negativa".

Este derecho también se encuentra reconocido y protegido en el artículo 17 de la Convención de Derechos del Niño de 1989.

En el 2001, la "Carta Democrática Interamericana de la Asamblea General de la OEA", estableció, en su artículo 4, que "son componentes

fundamentales del ejercicio de la democracia, la transparencia de las actividades gubernamentales, la probidad, la responsabilidad de los gobiernos en la gestión pública, el respeto por los derechos sociales y la libertad de expresión y de prensa" lo cual nos muestra que el derecho de acceso a la información es necesario para fortalecer la transparencia de las entidades de la administración pública.

En el 2008, durante la X Conferencia Iberoamericana de Ministros de Administración Pública y Reforma del Estado, se aprueba la Carta Iberoamericana de Calidad en la Gestión Pública, la cual establece que los ciudadanos pueden solicitar y obtener información pública de interés general relacionada con los asuntos públicos.

En el 2010, la Organización de Estados Americanos expide una "Ley Modelo de acceso a la información pública", la cual, "establece la más amplia aplicación posible del derecho de acceso a la información que esté en posesión, custodia o control de cualquier autoridad pública. Esta ley se basa en el principio de máxima publicidad, de tal manera que cualquier información en manos de instituciones públicas sea completa, oportuna y accesible, sujeta a un claro y preciso régimen de excepciones, las que deberán estar definidas por ley y ser además legítimas y estrictamente necesarias en una sociedad democrática" (Consejo Permanente de la Organización de los Estados Americanos, 2010).

6. El rol de la Autoridad Nacional de Transparencia

El artículo 3° del Decreto Legislativo N° 1353, creó la "Autoridad Nacional de Transparencia y Acceso a la Información", rol que ejecuta el Ministerio de Justicia y Derechos Humanos a través de la Dirección General de Transparencia, Acceso a la Información Públicos y Datos Personales del Ministerio de Justicia y Derechos Humanos".

Esta Autoridad depende del Viceministro de Justicia y tiene como funciones previstas en el artículo 4° del Decreto Legislativo N° 1353 las de proponer políticas en materia de transparencia y acceso a la información pública, emitir directivas y lineamientos que sean necesarios para el

cumplimiento de las normas en el ámbito de su competencia, supervisar el cumplimiento de las normas en materia de transparencia y acceso a la información pública, absolver las consultas que las entidades o las personas jurídicas o naturales le formulen respecto de la aplicación de normas de transparencia y acceso a información pública, fomentar la cultura de transparencia y acceso a la información pública, elaborar y presentar el informe anual sobre los pedidos de acceso a la información pública y supervisar el cumplimiento de la actualización del Portal de Transparencia.

Por su parte, el artículo 6° del Decreto Legislativo N° 1353, creó el "Tribunal de Transparencia y Acceso a la Información Pública" que depende administrativamente del Despacho Ministerial del Ministerio de Justicia y Derechos Humanos y es la última instancia administrativa en materia de transparencia y "derecho al acceso a la información pública" a nivel nacional.

En el artículo 7° del Decreto Legislativo N° 1353, se establece principalmente como funciones de este Tribunal, las de resolver los recursos de apelación contra las decisiones de las entidades comprendidas en el artículo I del Título Preliminar de la Ley Nº 27444, Ley del Procedimiento Administrativo General, en materias de transparencia y acceso a la información pública con la que se agota la vía administrativa. Asimismo, resuelve, en última instancia administrativa, los recursos de apelación que interpongan los funcionarios y servidores públicos sancionados por el incumplimiento de las normas de transparencia y acceso a la información pública.

Adicionalmente, en el numeral 2) del artículo 10° del Reglamento del Decreto Legislativo 1353, modificado por Decreto Supremo N° 011-2018-JUS, se señala que el Tribunal tiene como funciones proponer mejoras a la normatividad en materia de transparencia y acceso a la información pública y resolver, en última instancia administrativa, los recursos de apelación que interpongan las personas jurídicas a las que se refiere el artículo 9 del Texto Único Ordenado de la Ley Nº 27806 sancionadas por el incumplimiento de este dispositivo legal.

En la experiencia comparada latinoamericana, encontramos como ejemplo de autoridades administrativas encargadas de resolver los conflictos que se susciten por vulneración del "derecho de acceso a la información pública", al Consejo para la Transparencia de Chile y al Instituto Federal de Acceso a la Información Pública de México que son órganos autónomos y especializados.

Luego de agotada la vía administrativa se puede recurrir en sede judicial a través del hábeas data para reclamar la protección del derecho de acceso a la información pública que procede contra cualquier autoridad, funcionario o persona, que vulnera este derecho fundamental.

Cabe indicar que, la Autoridad Nacional de Transparencia ha sido concebida como un órgano dependiente del Viceministerio de Justicia y al encontrarse separada de su Tribunal de Transparencia y Acceso a la Información Pública se ha generado una suerte de doble estructura pues por un lado tenemos un órgano encargado de promover y vigilar el cumplimiento de las normas de acceso a la información pública y de otro lado, tenemos a un Tribunal que resuelve todas aquellas discrepancias que giran en torno a esta materia. Ello genera falta de independencia de la Autoridad de Transparencia que incide sobre la adecuada protección del derecho de acceso a la información pública; por lo que es necesario modificar el marco normativo existente para dotar de autonomía en el ejercicio de sus funciones a la Autoridad Nacional en materia de Transparencia y acceso a la información y por ende, crear un organismo Técnico especializado, ente rector del Sistema Nacional de Transparencia concebido como un sistema funcional de acuerdo a la Ley Orgánica del Poder Ejecutivo. De tal forma, que el Sistema Nacional de Transparencia se encontraría a cargo de la "Autoridad Nacional de Transparencia" como ente Rector.

Ahora bien, además de la falta de independencia de la Autoridad, se considera importante realizar modificaciones a la norma a fin de que la potestad disciplinaria cumpla su objetivo. En ese sentido,

coincidimos con lo señalado por el Tribunal Constitucional en el sentido que *"una de las maneras de promover la eficacia de este derecho son las sanciones a los funcionarios y servidores públicos que obstruyan de cualquier modo la materialización del derecho de acceso a la información pública. Estas sanciones no son solo necesarias sino inherentes a la defensa y protección de los derechos fundamentales. Y es que con las sanciones a las conductas contrarias a los derechos fundamentales se pretende también desincentivarlas"* (Sentencia recaída en el Exp. N° 04912-2008-PHD/TC).

En ese sentido, se ha observado que el procedimiento disciplinario aplicable a funcionarios, servidores y ex servidores que incumplen las normas de transparencia y acceso a la información pública contemplado en el artículo 35 del Reglamento de la Ley de Transparencia y Acceso aprobado por Decreto Supremo N° 072-2003-PCM[1], modificado por Decreto Supremo N° 019-2017-JUS que se encuentra a cargo de cada entidad en primera instancia en esta materia y como segunda y última instancia administrativa el Tribunal de Transparencia conforme a lo establecido en el artículo 7.2 y 8 del Decreto Legislativo N° 1353[2], no ha venido funcionando toda vez que hasta el año 2017 no se ha aplicado

[1] "(…) El artículo 35 del Reglamento de la Ley de Transparencia y Acceso aprobado por Decreto Supremo N° 072-2003-PCM señala lo siguiente: 35.1 El procedimiento sancionador está a cargo de cada entidad. Las fases del procedimiento y las autoridades a cargo de éste, son las establecidas en el Reglamento General de la Ley Nº 30057, Ley del Servicio Civil, aprobado por Decreto Supremo Nº 040-2014-PCM.

35.2 El procedimiento se inicia de oficio por parte de la autoridad instructora, lo cual tiene como origen, su propia iniciativa o como consecuencia de orden superior, petición motivada de otros órganos o por denuncia de un ciudadano (…)".

[2] El artículo 7.2 del Decreto Legislativo señala como una de las funciones del Tribunal de Transparencia "Resolver, en última instancia administrativa, los recursos de apelación que interpongan los funcionarios y servidores públicos sancionados por el incumplimiento de las normas de transparencia y acceso a la información pública" y el artículo 8 que "el Tribunal puede confirmar, revocar o modificar en todos sus extremos la decisión adoptada por la entidad en el procedimiento administrativo sancionador (…) En caso la sanción impuesta por la entidad sea la destitución o inhabilitación, corresponde que el Tribunal se pronuncie mediante un informe que constituye prueba pre-constituida que será remitido al Tribunal del Servicio Civil, para que este resuelva la apelación".

ninguna sanción y en los dos últimos años se han reportado aproximadamente 15 casos sin que la Autoridad haya podido verificar *in situ* la veracidad de la información reportada por las entidades; por lo que, sería interesante fortalecer la actual estructura con la que cuenta la Autoridad Nacional de Transparencia y Acceso a la Información Pública para establecer un órgano de línea dentro de esta Autoridad que se constituya como órgano instructor y otro como órgano sancionador en primera instancia, de tal manera que sea el "Tribunal de Transparencia y Acceso la Información Pública" el que se constituya como segunda instancia administrativa y resuelva los recursos de apelación que interpongan los funcionarios y servidores sancionados como actualmente sucede.

Entonces existe la necesidad de contar con los mecanismos idóneos orientados a proteger el derecho de acceso a la información pública, toda vez que los datos y cifras muestran un significativo número de solicitudes de acceso a la información pública no atendidas que desde el año 2004 al 2018 ascienden a 116,004 (según datos tomados de los informes anuales de la Presidencia del Consejo de Ministros y del Ministerio de Justicia y Derechos Humanos), un alto porcentaje de entidades que no reportan sus consolidados anuales[3], alto grado de insatisfacción de los ciudadanos por haberse vulnerado su derecho lo que se materializa en las 5,400 quejas formuladas por los ciudadanos ante la Defensoría del Pueblo, desde el año 2013 al 2018 por incumplimiento de plazo para entregar información, negativa a dar información por excepciones no contempladas en la normativa, negativa de dar información por inadecuada interpretación de las excepciones y cobros ilegales o arbitrarios.

Todos estos datos nos demuestran que se deben hacer algunos ajustes a la normativa vigente para poder garantizar una adecuada protección a este derecho fundamental; para ello, se puede mencionar el

[3] En relación al porcentaje de entidades que no reportaron sus consolidados anuales, desde el año 2004 hasta el 2018, el porcentaje de incumplimiento es mayor al 50% llegando al 90% en el año 2006.

caso Chileno en el que el Consejo para la Transparencia, sanciona, previa instrucción de una investigación sumaria, a los funcionarios y servidores por el incumplimiento injustificado de entregar la información de manera pecuniaria, con una multa de 20% a 50% de su remuneración y en caso de reincidencia se le suspende en el cargo por un lapso de 5 días, asimismo, las sanciones son publicadas en el portal del "Consejo para la Transparencia".

De acuerdo a ello, en nuestro país se podría modificar el tipo de sanción a imponer a los funcionarios y servidores con relación laboral vigente que incumplen las normas de transparencia y acceso a la información pública para incluir la sanción pecuniaria como sucede en Chile toda vez que en nuestra realidad, la multa solo es aplicable a los ex servidores y a las personas jurídicas, más no a los servidores con vínculo vigente en sus entidades en las que se incumple la normativa de transparencia y acceso a la información pública.

Por su parte, "en México, país en el que se ha conseguido que el acceso a la información pública sea un derecho y una práctica generalizada, existe el Instituto Federal de Acceso a la Información Pública y Protección de Datos como organismo autónomo que encabeza el Sistema Nacional de Transparencia" (Congreso de México, 2017). En este país, se pueden imponer las medidas de apremio de amonestación pública o multa de 150 veces el salario mínimo general, asimismo, el incumplimiento de los sujetos obligados es difundido en sus portales de transparencia.

Además, del procedimiento disciplinario mencionado, existe un procedimiento sancionador aplicable a las entidades que según el artículo 38 del "Reglamento de la Ley de Transparencia y Acceso" aprobado por Decreto Supremo N° 072-2003-PCM, modificado por Decreto Supremo N° 019-2017-JUS[4] comprende la fase instructora y la

[4] El artículo 38 del Reglamento de la Ley de Transparencia y Acceso señala que "(…) el Procedimiento sancionador a las personas jurídicas que "comprende la fase instructora y la sancionadora. La fase instructora está a cargo del órgano de línea de la

sancionadora. La fase instructora está a cargo del órgano de línea de la Autoridad que establezca el Reglamento de Organización y Funciones del Ministerio de Justicia y Derechos Humanos y la fase sancionadora está a cargo de la Autoridad.

Sin embargo, en el Reglamento de Organización y Funciones del Ministerio de Justicia y Derechos Humanos, no se ha precisado a cargo de qué órgano de línea de la Dirección General de Transparencia se encuentra la fase instructora. Entonces, es evidente que esta es una tarea pendiente que hasta la fecha la Autoridad no ha resuelto lo que demuestra que el procedimiento administrativo sancionador no se viene aplicando. Sumado a ello, cabe indicar también que el Decreto Legislativo N° 1353 no le ha otorgado expresamente facultad **sancionadora** a la Autoridad Nacional de Transparencia y Acceso a la Información Pública, ello en virtud al principio de legalidad.

7. Límites al ejercicio del derecho de acceso a la información pública

Una solicitud de acceso a la información pública debe ser atendida en un plazo máximo de 10 días hábiles y observando el principio de máxima publicidad y la presunción de que toda información creada o en posesión del Estado es pública y solo puede ser denegada por las excepciones que se encuentran expresamente establecidas por la norma de la materia. Estas excepciones son la información clasificada como secreta, reservada y confidencial.

7.1. Información Secreta

Según el artículo 15° del Texto Único Ordenado de la Ley N° 27806, información **SECRETA** es la información militar y de inteligencia cuya revelación originaría riesgo para las acciones destinadas

Autoridad que establezca el Reglamento de Organización y Funciones del Ministerio de Justicia y Derechos Humanos. La fase sancionadora está a cargo de la Autoridad (…)".

a proteger la seguridad nacional e integridad de las personas que desarrollan actividades en dicho ámbito, integridad territorial y subsistencia del régimen democrático.

Así pues, en este rubro se encuentra todo tipo de información relacionada con planes de defensa militar, operaciones y planes de inteligencia, información de personal militar que desarrolla actividades de seguridad nacional. Por ejemplo: Si un ciudadano solicita información sobre el personal destacado a la zona del VRAE, esa información por razones de seguridad es secreta.

7.2. Información Reservada

Según el artículo 16 del Texto *Ú*nico Ordenado de la ley N° 27806, información **RESERVADA** es aquella información que tiene por finalidad prevenir y reprimir la criminalidad y salvaguardar el orden interno.

En esa línea, se encuentra comprendida en esta categoría toda aquella información vinculada a los planes de operaciones policiales y de inteligencia destinados a combatir el terrorismo y tráfico ilícito de drogas.

Por ejemplo: Si un ciudadano solicita copia del plan de inteligencia para combatir los robos en los bancos, no se puede entregar esa información porque es de carácter reservado.

7.3. Información Confidencial

*Según el artículo 17 del Texto Único Ordenado de la ley N° 27806, s*e considera información **CONFIDENCIAL** toda aquella información relacionada con la intimidad personal y familiar. Así como, la información que contenga consejos, recomendaciones u opiniones del proceso deliberativo y consultivo previo a la toma de una decisión de gobierno, la información protegida por el secreto bancario, tributario, comercial, industrial, tecnológico y bursátil regulada por la Constitución y la normativa pertinente, la información vinculada a investigaciones en trámite referidas al ejercicio de la potestad sancionadora de la Administración

Pública cuando la resolución que pone fin al procedimiento queda consentida o cuando transcurren más de 06 meses desde que se inició el procedimiento administrativo sancionador, sin que se haya dictado resolución final y la información preparada u obtenida por asesores jurídicos o de las entidades cuya publicidad pudiera revelar la estrategia a adoptarse en la tramitación o defensa en un proceso administrativo o judicial. Esta excepción termina al concluir el proceso.

Es importante señalar que, cuando se da por denegado el acceso solicitado, se debe fundamentar de manera debida los motivos de la denegatoria de acuerdo a lo establecido en la Ley N° 27806. Es decir, no basta que el sujeto obligado alegue la excepción porque la carga de la prueba recae en éste (Sentencia, 2013).

Es oportuno resaltar que, el artículo 18° del Texto Único Ordenado de la ley señala que "*las excepciones deben interpretarse de manera restrictiva por tratarse de un derecho fundamental*" (Robert, 1993). Sin embargo, hay un considerable número de casos en el que la administración pública atiende o brinda respuesta al ciudadano señalando que no se cuenta con dicha información y por ende, no es posible su entrega invocando el artículo 13° del "Texto Único Ordenado de la Ley N° 27806" que señala que *"no existe obligación de las entidades de crear o producir información con la que no se cuenta al momento de efectuarse el pedido"* pero si la información ha existido y esta no es puesta a disposición del ciudadano porque no se encuentra o no se ubica debido a la desorganización de los archivos públicos o por haber sido destruida sin el procedimiento contemplado para tal fin, este hecho constituye una grave afectación a este derecho fundamental.

En ese sentido, existe una estrecha relación entre la atención de las solicitudes de acceso a la información pública con la adecuada administración de los archivos toda vez que la desorganización de los archivos de la administración pública genera hacinamiento y pérdida de información y ello, es consecuencia del incumplimiento de las normas archivísticas que preveen la ejecución de procesos técnicos archivísticos;

por lo que, para satisfacer los requerimientos de información es fundamental que se apliquen sistemas de gestión de documentos que hagan posible su recuperación y búsqueda rápida, así como se desarrollen y ejecuten sus procesos técnicos archivísticos de forma responsable y eficiente a fin de reducir toda posibilidad de pérdida de información. Sumado a ello, es importante que el ente rector del Sistema Nacional de Archivos supervise de forma efectiva el cumplimiento de la normativa archivística a nivel nacional dando cuenta de los resultados de su evaluación.

El rol que cumplen los archivos es clave para el correcto funcionamiento y la adecuada gestión de las entidades de la Administración Pública porque son fuente de información y contribuyen a transparentar los actos de gobierno. Los archivos custodian la memoria de la institución en los documentos los cuales son fuente primordial para brindar servicios al ciudadano a través del ejercicio del derecho fundamental y constitucional de acceso a la información pública.

La Defensoría del Pueblo en su Informe Defensorial 96 del año 2004 identificó que el incumplimiento del plazo legal previsto para la entrega de la información requerida se ha debido, principalmente, a ***"la inexistencia de archivos profesionalizados que permitan la ubicación rápida de la información solicitada"*** (Defensoría del Pueblo, 2004, pág. 87). Asimismo, en el Informe Defensorial 14 del año 2010 también se mencionó que la ***"falta de adecuación de los sistemas de archivos de las entidades públicas trae como consecuencia la demora en la atención de las solicitudes de acceso a la información pública"***. Es por ello, que la Defensoría del Pueblo resaltó la importancia de que las entidades de la administración pública cuenten con archivos organizados y profesionalizados (Defensoría del Pueblo, 2010, pág. 273).

En el año 2012, la Defensoría del Pueblo publicó un Diagnóstico realizado sobre el cumplimiento de las obligaciones en materia de acceso a la información pública en seis gobiernos regionales: Ayacucho, Ancash, Apurímac, Lambayeque, San Martín y Tacna en el que

se determinó que en dichos gobiernos regionales no se contaba con directivas archivísticas ni procedimientos que regulen sus archivos lo que genera deficiencias en la adecuada organización y conservación de la información que incide negativamente en la atención de solicitudes de acceso a la información (Defensoría del Pueblo, 2012).

Por su parte, en el Informe Defensorial 17 del año 2013 también se menciona que los procesos técnicos archivísticos que efectúan las entidades de la administración pública son aspectos que deben ser regulados de la manera más idónea por parte del ente rector a fin de generar una adecuada atención de las solicitudes de acceso a la información (Defensoría del Pueblo, 2013, pág. 74).

En el periodo comprendido entre el 2010 al 2016, la Presidencia del Consejo de Ministros en sus informes anuales[5]sobre acceso a la información pública, ha señalado reiteradamente que ***"el no encontrar la información" constituye uno de los factores por los cuales no se cumple con atender las solicitudes de acceso a la información pública.*** Esto también ha sido mencionado en el último Informe anual sobre solicitudes de acceso a la información pública del período 2018, emitido por la Autoridad Nacional de Transparencia y Acceso a la Información.

El Tribunal Constitucional ha desestimado el argumento de la inexistencia de la información para denegar una solicitud de acceso a la información pública teniendo en cuenta que el penúltimo párrafo del artículo 13 de la ley de transparencia señala que en caso un entidad no localiza información que está obligada a poseer o custodiar deberá acreditar que ha agotado la acciones necesarias para atender la solicitud tal como lo ha establecido en el fundamento 8 la sentencia recaída en el Expediente Nº 01410-2011-PHD/TC, que señala: "(…) *Es necesario*

[5] Antes de la creación de esta Autoridad la Presidencia del Consejo de Ministros a través de la Secretaría de Gestión Pública era la entidad responsable de la coordinación, consolidación y supervisión de los consolidados anuales de la atención de las solicitudes de acceso a la información de las entidades.

agotar las diligencias necesarias a efectos de localizar la documentación requerida. En su defecto y de quedar comprobado el extravío de la misma, disponer la reconstrucción del expediente administrativo correspondiente, para luego de ello cumplir con su entrega en copias a los interesados. Sobre el particular, el artículo 27° del Reglamento de la Ley de Transparencia señala en caso se extravíe información en poder de las entidades, se deberán agotar las acciones necesarias para recuperar dicha información; asimismo, que en dicho supuesto, corresponde a la entidad comunicar al solicitante dicha situación, así como los avances o resultados de las acciones orientadas a recuperar la información o la imposibilidad de brindarla por no haberse recuperado, sin perjuicio de las responsabilidades administrativas, civiles y penales (…)".

En suma, existe vulneración al derecho de acceso a la información pública cuando la información ha sido producida por la entidad pero esta no la pone a disposición por qué "no se ubica" o "no se encuentra" y la causa de esto es la inadecuada administración de los archivos que manejan las entidades.

En consecuencia, cuando se habla de administración y gestión pública se piensa en "información" y se vincula este término con conceptos como democracia y buen gobierno. Empero, vemos archivos en situación precaria y descuidados lo que es contradictorio toda vez que sino se adoptan acciones para la adecuada administración y conservación de los documentos no se tendrá información accesible y a disposición de los usuarios que lo requieran. En este orden de ideas, las entidades deben contar con sistemas de gestión de documentos que hagan posible la recuperación y búsqueda rápida de la misma a través de la creación de potentes bases de datos que permitan optimizar las guías, inventarios y catálogos que se elaboran en los archivos; asimismo, es importante que las entidades desarrollen y ejecuten sus proceso técnicos archivísticos de forma responsable a fin de que por ejemplo, el proceso de selección y eliminación de documentos se de a través de una evaluación consiente de valoración documental a fin de reducir toda posibilidad de pérdida de información.

8. CONCLUSIONES

- El "derecho de acceso a la información pública" es una herramienta clave para el control ciudadano respecto de la gestión pública y contribuye con el fortalecimiento de la trasparencia y lucha contra la corrupción.

- El derecho de acceso a la información pública es un derecho fundamental y solo puede ser restringido o denegado siempre que se trate de información secreta, reservada o confidencial que constituyen las únicas excepciones y límites para el ejercicio de este derecho. Todo pedido denegado fuera de estas excepciones constituye una vulneración a este derecho fundamental.

- Es importante que la Autoridad Nacional de Transparencia se fortalezca para que se constituya en una entidad autónoma, independiente y especializada que le permita enfrentar los problemas que persisten relacionados con los incumplimientos a las normas de transparencia y acceso a la información pública y que dentro de ella pueda constituirse el Tribunal de Transparencia y no de forma separada pues de acuerdo a los artículos 9 y 15 del Decreto Supremo N° 054-2018-PCM que regula los Lineamientos de Organización del Estado modificado por Decreto Supremo N° 131-2018-PCM los órganos resolutivos se encuentran dentro de la estructura orgánica de las diversas entidades como sucede con los tribunales administrativos de la "Autoridad Nacional del Servicio Civil" (SERVIR), "Superintendencia Nacional de Fiscalización Laboral" (SUNAFIL), "Superintendencia Nacional de Salud" (SUSALUD), "Organismo de Evaluación y Fiscalización Ambiental" (OEFA), "Organismo Supervisor de las Contrataciones del Estado" (OSCE), "Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual" (INDECOPI), entre otros.

Bibliografía

- Bustillos Roqueñi, Jorge & Carbonell, Miguel (Coordinadores) (2007). *Hacia una democracia de contenidos: La reforma constitucional en materia de transparencia*. México. Instituto de Investigaciones Jurídicas de la UNAM
- Caso Wilo Rodríguez Gutierrez, Exp. 1797-2002-PHD/TC, de fecha 29 de enero de 2003.
- Congreso de México. (27 de enero de 2017). Obtenido de http://www.diputados.gob.mx/LeyesBiblio/pdf/LFTAIP_270117.pdf
- Consejo Permanente de la Organización de los Estados Americanos. (29 de abril de 2010). Obtenido de www.oas.org: https://www.oas.org/dil/esp/CP-CAJP-2840-10_Corr1_esp.pdf
- Defensoría del Pueblo. (2004). *Informe Defensorial 96.* Lima.
- Defensoría del Pueblo. (2010). *Decimo Cuarto Informe Anual.* Lima: Ediciones Nova print SAC.
- Defensoría del Pueblo. (2012). *Diagnóstico sobre el cumplimiento de las obligaciones en materia de acceso a la información pública en seis gobiernos regionales.* Lima: WR impresiones.
- Defensoría del Pueblo. (2013). *Decimo Séptimo Informe Defensorial.* Lima: Ediciones Nova Print SAC.
- Diego, Z. V. (2009). El ejercicio del derecho de acceso a la información pública en el Perú. *Revista de Derecho Administrativo*, 315-340.
- Landa, C. (2003). *Teoría del Derecho Procesal Constitucional.* Lima: Palestra.

- OEA. (30 de diciembre de 2009). Obtenido de http://www.oas.org/es/cidh/expresion/docs/publicaciones/ACCESO%20A%20LA%20INFORMACION%20FINAL%20CON%20PORTADA.pdf
- Portocarrero, F. C. (11 de junio de 2019). Transcripción de entrevista. (H. S. Arce, Entrevistador)
- Puccinelli, O. (1999). *El Hábeas Data en Iberoamérica.* Bogotá: Editorial Temis.
- Rivera, J. A. (2008). *Transparencia y Democracia: Claves para un concierto.* México D.F.: Instituto federal de Acceso a la Información.
- Robert, A. (1993). *Teoría de los derechos fundamentales.* Madrid: Centro de Estudios Constitucionales.
- Sentencia, Exp. N° 4912-2008-HD/TC (Tribunal Constitucional 07 de setiembre de 2009).
- Sentencia, Exp. N° 3035-2012-HD/TC (Tribunal Constitucional 21 de agosto de 2013).

EL DERECHO DE ACCESO A LA INFORMACIÓN PÚBLICA COMO INSTRUMENTO PARA GARANTIZAR LOS DERECHOS DE LAS MUJERES A UNA VIDA LIBRE DE VIOLENCIA

María Candelaria Quispe Ponce*

1. El proceso constitucional de hábeas data y la protección del derecho de acceso a la información pública.

El *hábeas data* es un proceso constitucional que tiene por finalidad la protección de dos derechos fundamentales, a saber: (i) el derecho de acceso a la información pública, y (ii) el derecho a la autodeterminación informativa (o protección de datos personales)[1]. Ambos derechos reconocidos en los incisos 5 y 6 del artículo 2 de la Constitución Política del Perú de 1993, los cuales prescriben lo siguiente:

* Doctora en Estudios Avanzados en Derechos Humanos por la Universidad Carlos III de Madrid. Máster en Derecho Constitucional por el Centro de Estudios Constitucionales de la Presidencia del Gobierno de España, profesora de pre y postgrado de la Universidad Nacional Mayor de San Marcos.

[1] El proceso constitucional de hábeas data fue incorporado por primera en el sistema constitucional peruano por la Constitución de 1993. Ver: Landa. C, *El proceso constitucional de hábeas data*, Pontificia Universidad Católica del Perú, Lima, p. 139. Asimismo, fue desarrollada por la Ley N.º 26301 del 3 de mayo de 1994 (derogada desde la vigencia del Código Procesal Constitucional.

Toda persona tiene derecho:

5. A solicitar sin expresión de causa la información que requiera y a recibirla de cualquier entidad pública, en el plazo legal, con el costo que suponga el pedido. Se exceptúan las informaciones que afectan la intimidad personal y las que expresamente se excluyan por ley o por razones de seguridad nacional.

6. A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar.

El presente trabajo se centra en el primero de los derechos protegidos por el proceso constitucional de hábeas data: el derecho fundamental de acceso a la información pública. Este derecho constitucional fue materia de desarrollo legislativo a través de la Ley N.º 27806, de Transparencia y Acceso a la información pública[2], cuya finalidad es promover la transparencia de los actos del Estado y regular el derecho fundamental del acceso a la información. Ahora bien, el proceso constitucional de hábeas data, a través del cual se garantiza este derecho, se inicia, conforme al diseño instituido por el Constituyente peruano, en la justicia ordinaria, más precisamente, en el Poder Judicial –que conoce en primera y segunda instancia las demandas de hábeas data–. Sólo ante una resolución denegatoria emitida por la justicia ordinaria corresponde al Tribunal Constitucional conocer las demandas de hábeas data.

El artículo 202, inciso 2 de la Constitución prescribe que: "corresponde al Tribunal Constitucional conocer en última y definitiva instancia las resoluciones denegatorias (…) de hábeas data". Del análisis de esta disposición se infiere que el recurso impugnatorio a través del cual se accede al Tribunal Constitucional no tiene una denominación

[2] Texto Único Ordenado de la Ley N.º 27806, Decreto Supremo 021-2019-JUS, publicado en el diario oficial *El Peruano* el 11 de diciembre de 2019.

concreta en la Carta Fundamental (hasta antes del 01 de diciembre de 2004[3], se tramitaban bajo la denominación de recurso extraordinario. A título de ejemplo, se puede citar, entre otras, las sentencias recaídas en los expedientes: STC 526-1998-HD/TC y STC 0214-2000-PHD/TC. Desde la promulgación del Código Procesal Constitucional este medio impugnatorio es denominado Recurso de Agravio Constitucional. Veamos:

> **Artículo 18.-** *Recurso de agravio constitucional*
>
> "Contra la resolución de segundo grado que declara infundada o improcedente la demanda, procede **recurso de agravio constitucional** ante el Tribunal Constitucional, dentro del plazo de diez días contados desde el día siguiente de notificada la resolución. Concedido el recurso, el Presidente de la Sala remite al Tribunal Constitucional el expediente dentro del plazo máximo de tres días, más el término de la distancia, bajo responsabilidad".

Como se puede advertir, el primer nivel de garantía de los derechos fundamentales protegidos por el proceso constitucional de hábeas data –(i) derecho de acceso a la información pública y, (ii) derecho de protección de datos personales– se sitúa en sede del Poder Judicial. Es fundamentalmente labor del juez o jueza de este poder del Estado. Ante una resolución adversa (que declara improcedente o infundada la demanda) el ciudadano/a puede acudir a la jurisdicción constitucional, a través del Recurso de Agravio Constitucional. Con el pronunciamiento del intérprete supremo de la Constitución, que resuelve en última y definitiva instancia, se agota la jurisdicción interna. Agotada la vía interna, quien se considere lesionado en los derechos que la Constitución reconoce puede recurrir a los tribunales u organismos internacionales

[3] El Código Procesal Constitucional, promulgado mediante Mediante Ley N.º 28237, publicada en el Diario Oficial *El Peruano* el 31 de mayo de 2004, está vigente en el Perú desde el 01 de diciembre de 2004. Ello, en atención a lo dispuesto por la Segunda Disposición Transitoria y Derogatoria del mismo cuerpo normativo que dispuso una vacatio legis de seis meses.

constituidos según tratados o convenios de los que el Perú es parte (artículo 205 de la Constitución).

Desde esta óptica, es posible afirmar que el Tribunal Constitucional y la Corte Interamericana han desempeñado y desempeñan una labor sumamente importante en el proceso de consolidación del derecho de acceso a la información pública. Ello, si tenemos en consideración que las resoluciones emitidas por estos Altos Tribunales son de obligatorio cumplimiento por todos los Poderes del Estado, incluido el Poder Judicial[4]. Recordemos, en ese sentido, que la Corte IDH reiterada jurisprudencia se pronuncia y reafirma los efectos *erga omnes* de sus fallos para el derecho interno. A título de ejemplo se pueden citar los casos: "Barrios Altos vs. Perú", "El Tribunal Constitucional vs. Perú" y "La Cantuta vs. Perú", en los que efectúa precisiones sobre el carácter vinculante de sus sentencias (Hitters, 2008: 146).

Por su parte, el Tribunal Constitucional, en el emblemático caso Castillo Chirinos (02730-2006-PA/TC), se pronuncia –ya hace más de una década– sobre el carácter vinculante de las sentencias de la Corte IDH, y sostiene que esta "no se agota en su parte resolutiva, sino que se extiende a su fundamentación o *ratio decidendi*, con el agregado de que, por imperio de la Cuarta Disposición Final y Transitoria de la Constitución y el artículo V del Título Preliminar del Código Procesal Constitucional, en dicho ámbito la sentencia resulta vinculante para todo poder público nacional, incluso en aquellos casos en los que el Estado peruano no haya sido parte en el proceso. (Fundamento 12).

[4] De acuerdo con el Tribunal Constitucional, las sentencias que emite, "dado que constituyen la interpretación de la Constitución del máximo tribunal jurisdiccional del país, se estatuyen como fuente de derecho y vinculan a todos los poderes del Estado" (STC 03741-2004-AA/TC, Fundamento 42). Esta afirmación es corroborada, asimismo, por lo prescrito en el Código Procesal Constitucional: "los Jueces interpretan y aplican las leyes o toda norma con rango de ley y los reglamentos según los preceptos y principios constitucionales, conforme a la interpretación de los mismos que resulte de las resoluciones dictadas por el Tribunal Constitucional" (Artículo VI del Título Preliminar, tercer párrafo).

La cualidad constitucional de esta vinculación, argumenta el Alto Tribunal, "derivada directamente de la Cuarta Disposición Final y Transitoria de la Constitución, tiene una doble vertiente en cada caso concreto: a) reparadora, pues interpretado el derecho fundamental vulnerado a la luz de las decisiones de la Corte, queda optimizada la posibilidad de dispensársele una adecuada y eficaz protección; y, b) preventiva, pues mediante su observancia se evitan las nefastas consecuencias institucionales que acarrean las sentencias condenatorias de la Corte IDH, de las que, lamentablemente, nuestro Estado conoce en demasía. Es deber de este Tribunal y, en general, de todo poder público, evitar que este negativo fenómeno se reitere" (Fundamento 13)[5].

Bajo esta premisa, el caso *Claude Reyes Vs Chile* (sentencia emitida el 19 de septiembre de 2006) es sumamente importante en relación con el derecho de acceso a la información pública[6]. Esta sentencia marca un hito en la jurisprudencia de la Corte Interamericana de Derechos Humanos (Fernández, 2016). Un Tribunal que, hasta inicios del Siglo XXI emitía pronunciamientos, fundamentalmente, sobre violaciones masivas y sistemáticas de los derechos humanos cometidas en el marco de regímenes dictatoriales de una serie de países del Continente que, si bien –desde los noventa del siglo XX– habían transitado hacia regímenes democráticos, aún no conseguían salir del todo de la tradicional

[5] La doctrina de la obligatoriedad del cumplimiento de las sentencias emitidas por la Corte IDH por todos los Estados que han reconocido la competencia contenciosa de ese Alto Tribunal, reafirmada por el Tribunal Constitucional, ha sido ampliamente desarrollado por la Corte IDH en su jurisprudencia a través del control de convencionalidad, "herramienta que permite a los Estados concretar la obligación de garantía de los derechos humanos en el ámbito interno, a través de la verificación de la conformidad de las normas y prácticas nacionales, con la Convención Americana sobre Derechos Humanos (CADH) y su jurisprudencia´". Ver: Nash, C. (2019), Introducción al control de convencionalidad, *Cuadernillo de jurisprudencia de la Corte IDH*, núm. 7, p. 4. Disponible en: https://bit.ly/30S3Hy0

[6] Corte IDH. Caso *Claude Reyes y otros Vs. Chile*, Fondo, Reparaciones y Costas, Sentencia de 19 de septiembre de 2006, Serie C No. 151. Disponible en: https://bit.ly/34oduNh

opacidad y "cultura del secreto" arraigada en la Administración Pública (González, 2016: 59). A partir del caso *Claude Reyes*, el Tribunal Interamericano exige a los Estados parte del Sistema Interamericano, transparencia y máxima publicidad en todas sus actuaciones. Instalar una cultura de la transparencia, como condición de posibilidad de todo régimen democrático[7].

La Corte IDH fue el primer tribunal internacional en reconocer que el derecho de acceso a la información pública es protegido por el derecho internacional e impone a los Estados un conjunto de obligaciones específicas con el fin de garantizarlo (Comisión IDH, 2020: 4)[8]. En efecto, de acuerdo con lo establecido por el Tribunal Interamericano en el caso *Claude Reyes,* el derecho de acceso a la información pública está protegido por el artículo 13 de la Convención Americana. Al respecto, refiere lo siguiente:

> "El artículo 13 de la Convención, al estipular expresamente los derechos a "buscar" y a "recibir" "informaciones", protege el derecho que tiene toda persona a solicitar el acceso a la información bajo el control del Estado, con las salvedades permitidas bajo el régimen de restricciones de la Convención. Consecuentemente, dicho artículo ampara el derecho de las personas a recibir dicha información y la obligación positiva del Estado de suministrarla, de forma tal que la persona pueda tener acceso a conocer esa información o reciba una respuesta fundamentada cuando por algún motivo permitido por la Convención el Estado pueda limitar el acceso a la misma para el caso concreto. (Corte IDH.

[7] Con posterioridad al pronunciamiento de la Corte IDH, la Comisión Interamericana de Derechos Humanos reitera que, para garantizar el ejercicio pleno y efectivo del derecho de acceso a la información, la gestión estatal debe regirse por los principios de máxima divulgación. Ver: Comisión IDH (2011) *El derecho de acceso a la información en el marco jurídico interamericano*, Relatoría Especial para la Libertad de Expresión, párrafo 8.

[8] Comisión Interamericana de Derechos Humanos, *Derecho de acceso a la información y seguridad nacional*, Organización de Estados Americanos, 2020, p. 4.

Caso *Claude Reyes y otros Vs. Chile*, párrafo 77).

Además de reconocer que el derecho a recibir información pública es un derecho humano protegido por la Convención Americana, cuyo correlato es la obligación positiva de los Estados de suministrarla, el Tribunal Interamericano enfatiza tres cuestiones esenciales. En primer lugar, establece que la información debe ser entregada sin necesidad de que quien lo solicite acredite un interés directo o personal, salvo en aquellos casos en los que existan restricciones legítimas.

En segundo lugar, pone de relieve que, –en atención a la dispuesto por la Asamblea General de la Organización de Estados Americanos (OEA) en diversas resoluciones– el acceso a la información pública es un requisito indispensable para el funcionamiento mismo de la democracia y una buena gestión pública.

En tercer lugar, sostiene que las actuaciones del Estado deben regirse por los principios de máxima publicidad y transparencia, lo que posibilita que las personas bajo su jurisdicción ejerzan el control democrático de las gestiones estatales, de forma tal que puedan cuestionar, indagar y considerar si se está dando un adecuado cumplimiento de las funciones públicas.

Desde esta óptica, el Alto Tribunal considera que, el control democrático, por parte de la sociedad a través de la opinión pública, fomenta la transparencia de las actividades estatales y promueve la responsabilidad de los funcionarios sobre su gestión pública. Por ello, para que las personas puedan ejercer el control democrático es esencial que el Estado garantice el acceso a la información pública bajo su control. (Corte IDH. Caso *Claude Reyes Vs. Chile*, párr. 86).

Los estándares fijados por la Corte IDH, en relación con el contenido y límites del derecho de acceso a la información pública, no solo han permitido fortalecer este derecho en los Estados parte del Sistema Interamericano de Derecho Humanos –a través de la implementación de normas de transparencia y acceso a la información pública–, sino

que también han servido de base para que el Tribunal Europeo de Derechos Humanos cambie su jurisprudencia y reconozca el derecho de acceso a la información como manifestación de la libertad de expresión y como derecho autónomo que goza de toda la protección (Fernández, 2016: 322).

2. El derecho de acceso a la información pública en la jurisprudencia. Especial referencia a la transparencia activa

La jurisprudencia en materia de acceso a la información pública en el Perú es de dos tipos, administrativa y jurisdiccional: (i) administrativa, cuando emana del Tribunal de Transparencia y Acceso a la Información Pública (en adelante, TTAIP) –que inició sus funciones el 20 de diciembre de 2018–, y (ii) jurisdiccional, cuando es emitida por los Tribunales de justicia: el Poder Judicial y el Tribunal Constitucional. En este epígrafe nos centraremos, muy brevemente, en la jurisprudencia relevante sobre el derecho de acceso a la información pública emitida por el Tribunal Constitucional. Ahora bien, el tema que nos ocupa exige, previamente, hacer una referencia –aunque muy acotada– a la trasparencia activa[9]. Es decir, aquellas acciones desarrolladas por el Tribunal de Transparencia y Acceso a la Información Pública, el Poder Judicial y el Tribunal Constitucional para publicitar el contenido de las decisiones judiciales y de las resoluciones de la autoridad administrativa, respectivamente (Coteño, 2019:202).

2.1. Jurisprudencia administrativa y transparencia activa

La jurisprudencia administrativa, emitida por el Tribunal de Transparencia y Acceso a la Información Pública (TTAIP), es de

[9] Los esfuerzos desplegados por el Estado peruano con relación a la transparencia activa, durante la primera década de vigencia de la Ley, pueden encontrarse exhaustivamente detallados en el Informe Defensorial N.º 165, Balance a diez años de vigencia de la Ley de Transparencia y Acceso a la Información Pública 2003-2013, Defensoría del Pueblo, Lima, 2013. Disponible en: https://bit.ly/2SwVfzz.

reciente data en el Perú –el TTAIP entró en funciones el 20 de diciembre de 2018–. En efecto, este órgano resolutivo del Ministerio de Justicia y Derechos Humanos con dependencia administrativa del Despacho Ministerial e independencia funcional, fue instituido mediante el Decreto Legislativo N.º 1353 –que crea la Autoridad Nacional de Transparencia y Acceso a la Información Pública– cuenta en la actualidad, con dos salas encargadas de resolver, en última instancia administrativa, los recursos de apelación por denegatoria de las solicitudes de acceso a la información pública, y los recursos de apelación por sanciones (que no sean destitución o inhabilitación) impuestas a servidores y funcionarios público o personas jurídicas por infracción a las normas de trasparencia.

El Tribunal de Transparencia y Acceso a la Información Pública, cuya Primera Sala fuera instalada el 21 de diciembre de 2018, y la Segunda Sala, instalada el 20 de enero del año en curso, ha recibido hasta septiembre de 2020, un total de 2821 apelaciones. Asimismo, ha emitido un Precedente Vinculante[10]. Todas las resoluciones emitidas por este órgano se encuentran disponibles en el portal web del TTAIP (https://www.minjus.gob.pe/resoluciones-ttaip/). En consecuencia, cumple con

[10] El Tribunal de Transparencia y Acceso a la Información, en su pronunciamiento de fecha 28 de enero de 2020, contenido en la Resolución N.º 010300772020. Exp. N.º 00038-2020-JUS/TTAIP, declaró precedente administrativo de observancia obligatoria el siguiente criterio de interpretación normativa respecto de lo dispuesto por los artículos 3, 13 y 18 de la Ley de Transparencia: "Las entidades no podrán denegar el acceso a la información pública, argumentando únicamente que la documentación requerida no ha sido creada por ésta, atendiendo a que el derecho de acceso a la información pública abarca no solamente la posibilidad de obtener aquella ha sido denegada por la propia institución, sino también a la que no siendo creada por ésta, se encuentra en su posesión. En tal sentido, cuando las entidades denieguen el acceso a la información pública en virtud a la inexistencia de la documentación requerida, deberán previamente verificar mediante requerimientos a las entidades orgánicas que resulten pertinentes si la información: i) fue generada por la entidad; y ii) si ha sido obtenida, se encuentra en su posesión o bajo su control; asimismo, luego de descartar ambos supuestos, deberán comunicar de manera clara y precisa dicha circunstancia de dispensa de información al solicitante" (artículo 4).

la exigencia establecida en la Ley 27806, de acuerdo con la cual, el principio de trasparencia que debe regir todas las actuaciones de los poderes públicos.

Asimismo, la Autoridad Nacional de Transparencia y Acceso a la Información Pública, elabora un informe anual sobre los pedidos de acceso a la información pública tramitados por las entidades estatales al amparo de la Ley 2706[11]. El corolario de la transparencia activa de esta institución es el compendio normativo publicado por el Ministerio de Justicia y Derechos Humanos en el que se sistematiza el marco normativo, así como la jurisprudencia emitida por el Tribunal de Transparencia y Acceso a la Información Pública[12].

2.2. Jurisprudencia del Poder judicial y transparencia activa

En relación con la jurisprudencia emitida por los órganos jurisdiccionales, se debe precisar que, aun cuando en este trabajo se examinará exclusivamente la jurisprudencia relevante del Tribunal Constitucional, es necesario hacer una breve referencia a las acciones desarrolladas por el Poder Judicial para publicitar el contenido de sus decisiones judiciales (Transparencia activa). En ese sentido, es posible afirmar que las resoluciones judiciales emitidas por el Poder Judicial –autoridad que conoce en primera y segunda instancia las demandas de hábeas data– no son lo suficientemente accesibles a la ciudadanía en general[13].

[11] El informe anual sobre solicitudes de acceso a la información pública efectuadas a las entidades públicas en el año 2019, elaborado por la Autoridad Nacional de Transparencia y Acceso a la información pública, se encuentra disponible en: https://bit.ly/3lb1rJV

[12] Ministerio de Justicia y Derechos Humanos, *compendio Transparencia y acceso a la información pública: normativa y jurisprudenci*a, Lima, 2020. Disponible en: https://bit.ly/2GtnZ9T

[13] En el portal web institucional del Poder Judicial, en jurisprudencia sistematizada sólo figuran las ejecutorias de la Corte Suprema de Justicia: https://bit.ly/2SEbv21

En efecto, conforme con el diagnóstico jurisprudencial elaborado por el subgrupo de jurisprudencia y criterios administrativos de la Red de Transparencia y Acceso a la información[14], en el portal web institucional del Poder Judicial no se encuentran enlaces específicos que permitan acceder con facilidad a las sentencias, en general y, a las sentencias sobre hábeas data, en particular. Toda vez que, para acceder a dichos fallos, se requiere el número de expediente. Los criterios de búsqueda configurados –tales como el distrito judicial, tipo de órgano, especialidad, año-expediente– sólo permiten acceder a las sentencias, a quienes son parte en el proceso, lo que restringe su consulta a la ciudadanía en general (https://cej.pj.gob.pe/cej/forms/busquedaform.html).

En consecuencia, el acceso restringido al contenido de las resoluciones emitidas por el Poder Judicial supondría una inobservancia de dos disposiciones normativas. En primer lugar, de lo dispuesto por el Decreto Legislativo 1342, en relación con el derecho de acceso al contenido de las resoluciones de las instituciones de justicia, más concretamente, la obligación de las entidades que conforman el sistema de administración de justicia de desarrollar una plataforma de soporte tecnológico para la publicidad de las resoluciones judiciales con la finalidad de facilitar a la ciudadanía el acceso en forma sencilla a todas y cada una de las decisiones jurisdiccionales de los jueces o tribunales a nivel nacional (artículo 5, inciso 1).

En segundo lugar, supondría también el incumplimiento de la obligación de transparencia dispuesta por la Ley N.º 30934 (TUO de la Ley 27806), en virtud del cual, las entidades que forman parte del sistema de justicia –como es el caso del Poder Judicial– están obligadas a publicar en sus respectivos portales de transparencia: "todas las sentencias judiciales, dictámenes fiscales y jurisprudencia sistematizada

[14] Red de Transparencia y Acceso a la Información Pública, *Diagnóstico jurisprudencia Red de Transparencia y acceso a la información pública*. Disponible en: https://bit.ly/30qaX3N

de fácil acceso por materias, con una sumilla en lenguaje sencillo y amigable, conforme a los lineamientos y directrices establecidos por el Ministerio de Justicia y Derechos Humanos, a través de la Autoridad Nacional de Protección de Datos Personales, y en coordinación con el Poder Judicial y el Ministerio Público" (artículo 39, inciso 3).

2.3. Jurisprudencia del Tribunal Constitucional y transparencia activa

Las resoluciones emitidas por el Tribunal Constitucional se encuentran disponibles en el portal web institucional. Se puede acceder a la jurisprudencia en general y, a la jurisprudencia sobre el derecho de acceso a la información pública, en particular, anotando las palabras clave en: http://181.177.234.7/buscarRes/public/resolucionjur. Este Alto Tribunal también publica sus Memorias anuales, y libros que contienen la jurisprudencia relevante correspondiente a cada año juridicial. En tales volúmenes –disponibles en su portal web institucional– se pueden encontrar las decisiones resumidas de los procesos constitucionales orgánicos y de la libertad, como es el caso del proceso de hábeas data[15].

Desde el punto de vista de sus prácticas deliberativas y toma de decisión, el Tribunal Constitucional peruano se distinguió, desde el inicio de sus funciones en junio de 1996, por su carácter cerrado y secreto[16]. Sin embargo, recientemente, modificó su Reglamento Normativo –mediante Resolución Administrativa N.º 058-2020-P/TC, de 4 de mayo de 2020– con la finalidad de instaurar el sistema de deliberación pública de los Plenos Jurisdiccionales sobre procesos de

[15] El volumen IX de la jurisprudencia relevante del Tribunal Constitucional correspondiente al año 2018, publicado por el Centro de Estudios Constitucionales del Tribunal Constitucional, se encuentra disponible en: https://bit.ly/2SreVoI

[16] André Rufino Do Vale, analiza prolijamente la deliberación de los magistrados que integran los órganos colegiados de los tribunales constitucionales de España y Brasil. En el primero las deliberaciones son cerradas y secretas; en el segundo, públicas y transmitidas por radio y televisión. Ver: Do Vale, A. R (2016), *La deliberación en los Tribunales Constitucionales*, Centro de Estudios Políticos y Constitucionales, Madrid.

inconstitucionalidad y competenciales. Como se advierte en la precitada Resolución Administrativa, esta trascendental modificación fue justificada, fundamentalmente, en la optimización del derecho al acceso a la información pública. Veamos:

> "En aras de optimizar el derecho fundamental de acceso a la información pública y el derecho de la ciudadanía a relacionarse digital y tecnológicamente con las entidades del Estado, de promover la deliberación democrática (…), el Pleno ha acordado reformar el Reglamento Normativo del Tribunal, a efectos de poder celebrar Plenos abiertos al público, en tiempo real o simultáneo, en procesos de inconstitucionalidad y procesos competenciales, previo acuerdo de Pleno y con levantamiento expreso de la reserva propia de la función" (Resolución Administrativa N.º 058-2020-P/TC).

De este modo, el Tribunal Constitucional del Perú cumple con la exigencia de transparencia prescrita por el Decreto Legislativo N.º 1342, y la Ley N.º 30934 (TUO de la Ley 27806, Decreto Supremo 021-2019-JUS), en la medida que, cuenta con una plataforma de soporte tecnológico en la que publica sus resoluciones judiciales y facilita a la ciudadanía el acceso a sus decisiones. Además, a partir de este año, avanza hacia la transparencia en la deliberación de los procesos orgánicos, acordados por el Pleno.

3. El derecho de acceso a la información pública en la jurisprudencia del Tribunal Constitucional

Como ya se ha señalado, el derecho de acceso a la información pública cuenta con un robusto marco normativo diseñado por el constituyente, desarrollado por el legislador/a, y por el Poder Ejecutivo, en el ejercicio de su potestad reglamentaria y/o cuando le es delegada la facultad legislativa. En efecto, lo dispuesto por los artículos 2, inciso 5, y 200 inciso 3, de la Constitución –que, en líneas generales, reconoce el derecho de toda persona a solicitar información a cualquier entidad

pública y preceptúa las excepciones al ejercicio de este derecho[17], es ampliamente desarrollado –aunque después de una década y con el retorno del Estado peruano a la democracia– por la Ley N.º 27806, Ley de Transparencia y Acceso a la Información Pública, publicada en el diario oficial *El Peruano* el 3 de agosto de 2002, las diversas modificatorias y, el Texto Único Ordenado de la Ley N.º 27806, Decreto Supremo 021-2019-JUS, publicado en el diario oficial *El Peruano* el 11 de diciembre de 2019[18].

En este escenario se sitúa también el Decreto Legislativo N.º 1353 que crea la Autoridad Nacional de Transparencia y Acceso a la Información Pública y, entre otros, el Decreto Supremo N.º 164-2020-PCM, publicado en el diario oficial *El Peruano* el 4 de octubre de 2020, que aprueba el Procedimiento Administrativo Estandarizado de Acceso a la Información Pública creada u obtenida por la entidad, que se encuentre en su posesión o bajo su control[19]. Estas disposiciones normativas regulan, en forma detallada, el contenido del derecho de acceso a la información pública, los sujetos legitimados para ejercer este derecho, las entidades obligadas y, entre otras, las excepciones al ejercicio del

[17] Recientemente, en septiembre de 2020, la Relatoría para la Libertad de Expresión de la Comisión IDH publicó un informe temático sobre Derecho a la Información y Seguridad Nacional, en el que aborda los obstáculos legales y de hecho existentes en la región para armonizar la circulación de información de interés público y los intereses de seguridad nacional. Disponible en: https://bit.ly/30BmXjb. Por su parte, el Tribunal Constitucional, aborda este mismo tema en la sentencia recaída en el expediente 00005-2013-PI/TC, Caso transparencia y acceso a la información en el Sistema de Defensa Nacional, emitida en julio de 2018.

[18] Por disposición del artículo 2 del Decreto Supremo 021-2019-JUS, quedó derogado el Decreto Supremo 043-2003-PCM. En la sentencia recaída en el expediente N.º 02838-2009-PHD/TC, el Tribunal Constitucional señaló que esta disposición normativa forma parte del bloque de constitucionalidad.

[19] La revisión, mejora y actualización del marco normativo ha sido una constante en el ámbito del derecho de acceso a la información pública. Muestra de ello es, precisamente el Texto Único Ordenado, aprobado por Decreto Supremo 021-2019-JUS, publicado en el diario oficial El Peruano el 11 de diciembre de 2019. Disponible en https://bit.ly/3li1Pq0.

derecho de acceso a la información pública. Precisado, a su vez, por el Código Procesal Constitucional al disponer que este derecho implica:

> "Acceder a información que obre en poder de cualquier entidad pública, ya se trate de la que generen, produzcan, procesen o posean, incluida la que obra en expedientes terminados o en trámite, estudios, dictámenes, opiniones, datos estadísticos, informes técnicos y cualquier otro documento que la administración pública tenga en su poder, cualquiera que sea la forma de expresión, ya sea gráfica, sonora, visual, electromagnética o que obre en cualquier otro tipo de soporte material". (Código Procesal Constitucional, artículo 61, inciso 1)

Este importante desarrollo en el plano normativo no ha tenido una traducción adecuada en el plano fáctico. (i) La persistente renuencia de las entidades públicas (o entidades privadas que prestan servicio público) a proporcionar información, sin una justificación razonable de su denegatoria, (ii) la falta de respuesta a las solicitudes formuladas por los ciudadanos/as, (iii) la entrega parcial (incompleta) de la información solicita, (iv) las restricciones injustificadas para su acceso, (v) la interpretación y aplicación extensiva de las excepciones para su acceso, (vi) los cobros indebidos, y, entre otros, (vii) la exigencia de requisitos adicionales a los establecidos en el TUO de la Ley N.º 27806 (Abad, 2019: 7; Landa, 2018: 14; Defensoría del Pueblo, 2013)[20], han supuesto y, aún suponen, una forma de actuación persistente de las entidades públicas que ha hecho necesaria la intervención del Tribunal Constitucional.

[20] Al presentar el Informe Regional sobre Acceso a la Información Pública y las Instancias de Control y Apelación elaborada por la Alianza Regional por la Libre Expresión e Información, la Defensoría del Pueblo, señala que, a pesar de que el Perú cuenta con la Ley de Transparencia y Acceso a la Información Pública, recibe cada año numerosas quejas por la vulneración del derecho de acceso a la información pública, ya sea por incumplimiento de plazos de entrega, exigencia de cobros ilegales, la negativa ante una solicitud amparada por ley, entre otros. El precitado informe se encuentra disponible en: https://bit.ly/2SwYUxk

En efecto, como ya se mencionó, el Tribunal Constitucional ha desarrollado y desarrolla un papel clave en la garantía del ejercicio pleno y efectivo del derecho de acceso a la información pública, y en la consolidación de una cultura de la transparencia. La vasta jurisprudencia emitida sobre la materia por este Alto Tribunal –en sus 24 años de funcionamiento– dan buena cuenta de ello. No es objetivo de este trabajo realizar un estudio sistemático de la jurisprudencia, sino sólo destacar aspectos centrales en relación con el derecho de acceso a la información pública como instrumento para garantizar los derechos de las mujeres a una vida libre de violencia. Bajo esta premisa, se hará una breve referencia a los pronunciamientos del Tribunal Constitucional en relación con tres aspectos esenciales: (i) el contenido constitucionalmente protegido por este derecho, (ii) los sujetos obligados a brindar información pública, y (iii) las excepciones al acceso a la información pública.

3.1. El contenido constitucionalmente protegido del derecho de acceso a la información pública

La cultura de transparencia, inherente a todo Estado democrático constitucional, exige garantizar el derecho fundamental protegido por el artículo 2, inciso 5 de la Constitución. Desde esta óptica, el Tribunal Constitucional sostiene que "el contenido constitucionalmente protegido del derecho de acceso a la información pública es que nadie pueda ser arbitrariamente impedido de acceder a la información que guarden, mantengan o elaboren las diversas instancias y organismos del Estado o personas jurídicas bajo el régimen privado que prestan servicios públicos o ejerzan función administrativa, en virtud de concesión, delegación o autorización" (STC 04912- 2008-PHD/TC, fundamento 6)[21].

[21] La Defensoría del Pueblo realizó una exhaustiva recopilación de la jurisprudencia del Tribunal Constitucional en la que sistematiza los principales criterios de interpretación emitidos por el intérprete supremo de la Constitución en torno al derecho de acceso a la información pública. Ver: Defensoría del Pueblo (2012) *Compendio de Normas: Acceso a la Información Pública*, Lima, pp. 324-398. Asimismo, en el Informe N.º 165, analiza el

Asimismo, en distintos pronunciamientos precisa que, no sólo se afecta el derecho de acceso a la información pública cuando se niega su suministro, sin existir razones constitucionalmente legítimas para ello, sino también cuando la información que se proporciona es fragmentaria, desactualizada, incompleta, imprecisa, falsa, no oportuna o errada (STC 01797-2002-PHD/TC, fundamento 16; STC 04042-2011-PHD/TC, fundamento 10). Del mismo modo, enfatiza que es deber del Estado dar a conocer a la ciudadanía sus decisiones y acciones de manera completa y transparente (STC 05586-2015- PHD/TC, fundamento 2).

3.2. Los sujetos obligados a brindar información pública

En consonancia con lo estipulado por la Ley Modelo Interamericana sobre Acceso a la Información Pública[22], y con lo dispuesto por el artículo 2 de la Ley N.º 27806[23], en constante y uniforme jurisprudencia,

rol del tribunal constitucional en el proceso de hábeas data como mecanismo de tutela judicial del derecho fundamental de acceso a la información pública. Ver: Defensoría del Pueblo (2013), *Balance a diez años de vigencia de la Ley de Transparencia y Acceso a la Información Pública 2003-2013*, Op. Cit., pp. 240-246.

[22] Ley modelo interamericana sobre acceso a la información pública, AG/RES. 2607 (XL-O/10), Aprobada en la cuarta sesión plenaria, celebrada el 8 de junio de 2010. Disponible en: https://bit.ly/3d36Akm

[23] La versión actualizada del artículo 2º de la Ley Nº 27806 (TUO de la Ley 27806, Decreto Supremo 021-2019-JUS), Ley de Transparencia y Acceso a la información pública señala que "se entiende por entidades de la Administración Pública a las señaladas en el artículo I del Título Preliminar de la Ley 27444, Ley del Procedimiento Administrativo General. Pues bien de acuerdo con esta disposición normativa, se entenderá por «entidad» o «entidades» de la Administración Pública: 1. El Poder Ejecutivo, incluyendo Ministerios y Organismos Públicos Descentralizados; 2. El Poder Legislativo; 3. El Poder Judicial; 4. Los Gobiernos Regionales; 5. Los Gobiernos Locales; 6. Los organismos a los que la Constitución Política del Perú y las leyes confieren autonomía; 7. Las demás entidades y organismos, proyectos y programas del Estado, cuyas actividades se realizan en virtud de potestades administrativas y, por tanto se consideran sujetas a las normas comunes de derecho público, salvo mandato expreso de ley que se refiera a otro régimen; y las personas jurídicas bajo el régimen privado que prestan servicios públicos o ejercen función administrativa, en virtud de concesión, delegación o autorización del Estado, conforme a la normativa de la materia.

el Tribunal Constitucional ha precisado quiénes son los obligados a garantizar este derecho. En ese sentido, establece, en primer lugar, que toda autoridad pública perteneciente a todas las ramas del Gobierno (Poderes Ejecutivo, Legislativo y Judicial) y en todos los niveles de la estructura gubernamental interna (central, regional, provincial o distrital) está obligada a responder a las solicitudes de información pública y de desempeñar la función pública bajo el principio de máxima publicidad. (STC 0959- 2004-PHD/TC; STC 03619- 2005-PHD/TC)[24].

En segundo lugar, reafirma lo dispuesto por la Ley de Transparencia y acceso a la información pública y establece que las empresas del Estado están obligadas a suministrar la información con la que cuenten (STC 06674-2013-PHD/TC, fundamento 3). Agrega que tanto el Estado como sus empresas públicas se encuentran en la ineludible obligación de materializar estrategias viables para gestionar sus recursos públicos de manera transparente (STC 04282-2015-PHD/TC, fundamento 4).

En tercer lugar, precisa que las personas jurídicas privadas que efectúen servicios públicos o funciones administrativas también están obligados a brindar información pública. Esta obligación se circunscribe a la información sobre las características de los servicios públicos que prestan, sus tarifas y las funciones administrativas que ejercen (STC 0390-2008-PHD/TC, fundamento 7). Se incluye a las empresas privadas que brindan servicio de transporte aéreo (STC 02636-2009-PHD/TC, fundamento 11).

En este mismo orden de ideas, la Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos, señala que el derecho de acceso a la información pública también vincula a quienes cumplen funciones públicas, presten servicios

[24] Es importante destacar que en relación a la titularidad del derecho de acceso a la información pública, el Tribunal Constitucional precisa que el sujeto activo es toda persona sea natural o jurídica (STC 04877-2006-HD/TC; STC 0644-2004-HD/TC).

públicos o ejecuten, en nombre del Estado, recursos públicos. Respecto de estos últimos, el derecho de acceso a la información pública obliga a suministrar información relacionada con el manejo de los recursos públicos, la satisfacción de los servicios a su cargo y el cumplimiento de las funciones públicas mencionadas[25].

La información suministrada en atención al derecho de acceso a la información pública debe ser gratuita, el/la solicitante debe cubrir sólo el costo de reproducción. En consolidada jurisprudencia, el Tribunal Constitucional ha establecido que el pago solo debe cubrir el costo real de la reproducción de la información (STC 01847- 2013-PHD/TC, fundamento 8; STC 07675-2013-PHD/TC, fundamento 15; STC 03351-2008-PHD/TC)[26]. Refiriéndose al costo y a la forma de entrega de la información solicitada, el Alto Tribunal es enfático en señalar que, en un Estado Social y Democrático de Derecho, la Administración Pública se encuentra en la ineludible obligación de adecuar sus procedimientos a la satisfacción de los ciudadanos y no al revés. La procura de la satisfacción de las necesidades de la ciudadanía es, precisamente, su razón de ser. Por ello, la Administración Pública debe ser la principal garante de la efectividad de los derechos fundamentales que no solamente tienen una dimensión subjetiva [esto es, no valen solo como derechos subjetivos], sino también una dimensión objetiva, puesto que constituyen el orden material de valores en los cuales se sustenta el ordenamiento constitucional (STC 0092-2013-PHD/TC, fundamento 9).

[25] Comisión Interamericana de Derechos Humanos (2011), *El derecho de acceso a la información en el marco jurídico interamericano*, Segunda Edición, Relatoría Especial para la Libertad de Expresión, párrafo 19.

[26] La Defensoría del Pueblo realiza un estudio detallado sobre la jurisprudencia del Tribunal Constitucional en materia de derecho de acceso a la información pública en la que, entre otros, se examinan los pronunciamientos relacionados con los costos de reproducción de la información pública, así como las entidades obligadas a brindar información pública. Ver: Defensoría del Pueblo (2009), *El derecho de acceso a la información pública Normativa, jurisprudencia y labor de la Defensoría del Pueblo*, Documento Defensorial, Núm. 9, Lima. Disponible en: https://bit.ly/3nzk7oS

3.3. Las excepciones al derecho de acceso a la información pública

Un importante número de decisiones del Tribunal Constitucional han recaído sobre las excepciones al derecho fundamental de acceso a la información pública. La premisa de la que parte el Alto Tribunal es que ningún derecho fundamental es absoluto, en consonancia con lo dispuesto por la Constitución y la Ley de Transparencia, sostiene que "ni siquiera la condición de libertad preferida de la que goza el derecho de acceso a la información hace de ella un derecho constitucional que no pueda ser objeto de limitación" (STC 01219-2003-PHD/TC, fundamento 7; STC 03769-2012-PHD/TC; STC 0776-2010-PHD/TC). No obstante, precisamente por tratarse de un derecho fundamental, las excepciones a este derecho se rigen por el principio de taxatividad y por el principio de interpretación restrictiva (STC 03035-2012-PHD/TC; STC 0937-2013-PHD/TC).

El carácter excepcional de las limitaciones al derecho de acceso a la información pública es, a juicio de la Comisión IDH, una consecuencia del principio de máxima divulgación[27]. Desde esta óptica, la Constitución prescribe que el derecho de acceso a la información pública no podrá ser ejercido respecto a informaciones que afecten la intimidad personal, la seguridad nacional, el secreto bancario, la reserva tributaria y las que expresamente sean excluidas por ley (artículo 2, inciso 5). De este modo, la Norma Fundamental establece un sistema restringido de excepciones al derecho de acceso a la información pública.

El Tribunal Constitucional al interpretar las disposiciones constitucionales sobre la materia, establece que las excepciones al derecho de acceso a la información reguladas por el legislador, para ser válidas, deben cumplir las siguientes condiciones: i) deben estar *previstas en*

[27] Comisión IDH (2015) *Acceso a la información, violencia contra las mujeres y la administración de justicia en las Américas, Organización de Estados Americanos*, OEA/Ser.L/V/II.154 Doc.19, párrafo 31.

la ley de forma expresa y estricta, no pudiendo quedar al libre arbitrio de cada entidad de la Administración Pública; ii) deben perseguir *objetivos legítimos* que estén indesligablemente unidos a la protección de un *fin constitucional*; iii) deben ser *estrictamente necesarias* lo que implica además elegir la medida menos restrictiva posible; y iv) deben ser *proporcionales* con el grado de restricción del derecho de acceso a la información pública, de modo que el grado de ventajas o satisfacción del fin constitucional que se quiere proteger con la excepción sea, por lo menos, mayor que el grado de desventajas o restricción del derecho de acceso a la información pública. (STC 0005-2013-PI/TC, fundamento 29)[28].

La Ley sobre la materia, TUO de la Ley N.º 27806, prevé que las excepciones al ejercicio del derecho de acceso a la información pública en sus artículos 15, 16 y 17. Se trata de tres tipos de información taxativamente establecidas: información clasificada expresamente como secreta, información reservada e información confidencial. A este respecto, el Alto Tribunal precisa que, las precitadas excepciones deben ser aplicadas de modo restrictivo y sólo cuando la Administración haya justificado su clasificación como secreta, reservada o confidencial. Si no se ha justificado debidamente, la respectiva clasificación carece de efectos la sola nominación formal (colocación de sellos con las expresiones "secreto" o "reservado"), debiendo en todo caso ser la última instancia administrativa en materia de transparencia y acceso a la información pública la encargada de examinar si la información calificada de secreta o reservada reviste realmente o no tal carácter. (STC 0005-2013-PI/

[28] La defensoría del Pueblo elaboró un Manual destinado a los funcionarios públicos en el que, a través de preguntas y respuestas sobre la aplicación e interpretación de las excepciones al derecho de acceso a la información pública elaboradas sobre la base de lo prescrito por la Ley de Transparencia y la jurisprudencia del Tribunal Constitucional, da cuenta del sistema restringido de excepciones al derecho de acceso a la información pública. Ver: Defensoría del Pueblo (2016), *Manual para funcionarios sobre excepciones al derecho de acceso a la información pública,* Lima. Disponible en: https://bit.ly/2Il4QI5

TC, fundamento 33; STC 0950-00-PHD/TC; STC 01805-2007-PHD/TC; 5173-2011-PHD/TC; STC 01805-2007-PHD/TC; STC 01388-2012-PHD/TC)[29].

4. El derecho de acceso a la información pública como instrumento para garantizar los derechos de las mujeres a una vida libre de violencia

El derecho de acceso a la información pública es un derecho convencional y constitucional. La importancia de este derecho reside no sólo en su carácter consustancial al régimen democrático, en la medida que –como bien señala el Tribunal Constitucional– concreta el principio de dignidad de la persona humana y constituye un elemento esencial de las exigencias propias de la sociedad democrática (Sentencia 01797-2002-PHD/TC, fundamento 11), sino también su carácter relacional o dimensión instrumental.

En reiterada jurisprudencia, el Tribunal Constitucional se pronuncia sobre la importancia del carácter relacional del derecho de acceso a la información pública. Tempranamente, deja establecido que este derecho tiene una doble vertiente: individual y colectiva. En su vertiente individual, nos dice el Alto Tribunal, garantiza que nadie sea arbitrariamente impedido de acceder a la información que guarden, mantengan o elaboren las diversas instancias y organismos que pertenezcan al Estado, sin más limitaciones que aquellas que se han previsto como constitucionalmente legítimas. A través de este derecho se posibilita que los individuos (…) puedan trazar, de manera libre, su proyecto de vida, pero también el pleno ejercicio y disfrute de otros

[29] A título de ejemplo, se pueden citar las siguientes sentencias sobre procesos de hábeas data en los que se abordan los tipos de información sujetos a excepción: (i) información secreta: STC 950-00-PHD/TC; STC 01805-2007-PHD/TC, (ii) Información reservada: STC 05517-2011-PHD/TC, y (iii) Información confidencial: STC 01480-2003-PHD/TC; 04407-2007-PHD/TC. Un resumen de estos fallos puede encontrarse en: Defensoría del Pueblo (2016), *Manual para funcionarios sobre excepciones al derecho de acceso a la información pública,* Op. Cit., pp. 88-95.

derechos fundamentales. Desde esta perspectiva, en su vertiente individual, el derecho de acceso a la información se presenta como un presupuesto o medio para el ejercicio de otras libertades fundamentales (STC 1707-2002-PHD/TC; STC 1219-2003-PHD/TC; STC 04912-2008-PHD/TC)[30].

En esta misma línea argumentativa, la Comisión Interamericana de Derechos Humanos afirma que, el derecho de acceso a la información pública está estrechamente vinculado con el disfrute de otros derechos humanos[31]. Bajo esta premisa, emite un importante informe sobre la materia: «Acceso a la información, violencia contra las mujeres y la administración de justicia en las Américas» en el que examina la dimensión instrumental de este derecho para el respeto y garantía del derecho de las mujeres a una vida libre de violencia por razones de género[32].

En el referido *Informe,* la Comisión IDH precisa dos cuestiones esenciales en relación con el derecho de acceso a la información pública en su dimensión instrumental para el derecho de las mujeres a una vida libre de violencia. La primera es que, el citado carácter se asocia tanto a la prevención de la discriminación y la violencia, como al acceso a la justicia de las mujeres. La segunda precisión está referida a las obligaciones que genera para los Estados parte del Sistema Interamericano de Derechos Humanos, las cuales, a juicio de la Comisión son tres: (i) la obligación de recolectar y producir información, (ii) la obligación de transparencia activa y (iii) la obligación de responder de manera oportuna las solicitudes de acceso a la información y garantizar un recurso efectivo que permita la satisfacción del derecho.

[30] En la sentencia recaído en el Expediente N.º 1219-2003-PHD/TC, el Alto Tribunal precisa que el derecho de acceso a la información tiene una naturaleza relacional, en tanto permite la realización de otros derechos fundamentales (fundamento 4).

[31] Comisión IDH (2011), El derecho de acceso a la información en el marco jurídico interamericano, Relatoría Especial para la Libertad de Expresión, párrafo 4.

[32] Comisión IDH (2015) *Acceso a la información, violencia contra las mujeres y la administración de justicia en las Américas, Organización de Estados Americanos,* OEA/Ser.L/V/II.154 Doc.19. Disponible en: https://bit.ly/2SJAwIU

4.1. La obligación de recolectar y producir información

En relación con la obligación de recolectar y producir información, la Convención Interamericana para Prevenir, Sancionar y Erradicar la violencia contra las Mujeres (Convención Belém do Pará) establece que los Estados parte, como es el caso de Perú[33], convienen en adoptar, en forma progresiva, medidas específicas inclusive programas para:

> "H) garantizar la investigación y recopilación de estadísticas y demás información pertinente sobre las causas, consecuencias y frecuencia de la violencia contra la mujer, con el fin de evaluar la eficacia de las medidas para prevenir, sancionar y eliminar la violencia contra la mujer y de formular y aplicar los cambios que sean necesarios".

En coherencia con los lineamientos establecidos por la Convención Belém do Pará, las recomendaciones del Comité para la Eliminación de la Discriminación contra la Mujer (CEDAW)[34] y el Informe del Secretario General de Naciones Unidas sobre la intensificación de los esfuerzos para eliminar todas las formas de violencia contra las mujeres [35], la Comisión IDH sostiene que los Estados parte tienen una obliga-

[33] La Convención Belém do Pará fue suscrita en el Vigésimo Cuarto Periodo Ordinario de Sesiones de la Asamblea General de la Organización de los Estados Americanos en Belém do Pará Brasil, el 9 de junio de 1994. En el Perú la Convención Belém do Pará fue aprobada por Resolución Legislativa N.º 26583 de 22 de marzo de 1996. Fue ratificada el 4 de abril de 1996 y depositada el 4 de junio de 1996. Finalmente, entró en vigencia el 4 de julio de 1996.

[34] Bareiro, L. (2017), Entre la igualdad legal y la discriminación de hecho Recomendaciones del Comité para la Eliminación de la Discriminación contra la Mujer (CEDAW) a los Estados de América Latina y el Caribe, Comisión Económica para América Latina y el Caribe (CEPAL). Disponible en: https://bit.ly/3jRcW97. La Convención sobre la Eliminación de todas formas de Discriminación contra la Mujer (CEDAW), fue aprobada en el Perú mediante Resolución Legislativa N.º 23432 publicada el 4 de junio de 1982. Fue ratificada el 20 de agosto de 1982 y entró en vigencia el 13 de octubre del mismo año.

[35] Naciones Unidas (2012), Intensificación de los esfuerzos para eliminar todas las formas de violencia contra la mujer. Informe del Secretario General, U.N. Doc. A/67/220.

ción específica de producir estadísticas adecuadas e información pertinente sobre las causas, consecuencias y frecuencia de la violencia contra las mujeres. Información que debe servir de base para la formulación, diseño y la evaluación de las políticas públicas adoptadas para prevenir, sancionar y erradicar la violencia y la discriminación contra las mujeres. (Comisión IDH, 2015, párrafo 50).

El cumplimiento de esta obligación es aún una tarea pendiente en los países signatarios de la Convención Belém do Pará y también de los Estados parte de la CEDAW. En ese sentido, Bareiro pone de relieve que un problema generalizado en las Observaciones y Recomendaciones del Comité CEDAW a los países ha sido la recogida, el análisis y la difusión de datos desagregados por sexo (…). Del mismo modo, la Política Nacional de Igualdad de Género, aprobada por Decreto Supremo N.º 008 -2019-MIMP, da cuenta que en el Perú, hacia abril de 2019, fecha en fuera publicada la disposición normativa, la invisibilización de la discriminación contra las mujeres en procesos de generación de conocimiento e información estadística, así como la ausencia de estudios estadísticos específicos encargados de identificar patrones discriminatorios y su grado de prevalencia, son problemas públicos persistentes. En consecuencia, se enfatiza en la necesidad de implementar mejoras en los mecanismos de recolección de información del Instituto Nacional de Estadística e Informática (INEI) y de los registros administrativos que miden los avances en el cumplimiento de los objetivos prioritarios de la Política Nacional de Igualdad de Género.

4.2. La obligación de transparencia activa

La transparencia activa en relación con el derecho de acceso a la información pública en su dimensión instrumental para el derecho de las mujeres a una vida libre de violencia implica obligación del Estado de difundir información sobre los derechos de las mujeres y las vías legales para exigirlos y hacerlos efectivos, así como información relacionada con el desarrollo de leyes y políticas públicas sobre violencia y discriminación. La Comisión subraya que dicha información debe ser

completa, comprensible, con un lenguaje accesible y encontrarse actualizada (Comisión IDH, 2015, párrafo 62).

En el ámbito judicial, la obligación de transparencia activa implica el deber del Estado de promover un acceso efectivo de las mujeres a información, en su idioma, sobre sus derechos, la forma de acceder a las instancias judiciales de protección y prevención, el procesamiento de los casos y las formas de contribuir a la investigación y el esclarecimiento de los hechos. Al respecto, la CIDH ha recomendado a los Estados que garanticen, especialmente, el acceso a la información necesaria para que las mujeres conozcan las medidas de protección que contempla la legislación ante un riesgo inminente de violencia, así como las vías para exigirlas judicialmente y para obtener su ejecución e implementación por parte de la policía. (Comisión IDH, 2015, párrafo 62)

4.3. La obligación de responder de manera oportuna las solicitudes de acceso a la información y garantizar un recurso efectivo que permita la satisfacción del derecho.

Esta obligación supone que los Estados deben responder de manera oportuna, completa y accesible a las solicitudes de información que les sean formuladas. En consecuencia, a juicio de la Comisión IDH, los Estados deben contar con un recurso que permita la satisfacción del derecho de acceso a la información y a contar con un recurso judicial idóneo y efectivo para la revisión de las negativas de entrega de información.

La Comisión IDH advierte que, en relación con la información para prevenir y erradicar la violencia contra las mujeres, los Estados deben asegurar de manera proactiva que la información de interés público que se obtiene mediante solicitudes de información sea posteriormente divulgada y esté disponible a toda la sociedad, de manera que no sea necesario el uso de recursos para obtenerla.

La Corte Constitucional de Colombia, en la sentencia T-735/17, emitida en diciembre de 2017, se ha pronunciado sobre el derecho de

acceso a la información como instrumento para garantizar los derechos de las mujeres a una vida libre de violencia. En el citado fallo, sostiene que la prerrogativa de hábeas data en los casos de mujeres que han sido víctimas de violencia adquiere un carácter instrumental para el ejercicio de su derecho al acceso a la justicia y para hacer efectivas ante las distintas autoridades las medidas de protección dictadas en su favor en cualquier lugar del país y ante cualquier entidad.

Una cuestión sumamente relevante sobre la que pone énfasis la Corte Constitucional es en que la falta de información sobre el estado del proceso puede impedir el derecho a la defensa. En consecuencia, a juicio de este Alto Tribunal, resulta indispensable que las entidades públicas y privadas encargadas y responsables de las bases de datos que contienen información sobre actos de violencia en contra de mujeres garanticen el ejercicio pleno y efectivo del derecho al hábeas data, poniendo a su disposición la información que requieran y los medios para lograr la actualización, la rectificación y la supresión o cancelación de la información, de forma que puedan ejercer su derecho al acceso a la justicia, así como hacer uso de los distintos mecanismos de protección previstos por el ordenamiento jurídico[36].

Para finalizar, es preciso señalar que, cualquier persona que considere vulnerado su derecho de acceso a la información pública (frente a la negativa de entregar información pública), tiene dos vías alternativas para hacer efectivo su derecho: (i) acudir al Tribunal de Transparencia y Acceso a la Información –creado por el Decreto Legislativo 1353–, o (ii)

[36] Corte Constitucional de Colombia, sentencia T-735/17, 15 de diciembre de 2017. Disponible en: https://bit.ly/3iVlpXr. El Tribunal Constitucional se ha pronunciado hasta en cuatro oportunidades en relación con el derecho fundamental de las mujeres a una vida libre de violencia. Se trata de: (i) tres procesos de amparo iniciados contra resoluciones fiscales que archivaron denuncias penales por delitos de violación de la libertad sexual (STC 03090-2012-PA/TC; 05121-2015-PA/TC; STC 01479-2018-PA/TC), y (ii) una demanda de amparo contra una resolución judicial que dictó medidas de protección en favor de una mujer víctima de violencia psicológica, en el marco de la Ley N.º 30364. (STC 03378-2019-PA/TC).

acudir directamente a la autoridad judicial (Poder Judicial)[37]. Conforme al diseño normativo actual, no es necesario acudir previamente, sino alternativamente, al Tribunal de Transparencia y Acceso a la Información.

5. A modo de conclusiones

Una de las finalidades principales del proceso constitucional de hábeas data es la protección del derecho fundamental de acceso a la información pública. Derecho que cuenta con un amplio marco normativo convencional, constitucional y legal, reforzado por la jurisprudencia de la Corte Interamericana de Derechos Humanos y el Tribunal Constitucional.

La Corte IDH y el Tribunal Constitucional desempañan un papel sumamente importante en el desarrollo y consolidación del derecho de acceso a la información pública. Los criterios interpretativos fijados por el Tribunal Constitucional en relación con el contenido constitucionalmente protegido por el derecho de acceso a la información pública, los sujetos obligados a brindar información y, entre otros, el régimen limitado de excepciones, son de obligatorio cumplimiento por el Poder Judicial y el Tribunal de Transparencia y Acceso a la Información que son los garates, en primera instancia del derecho de acceso a la información pública.

El derecho fundamental de acceso a la información pública en su dimensión relacional es un instrumento esencial para garantizar el derecho de las mujeres a una vida libre de violencia. Desde esta óptica, genera tres tipos de obligaciones concretas a los Estados parte del sistema Interamericano de Derechos Humanos: (i) la obligación de recolectar y producir información, (ii) la obligación de transparencia activa

[37] Conforme lo dispone el Código Procesal Constitucional, el requisito para iniciar el proceso constitucional de hábeas data es que la persona afectada debe requerir a la autoridad pública la entrega de la información con un documento de fecha cierta. Luego de diez días de presentado el documento con respuesta negativa, parcial o sin respuesta, tiene expedito su derecho para iniciar el proceso de hábeas data. (artículo 62)

y (iii) la obligación de responder de manera oportuna las solicitudes de acceso a la información y garantizar un recurso efectivo que permita la satisfacción del derecho.

Bibliografía

- Abad Yupanqui, S. (2019), "Prólogo", Ministerio de Justicia y Derechos Humanos, *Compendio. Transparencia y acceso a la información pública,* Tribunal de Transparencia y Acceso a la Información Pública, Lima. Disponible en: https://bit.ly/30WSUCy
- Bareiro, L. (2017), Entre la igualdad legal y la discriminación de hecho Recomendaciones del Comité para la Eliminación de la Discriminación contra la Mujer (CEDAW) a los Estados de América Latina y el Caribe, Comisión Económica para América Latina y el Caribe (CEPAL). Disponible en: https://bit.ly/3jRcW97.
- Comisión IDH (2015), *Acceso a la información, violencia contra las mujeres y la administración de justicia en las Américas, Organización de Estados Americanos*, OEA/Ser.L/V/II.154 Doc.19. Disponible en: https://bit.ly/2SJAwIU
- Comisión IDH (2020), *Derecho de acceso a la información y seguridad nacional,* Relatoría Especial para la Libertad de Expresión de la Comisión IDH, Organización de Estados Americanos OEA/Ser.L/V/II CIDH/RELE/INF.24/20. Disponible en: https://bit.ly/3iONoIA
- Corte IDH (2019), Control de Convencionalidad, *Cuadernillo de jurisprudencia de la Corte IDH,* núm. 7. Disponible en: https://bit.ly/30S3Hy0
- Coteño Muñoz, A. (2019) "Transparencia (judicial)", *Eunomía. Revista en Cultura de la Legalidad*, Núm.16, pp. 198-218.

- Defensoría del Pueblo (2012), *Compendio de Normas: Acceso a la Información Pública*, Compendio 5, Lima. Disponible en: https://bit.ly/2GOoPhU

- Defensoría del Pueblo (2013), *Balance a diez años de vigencia de la Ley de Transparencia y Acceso a la Información Pública 2003-2013*, Informe Defensorial N.º 165, Lima.

- Defensoría del Pueblo (2016), *Manual para funcionarios sobre excepciones al derecho de acceso a la información pública,* Lima. Disponible en: https://bit.ly/2Il4QI5

- Do Vale, A. R (2016), *La deliberación en los Tribunales Constitucionales,* Centro de Estudios Políticos y Constitucionales, Madrid.

- Fernández Visa, Y. (2016), "La influencia de la Sentencia de la Corte Interamericana de Derechos Humanos "Claude Reyes contra Chile" en la jurisprudencia del Tribunal Europeo de Derechos Humanos", *Eunomía. Revista en Cultura de la Legalidad,* Núm. 9, pp. 321-333.

- González Morales, F. (2016) "Pasado, presente y futuro del sistema interamericano de derechos humanos", Santolaya, P. y Wences, I. (Coords.), *La América de los Derechos,* Centro de Estudios Políticos y Constitucionales, Madrid, pp. 55- 80.

- Hitters, J. C. (2008) ¿Son vinculantes los pronunciamientos de la Comisión y de la Corte Interamericana de derechos humanos? Control de constitucionalidad y convencionalidad, *Revista iberoamericana de Derechos Procesal Constitucional,* Núm. 10, pp. 131-155.

- Landa Arroyo, C. (2018), El proceso constitucional de hábeas data, en *Derecho procesal constitucional,* Pontificia Universidad Católica del Perú, Lima, pp. 139-144.

HÁBEAS DATA
DE ACCESO A LA INFORMACIÓN PÚBLICA

Comentarios a la jurisprudencia
STC Exp N.° 1508-2016-PHD/TC

(Publicada el 21 de agosto de 2019)

✍ Susana Távara Espinoza*

1. Introducción

El análisis jurisprudencial del proceso signado como expediente 01508-2016-PHD/TC, intenta cumplir con los objetivos del presente trabajo Colectivo, en el sentido de colaborar con un aporte sencillo pero actualizado de lo que, el Tribunal Constitucional del Perú, viene trabajando en materia del proceso de hábeas data. Resulta interesante que la Dirección de Publicaciones y Documentación del Centro de Estudios Constitucionales haya optado por abordar un proceso de alta importancia y que, salvo excepciones, no ha sido analizado detenidamente por la doctrina procesal constitucional peruana.

Es por ello, que estoy segura que esta obra, resultará de gran ayuda a los interesados y estudiosos en Derecho pero sobre todo a los estudiantes y futuros profesionales.

* Abogada, Maestría en Derecho de la Empresa por la PUCP, estudios en Argumentación Jurídica en la Universidad de Pisa- Italia, docente, ex Secretaria General del TC y actual Directora Académica del Centro de Estudios Constitucionales del Tribunal Constitucional del Perú.

En cuanto al proceso constitucional de hábeas data el Tribunal Constitucional como órgano supremo de interpretación y control de la constitucionalidad, es ya conocido que es autónomo e independiente, porque en el ejercicio de sus atribuciones no depende de ningún órgano constitucional. Se encuentra sometido a la Constitución (artículo 202, inciso 2, establece que corresponde al TC…conocer, en última y definitiva instancia, las resoluciones denegatorias de los procesos de hábeas corpus, amparo, hábeas data y cumplimiento), y a su Ley Orgánica, donde se especifica que se trata de un proceso de tutela de derechos, que tiene por objeto la tutela jurisdiccional de los derechos constitucionales.

El hábeas data tiene por objeto la protección de los derechos reconocidos en los incisos 5) y 6) del artículo 2º de la Constitución, donde se establece que "toda persona tiene derecho a solicitar sin expresión de causa la información que requiera y a recibirla de cualquier entidad pública, en el plazo legal, con el costo que suponga su pedido. Se exceptúan las informaciones que afectan la libertad personal y las que expresamente se excluyan por ley o por razones de seguridad nacional"; y, "que los servicios informáticos, computarizados o no, o privados, no suministren informaciones que afecten la intimidad personal y familiar, respectivamente (STC 06227-2013-PHD/TC, Fd. 9)

2. Antecedentes del caso:

Con fecha 25 de agosto de 2015, don Segundo Demetrio Pastor Cerna interpone demanda de hábeas data solicitando que se ordene a la Intendencia Regional de Lambayeque de la Superintendencia Nacional de Aduanas y de Administración Tributaria (Sunat) a entregarle copias de todas las páginas del expediente coactivo iniciado contra la empresa Madre Dolorosa Distribuidores E.I.R.L., de la cual es su gerente. Señala que, mediante documento de fecha 03 de julio de 2015, solicitó

las referidas copias, petición que fue reiterada mediante documento de fecha 06 de julio de 2015; sin embargo, hasta la fecha no ha sido atendida por la Sunat. En este sentido, pese a los requerimientos del actor, la emplazada no ha cumplido con proporcionarle la información requerida; por tanto, considera que se ha vulnerado su derecho de acceso a la información pública reconocido en el artículo 2, inciso 5, de la Constitución.

3. Materias constitucionalmente relevantes

En la STC **N° 01508-2016-PHD/TC** el Tribunal Constitucional debe determinar la demanda por haberse acreditado la vulneración al derecho de acceso a la autodeterminación informativa y acceso a la información pública, ambas como contenido objetivo del desarrollo jurisprudencial del Tribunal Constitucional en esta materia.

4. Cuestión procesal previa

El hábeas data es un proceso constitucional que en el Perú tiene por objeto la protección de los derechos reconocidos en los incisos 5 y 6 del artículo 2 de la Constitución, los cuales establecen lo siguiente:

> *"Toda persona tiene derecho:*
>
> *(…)*
>
> *5. A solicitar sin expresión de causa la información que requiera y a recibirla de cualquier entidad pública, en el plazo legal, con el costo que suponga el pedido. Se exceptúan las informaciones que afectan la intimidad personal y las que expresamente se excluyan por ley o por razones de seguridad nacional.*
>
> *(…)*
>
> *6. A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar".*

5. Justificación del acceso a la información pública:

5.1. Estado democrático, transparencia y publicidad de los asuntos públicos[1]

Una de las características esenciales de un Estado democrático es la publicidad de sus actos y la transparencia de la administración estatal sobre la gestión de los asuntos públicos, lo cual implica que todas las entidades del Estado rindan cuentas a la ciudadanía y que las personas puedan solicitar la información que obra en poder de dichas entidades, pues una forma de combatir la corrupción es erradicar "el secretismo" y fomentar una "cultura de transparencia". En este sentido, los funcionarios y servidores públicos deben ser considerados como gestores de una organización creada al servicio de la ciudadanía, encontrándose expuestos permanentemente a la fiscalización de la sociedad respecto de las decisiones que adoptan.

Por ello, en un Estado democrático se debe poner a disposición de la ciudadanía, en forma accesible, todos aquellos datos relacionados con la gestión de los asuntos públicos y, asimismo, se debe reconocer el derecho de las personas a solicitar y obtener la información que obra en su poder. Esta moderna concepción sobre el derecho de los ciudadanos a acceder a la información del Estado ha sido reconocida en diversos instrumentos nacionales y de derechos humanos.

Habiéndose reconocido el derecho de acceso a la información pública en el artículo 2º, numeral 5) de la Constitución Política y específicamente en la Ley de Transparencia y Acceso a la Información Pública, Ley Nº 27806,10 modificada por la Ley Nº 27927.11.

[1] Defensoría del Pueblo(2009). "El derecho de acceso a la información pública, Normativa, jurisprudencia y labor de la Defensoría del Pueblo". Primera edición: Lima, Perú, pp. 23-24.

5.2. Demanda Hábeas Data Caso Rodrigo Villarán Contavalli[2]

(…)

Fundamento 4: El principio de publicidad de la actividad estatal debe promover las condiciones para que la sociedad pueda exigir sin mayores trámites, papeleos o demoras la información pública requerida. Se pretende con ello erradicar cualquier vestigio de la "cultura del secreto", bajo la cual la Administración se estimaba "propietaria" de los documentos, archivos e información de naturaleza pública. Desde esta equivocada perspectiva, las entidades estatales muchas veces sentían que podían decidir discrecionalmente si entregaban o no la información pública solicitada.

6. Análisis:

El artículo 11 del Código Tributario, prescribe que el domicilio fiscal del contribuyente es fijado para todo efecto tributario; mas no, para la notificación de la respuesta al procedimiento administrativo de acceso a la información propia del administrado que consta en su expediente administrativo o en cualquier otra fuente de almacenamiento o registro (derecho a la autodeterminación informativa). El administrado (su representante o abogado) puede solicitar, de manera directa y verbalmente, el acceso en físico al expediente administrativo o a cualquier otro documento referido a su persona; así como solicitar, en ese mismo acto y de manera verbal, la entrega copias del expediente o de los documentos accedidos. Con la sola solicitud verbal del administrado, las referidas peticiones deben ser aceptadas inmediatamente por la Administración, sin excusa alguna de programación previa, carga procesal, falta de personal, etc. y previo pago del costo de reproducción en caso de la solicitud de copias. De allí que los artículos 55 y 160 de la Ley 27444, vigentes al momento de ocurridos los hechos, dispongan:

[2] STC 04912-2008-PHD/TC- Tribunal Constitucional del Perú

"Artículo 55.- Derechos de los administrados

Son derechos de los administrados con respecto al procedimiento administrativo, los siguientes:

(…)

Acceder, en cualquier momento, de manera directa y sin limitación alguna a la información contenida en los expedientes de los procedimientos administrativos en que sean partes y a obtener copias de los documentos contenidos en el mismo sufragando el costo que suponga su pedido, salvo las excepciones expresamente previstas por ley".

"Artículo 160.- Acceso a la información del expediente

160.1 *Los administrados, sus representantes o su abogado, tienen derecho de acceso al expediente en cualquier momento de su trámite, así como a sus documentos, antecedentes, estudios, informes y dictámenes, obtener certificaciones de su estado y recabar copias de las piezas que contiene, previo pago del costo de las mismas. (...)*

160.2 *El pedido de acceso podrá hacerse verbalmente y se concede de inmediato, sin necesidad de resolución expresa, en la oficina en que se encuentre el expediente, aunque no sea la unidad de recepción documental.*

El Tribunal Constitucional ya ha tenido la oportunidad de pronunciarse sobre la obligación de la Administración de notificar, en el domicilio del peticionante, la respuesta a su solicitud de acceso a su información propia (autodeterminación informativa), en el Expediente Nº 00742-2017-HD/TC, fundamento 6, se expresó que:

"(. ..) la emplazada debió comunicar a la actora que la información solicitada se encontraba a su disposición, previo pago del costo de reproducción, máxime si la recurrente en su solicitud de información (...) señaló su domicilio. También debió ser informado, a criterio de este Tribunal, del monto que debía pagar la actora, a fin que pueda iniciar los trámites correspondientes. Por consiguiente, al no haberse cumplido con notificar a la administrada para que pudiera apersonarse a la institución emplazada a recoger la información solicitada, corresponde estimar la demanda".

Por tanto, no habiéndose acreditado que el recurrente haya recibido efectivamente la información solicitada, es evidente que se vulneró su derecho a la autodeterminación informativa, debiendo estimarse la demanda.

En consecuencia, el Tribunal Constitucional del Perú, declaró fundada la demanda por haberse acreditado la vulneración al derecho de acceso a la autodeterminación informativa. y, de conformidad con lo dispuesto por el artículo 56 del Código Procesal Constitucional, ordenó que la demandada asuma el pago de los costos procesales, que serán liquidados en la etapa de ejecución de sentencia.

7. Sobre el Fallo

El Tribunal Constitucional decide declarar FUNDADA la demanda por haberse acreditado la vulneración al derecho de acceso a la autodeterminación informativa.

Como medida adicional, ordena a la Intendencia Regional de Lambayeque de la Superintendencia Nacional de Aduanas y de Administración tributaria - SUNAT, a brindar la información requerida, previo pago del costo de reproducción.

De igual forma, ordena a la Intendencia Regional de Lambayeque de la Superintendencia Nacional de Aduanas y de Administración tributaria - SUNAT el pago de costos procesales a favor del recurrente.

De esta manera se hace un análisis del hábeas data de naturaleza administrativo/tributaria de como se viene dotando de contenido a este proceso en la actual jurisprudencia constitucional.

BREVES APUNTES SOBRE LOS PRINCIPALES AUTORES Y CASOS CLÁSICOS QUE DIERON ORIGEN A LA PROTECCIÓN DEL DERECHO A LA PRIVACIDAD

A propósito del derecho fundamental a la *autodeterminación informativa*

Bruno Novoa Campos*

1. Justificación previa

Nuestra Constitución Política en el numeral 6 del artículo 2, establece que toda persona tiene derecho "a que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar". (CP, 1993). Mientras que el Código Procesal Constitucional establece en el numeral 2 del artículo 61, que toda persona puede acudir al proceso constitucional de hábeas data para "conocer, actualizar, incluir y suprimir o rectificar la información o datos referidos a su persona que se encuentren almacenados o registrados en forma manual, mecánica o informática, en archivos, bancos de datos o registros de entidades públicas o de instituciones privadas que brinden servicio o acceso a terceros. (…)". (CPC, 2004).

* Miembro de la Asociación Peruana de Derecho Constitucional.

Al respecto, el Tribunal Constitucional estableció que el derecho reconocido en el numeral 6 del artículo 2, de la Constitución Política "es denominado por la doctrina derecho a la *autodeterminación informativa* y tiene por objeto proteger la intimidad, personal o familiar, la imagen y la identidad frente al peligro que representa el uso y la eventual manipulación de los datos a través de los ordenadores electrónicos" (TC, 2003).

De este modo, el derecho a la *autodeterminación informativa* a través del proceso constitucional de hábeas data comprende:

i) "Acceder a los registros de información, computarizados o no, cualquiera que sea su naturaleza, en los que se encuentren almacenados los datos de una persona. Tal acceso puede tener por objeto que se permita conocer qué es lo que se encuentra registrado, para qué y para quién se realizó el registro de información así como la (o las) persona(s) que recabaron dicha información" (TC, 2003);

ii) "Agregar datos al registro que se tenga, ya sea por la necesidad de que se actualicen los que se encuentran registrados, o bien con el fin de que se incluyan aquellos no registrados, pero que son necesarios para que se tenga una cabal referencia sobre la imagen e identidad de la persona afectada" (TC, 2003);

iii) "Rectificar la información, personal o familiar, que se haya registrado" (TC, 2003);

iv) "Impedir que esta se difunda para fines distintos de aquellos que justificaron su registro" (TC, 2003); o, incluso,

v) "Cancelar aquellos que razonablemente no debieran encontrarse almacenados" (TC, 2003).

En este sentido, el derecho a la *autodeterminación informativa* debe considerarse "un derecho de naturaleza relacional, pues las

exigencias que demandan su respeto, se encuentran muchas veces vinculadas a la protección de otros derechos constitucionales" (TC, 2003); por lo que se debe diferenciar:

i) Del derecho a la intimidad, personal o familiar, reconocido en el inciso 7) del mismo artículo 2° de la Constitución Política, en tanto este derecho protege el derecho a la vida privada, esto es, el poder jurídico de rechazar intromisiones ilegítimas en la vida íntima o familiar de las personas, mientras que la *autodeterminación informativa* garantiza la facultad de todo individuo de poder preservarla controlando el registro, uso y revelación de los datos que les conciernen (TC, 2003);

ii) Del derecho a la imagen, reconocido en el inciso 7) del artículo 2° de la Constitución Política que protege básicamente la imagen del ser humano, derivada de la dignidad de la que se encuentra investido, mientras que el derecho a la *autodeterminación informativa*, en este extremo, garantiza que el individuo sea capaz de disponer y controlar el tipo de datos que sobre él se hayan registrado, a efectos de preservar su imagen derivada de su inserción en la vida en sociedad (TC, 2003); y,

iii) "Del derecho a la identidad personal, esto es, del derecho a que la proyección social de la propia personalidad no sufra interferencias o distorsiones a causa de la atribución de ideas, opiniones, o comportamientos diferentes de aquellos que el individuo manifiesta en su vida en sociedad" (TC, 2003).

Planteado el panorama del derecho fundamental a la *autodeterminación informativa*, consideramos necesario presentar breves apuntes sobre los principales autores y casos clásicos que dieron origen a la protección del derecho a la privacidad, con el propósito de conocer de primera mano los aportes más destacados y casos emblemáticos que han contribuido y contribuyen al permanente debate sobre el derecho a la privacidad.

2. Autores clásicos

- **Thomas McIntyre Cooley**

Cooley publicó en 1878 su obra denominada *A Treatise on the Law of Torts or the Wrongs Which Arise Independently of Contract.* En esta obra sobresale lo que Cooley denominaría "the right to be let alone" ("el derecho a ser dejado solo").

De este modo, al momento de abordar el derecho a la inmunidad personal, Cooley consideró que el *derecho a estar solo* cristaliza una suerte de inmunidad personal completa, como se aprecia a continuación:

> **Inmunidad personal.** Se puede decir que este derecho puede ser llamado derecho de inmunidad completa: A ser dejado solo. El deber correspondiente es, no infligir daño, y no, dentro de tal proximidad que pueda hacer que tenga éxito, para intentar infligir una herida (…). Por lo general, implica un insulto, un miedo (…). Es muy probable que haya un shock en los nervios y la paz y la tranquilidad del individuo se altera durante un período de mayor o menor duración. Por consiguiente, hay abundantes razones en apoyo del Estado de derecho (…) (Cooley, 1879, 29)

- **Samuel D. Warren y Louis D. Brandeis**

Samuel D. Warren y Louis D. Brandeis publicaron su artículo denominado "The right to privacy", en Harvard Law Review el 15 de diciembre de 1890. Los principales argumentos para defender la tesis sobre el derecho a la privacidad de las personas se centran en dos grandes pilares.

El primero de ellos presenta un interesante enfoque de continuidad y constante actualización de los derechos que supera el mismo nombre de su artículo y mantiene vigencia a pesar de haber sido escrito hace poco más de 129 años, como se puede apreciar de sus ideas fuerza que se muestran a continuación:

i) La protección de la persona es un principio muy antiguo en el derecho que de vez en cuando requiere de nuevo definir su naturaleza y el alcance de dicha protección;

ii) Los pensamientos, emociones y sensaciones del hombre también exigen su reconocimiento en el desarrollo y crecimiento de la ley y la jurisprudencia;

iii) No se puede justificar la vulneración de un derecho mostrando las desgracias y flaquezas de nuestro prójimo;

iv) Cada individuo determina en qué medida comunica a los demás sus pensamientos, sentimientos y emociones; y,

v) La protección de los pensamientos, sentimientos y emociones de hombre forman parte de un derecho más general para ser dejado solo (Warren y Brandeis, 1890).

El segundo pilar de su tesis se justifica sobre la base de lo establecido en la jurisprudencia más relevante de la época. De este modo, ambos pilares apuntan a superar la idea de un abuso de confianza y/o de contratos implícitos en las actuaciones de las personas y defiende la independencia de un verdadero derecho a la privacidad que responde de mejor modo a las diferentes circunstancias que pueden vulnerar este derecho.

Al respecto, Patricia Sánchez Abril, Doctora en Derecho por Harvard Law School, relacionó de manera bastante interesante los argumentos de Warren y Brandeis con la obra de Charles Fried (Cf. *An Anatomy of Values: Problems of personal and social choice*. Cambridge: Harvard University Press, 1970).

Así, considerando que para Fried "la intimidad es el intercambio de información sobre las acciones de uno, creencias o emociones que uno no comparte con todos, y que tiene derecho a no compartir con cualquiera. Y que, al conferir este derecho, la privacidad crea el capital moral que traslada nuestra amistad y amor" (Charles Fried, 1970:

142), Sánchez Abril señaló que, "la normativa relacionada a los daños por privacidad, debe cumplir los códigos de civilidad socialmente aceptados entre los miembros de una comunidad, con el propósito de salvaguardar la intimidad y los lazos sociales" (Harvard Journal of Law & Technology, 2007).

- **William L. Prosser**

Asimismo, William L. Prosser publicó su artículo denominado "Privacy", en California Law Review en agosto de 1960. Lo resaltante de su publicación se centra en la clasificación que utiliza para analizar la invasión de la privacidad de las personas, la cual puede darse por:

i) la intrusión;

ii) la divulgación pública de hechos privados;

iii) la publicidad que falsea la imagen de una persona; y,

iv) la apropiación del nombre o de la imagen de una persona (Prosser, 1960).

Sobre la teoría de Prosser, Paul M. Schwartz, Profesor de Derecho de la Universidad de California, Berkeley y, Karl-Nikolaus Peifer, Profesor de Derecho de la Universidad de Colonia, Alemania, concluyeron lo siguiente:

> Si bien la tesis de privacidad de William Prosser puede que no sea perfecto, ha demostrado ser previsor, pragmático y muy persuasivo. Sus cuatro categorías de daños han proporcionado una seguridad conceptual útil para los jueces y legisladores estatales y alentó la aceptación de la protección de la privacidad en el derecho de responsabilidad civil. Prosser "tradujo" a Warren y Brandeis en términos que el sistema legal puede adoptar y ser viable (Schwartzt, Peifer, 2010: 1986).

- **Edward J. Bloustein**

Bloustein es importante para los contornos actuales del Derecho Constitucional contemporáneo, en tanto reconoce en el derecho

a la privacidad un principio muy recurrente: la dignidad humana. Así, en *Privacy as an aspect of Human Dignity: an answer to Dean Prosser,* publicada en 1964 en el New York University Law Review, señaló lo siguiente:

> En estos casos la dignidad del individuo ha estado sujeta a desafío (…). El respeto a la libertad individual no solo ordena protección contra intrusos en el hogar de una persona o, ante un espectáculo público con publicidad indebida sobre sus asuntos privados o, degradarlo comercializando su nombre o semejanza o, usándolo en una "falsa imagen". Cada uno de estos males constituye una intrusión en la personalidad, un ataque a la dignidad humana (…) (Bloustein, 1964: 995)

- **Alan F. Westin**

Alan F. Westin publicó su libro denominado "Privacy and Freedom" en Nueva York en 1967. Donde conceptualizó la privacidad como el reclamo de las personas, grupos o instituciones para determinar por sí mismos cuándo, cómo y en qué medida se comunica información sobre ellos a otros (Westin, 1967: 7).

Acerca de Westin, Daniel Solove, Profesor Derecho de la Universidad George Washington, estuvo a cargo de la introducción de última edición de su obra, razón por la cual resaltó su importancia del modo siguiente:

> En el núcleo del libro se encuentra una de las discusiones más duraderas sobre la definición y el valor de la privacidad. La privacidad es un concepto muy complejo, y los académicos y otros han luchado durante siglos para definirlo y articular su valor. Privacidad y libertad contiene una de las discusiones sobre privacidad más sofisticadas, interdisciplinarias y profundas que se hayan escrito. Westin entrelaza filosofía, sociología, psicología y otras disciplinas para explicar qué es la privacidad y por qué debemos protegerla (Westin, 2015).

Esta pequeña lista de clásicos ha sido corroborada, por ejemplo, por Thomas I. Emerson, quien fuera un destacado profesor de Derecho de la Universidad de Yale, en *The right of privacy and freedom of the*

press, publicado en Harvard Civil Rights-Civil Liberties Law Review de 1979, donde resumió magistralmente el origen del derecho a la privacidad del modo siguiente:

> Como concepto independiente, el derecho a la privacidad es relativamente tardío en el sistema de derechos individuales. Hizo su primera aparición en la ley estadounidense como un agravio, en una demanda civil por daños o, en una orden judicial para proteger contra una invasión injustificada de otros en mérito al vago "derecho a ser dejado solo". Originado por Samuel D. Warren y Louis D. Brandeis en su famoso artículo en Harvard Law Review en 1890, el agravio de privacidad fue estructurado por William L. Prosser en 1960 y sus dimensiones más amplias fueron expuestas por el profesor Edward J. Bloustein y por el profesor Alan F. Westin poco después (Emerson, 1979: 329)

3. Casos clásicos

No existe una lista exacta de casos clásicos sobre el derecho a la privacidad, pero si existen autores clásicos que han aportado a este importante derecho. Por esta razón, citamos en primer término y como una suerte de casos clásicos genéricos, a los juristas Samuel D. Warren y Louis D. Brandeis; quienes, para defender el segundo pilar de su tesis referida al derecho a la privacidad de las personas, recurrieron a los siguientes casos:

- Caso Wyatt v. Wilson (1820), que impidió la difusión del grabado del Rey Jorge III durante su enfermedad;
- Caso Abernethy v. Hutchinson (1825), que impidió la publicación de conferencias inéditas brindadas por un distinguido cirujano;
- Caso Prince Albert v. Strange (1849), que impidió que se publicaran diferentes grabados de la vida diaria de la familia de la Reina Victoria y del Príncipe Alberto en tanto se vulneraba la confianza o el contrato inicial que no lo permitía;
- Caso Tuck v. Priester (1887), donde se estableció daños por incumplimiento de contrato, al haber realizado el demandado

copias adicionales de una imagen y venderlas a un precio más bajo; y,

- Caso Pollard v. Photographic (1888), que restringió el uso de la fotografía de una señorita en una tarjeta de navidad sin su consentimiento (Warren y Brandeis, 1890).

Llegados a este punto, si bien existe una lista inicial de casos, que hemos denominado clásicos al haber configurado inicialmente el derecho a la privacidad, también puede existir una lista de casos clásicos que a la vez sean más específicos.

De este modo, si recurrimos a nuestra lista de autores clásicos, podemos organizar diferentes listas de casos clásicos que consideren:

i) "Un derecho a ser dejado solo" (Cooley); o,

ii) "Un derecho a la privacidad en sentido amplio" (Warren y Brandeis); o,

iii) "Casos sobre intrusión, divulgación pública de hechos privados, publicidad que falsea la imagen de una persona y apropiación del nombre o de la imagen de una persona" (Prosser); o,

iv) "Casos que vulneren la dignidad humana" (Bloustein); y/o,

v) "Casos que justifiquen cuándo, cómo y en qué medida se comunicó cierta información a otros" (Westin).

Todas las listas de casos que se podrían organizar serían válidas y todas ellas podrían ser parte de otra. Así, bien pueden encontrarse listas de casos que consideren:

i) La tesis de Cooley y la de Warren y Brandeis; o,

ii) Las tesis de Prosser y Westin; y/o,

iii) Aquellas que siempre citen la tesis de Bloustein.

En Perú, por ejemplo, Juan Morales Godo, considerando la tesis de bachiller de Alfredo Ballón-Landa denominada *El Derecho a la Intimidad en el Perú* de 1981, estableció en *El right of privacy norteamericano y el derecho a la intimidad en el Perú. Estudio comparado*, publicado en DERECHO-PUC en 1995, una lista de casos clásicos siguiendo la tesis Prosser. Así, señaló:

- En referencia a la intrusión

  - Mc Daniel vs. Atlanta Coca Cola Bottling
    (60 GiorgiaApp. 92 2d.810. 1939)

    > La abierta, pública y persistente persecución de una persona, sin ninguna discreción ni secreto y de manera que se hace evidente al público que ella es perseguida y observada, constituyen los casos de «fisgoneo», figura conocida en el Derecho norteamericano como «peeping tom», o sea, como el de la persona que atisba a través de la ventana u otros lugares análogos hacia la propiedad de otros, con el propósito de espiar o invadir la vida privada de las personas, así como la realización de cualquier acto de naturaleza similar (Morales, 1995: 175).

  - Parrish vs. Civil Service Comission
    (66 California 2d-260. 1970)

    > Se destituyó a un asistente social porque se negó a ser copartícipe de un plan de la oficina de Bienestar Público de California, consistente en la «operación bedchek».
    >
    > El plan consistía en acudir a los hogares de los indigentes que recibían ayuda del Estado, un domingo por la mañana, en las primera horas, y buscar si había «*unauthorized males*», (traducido al español: «varones sin permiso»).
    >
    > La operación sería efectuada por dos personas: una estaría en la puerta de entrada y la otra en la puerta trasera y realizarían un registro entre ambos, evitando que pudiera salir persona alguna sin ser vista.

Parrish se niega a realizar la labor encomendada y es destituido de su trabajo. Al llevar la acción a los tribunales, Parrish levanta la defensa de que el método que le obligaban a emplear ofendía a la dignidad humana, siendo una violación constitucional a la intimidad de aquellas personas que serían investigadas. El tribunal, entonces, procedió a declarar inconstitucional el método «*operación bedchek*» (traducido al español: «operación de chequeo de camas») y restituyó al empleado en sus labores (Morales, 1995: 176).

- Schultz vs. Frankfurt
  (130 Wisconsin. 2d.179. 1914)

  En 1913 se entabla una demanda contra la Compañía de Seguros Frankfurt Company, que tenía en una acción civil como testigo adverso a Schultz, y mediante el uso de detectives y maquinaciones interferentes con su vida íntima trató que se mudara del lugar para que no declarara en la vista del caso. El Tribunal Supremo de Wisconsin calificó la conducta de la compañía aseguradora como equivalente a una conducta libelosa y ofensiva, procediendo a declarar la acción con un «si ha lugar» al derecho a la intimidad invocado (Morales, 1995: 176).

- En referencia a la divulgación pública de hechos privados

  - Melvin v. Reid.
    (112 California appelations. 285 -1931)

    En el Cuarto Distrito Tribunal de Apelaciones de California, se desarrolló el caso denominado "Melvin v. Reid" el 28 de febrero de febrero de 1931. La apelación fue presentada por la Sra. Melvin que años atrás fue prostituta y estuvo envuelta en un juicio por homicidio; luego de ser absuelta, abandonó su vida anterior y se rehabilitó hasta casarse en 1919. Sin embargo, a mediados de 1925 se estrenó la película "The Red Kimono" que se basó en la historia real de la apelante utilizando su apellido de soltera, Gabrielle Darley; situación que mereció que fuera abandonada y expuesta a la deshonra familiar.

Al respecto, el Tribunal consideró, sobre la base que "los principales objetivos de la sociedad es la rehabilitación de los caídos y la reforma del criminal" (Melvin v. Reid, 1931), lo siguiente:

i) "una persona que se ha rehabilitado por sus propios esfuerzos debe continuar en el camino de la rectitud y no debe volver a una vida de vergüenza o crimen" (Melvin v. Reid, 1931); y,

ii) "no se encuentra justificada por ningún estándar de moral o ética que conozcamos la invasión directa de su derecho inalienable que le garantiza la Constitución de perseguir y obtener la felicidad" (Melvin v. Reid, 1931).

- Douglas vs. Stockes
(149 Kentucky 506-149-1912)

El actor es padre de mellizos que nacen ligados desde los hombros hasta las caderas. A la muerte de los siameses, el actor contrató los servicios del demandado -un fotógrafo- para obtener placas de los cuerpos desnudos de sus hijos, indicando al fotógrafo que éste no podía reproducir más copias que para las cuales fue contratado.

El fotógrafo reproduce varias copias y obtiene el derecho de autor de la respectiva oficina de gobierno. El padre inicia acción, reclamando indemnización por los daños y perjuicios ocasionados por la humillación a sus sentimientos y a su sensibilidad.

El tribunal falla en favor del actor y la sentencia es confirmada por la Corte de Apelaciones del Estado de Kentucky (USA). En la sentencia se hizo mérito, en primer lugar, de un caso inglés que dijo: «los más tiernos afectos del corazón humano están encerrados en el cuerpo de un niño muerto». Un hombre puede ser indemnizado por cualquier daño e in-dignidad hechos al cuerpo, pero podría hacerse un reproche a la ley si solamente se pudieran indemnizar las heridas físicas y no aquellas injurias corporales que pueden causar muchos más

sufrimientos y humillación. Si el demandado ha tomado posición ilegalmente del cuerpo humano desnudo del hijo fallecido del actor y lo expuso a la vista del público, en un esfuerzo para ganar dinero con ello, no hay duda de que ha ocasionado un daño, lo cual puede originar una acción de daños y perjuicios (Morales, 1995: 179).

- Hemingway vs. Randon House
  (29 appelations Div. 2d. 6333-1968, confirmado en 23 New world 2d. 341 -1968)

  E. Hotchner escribió la obra Papa Hemingway, la cual es una compilación de las memorias del autor en sus relaciones amistosas con el famoso novelista Ernest Hemingway durante el período de 1948 a 1961

  Muchos de los pasajes de la obra contienen citas exactas del señor Hemingway, las cuales fueron obtenidas mediante grabaciones magnetofónicas por Hotchner, en sus diálogos con el novelista, y mediante cartas cursadas entre ambos.

  Al fallecer el novelista y estando en trámite la publicación de la obra, la esposa de Hemingway presentó un entredicho con el propósito de evitar dicha publicación. Posteriormente fue denegado el pedido presentado por dicha señora, quien a su vez presentó una demanda de daños y perjuicios alegando que la obra constituía una violación de su derecho a la intimidad.

  La Corte de Apelaciones declaró sin lugar la acción, y uno de sus razonamientos fue que siendo la señora Hemingway una figura pública, su derecho a la intimidad no estaba protegido por el estatuto de la ciudad de Nueva York (Morales, 1995: 179).

• En referencia a la publicidad que falsea la imagen de una persona

  - Pinkerton National Detective Agency vs. James A. Stevens
    (162 South Dakota. 2d. 474 -1964).

Una señora presenta una reclamación a una compañía de seguros por lesiones sufridas. Esto trajo como consecuencia que varios detectives estuvieron espiándola en forma insistente en la comarca, hasta que se llegó a pensar en el vecindario que la señora había cometido un delito, perjudicando en todo esto su reputación.

El tribunal accedió a su demanda ordenando pagar una suma de dinero por el daño ocasionado, ya que los métodos empleados por la compañía resultaban atentatorios al derecho a la intimidad y la libertad individual (Morales, 1995: 181).

- Lyman vs. New England Newspaper
  (286 Massachusetts 258-190 NL 542 -1934)

  En una acción tramitada ante los tribunales de Massachusetts en 1934, el diario demandado publicó en una de sus columnas que los actores, marido y mujer, no eran felices en sus relaciones conyugales. La principal defensa del diario demandado fue que las informaciones o las fotografías publicadas eran noticias de legítimo interés público puesto que se trataba de una pareja de artistas, los cuales no eran desconocidos por nadie. En la sentencia el tribunal falló en favor de los demandantes, reconociendo que se había violado el derecho a la intimidad (Morales, 1995: 182).

- En referencia a la apropiación del nombre o de la imagen de una persona

  - Donohue vs. Warner Brothers Pictures lnc.
    (194 Florida 2d. 6-1 O -1970)

    El juez supremo Bratton, al fallar el caso Donohue, dijo que afectar el derecho que tiene una persona común «de gozar de la existencia sin que su nombre o su vida sean explotados para fines comerciales o con el uso de su nombre o por la publicación de su retrato o carrera, en la pantalla de los cines, en la prensa, en periódicos, en boletines, circulares, catálogos o de cualquier otra manera, debe ser prohibido a menos que se obtenga para ello previamente su consentimiento» (Morales, 1995: 183).

- Daily Times Democrat vs. Graham
(13 Colorado 2d. 119 - 1963)

  Una joven fue fotografiada mientras se encontraba en un parque de diversiones y una corriente de aire levantó su vestido.

  Ella demanda, y el tribunal accede a la demanda por violación al derecho a la intimidad que tenía la dama, fundamentando su fallo en que «aun en lugares públicos hay ciertas cosas que aunque estén a la vista siguen siendo privadas» (Morales, 1995: 183).

- Young vs. Geneker Studies Inc.
(175 Misc. 1027 New York State 2d. 557-1951)

  La actora, una modelo profesional de ropas infantiles, empleada en el departamento de una tienda, posó en el estudio del demandado con el único propósito de rehabilitarlo para hacer maniquíes para el uso exclusivo de dicha tienda.

  Los demandados fabricaron y vendieron a numerosas personas «maniquíes hechos a la medida y la forma de la actora», con fines comerciales y sin su consentimiento. El tribunal dijo que si ella dio su consentimiento solamente a su empleador para usar el maniquí para tales propósitos, ello no la privaba para poder invocar ese derecho contra cualquier otra persona que hiciera lo mismo en contra de su voluntad (Morales, 1995: 183).

- Bazemore vs. Savannah Hospital
(174 Giorgia 2d. 194-1983)

  El hijo del actor nació con el corazón fuera del cuerpo, y el demandado, maliciosamente, tomó fotografías del cadáver desnudo del niño.

  La Corte Suprema de Georgia revocó la sentencia de primera instancia, concediendo al actor una indemnización por daños, y prohibió la publicación de la fotografía, aun cuando el derecho violado pertenecía al niño muerto y no al actor (Morales, 1995: 175).

4. Palabras finales

Aunque estos breves apuntes recuerdan los principales autores y casos clásicos que dieron origen a la protección del derecho a la privacidad; mantienen, en esencia, su vigencia e importancia en plena revolución digital.

Por otro lado, si bien nuestros breves apuntes no desarrollan las limitaciones y/o excepciones del derecho a la privacidad, muestran de manera clara las líneas directrices de un tema que, a pesar del tiempo, aún debate la misma pregunta que Warren y Brandeis nos dejaron planteada: "¿deberían los tribunales cerrar la entrada principal a la autoridad constituida y abrir de par en par la puerta trasera a la curiosidad ociosa y lasciva?" (Warren y Brandeis, 1890).

Bibliografía

- En referencia a la justificación previa: i) *Constitución Política del Perú*. Lima, 29 de diciembre de 1993; ii) Ley N.° 28237. *Código Procesal Constitucional*. Lima, 28 de mayo de 2004; y, iii) sentencia recaída en el expediente número 1797-2002-HD/TC, emitida por el Tribunal Constitucional el 29 de enero de 2003.

- En referencia a los autores clásicos: i) Cooley, Thomas M. Un tratado sobre la ley de agravios o los errores que surgen independientemente del contrato. Chicago: Callaghan and Company, 1879; ii) Samuel D. Warren y Louis D. Brandeis. *The right to privacy*. Harvard Law Review, Vol. IV, N.° 5, 15 de diciembre, 1890, págs.194-220; iii) Patricia Sánchez Abril. *Recasting Privacy Torts in a Spaceless World*. Harvard Journal of Law & Technology. Volume 21, Number 1 Fall 2007; iv) Charles Fried. *An Anatomy of Values: Problems of personal and social choice*. Cambridge: Harvard University Press, 1970, citado por Patricia Sánchez Abril; v) William L. Prosser. *Privacy*. California Law Review, agosto de 1960. Vol. 48. N.º 3,

págs. 383-423; vi) Paul M. Schwartzt, Karl-Nikolaus Peifer. *Prosser's Privacy and the German Right of Personality: Are Four Privacy Torts Better than One Unitary Concept?* California Law Review, vol. 98, Número 6 (diciembre de 2010), págs. 1925-1988; vii) Edward J. Bloustein. *Privacy as an aspect of Human Dignity: an answer to Dean Prosser*. Vol. 39. New York University Law Review, 1964, págs. 962-1007; viii) Alan F. Westin. *Privacy and Freedom*. Nueva York, 1967: Atheneum; ix) Introducción de Daniel Solove. *Privacy and Freedom,* 2015; y, x) Thomas I. Emerson. *The right of privacy and freedom of the press.* Harvard Civil Rights-Civil Liberties Law Review,1979, págs. 329-360.

- En referencia a los casos clásicos: i) Samuel D. Warren y Louis D. Brandeis, op. cit.; ii) Court of Appeal of California, Fourth District. *Melvin v. Reid*. Docket No. 346. Decided Feb 28, 1931; y, iii) Juan Morales Godo. *El right of privacy norteamericano y el derecho a la intimidad en el Perú. Estudio comparado.* DERECHO-PUC, número 49, diciembre de 1995.

EL DERECHO A LA AUTODETERMINACIÓN INFORMATIVA.

Algunos aspectos relevantes de su configuración desde el proceso del hábeas data.

✍ Lourdes Zamudio Salinas*

En pleno siglo XXI, ya iniciando su tercera década, es más evidente que estamos en una sociedad donde el uso de los datos de las personas es cada día más intenso e indispensable para la vida individual y social. La realización de las actividades privadas y públicas siempre ha requerido usar datos personales[1], lo sigue y continuará

* Abogada por la Universidad de Lima, con Maestría en Derecho Constitucional en la Pontificia Universidad Católica del Perú. Docente de la Facultad de Derecho de la Universidad de Lima. Miembro nata de la Red Iberoamericana de Protección de Datos 2003-2008. Experta invitada de la Red Iberoamericana de Protección de Datos, desde el 2008. Miembro fundadora y secretaria de actas y legislación de la "Red académica internacional de protección de datos personales y acceso a la información". Monterrey- México. 2011-2013. Experta Certificada en Protección de Datos. IAIT G. Institute of Audit & IT-Governance. Miembro de la Asociación Peruana de Derecho Constitucional. Consultora, articulista y expositora nacional e internacional en materia de protección de datos. Miembro de la Comisión Consultiva, que en calidad de especialista asesoró a la Comisión Multisectorial encargada de elaborar el Reglamento de la Ley N° 29733, Ley de protección de datos personales, creada mediante Resolución Suprema N° 180-2011-PCM. Miembro de la Comisión Especial encargada de proponer el Proyecto de ley de Protección de Datos Personales y elaborar las propuestas legislativas y administrativas que correspondan. Creada por Resolución Ministerial N° 094-2002-JUS.

[1] Ley N° 29733. Artículo 2, inciso 4. "Datos personales. Toda información sobre una persona natural que la identifica o la hace identificable a través de medios que pueden ser razonablemente utilizados."

haciéndolo; más aún en un mundo caracterizado por el uso y adopción, en la vida cotidiana, de las tecnologías de la información y la comunicación (TIC).

Esta sociedad de la información, de la globalización de las comunicaciones, del imparable incremento de la tecnología y de sus capacidades, permite la recopilación y el tratamiento de los datos personales de maneras antes inimaginables, a gran escala, en tiempo real y a nivel mundial, sin respetar fronteras.

La invasión masiva y en todas partes de las cámaras de videovigilancia, cada vez más pequeñas y con más capacidades, que no se restringen a su alegada finalidad de la seguridad; los drones que no respetan límites, como la inviolabilidad de domicilio, y están al alcance de cualquiera en el mercado; los teléfonos inteligentes, que almacenan gran parte de nuestra vida personal y social; los sistemas de geolocalización o rastero, las computadoras; las tabletas digitales; el internet de las cosas (relojes, pulseras, lentes, casacas, espejos, electrodomésticos… inteligentes) que recogen datos de nuestro cuerpo, de nuestra vida personal y familiar; las redes sociales; las aplicaciones electrónicas; la Red que interconecta casi todo; hacen que abundante información que concierne a una persona sea accedida y usada por terceros -Estado o particulares- muchas veces sin el conocimiento, sin consentimiento o sin plena conciencia, para quien es el titular de los datos, sobre los usos y fines a los que será sometida su información; y por ende con desconocimiento de las verdaderas implicancias y riesgos para sus derechos, para su dignidad y eventualmente, para sus propias vidas.

En la actualidad esa metáfora actualizada del "hombre de vidrio"[2] vigilado, invadido, sin control real sobre su información personal,

[2] Ver Stefano Rodotá. Democracia y protección de datos. Cuadernos de Derechos Público. N°s. 19-20. (mayo - diciembre 2003). Pp. 15-16. Puede ser visualizado en la siguiente dirección al 06 de setiembre de 2020: https://revistasonline.inap.es/index.php/CDP/article/view/690/745

cuestiona los límites del Estado Constitucional de Derecho, que tiene a la persona o a la defensa de su dignidad, como fin supremo de la sociedad y del Estado.

Frente al uso, a través de medios mecánicos o automatizados, de la información de las personas, motivado fundamentalmente por el tratamiento de la información personal por medio de la informática, es que en la década de los setenta, se comenzaron a dar las primeras regulaciones sobre la materia de autodeterminación informativa o protección de datos personales; así podemos encontrar a nivel de Europa, a las constituciones de Portugal de 1976 y de España de 1978, como las primeras en hacer una referencia específica a la protección de datos personales; y a nivel de América Latina, se introduce el tema con la institución del hábeas data en la constitución de la República Federativa de Brasil de 1988.[3]

1. Marco normativo peruano de la protección de datos personales

El reconocimiento del derecho fundamental a la protección de datos personales viene a darse en Perú con la constitución política de 1993[4], por medio de su artículo 2°, inciso 6), "Toda persona tiene de-

[3] Ver evolución de las regulaciones sobre la materia de protección e datos en: Troncoso Reigada, A. La protección de datos personales. Una reflexión crítica a la jurisprudencia constitucional pág. 233. 2003. https://revistasonline.inap.es/index.php/CDP/article/view/698/753 ; y Puente Escobar, A. página 55-59. Breve descripción de la evolución histórica y del marco normativo internacional del derecho fundamental a la protección de datos de carácter personal. Protección de datos de carácter personal en Iberoamérica. Valencia. Tirant lo Blanch. 2005; entre otros.

[4] La regulación sobre la protección de datos personales en el Perú surge dentro de un contexto normativo internacional y concretamente regional que lo condiciona y explica. Ver: Ma. de Lourdes Zamudio Salinas. "El marco normativo latinoamericano y la Ley de Protección de Datos Personales del Perú" En Revista de la red académica internacional de protección de datos personales N. 1. Julio - diciembre de 2012. Pp.2-21. Puede ser visualizada en la siguiente dirección al 06 de setiembre de 2020: https://hábeasdata colombia.uniandes.edu.co/wp-content/uploads/ok3_Ma.-de-Lourdes-Zamudio_FINAL.pdf; y Zamudio Salinas, Ma. de Lourdes. Régimen Jurídico de los datos personales. T. II. Buenos Aires. ABELEDO PERROT. 2014. Pp. 1159 – 1162.

recho: "A que los servicios informáticos computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal o familiar".

La misma constitución política de 1993, en su artículo 200, inciso 3 crea una nueva garantía constitucional, el hábeas data, con el objeto de brindar una mayor protección, propia de un derecho fundamental, a dos derechos: al derecho de acceso a la información pública (art. 2, inciso 5) y al derecho de protección de datos personales (art. 2, inciso 6).

Si bien, por la redacción del artículo constitucional 2°, inciso 6), se reconoce este nuevo derecho, a la autodeterminación informativa vinculado al derecho a la intimidad personal y familiar, (contenido en el inciso 7), y como un medio del defensa del mismo, la protección de datos personales es un derecho autónomo cuyo desarrollo y configuración de su contenido se irá completando y perfeccionando con el Código Procesal constitucional, aprobado por La Ley Nº 28237,[5] en adelante el CPC; el desarrollo de la jurisprudencia del Tribunal Constitucional; y la ley de desarrollo constitucional sobre la materia, concretada en la Ley N° 29773, Ley de Protección de Datos Personales, en adelante, la Ley, publicada el 03 de julio de 2011[6].

El CPC, en su artículo 61, inciso 2), va dotando legalmente de contenido al nuevo derecho cuando establece que toda persona puede recurrir al proceso de hábeas data para:

> "Conocer, actualizar, incluir y suprimir o rectificar la información o datos referidos a su persona que se encuentren almacenados o registrados en forma manual, mecánica o informática, en archivos, bancos de datos o registros de entidades públicas o de instituciones privadas

[5] Comenzó a regir el 01 de diciembre de 2004.

[6] Modificada por el Decreto Legislativo N° 1353; su Reglamento, aprobado por el Decreto Supremo N° 003-2013-JUS; y éste modificado por el Decreto Supremo N° 019-2017-JUS.

> que brinden servicio o acceso a terceros. Asimismo, a hacer suprimir o impedir que se suministren datos o informaciones de carácter sensible o privado que afecten derechos constitucionales".

Como podemos ver, el CPC, 11 años después del reconocimiento constitucional del derecho a la protección de datos personales, va completando su contenido haciendo referencia a los derechos[7] que le corresponden al titular de los datos personales, sea frente a una institución privada o entidad pública; con el fin de conocer (derecho de acceso) qué datos personales están siendo objeto de tratamiento; actualizar, una información que ha dejado de responder a la situación actual de su titular; incluir, alguna información que sea necesaria o pertinente para la finalidad para la que se recogieron los datos; suprimir, una información, que por ejemplo, ya cumplió con la finalidad de su recogida o venció el plazo autorizado para su tratamiento; rectificar, una información errada o inexacta; refiriéndose de manera particular a los derechos a hacer suprimir o impedir el suministro de datos o informaciones de carácter sensible[8] o privado que afecten derechos constitucionales.

Con la Ley de protección de datos personales, Ley N° 29733, en el año 2011, se desarrolla el derecho a la autodeterminación informativa, dieciocho años después de su reconocimiento constitucional, aprobándose una norma de carácter general sobre la materia, que toma como base fundamental a la legislación que tenía España, en ese entonces, la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal,[9] y que reconoce al titular del

---

[7] Derechos que a nivel internacional suelen nombrarse - de manera resumida- con el acrónimo ARCO: Acceso, Rectificación, Cancelación y Oposición.

[8] Artículo 2, de la Ley, inciso 5: "Datos sensibles. Datos personales constituidos por los datos biométricos que por sí mismos pueden identificar al titular; datos referidos al origen racial y étnico; ingresos económicos; opiniones o convicciones políticas, religiosas, filosóficas o morales; afiliación sindical; e información relacionada a la salud o a la vida sexual."

[9] Sustituida en la actualidad por La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de datos personales y garantía de los derechos digitales.

dato determinados derechos, y establece una serie de principios a los que debe someterse todo tratamiento de datos personales sea por parte del titular del banco de datos[10] o responsable del tratamiento[11], o encargado del mismo[12]; o cualquier persona que intervenga en alguna actividad del tratamiento, sea que pertenezcan, al sector público o al sector privado.

Los derechos que reconoce la Ley[13] al titular del dato son los de: información, acceso, actualización, inclusión, rectificación, supresión, impedir el suministro, oposición, al tratamiento objetivo y el derecho a la tutela.

Los principios reconocidos por la Ley[14] son los de: legalidad, consentimiento, finalidad, proporcionalidad, calidad, seguridad, de disposición de recurso y de nivel de protección adecuado.

Derechos y principios que configuran el contenido esencial de este derecho a la protección de datos personales; porque es en virtud a su observación y cumplimiento, que se podrá considerar que se está frente a un debido tratamiento de la información y, que su titular goza de las facultades de disposición y de control, propias de este derecho.

---

[10] Artículo 2, inciso "17. Titular del banco de datos personales. Persona natural, persona jurídica de derecho privado o entidad pública que determina la finalidad y contenido del banco de datos personales, el tratamiento de estos y las medidas de seguridad."

[11] Reglamento de la Ley: artículo 2, inciso "14. Responsable del tratamiento: Es aquél que decide sobre el tratamiento de datos personales, aun cuando no se encuentren en un banco de datos personales."

[12] Reglamento de la Ley: artículo 2, inciso "10. Encargado del tratamiento: Es quien realiza el tratamiento de los datos personales, pudiendo ser el propio titular del banco de datos personales o el encargado del banco de datos personales u otra persona por encargo del titular del banco de datos personales en virtud de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación. Incluye a quien realice el tratamiento de datos personales por orden del responsable del tratamiento cuando este se realice sin la existencia de un banco de datos personales."

[13] Artículos del 18 al 24.

[14] Artículos del 4 al 11.

Por disposición de la Ley, además, se crea una autoridad administrativa de control, la Autoridad Nacional de Protección de Datos Personales, que reside en el Ministerio de Justicia y Derechos Humanos[15]; con lo que se suma a la protección jurisdiccional que brindaba el hábeas data, otra de carácter administrativo[16] para las personas que se vean afectadas por un indebido tratamiento de su información personal. La Ley ha denominado a este recurso, el derecho de tutela[17]; el que procederá en caso de que el titular del banco de datos, responsable del tratamiento o encargado del mismo, denieguen total o parcialmente, el ejercicio de los derechos que la Ley le reconoce al titular del dato.

Apreciamos entonces, que los alcances de este derecho fundamental, comprenden una tutela jurisdiccional y otra administrativa. El titular de los datos personales, que se considere lesionado en su derecho, puede recurrir alternativamente para la defensa del mismo, a la vía administrativa, en ejercicio del derecho de tutela; o directamente al ámbito constitucional, mediante el proceso del hábeas data, no constituyendo vía previa a la constitucional, el procedimiento administrativo ante la autoridad de control.[18]

2. Denominación del derecho

La denominación del derecho reconocido en el artículo 2°, inciso 6) de la Constitución, puede ser de dos formas en Perú: como derecho a la autodeterminación Informativa o, como derecho a la protección de datos personales.

---

[15] Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales.

[16] ZAMUDIO SALINAS, Ma. de Lourdes. Régimen Jurídico de los datos personales. T. II. Buenos Aires. ABELEDOPERROT. 2014. Pp. 1172 – 1173.

[17] Artículo 24.

[18] Disposición complementaria final sexta de la Ley.

- Derecho a la autodeterminación informativa, es la forma usada por el Tribunal Constitucional peruano, en la abrumadora mayoría de sus resoluciones de hábeas data donde el derecho cuestionado es el contemplado en el artículo 2°, inciso 6) constitucional; (como una pequeña muestra podemos citar a los expedientes Nos.: 1797-2002-HD/TC, 04729-2011-HD/TC, 03859-2012-HD/TC, 06841-2013-HD/TC, 01331-2014-HD/TC, 02365-2015-HD/TC, 03965-2016-HD/TC, 1095-2018-HD/TC, 0262-2019-HD/TC,); solo en muy pocas ocasiones el Tribunal Constitucional lo llama derecho a la protección de datos personales, como es el caso de la sentencia recaída en el expediente N° 04387-2011-PHD/TC, en su fundamento jurídico 9.

- Derecho a la protección de datos personales, es la denominación que le coloca la ley de desarrollo constitucional del artículo 2°, inciso 6), Ley N° 29733, Ley de Protección de Datos Personales y que es la denominación que predomina a nivel de las legislaciones sobre la materia en Europa[19] y en América latina[20]. Por lo señalado, usaremos indistintamente ambas denominaciones.

2.2. Algunos aspectos importantes de la configuración del derecho a la autodeterminación informativa o protección de datos personales

El Tribunal Constitucional, en diversas sentencias recaídas en procesos de hábeas data, desde la vigencia de la Constitución de 1993, ha venido definiendo e integrando el contenido del derecho a la protección de datos personales; labor especialmente necesaria, teniendo en cuenta el reconocimiento del derecho en el artículo 2, inciso 6) de la

[19] El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo. RGPD.

[20] México, Argentina, Uruguay, Brasil.

Constitución de 1993, a través de una redacción muy limitada; sumado al hecho de que su norma de desarrollo constitucional, la Ley N° 29733, se da en el 2011, por lo que era necesario el aporte de la labor jurisprudencial sobre este nuevo derecho fundamental que aún se encuentra en un nivel bajo de conocimiento en la sociedad peruana.

Vamos a referirnos a algunos aspectos relevantes, del derecho que nos ocupa, que han sido desarrollados por las sentencias del Tribunal Constitucional.

3. Conceptualización y naturaleza del derecho.

El derecho a la protección de datos personales le confiere a su titular un poder de disposición y de control de su información personal.

En reiteradas ocasiones el Tribunal Constitucional fue dando definiciones de este derecho, resaltando distintas facultades que se le reconoce al titular de la información. Así citando a diversas sentencias como las recaídas en los expedientes Nos. 04739-2007-PHD/TC, 0300-2010-PHD/TC, 746-2010-PHD/TC, 051-2010-PHD/TC, 4227-2009-PHD/TC, entre otras, referidas por la sentencia 04729-2011-PHD/TC, FJ 4; donde se señala lo siguiente:

> "El derecho a la autodeterminación informativa consiste en la serie de facultades que tiene toda persona para ejercer control sobre la información personal que le concierne, contenida en registros ya sean públicos, privados o informáticos, a fin de enfrentar las posibles extralimitaciones de los mismos. Se encuentra estrechamente ligado a un control sobre la información, como una autodeterminación de la vida íntima, de la esfera personal. (…)."

El poder de control que le concierne a la persona, se ejerce, sea que su información esté siendo tratada[21] por una entidad del

21 La definición del tratamiento de los datos, que da la Ley, comprende variadas actividades: Artículo 2°, "19. Tratamiento de datos personales. Cualquier operación o procedimiento técnico, automatizado o no, que permite la recopilación, registro, organización,

Estado[22] o por un particular[23]; control que tiene como uno de sus fines fundamentales el contrarrestar posibles extralimitaciones, en el tratamiento del que sea objeto su información personal.

Asimismo, el titular de los datos es quien debe, consentir o autorizar[24] (principio de consentimiento) el tratamiento de su información personal; lo que será manifestación del poder de disposición de sus datos. Salvo las limitaciones al consentimiento que se encuentran reguladas en el artículo 14 de la Ley, y que, como tales, deben ser interpretadas restrictivamente.

La potestad de controlar sus datos, frente a cualquier persona, se encuentra dentro del ámbito constitucionalmente protegido de este derecho; en este sentido, lo pone de manifiesto el Tribunal Constitucional, en su sentencia recaída en el expediente N° 01127-2013-HD/TC, en su FJ. 6:

almacenamiento, conservación, elaboración, modificación, extracción, consulta, utilización, bloqueo, supresión, comunicación por transferencia o por difusión o cualquier otra forma de procesamiento que facilite el acceso, correlación o interconexión de los datos personales."

[22] Por ejemplo con relación a datos contenidos en bancos de datos administrados por el Estado, tenemos que un gran número de sentencias de hábeas data, sobre el derecho a la autodeterminación informativa, que se refieren a pedidos de los ex trabajadores sobre las constancias de sus aportes a la ONP, realizados por sus ex empleadores.

[23] Salvo que no se encuentren dentro del ámbito de aplicación de la ley, lo que está regulado en el artículo 3, "… Las disposiciones de esta Ley no son de aplicación a los siguientes datos personales:

1. A los contenidos o destinados a ser contenidos en bancos de datos personales creados por personas naturales para fines exclusivamente relacionados con su vida privada o familiar.
2. A los contenidos o destinados a ser contenidos en bancos de datos de administración pública, solo en tanto su tratamiento resulte necesario para el estricto cumplimiento de las competencias asignadas por ley a las respectivas entidades públicas, para la defensa nacional, seguridad pública, y para el desarrollo de actividades en materia penal para la investigación y represión del delito."

[24] Principio de consentimiento, artículo 5 de la Ley.

> "El ámbito constitucionalmente garantizado del derecho a la autodeterminación informativa protege la potestad del titular de sus datos de controlar si, y hasta qué punto, otras personas "tienen el derecho a exponer en público una imagen de la vida de una persona en su totalidad o en acontecimientos determinados de la misma" [Ernest Denninger,…1987] y éste depende exclusivamente de su titular, y no está sujeto a la autorización, (o a la concesión) de ninguna autoridad pública. (…)".

El nacimiento de este derecho y su reconocimiento vinculado al derecho a la intimidad personal y familiar, no pueden restringir el derecho a la protección de datos personales, solo como un instituto de garantía del primer derecho, y limitar el contenido y la naturaleza que le corresponden, como derecho fundamental autónomo. Este sentido, es el que se desprende, de lo señalado en la sentencia recaída en el expediente N° 04729-2011-PHD/TC, FJ 4:

> "…Mediante la autodeterminación informativa se busca proteger a la persona en sí misma, no únicamente en los derechos que conciernen a su esfera personalísima, sino a la persona en la totalidad de ámbitos; por tanto, no puede identificarse con el derecho a la intimidad, personal o familiar, ya que mientras éste protege el derecho la vida privada, el derecho a la autodeterminación informativa busca garantizar la facultad de todo individuo de poder preservarla ejerciendo un control en el registro, uso y revelación de los datos que le conciernen".

En efecto, el derecho a la autodeterminación informativa busca "proteger a la persona en sí misma", en la "totalidad de sus ámbitos" frases que expresan la naturaleza amplia y relacional del derecho a la protección de datos personales. El alto tribunal ha de destacar este aspecto importante de la naturaleza del derecho a la autodeterminación informativa, en diversas sentencias en las que ha señalado las diferencias que existen entre el derecho que nos ocupa y otros derechos con los que se le suele vincular[25]; a la vez de pronunciarse cómo un

[25] Una de las sentencias, previas a la dación del CPC, en las que se refiere a la naturaleza relacional del derecho a la autodeterminación informativa es la sentencia recaída en

indebido tratamiento de datos personales puede afectar otros derechos fundamentales.

En la misma línea, la Ley de protección de datos personales, N° 29733, señalará que su objeto es el "… de garantizar el derecho fundamental a la protección de los datos personales, previsto en el artículo 2 numeral 6 de la Constitución Política del Perú, a través de su adecuado tratamiento, en un marco de respeto de los demás derechos fundamentales que en ella se reconocen". Muchas veces, un adecuado tratamiento de los datos personales permitirá, a su vez, la salvaguarda de otro derecho.

Los datos personales pueden estar vinculados con cualquier aspecto de la vida de la persona; y dependiendo del dato que se trate de manera indebida, se verá afectado tanto el derecho a la autodeterminación informativa, como otro u otros derechos.

Pongamos un ejemplo. Si se publica sin el consentimiento del titular, una foto o un vídeo, donde dicha persona aparece en una situación vergonzosa (en estado de ebriedad, pronunciando palabras soeces, vestido inapropiadamente, etc.) no solo se estaría frente a un indebido tratamiento de su dato de la imagen y/o voz, con lo que ya estaríamos frente a la violación de su derecho a la autodeterminación informativa; sino que a su vez, se podría estar afectando su honor, su imagen, su intimidad, su acceso al trabajo (podría darse el caso que un empleador, que esté evaluando su posible contratación, vea dicha foto o vídeo y a partir de ello, considere inapropiada a dicha persona para la imagen de la empresa o del opuesto que le iba a dar, y lo descarte por ello.), o afectando su libre desarrollo de la personalidad, etc. según sea el caso.

En varias ocasiones se ha solicitado por medio del hábeas data la rectificación del estado civil consignado en el RENIEC, (Expediente

el expediente 1797-2002-HD/TC. En la que también hace la diferencia entre el derecho que nos ocupa y los derechos a la intimidad, a la imagen, e identidad.

N° 00237-2011-PHD/TC, Expediente N° 0047-2011-PHD/TC, etc.). Solo refiriéndonos a la naturaleza relacional del derecho a la protección de datos personales; si una persona estuviera registrada por error como casada, siendo soltera, es decir, se le atribuye por el registro un estado civil que no le corresponde, nos encontraríamos ante el tratamiento de un dato personal erróneo o inexacto, que de no corregirse, no sólo afectaría la autodeterminación informativa del titular, sino su identidad y eventualmente su libertad de contratar, entre otros posibles derechos.

La sentencia ya citada, recaída en el expediente N° 04729-2011-PHD/TC, FJ 4, ponía de manifiesto que los datos personales no se circunscriben al ámbito íntimo o privado; lo cual es correcto; pues los datos que sean objeto de tratamiento, pueden ser datos públicos o recogidos de una fuente de acceso al público; pero que no por ello, pueden ser objeto de una tratamiento arbitrario por nadie. Así, una persona que saca un reporte de otra, a través de los servicios que presta el RENIEC por el pago de una tasa, con solo colocar el DNI o nombre completo de otra persona, no podría utilizar esa información (no estaría legitimado), por ejemplo, para enviar publicidad comercial, a los titulares de las direcciones de los domicilios a los que accedió de esa manera.[26]

Los datos obtenidos de una fuente de acceso público deben utilizarse para la finalidad para la que ha sido creada dicha fuente (principio de finalidad[27]); pues en caso de requerir realizar un tratamiento,

[26] Esto sin pronunciarnos sobre si el RENIEC cumple o no con los principios de legalidad, proporcionalidad, finalidad, calidad y consentimiento, al dar publicidad de la forma señala a variada información concerniente a las personas a cualquier tercero solo por el pago de una tasa. Tema que daría para una investigación y corrección en lo que corresponda, a la luz de lo que disponen la Constitución Política, artículo 2, inciso 6), la Ley N ° 29733, artículo 3° primer párrafo, y las funciones constitucional y legalmente asignadas a este organismo constitucional autónomo, así como una debida interpretación de la excepción al consentimiento contenida el artículo 14°, inciso 1) de la Ley.

[27] La Ley, "Artículo 6. Principio de finalidad

Los datos personales deben ser recopilados para una finalidad determinada, explícita y lícita. El tratamiento de los datos personales no debe extenderse a otra finalidad que no haya sido la establecida de manera inequívoca como tal al momento de su

de dicha información, para finalidades diferentes, se deberá solicitar y obtener el consentimiento de su titular.[28] De lo contrario, el titular de la información perdería los poderes de disposición y de control de los datos que le conciernen por el hecho de que éstos se encuentran en una fuente de acceso público. Lo cual sería inaceptable frente a las facultades derivadas del derecho a la protección de datos personales, para su titular, en el contexto de un Estado Constitucional de Derecho.

4. Derechos del titular del dato[29]

Vamos a citar algunos ejemplos de pronunciamientos del Tribunal Constitucional que ponen de manifiesto criterios relacionados con algunos derechos que le corresponden al titular del dato personal.

Derechos que concretan el poder de control[30] que tiene la persona sobre su información personal y, que es justamente, a partir de esos derechos, que puede seguir ejerciendo ese control sobre su información cuando es tratada por otras personas, sea luego de haber dado su consentimiento; o sea que, el tratamiento se esté realizando sin su consentimiento, pero en virtud a alguna de las excepciones, al mismo, que están reguladas en el artículo 14 de la Ley.

En la STC, recaída en el expediente N° 03052-2007-PHD/TC, el Tribunal Constitucional describió varios de los derechos que el titular de la información puede ejercer jurisdiccionalmente a través del hábeas data:

---

recopilación, excluyendo los casos de actividades de valor histórico, estadístico o científico cuando se utilice un procedimiento de disociación o anonimización."

[28] Oficio N° 156 2017-JUS/DGTAIP (Opinión consultiva N° 23).

[29] En la sentencia recaída en el Expediente N° 06164-2007-HD/TC, el Tribunal Constitucional dio una clasificación de los tipos de hábeas data en relación con las distintas facultades (derechos) que le corresponden al titular de la información, en virtud del derecho a la autodeterminación informativa

[30] ZAMUDIO SALINAS, Ma. de Lourdes. Régimen Jurídico de los datos personales. T. II. Buenos Aires. ABELEDOPERROT. 2014. Pp. 1168 – 1169.

> "(...) la protección del derecho a la autodeterminación informativa a través del hábeas data comprende, en primer lugar, la capacidad de exigir jurisdiccionalmente la posibilidad de acceder a los registros de información, computarizados o no, cualquiera que sea su naturaleza, en los que se encuentren almacenados los datos de una persona. Tal acceso puede tener por objeto que se permita conocer qué es lo que se encuentra registrado, para qué y para quién se realizó el registro de información así como la (o las) persona(s) que recabaron dicha información. En segundo lugar el hábeas data puede tener la finalidad de agregar datos al registro que se tenga, sea por la necesidad de que se actualicen los que se encuentran registrados, o con el fin de que se incluyan aquellos no registrados, pero que son necesarios para que se tenga una cabal referencia sobre la imagen e identidad de la persona afectada. Asimismo con el derecho en referencia, y en defecto de él, mediante el hábeas data, un individuo puede rectificar la información, personal o familiar, que se haya registrado; impedir que esta se difunda para fines distintos de aquellos que justificaron su registro o, incluso tiene la potestad de cancelar aquellos que razonablemente no debieran encontrarse almacenados." FJ. 3.

Los derechos mencionados específicamente en esta sentencia fueron los siguientes:

- Derecho de acceso [31] y parte de lo que comprende el mismo: en qué consiste lo registrado, con qué fin, y para quién (responsable del tratamiento);

- Derechos de rectificación, inclusión y actualización[32]; para que la información que se esté tratando responda a la situación actual del titular del dato y, por lo tanto, sea información de calidad[33].

- Derecho de impedir el suministro; supuesto que puede

[31] Regulado posteriormente en el artículo 19 de la Ley.

[32] Regulados posteriormente en el artículo 20 de la Ley.

[33] Principio de calidad. Artículo 8 de la Ley.

referirse a cuando ya se cumplió la finalidad[34] que autorizó la recogida del dato o cuando la trasferencia de su información afecte sus derechos fundamentales.[35]

- Derecho de cancelación o supresión;[36] que se podrá ejercer cuando los datos hayan dejado de ser necesarios o pertinentes a la finalidad para la cual hayan sido recopilados o cuando hubiera vencido el plazo establecido para su tratamiento.

Veamos, desde los pronunciamientos del Tribunal Constitucional, el desarrollo más específico de dos de los derechos que le corresponden al titular de la información: acceso y rectificación.

4.1. Derecho de acceso

Por el derecho de acceso, el titular del dato debe poder obtener la información, que sobre él mismo, esté siendo objeto de tratamiento; la forma en que sus datos fueron recopilados; las razones que motivaron su recopilación; a solicitud de quién se realizó la recopilación; así como las trasferencias realizadas o que se prevén hacer de ellos (artículo 19 de la Ley). Lo que comprendería el objeto de los hábeas data de cognición, informativo e inquisitivo, si aludimos a la clasificación del hábeas data que el Tribunal Constitucional diseñó, cuatro años antes de la dación de la Ley, en la sentencia recaída en el expediente N° 06164-2007-HD/TC.

El derecho de acceso es un derecho amplio y necesario para que el titular del dato supervise, verifique o de ser el caso, conozca el tratamiento que se le está dando a su información y las condiciones del mismo; verifique si ese tratamiento responde a lo consentido, y cumple con las obligaciones y principios que la Ley impone al responsable de su tratamiento. Por lo que, de no poder acceder o negarle, al titular del dato, el

[34] Principio de finalidad. Artículo 6 de la Ley.

[35] Regulado posteriormente en el artículo 21 de la Ley.

[36] Regulado posteriormente en el artículo 20 de la Ley.

acceso a la información, que sobre él se está tratando, se limitaría seriamente el control que le corresponde sobre su información y, se afectaría el contenido esencial de su derecho a la protección de datos personales.

La no entrega de la información que se está tratando, a su titular quien la solicita, no es el único supuesto de violación del derecho a la protección de datos personales, en el ejercicio del derecho de acceso; sino también cuando la información se entrega de manera extemporánea; o a pesar de que el responsable del tratamiento alegue que entregó la información solicitada, pero no cumple con acreditar dicha entrega[37]. El Tribunal Constitucional se ha referido a la violación del derecho a la autodeterminación informativa por no atención adecuada del derecho de acceso en diversas sentencias, como en las recaídas en los expedientes N° 00585-2018-HD/TC, en los fundamentos jurídicos 8 y 12; y en el N° 014-2012-PHD/TC: " …la emplazada atendió el pedido de la autora con fecha 16 de abril de 2013, esto es, de forma notoriamente extemporánea, (…) reconociendo entonces que sí contaba con la información requerida, hecho por el cual se evidencia, que la respuesta que otorgó al demandante (…) lesionó su derecho a la autodeterminación informativa". FJ. 4.

En adición a lo señalado, la entrega de la información solicitada por el derecho de acceso, no incluye que el responsable del tratamiento o titular del banco de datos deba entregar "copias certificadas" de dicha información personal que está tratando, pues: "el derecho a la entrega de la información de los datos personales (derecho a la autodeterminación informativa) no incluye, como parte de su contenido constitucionalmente protegido, que la información entregada deba constar en copias certificadas, por lo que dicha pretensión se encuentra incursa en la causal de improcedencia…" Expediente N° 0133-2014-HD/TC. FJ. 2.

[37] En la misma línea el Reglamento de la Ley en su artículo 54, establece que corresponde al titular del banco de datos o responsable del tratamiento la prueba del cumplimiento del deber de respuesta, debiendo conservar los medios para hacerlo.

Tampoco el derecho de acceso supondrá la transcripción de la información solicitada, porque sería, para el alto Tribunal, la creación o consolidación de una nueva información con la cual el titular del banco de datos, no cuenta. El supuesto fue abordado por la sentencia recaída en el expediente N° 1331 - 2014-PHD/TC, en la que el titular del dato, el paciente, solicitó el acceso a la información consistente en la trascripción de todas sus atenciones médicas en la especialidad de gastroenterología del Hospital III de Essalud Yanahuara, Arequipa, las misma que se encontrarían en la historia clínica respectiva. Lo que el tribunal declaró improcedente es que se debe entregar la información previa trascripción de la misma, no el acceso de su titular a la historia clínica en sí; a lo que está legitimado no solo por la legislación sobre protección de datos, sino por la de salud.

Consideramos oportuno mencionar que, en sentido diverso a lo que hemos venido desarrollando sobre el derecho de acceso a la información que le corresponde al titular de los datos, en la sentencia recaída en el expediente N° 03310-2015-PHD/TC, se le ordena a una AFP que entregue no solo la información con la que cuenta sino que, prácticamente sirva de intermediario y solicite a otra institución, información para que le entregue al titular, o en este caso, a las herederas del titular.

En dicho expediente, las recurrentes interponen demanda de hábeas data contra la Administradora Privada de Fondo de Pensiones Prima (AFP Prima), en su condición de hijas de su padre difunto. La reclamación constitucional estuvo constituida por dos solicitudes: la primera referida a la entrega de la copia fedateada del expediente administrativo del difunto padre de las actoras; y la segunda, a la copia del contrato de seguro que suscribió el causante de las peticionantes con la compañía de seguros Pacífico Vida.

No obstante el reconocimiento del Tribunal Constitucional que cuando una entidad, pública o privada, no cuenta con una determinada información, no está obligada a entregarla; dispone en la parte

resolutiva de su sentencia, que la AFP Prima, debía realizar el trámite correspondiente, ante Pacífico Vida, para cumplir con la entrega del contrato de seguro –que el causante celebró con esta aseguradora– a las demandantes.[38]

El fundamento para este mandato, que da el Tribunal, es aludiendo a una relación de consumo; señalando que los consumidores o usuarios no mantienen una relación simétrica con las proveedoras del bien o servicio, por lo que considera que las AFP poseen mayor información sobre las empresas aseguradoras y mantienen contacto comercial permanente con ellas, con relación a los asegurados. Sustento que nos parece impertinente desde el derecho a la protección de datos personales; pues además, no se está cuestionando el derecho de las demandantes a obtener el contrato de seguro que su padre fallecido celebró con la Compañía Pacífico Vida; pero, a la vez, tampoco puede obligarse a un titular de un banco de datos (AFP Prima) a dar una información que no posee, como ocurre en el presente caso, en virtud al derecho a la protección de datos personales, porque no es parte de su contenido.[39]

En muchas ocasiones el derecho de acceso facilita que el titular del dato tome conocimiento de un indebido tratamiento de su información personal y, pueda, a partir de ello, ejercer el control de la misma a través del ejercicio de los otros derechos como los de rectificación, actualización o cancelación, por ejemplo.

Un importante número de procesos de hábeas data, en ejercicio del derecho a la autodeterminación informativa, se refiere al derecho de acceso de los pensionistas sobre períodos de sus aportaciones al Sistema Nacional de Pensiones, SNP, efectuados por sus empleadores.

---

[38] ZAMUDIO, M. de Lourdes. Algunos comentarios desde el derecho a la autodeterminación informativa. Expediente N° 03310-2015-PHD/TC. Gaceta constitucional & Procesal Constitucional. N° 139-julio.2019.

[39] Sentido en el que se fundamentó uno de los votos dirimentes de la sentencia.

El titular del banco de datos, frente al ejercicio del derecho de acceso, debe revisar todos los bancos de datos que posee[40] para poder dar una respuesta al titular de la información, que necesita conocer los datos que se están tratando sobre él y las condiciones de dicho tratamiento. Una revisión incompleta, por ejemplo, que busque la información en determinados bancos de datos sistematizados, pero no en todos ellos, constituiría una violación al derecho a la protección de datos personales, del titular de la información, porque le impediría a éste ejercer el control efectivo sobre la información que le concierne, independientemente de una respuesta no ajustada a la verdad por parte del titular del banco de datos, con las implicancias que ello pueda tener, según sea el caso.

Esto fue lo que sucedió en el caso de la sentencia recaída en el Expediente N ° 07189-2013-PHD/TC, en donde la recurrente solicitó a la ONP poder acceder a la información que custodiaría, dicha entidad, respecto de su vida laboral desde el mes de enero de 1976 al mes de diciembre de 1997. La búsqueda realizada por la ONP para dar respuesta, al requerimiento del Tribunal Constitucional, se limitó a la base de datos de los aportantes solicitantes de pensión y de los pensionistas; pero omitió la búsqueda en la base de datos de los aportantes no pensionistas, base que no estaba sistematizada con la primera. Lo cual para el Tribunal Constitucional significó "una limitación irrazonable de acceso a la información personal de la recurrente", razón por la cual declaró fundada la demanda, y ordenó a la ONP "efectuar una búsqueda integral de la información laboral de la demandante en todas sus bases de datos físicas y digitales, a fin de que proceda a efectuar la entrega de la información que sobre ella ubique (…)" FJ. 13.

El derecho de acceso, supone que el titular del banco de datos responda en todas las circunstancias al titular de la información, aún en el caso en que no tuviera información personal sobre el solicitante. La

[40] incluso dar cuenta también de datos personales que pudiera estar tratando sin que figuren en un banco de datos.

inexistencia de la obligación de contar con cierta información no elimina la obligación de dar respuesta oportuna a la solicitud de acceso, "la cual se funda en el derecho de acceso del titular de datos contenido en la autodeterminación informativa (…)" tal como lo señaló el Tribunal Constitucional en la sentencia recaída en el Expediente N° 4538-2015-PHD/TC. FJ. 7.

En la misma sentencia, (FJ. 8) el Tribunal señala, cómo la entidad requerida, puede dar respuesta frente a una solicitud que resulte insuficiente, a efectos de dar lugar a la búsqueda de información:

- Denegar motivadamente la solicitud, sobre la base de lo previsto legislativamente, como límite al ejercicio de la autodeterminación informativa;
- Solicitar mayor información para que se pueda realizar la búsqueda;
- Informar sobre la imposibilidad de dar cobertura a la solicitud por inexistencia de la información, pérdida, destrucción; entre otras razones.

Sentenciando contundentemente que "lo inadmisible constitucionalmente es la denegatoria, arbitraria incomunicada al solicitante que busca ejercer su derecho a la autodeterminación informativa" (FJ. 8). El responsable del tratamiento está obligado a realizar una atención, y por ende en este caso, una búsqueda diligente de la información solicitada. (FJ. 13)

4.2. Derecho de rectificación[41]

El Tribunal Constitucional en diferentes sentencias ha reiterado, en la línea de lo dispuesto por el CPC, que "… mediante el

[41] Expediente N° 06164-2007-HD/TC. FJ. 2.1…1.2.2. Hábeas Data Correctivo: Tiene como objeto modificar los datos imprecisos y cambiar o borrar los falsos.

hábeas data, un individuo puede rectificar la información, personal o familiar, que se haya registrado; impedir que ésta se difunda para fines distintos a aquellos que justificaron su registro o, incluso, tiene la potestad de cancelar aquellos que razonablemente no debieran encontrarse almacenados" (sentencias emitidas en los expedientes Nos. 01797-2002-PHD/TC, 1988-2009-PHD/TC y 00975-2013-PHD/TC, entre otras).

La rectificación de una información personal debe realizarse cuando se trata de una información que no responde a la situación actual de interesado (titular de la información) por tratarse de una información inexacta o falsa. Caso en el cual nos encontraríamos frente a un dato que no es de calidad. Por un lado, el titular del banco de datos debe cuidar y tomar las previsiones necesarias para cuidar que sus registros contengan información verdadera[42], y por otro lado; sin perjuicio de lo primero, por supuesto, está el derecho del titular de la información, de solicitar su rectificación, actualización y en buena cuenta su modificación.

Así por ejemplo, si una empresa reporta a alguien como moroso ante la central de riesgos de la SBS, no siéndolo, es evidente que se requiere rectificar esa información, pues dicha pretensión guardaría relación directa con el contenido constitucionalmente protegido por el derecho a la autodeterminación informativa. (Expediente N ° 02365-2015-PHD/TC FJ. 7). En el ejercicio del derecho de rectificación será también preciso, señalar qué datos son los que se solicitan sean modificados.

[42] Expediente N° 4729-2011-PHD/TC "…Es por ello que los datos consignados en RENIEC son de su entera responsabilidad, lo que importa el deber de velar no solo por su autenticidad, sino, además, porque tanto la inscripción o registro, de datos como sus modificaciones tengan el debido sustento técnico y fáctico. Por ello, corresponde que, cuando advierta que algunos datos de su registro presenten imprecisiones o sean falsos, dicha entidad realice los actos necesarios para su corrección". FJ 8

A diferencia del derecho de acceso, para cuyo ejercicio el titular del dato no requiere presentar una prueba o justificación, para el ejercicio del derecho de rectificación, si será necesario hacerlo para modificar el dato inexacto o errado; porque de lo contrario, tampoco se estaría cuidando de la calidad de la información.

En este sentido lo sostuvo el Tribunal Constitucional en la sentencia recaída en el expediente N° 02365-2015-PHD/TC. FJ.4, donde ante el pedido de que se rectifique una información histórica de riesgos referida a una supuesta deuda que se venía reportando por una empresa, en contra de la recurrente, ante la central de riesgos de la SBS; no se amparó dicha pretensión pues, la titular de la información, no acompañó el sustento de su pedido de rectificación, a pesar de habérselo requerido; trámite necesario para demostrar que la información sobre su supuesta deuda era efectivamente supuesta o errónea.

5. Titularidad para el ejercicio de los derechos

Los derechos del titular del dato personal, conocidos comúnmente en la doctrina internacional como derechos ARCO[43], deben ser ejercidos por la persona a quien corresponden los datos personales; o en su caso, por su representante acreditado.

No es posible que una persona pueda ejercer el control sobre los datos de otra persona, porque justamente se iría contra el contenido del derecho a la protección de datos personales de esta última, pues se desconocerían los poderes de disposición y de control, que le corresponden al verdadero titular, sobre su propia información; se incumplirían, además, los deberes de confidencialidad[44] y de secreto[45], del titular del

[43] Acceso, rectificación, cancelación y oposición. Acrónimo que resumen los derechos que la legislación sobre protección de datos le reconoce al titular con relación su información personal.

[44] Artículo 17 de la Ley.

[45] Según sea el caso.

banco de datos o responsable del tratamiento, entre otros incumplimientos posibles[46].

Vamos a ver determinados supuestos, en los que, en el marco del proceso del hábeas data, se ha analizado la procedencia de la extensión de la titularidad para el ejercicio de los derechos ARCO, o de situaciones razonables de relativización del derecho a la autodeterminación informativa[47] en atención a intereses legítimos de los recurrentes, emitiéndose consideraciones sobre la procedencia o no, de la legitimidad para obrar activa.

- La sociedad conyugal. Que presupone un conjunto de derechos y obligaciones que afectan por igual a ambos cónyuges. En tal sentido uno de los cónyuges podría acceder a la información del otro, con el objetivo de conocer la capacidad económica que tiene, con el fin de exigir el cumplimiento de sus obligaciones conyugales de tipo patrimonial, como la obligación de alimentos. En cuyo caso, el Tribunal Constitucional señaló que: "el cónyuge solicitante deberá acreditar el vínculo matrimonial con la respectiva acta registral y justificar su pedido (…) a efectos de acreditar su legitimidad para obrar". Expediente N° 1887-2012-PDH/TC. FJ. 6.

- Condición de cónyuge supérstite; o que mantuvo una unión de hecho que generó descendencia con el fallecido y que ejerce la representación de aquélla. En el Expediente N.° 05379-2015-PHD/TC, se descartó la legitimidad para obrar activa, para el ejercicio del derecho de acceso de la autodeterminación informativa, de una recurrente que solicitaba información de un fallecido. Las razones fueron: no acreditó que estuvo casada con el difunto, ni que tuvieron una relación de hecho;

[46] Como podrían ser las medidas de seguridad.

[47] Expediente N° 1887-2012-PDH/TC. FJ. 6

tampoco que los hijos -que sí tuvieron en común- sean menores de edad o, que al ser mayores, le hayan otorgado poder de representación para presentarse en el proceso, en atención a intereses legítimos. (FJ. 5)

- Solicitar información sobre aportaciones de la difunta madre, para tramitar pensión de orfandad. En el Expediente N° 06691-2013-PHD/TC. Hay un interés legítimo de la recurrente para poder, en atención a la información personal de su difunta madre, tramitar un beneficio económico que le correspondería.

El titular del dato personal es a quien le corresponde el ejercicio de los derechos ARCO. Derechos, que se constituyen como mecanismos indispensables para ejercer el control sobre su información personal. Sólo en determinados supuestos, se ha extendido esta titularidad, a otras personas vinculadas al titular directo y para la atención de intereses legítimos.

6. Consideraciones finales

El derecho a la protección de datos personales, es un derecho fundamental de última generación, que se torna cada día más relevante, por el incesante incremento del uso de las tecnologías de la información y de la comunicación, en el contexto de la sociedad global de la información, donde nos encontramos; lo que no debe suponer que la persona pierda el control sobre su información personal.

Es necesario usar los datos personales, con plena conciencia de que su indebido tratamiento supondrá una afectación al derecho a la autodeterminación informativa; lo que, en atención a su naturaleza relacional, en muchos casos, supondrá la vulneración de otros derechos de la persona.

En Perú, existe el reconocimiento constitucional del derecho a la protección de datos personales; tenemos una ley general sobre

la materia; contamos con dos vías para su tutela: una administrativa y otra jurisdiccional.[48]

No obstante, no es suficiente lo señalado; se necesita un mayor conocimiento de este derecho, que lleve a una mayor toma de conciencia del mismo, por parte: de los titulares de la información; de los titulares de los bancos de datos o responsables del tratamiento, así como de los encargados del mismo; es decir, de la sociedad en general. Esto exige la implantación de una cultura de la protección de datos personales.

Bibliografía

- Puente Escobar, A. Breve descripción de la evolución histórica y del marco normativo internacional del derecho fundamental a la protección de datos de carácter personal. Protección de datos de carácter personal en Iberoamérica. Valencia. Tirant lo Blanch. 2005.
- Rodotá, S. (2011). Democracia y protección de datos. Cuadernos de Derecho Público, (19-20). Recuperado a partir de https://revistasonline.inap.es/index.php/CDP/article/view/690.
- Troncoso Reigada, A. La protección de datos personales. Una reflexión crítica a la jurisprudencia constitucional. 2003. https://revistasonline.inap.es/index.php/CDP/article/view/698/753.
- Zamudio Salinas, Ma. de Lourdes. (2012) "El marco normativo latinoamericano y la Ley de Protección de Datos Personales del Perú". En Revista de la red académica internacional de protección de datos personales. N° 1 Julio-diciembre de 2012. https://hábeasdatacolombia.uniandes.edu.co/wp-content/uploads/ok3_Ma.-de-Lourdes-Zamudio_FINAL.pdf

[48] Al margen de las mejoras que se podrían implementar, en lo que suponen estas dos vías de tutela, para una garantía más efectiva del derecho.

- Zamudio Salinas, Ma. de Lourdes. Régimen jurídico de los datos personales. T. II. Buenos Aires. ABELEDO PERROT. 2014.
- Zamudio, Ma. de Lourdes. Algunos comentarios desde el derecho a la autodeterminación informativa. Expediente N° 03310-2015-PHD/TC. Gaceta constitucional & Procesal Constitucional, N° 139, julio 2019.

EL DERECHO A LA AUTODETERMINACIÓN INFORMATIVA EN LA ERA DE LA GLOBALIZACIÓN

✍ Oscar Andrés Pazo Pineda*

I. Introducción

No es ningún secreto que la globalización ha impactado notablemente en diversas disciplinas, tanto de las ciencias naturales como sociales. En este contexto, el derecho -y particularmente el derecho constitucional- no podía ser una excepción. En lo que respecta a esta disciplina, dicha influencia se ha advertido en cuestiones tales como el debate sobre la posibilidad y conveniencia de la adopción de un modelo de constitucionalismo global, sobre la constitucionalización de la comunidad internacional, o la manifiesta necesidad de articular esfuerzos interestatales para la adecuada protección de los derechos fundamentales.

En este último escenario, los distintos avances tecnológicos han puesto en evidencia que el clásico modelo estatocéntrico de tutela de las libertades -esto es, la configuración de un sistema de protección que depende exclusivamente del Estado en cuya jurisdicción se encuentra

* Docente de los cursos de Derechos Fundamentales e Historia Constitucional Peruana en la Universidad de San Martín de Porres. Ha sido docente de la Universidad Nacional Mayor de San Marcos y de la Academia de la Magistratura. Miembro de la Asociación Peruana de Derecho Constitucional.

la persona afectada- es insuficiente para afrontar nuevos desafíos relacionados con ciertas conductas que ponen en riesgo ciertos bienes jurídicos. En ese sentido, el flujo global de la información, la existencia de actores transnacionales y el hecho que, a diferencia de lo que ocurría hace unas décadas, los datos de cualquier persona se puedan encontrar expuestos frente a potenciales peligros por actos cometidos fuera de la jurisdicción peruana, revelan que es pertinente la generación de espacios de coordinación que involucren a la comunidad internacional.

Este artículo pretende brindar algunos elementos iniciales para comprender la magnitud de este fenómeno. En ese sentido, y a fin de explicar el escenario actual, se formularán algunas consideraciones respecto del impacto de la globalización en el goce y ejercicio de los derechos fundamentales. Con posterioridad, se efectuarán algunas reflexiones en torno a los alcances del derecho a la autodeterminación informativa en el marco de los procesos de globalización, y se finalizará analizando la forma en que estos fenómenos han impactado (o pueden impactar) en el Perú.

II. El impacto de la globalización en el derecho constitucional y en los derechos fundamentales

La globalización, entendida como el proceso en el que se efectúa una comunicación y acercamiento entre las economías, sociedades y las diversas culturas existentes dentro de la mayor cantidad de Estados[1],

[1] *Cfr.* FLORES, VÍCTOR Y MARIÑA, Abelardo. *Crítica de la globalidad. Dominación y liberación en nuestro tiempo. México* D.F: Fondo de Cultura Económica, 2000, p. 11. Se efectúa la precisión de "la mayor cantidad" y no se hace referencia a la totalidad de Estados a nivel mundial por diversas razones, las cuales no son necesariamente ideológicas. En la actualidad, se sabe bastante bien que culturas marcadamente distintas a la occidental, como ocurre con China y con diversos países islámicos, también se han mostrado abiertos a esta clase de conexiones, aunque básicamente en el terreno económico. En estos casos, suelen ser los países con mayores desventajas a nivel financiero los que no participan en la misma medida que las potenciales mundiales. Por otro lado, en lo que respecta a la globalización en el terreno de los derechos humanos, sí se advierte que estas culturas han demostrado una importante resistencia a la incorporación de algunos estándares

ha tenido diversas repercusiones en distintas disciplinas, y el derecho no podía ser una excepción. En esta oportunidad, y antes de ingresar al tema del manejo o la manipulación de la información, es pertinente formular algunas consideraciones, a modo de introducción, de la forma cómo la globalización ha generado un considerable impacto en el derecho constitucional.

Una de las primeras evidencias relacionadas con el impacto de la globalización se puede advertir en la idea misma de "constitución". Sobre ello, es importante recordar que el clásico estado-nación (aun subsistente en la actualidad) se configuró esencialmente a través de tres elementos (territorio, soberanía y pueblo) que eran disciplinados a través de la norma fundamental respectiva. Sin embargo, en la actualidad no quedan dudas que cada uno de estos conceptos se ha visto sensiblemente alterado por el advenimiento de la globalización. En el caso del territorio, las fronteras estatales cada vez se diluyen con más frecuencia para la apertura de los mercados (cuestión que, como se verá, tiene un considerable impacto en la protección de datos personales); en lo que respecta a la soberanía no quedan dudas que las más trascendentales decisiones ya no se adoptan a nivel estatal, sino que suelen ser elaboradas e implementadas por diversos actores transnacionales; y, finalmente, en cuanto a la idea misma de constitución, experiencias como las de la Unión Europea demuestran que existe, cada vez en mayor medida, una importante multiplicación de normas que son llamadas a ser consideradas como fundamentales[2].

Otra forma en la que puede demostrarse la influencia de la globalización en el derecho constitucional –y que es relevante para el desarrollo de esta investigación– es el ámbito de la expansión del

occidentales, básicamente por entenderlas como una suerte de imposición ideológica y cultural.

[2] *Cfr*. RAMÍREZ, Gonzalo, "Transformaciones del constitucionalismo en el contexto de la globalización". En Ramírez, Gonzalo (editor). El Derecho en el contexto de la globalización. Bogotá: Universidad Externado de Colombia, 2007, p. 202.

reconocimiento de los derechos fundamentales, lo cual se ha manifestado en la adopción de distintos instrumentos internacionales que, como no podía ser de otro modo, han ejercido una considerable influencia en las constituciones nacionales. Ciertamente, aun no existe un consenso ideológico mundial sobre este punto[3], pero algo que no puede negarse es que "[l]a globalización de la protección de los derechos humanos y la creciente multiculturalidad de nuestras sociedades implica también que antiguos hábitos sociales se pongan en cuestión"[4].

Sin embargo, la realidad demuestra cómo las personas y/o entidades que adoptan -al menos en materia económica o financiera- las decisiones más relevantes no han visto limitado su accionar por la vigencia de los derechos fundamentales. Esto se explica por la idea que, desde sus orígenes, siempre había sido el derecho público el que había impuesto restricciones al accionar estatal. Sin embargo, el desarrollo de este sistema de garantías no fue de la mano con el establecimiento de reglas de juego para los privados y el mercado[5].

Esta última problemática se encuentra estrechamente vinculada con el debate a propósito de la conveniencia de adoptar alguna clase de constitucionalismo de carácter global. La doctrina, con este propósito,

[3] El mundo islámico, en el que la cuestión religiosa juega un rol preponderante en la vida nacional, así lo demuestra. Aunque la "Primavera árabe" parecía dar indicios de un viraje en esta materia, lo cierto es que se trata, aún, de un territorio que maneja tradiciones y prácticas bastante alejadas a lo que se suele advertir en occidente.

[4] PAULUS, Andreas, "La globalización en el derecho constitucional". En Stolleis, Michael; Paulus, Andreas y Gutiérrez, Ignacio. *El derecho constitucional de la globalización.* Madrid: Fundación Coloquio Jurídico Europeo, 2013, p. 82.

[5] En ese sentido, Ferrajoli explica que esto puede notarse, por ejemplo, en la acuñación del término "Estado de Derecho". Indica el profesor italiano que "no se desarrolló un constitucionalismo de derecho privado. Tanto en la tradición liberal-democrática como en la socialdemócrata, el único poder frente al que siempre se ha considerado justificadas las garantías […] ha sido el poder público. La expresión estado de derecho es emblemática: es solo el estado, pero no también el mercado, el sujeto frente al que se justifican reglas, prohibiciones, obligaciones y controles dirigidos a impedir sus atropellos y abusos en perjuicio de los derechos fundamentales de las personas". Ferrajoli, Luigi. *Constitucionalismo más allá del Estado*. Madrid: Editorial Trotta, 2018, p. 34

ha elaborado una gran cantidad de definiciones y enfoques sobre esta temática, pero existe cierto acuerdo en sostener que el constitucionalismo global es un agenda académica y política que defiende la idea de la aplicación de principios constitucionales en el ordenamiento internacional, a fin de poder mejorar su efectividad y justicia[6].

Ahora bien, aunque se trata de una cuestión novedosa -y que, por lo demás, ha despertado importantes debates en la academia-, no puede dejar de mencionarse que enfrenta una importante limitación, la cual consiste en la inexistencia de alguna constitución más allá de la esfera nacional, por lo que cualquier argumento sobre su conveniencia y necesidad permanece como controversial[7]. Este problema de la falta de una autoridad que se superponga a los Estados también ha puesto en evidencia que no existe alguna entidad que, por sí sola, sea capaz de enfrentar los graves problemas actuales. La situación es aún más preocupante si se advierte que los actores privados transnacionales no se han visto tan limitados como los Estados en cuando a la realización de sus actividades[8]. De hecho, muchos de los peligros que se vinculan con los datos personales tienen a estos últimos como sus protagonistas.

[6] PETERS, Anne: "The Merits of Global Constitutionalism". *Indiana Journal of Global Legal Studies*. Vol. 16, nº 2, 2009, p. 397.

[7] ATILGAN, Aydin. *Global Constitutionalism*. Berlín: Springer, 2018, p. 74.

[8] Uno de los casos más usuales en los que se ven comprometidos los datos personales es el que ocurre con la red social Facebook. Distintos tribunales de justicia han examinado casos relacionados con la información que se maneja dentro de ella. La Corte Constitucional de Colombia, por ejemplo, se ha pronunciado sobre esta problemática, y ha indicado que "la afectación de los derechos fundamentales en redes sociales como Facebook puede ocurrir no sólo respecto de la información que los usuarios de esta red social ingresan a la misma o cuyo ingreso permiten a través de su perfil, sino también con relación a información de personas, usuarias o no, que ha sido publicada y usada por terceros en las redes sociales. Ante los usos que pueden darse en las redes sociales de la propia imagen, un contenido mínimo del derecho a la imagen es la posibilidad de excluirla de las redes, bien porque se está haciendo un uso indebido de ella, o por simple voluntad del titular. Lo anterior encuentra fundamento en la protección constitucional debida a la imagen como expresión directa de la individualidad, identidad y dignidad de las personas. En este sentido, la disponibilidad de la propia imagen exige la posibilidad de decidir sobre su cambio o modificación, lo cual constituye a su vez un presupuesto ineludible del

De hecho, esto fue lo que ocurrió en uno de los casos más importantes que, sobre esta materia, se desarrolló en Estados Unidos. Así, en la controversia *Microsoft Corporation vs. United States*, se sometió a conocimiento del Tribunal Supremo de ese país una cuestión relacionada con el manejo de datos personales en manos de entidades transnacionales. Este órgano afrontaba el problema de que la ley que regulaba esta clase de datos se remonta, esencialmente, a 1986, una época en la que aun no se habían advertido los vertiginosos avances de la ciencia. La controversia terminó con una suerte de declaración de sustracción de la materia, ya que, con posterioridad a la audiencia, el gobierno de Donald Trump aprobó la controvertida *Cloud Act*[9].

Como puede advertirse, el proceso de globalización ha impactado –y seriamente– al derecho constitucional. En todo caso, no puede dejar de advertirse que, pese a su ocaso[10], el Estado-Nación sigue constituyéndose como una figura indispensable para articular esfuerzos importantes de colaboración para la protección de los derechos. Esto ha sido, en parte, porque los Estados han asumido que existen males que no pueden ser combatidos con las clásicas herramientas del derecho de los siglos XVIII y XIX, sino que, antes bien, demandan el desarrollo de normas que partan de la premisa que estamos frente a un fenómeno de magnitud y alcance global.

ejercicio del libre desarrollo de la personalidad". Ver, al respecto: Corte Constitucional de Colombia. Sentencia T-634/13, de fecha 13 de septiembre de 2013.

[9] Sobre este interesante debate, consultar: Daskal, Jennifer, "Microsoft Ireland, the Cloud Act and International Lawmaking 2.0". *Stanford Law Review Online*. Nº 71, 2018.

[10] Como se conoce, el moderno Estado-Nación surgió, esencialmente, como una respuesta a la dispersión del poder propio de la era feudal. De este modo, cuestiones como la existencia de un ejército permanente o la delimitación clara de fronteras fueron fundamentales para su surgimiento. Sin embargo, como bien expone Ayuso, en la actualidad el panorama geopolítico juega en su contra, ya que la presencia de armas nucleares ha supuesto un modo nuevo de guerrear, y el desarrollo de nuevas tecnologías ha generado que las fronteras no tengan la utilidad de antaño. Ayuso, Miguel. ¿Ocaso o eclipse del Estado? *Las transformaciones del derecho público en la era de la globalización*. Madrid: Marcial Pons, 2005, p. 44.

Corresponde, pues, examinar en qué medida esta evolución de las sociedades ha impactado en el caso particular del flujo y manipulación de la información.

III. Reflexiones acerca del derecho a la autodeterminación informativa en el marco de los procesos de globalización

Como se mencionó con anterioridad, la globalización ha impactado en distintas áreas del propio derecho constitucional, y particularmente a los derechos fundamentales. Se había mencionado que existían importantes esfuerzos académicos orientados a la construcción de un estándar universal de protección a través del movimiento del constitucionalismo global. Sin embargo, este proceso también ha generado consecuencias negativas para los derechos, ya que no solo se han globalizado los beneficios, sino también serios peligros que alteran la seguridad y el orden público de los Estados. Como bien refiere Beck, la globalización ha generado la aparición de "jugadores adicionales, nuevos papeles, nuevos recursos, reglas desconocidas, contradicciones y conflictos nuevos"[11].

En lo que respecta al derecho a la autodeterminación informativa, quizás su principal peligro radica en que, a diferencia de otras libertades, su protección no necesariamente está vinculada con algún espacio físico determinado. En efecto, las nuevas tecnologías, al mismo tiempo que han reportado importantes beneficios para la humanidad, también han fomentado escenarios de riesgo en relación con el empleo de los datos de las personas.

Quizás uno de los aspectos más problemáticos de estos nuevos peligros lo constituye el hecho de que la dispersión de la información supera el control de las fronteras y, por consiguiente, también a la fiscalización estatal. En un escenario de este calibre, pareciera ser intuitivo

[11] BECK, Ulrich. *Poder y contra-poder en la era global*. La nueva economía política mundial. Barcelona: Paidós, 2015, p. 27.

que la disciplina convocada a solucionar estos riesgos sea el derecho internacional, ya que nos encontramos frente a una situación que supera la capacidad de reacción de los Estados por separado.

Sin embargo, el propio derecho internacional cuenta con ciertas limitaciones (tanto teóricas como prácticas) para abordar los problemas relacionados con el uso de datos por un actor que se encuentra fuera del territorio nacional. De hecho, los conceptos centrales que sustentan esta disciplina -esto es, la soberanía, la no intervención y la prohibición del uso de la fuerza- no hacen más que reflejar la vulnerabilidad de las operaciones cibernéticas, ya que ellos no suelen brindar o justificar -al menos no de manera contundente- la adopción de medidas de respuesta frente a un daño de este tipo. Aquí puede advertirse, también, una seria exposición que compromete tanto al principio de seguridad nacional como a los derechos de la propia persona afectada, por lo que también puede añadirse que una distinción entre lo público y lo privado es de poca relevancia[12]. De este modo, la manipulación de datos no solo es una afrenta para la persona perjudicada, sino para la propia autoridad del Estado, cuyas fronteras nada pueden hacer para frenar esta clase de actos.

Sin perjuicio de ello, es importante recordar que estos problemas para caracterizar si se trata más de un perjuicio a la autoridad estatal o a la persona no deben conducirnos a equívocos sobre la naturaleza de los datos que se encuentran en el mercado. Como bien ha indicado el Tribunal Constitucional de España, "el hecho de que circulen datos privados por las redes sociales en Internet no significa de manera más absoluta –como parece defender la demandante de amparo– que lo privado se haya tornado público, puesto que el entorno digital no es equiparable al concepto de «lugar público» del que habla la Ley Orgánica 1/1982, ni puede afirmarse que los ciudadanos de la

[12] KILOVATY, Ido, "An Extra Territorial Human Right to Cybersecurity". *Notre Dame Journal of International & Comparative Law*. Vol. 10, Nº 1, 2020, p. 41.

sociedad digital hayan perdido o renunciado a los derechos protegidos en el artículo 18 CE"[13].

Todo ello refleja que existe la necesidad de implementar dos tipos de soluciones: o se precisan los adecuados contornos de estos principios -y, por ejemplo, se reformulan las ideas de soberanía y de no intervención-, o se les reemplaza por otros que puedan abordar directamente el núcleo del problema. Lo primero no ha sido ninguna novedad, ya que, por ejemplo, bien ha advertido Grimm[14] que el continuo uso de un término como el de "soberanía", no implica que estemos hablando necesariamente de la misma idea que fundamentó su surgimiento desde aproximadamente el siglo XIII. La segunda salida encuentra como uno de sus principales exponentes a la Unión Europea, cuya forma de proteger los datos personales -colocando a la autoridad supranacional como principal responsable de esta labor- ha sido un ejemplo que sería importante imitar.

Ahora bien, la discusión en torno a la idea de soberanía nos presenta un escenario distinto al clásicamente denominado como modelo westfaliano. Como se conoce, este sistema se caracterizaba por la existencia de un derecho internacional absolutamente dependiente de la voluntad estatal, "pero con un entramado jurídico y *modus operandi* distinto del derecho interno de los Estados. […] En primer lugar, el mundo está compuesto y dividido por Estados soberanos que no reconocen autoridad superior alguna. Segundo, los procesos de elaboración de leyes, la resolución de disputas y la aplicación de la ley están básicamente en manos de Estados individuales"[15].

---

[13] Tribunal Constitucional de España. Sala Segunda. Sentencia 27/2020, de 24 de febrero de 2020, fundamento jurídico 3.

[14] GRIMM, Dieter. *Sovereignty*. Nueva York: Columbia University Press, 2015, p. 3.

[15] CORTÉS, Francisco y PIEDRAHITA, Felipe. *De Westfalia a Cosmópolis. Soberanía, ciudadanía, derechos humanos y justicia económica global*. Bogotá: Siglo del Hombre Editores, 2011, p. 47.

En cambio, en el escenario contemporáneo se presentan fenómenos marcadamente distintos. Ciertamente, en muchos ámbitos los Estados siguen reteniendo un importante poder. No en vano han sido denominados en diversas oportunidades como los "amos y señores de los tratados". Sin embargo, es innegable que, en la actualidad, no son los únicos actores que se desenvuelven y participan activamente en el escenario internacional. Importantes empresas transnacionales, que en muchas oportunidades superan en poder económico a algunos Estados, han demostrado lo relevantes que pueden ser en el marco del diseño y establecimiento de políticas de alcance global. Esto, como no podía ser de otro, ocasiona que se vuelvan a indagar las bases que sostienen la soberanía estatal.

Sin perjuicio de ello, la reconfiguración de la idea de la soberanía estatal no es el único reto que deben afrontar las autoridades judiciales que suelen enfrentar los problemas concernientes a la manipulación de datos. Y es que existen ordenamientos constitucionales en los que existe un considerable desfase temporal entre la fecha en que fue aprobada la norma fundamental estatal y la era actual. Esto ha generado, particularmente en los Estados Unidos, un intenso debate en relación con las posturas originalistas y evolutivas[16]. El problema concreto radica en determinar si es que un derecho como el de la privacidad –reconocido en la Cuarta Enmienda a la Constitución de Estados Unidos, que se remonta a 1791– puede ser adaptado a las circunstancias y necesidades actuales.

[16] En esencia, porque existen múltiples variables, el originalismo postula que la interpretación debe tener en cuenta la opinión de los constituyentes o lo que se ha denominado como el "significado público original de la Constitución", mientras que los partidarios de las doctrinas denominadas como de "árbol viviente", postulan que la norma fundamental es un documento que, al sobrevivir a varias generaciones, debe preocuparse más de responder a las demandas actuales que en preocuparse del pasado. Para mayor información sobre ello, se recomienda revisar: Balkin, Jack: "The New Originalism and the uses of the history". *Fordham Law Review*. Vol. 82, 2013.

El debate en ese país sobre los alcances del derecho a la privacidad ha puesto de manifiesto la dificultad relacionada con la antigüedad de los textos y los problemas contemporáneos. Ahora bien, se podría simplemente señalar que, como cualquier otra cláusula constitucional, esa Cuarta Enmienda a la Constitución de los Estados Unidos es vaga e indeterminada, por lo que solo se requiere que la autoridad judicial, cuando conoce un caso en el que ella se encuentre comprometida, deba simplemente actualizar su significado.

Sin embargo, la problemática que aquí se expone no es tan sencilla como lo podría reflejar esta primera impresión. Y es que, como ha señalado Andrew DeFilippis[17], debe considerarse que establecer guías o pautas específicas podría suponer, en los hechos, contravenir los alcances de la Cuarta Enmienda, las cuales no contienen parámetros congelados en el tiempo, sino más bien definiciones razonables de palabras comunes, lo cual puede permitir modernizar las interpretaciones de esta cláusula constitucional.

De hecho, es evidente que el mundo no es igual al del siglo XVIII o XIX, y esa realidad no debería ser ignorada por las autoridades encargadas de aplicar la ley. Los textos pueden, ciertamente, presentar limitaciones en algunas áreas (piénsese, por ejemplo, en el derecho penal, en el que no es posible imponer una pena sin la existencia de una ley previa), pero ello de ninguna manera puede ser un obstáculo para brindar una adecuada protección de los datos personales en el marco del complejo sistema actual. En el siguiente apartado se evidenciarán algunos problemas que precisamente surgen cuando solo se centra en el Estado -como ocurría en los siglos XIX e inicios del XX- la protección de los derechos fundamentales.

[17] *Cfr*. DEFILIPPIS, Andrew: "Securing informationships: Recognizing a Right to Privity in Fourth Amendment Jurisprudence". *The Yale Law Journal*. Vol. 115, 2006, p. 1121.

IV. Consideraciones sobre la protección brindada a los datos personales desde un enfoque estatocéntrico

Como se ha podido advertir, difícilmente puede ser sostenido en la actualidad que el flujo de la información tenga como único responsable de la protección de datos a un Estado en específico. La tutela frente a ataques cibernéticos debe ser -si es que se pretende que sea efectiva- un esfuerzo articulado por la comunidad internacional en su conjunto. Ahora bien, como se pudo explicar con anterioridad, el derecho internacional actual no ha centrado mucho interés en esta temática, ya que al parecer sigue aún percibiéndose como una disciplina que regula las relaciones entre Estados, pero no entre actores privados. En esta clase de escenarios, sigue siendo fundamental que la autoridad estatal pueda desarrollar iniciativas en cooperación con autoridades extranjeras o, por qué no, con autoridades internacionales.

Desde este punto de vista, ciertos estándares fijados por el Derecho Internacional de los Derechos Humanos pueden ser relevantes para comprometer a los Estados a la adopción de medidas que puedan combatir de manera efectiva contra los ataques cibernéticos. Por lo general, siempre la responsabilidad internacional por la vulneración de derechos se había enfocado en el territorio de un Estado, ya que existía una clara asociación entre el lugar en el que se cometió el acto ilícito y los deberes que le correspondían adoptar a las autoridades nacionales para prevenirlo o castigarlo.

Sin embargo, los organismos internacionales empezaron a conocer de casos relativos a violaciones de derechos fuera del territorio del Estado afectado, lo cual generó el uso de la doctrina del "control efectivo", según la cual las autoridades no solo son responsables de las conductas que puedan advertirse dentro de su territorio, sino también de todos aquellos lugares o circunstanciales en las que hubieran tenido un control efectivo de la situación. Ahora bien, diversas entidades tuvieron ciertas dudas respecto de la posibilidad de que estos criterios sean empleados no solo para dominios físicos –que es el factor

que primordialmente se tomó en cuenta en estos casos–, sino también para lo que podrían denominarse como "controles en línea"[18], que es precisamente lo que se presenta cuando nos referimos a ataques cibernéticos.

Esto demuestra que, pese a sus limitaciones, las autoridades estatales deben ser el primer fuerte de protección de los derechos. De hecho, la práctica comparada demuestra que, incluso desde leyes nacionales, es posible configurar importantes medidas para la protección de datos. En efecto, existen ejemplos que demuestran que las leyes locales pueden tener importantes repercusiones en lo que respecta al flujo y manipulación de datos personales. En Estados Unidos, el Congreso aprobó la *Judicial Redress Act*, la cual permite a los ciudadanos europeos presentar recursos jurisdiccionales ante las cortes norteamericanas frente a una eventual vulneración relacionada con la manipulación de sus datos[19].

En todo caso, es importante recordar que, sobre este punto, existe un importante nivel de corresponsabilidad entre las autoridades legislativas y judiciales, ya que, en muchas oportunidades, estas últimas se encuentran en una comprometida situación cuando deben aplicar una norma obsoleta (esto es, una ley aprobada con anterioridad al avance descomunal de la tecnología) frente a una controversia digital. Y es que, aunque un tribunal pueda ciertamente brindar una solución a un caso concreto, lo cierto es que, mientras no se adopten disposiciones generales que aborden esta temática, la protección de los datos personales a escala global seguirá siendo incierta.

---

[18] KILOVATY, Ido, "An Extra Territorial Human Right to Cybersecurity". *Notre Dame Journal of International & Comparative Law.* Vol. 10, Nº 1, 2020, p. 44.

[19] LÓPEZ, Juan, "La protección de datos personales en la más reciente jurisprudencia del TJUE: Los derechos de la CDFUE como parámetro de validez del derecho europeo, y su impacto en la relación transatlántica UE-EEUU. *UNED. Teoría y Realidad Constitucional,* Nº 39, 2017, p. 563.

En el caso peruano existe un riesgo palpable, ya que, a diferencia de países como los Estados Unidos o los pertenecientes a la Unión Europea, la capacidad de respuesta tecnológica no es la deseable. Esto generaría que se pueda depender de otros Estados -que sí cuenten con esta clase de medios- para responder a ataques cibernéticos que afecten los datos personales, con todas las interrogantes que estos generan para la idea misma de soberanía, y su al parecer poca relevancia cuando nos referimos al mundo virtual[20].

Es importante resaltar que esta problemática ha encontrado una lenta pero progresiva respuesta por parte del Estado peruano. De este modo, en el año 2013 se aprobó la Ley 30096, Ley de Delitos Informáticos, cuyo objeto principal es, de conformidad con su artículo 1, "prevenir y sancionar las conductas ilícitas que afectan los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal, cometidas mediante la utilización de tecnologías de la información o de la comunicación, con la finalidad de garantizar la lucha eficaz contra la ciberdelincuencia". Este cuerpo normativo incorpora diversos delitos informáticos, lo cuales, en esencia, se agrupan en delitos contra datos y sistemas, contra la indemnidad y libertad sexuales, contra la intimidad y el secreto de las comunicaciones, contra el patrimonio y contra la fe pública.

Ahora bien, este paso –novedoso en el derecho nacional– es ciertamente insuficiente si es que no se acude a la cooperación internacional. En efecto, una ley de este tipo esencialmente se encarga de reprimir las conductas en los escenarios en los que el sujeto activo se encuentra en territorio nacional. Sin embargo, y como ha sido enfatizado recurrentemente en esta investigación, los ataques cibernéticos también pueden originarse en el exterior, o incluso en algunos casos se van a requerir considerables esfuerzos para identificar el lugar en el que

[20] Sobre ello, consultar: SCHMITT, Michael y VIHUL, Liis, "Respect for Soverignity in Cyberspace". *Texas Law Review*. Vol. 95, 2017, p. 1670.

se vulneró la protección de datos personales. La extradición podría ser, en este punto, una solución provisional, pero también demanda de una activa cooperación internacional para poder materializarse.

Es por ello que, consciente de este déficit, el Estado peruano, a través de la Resolución Legislativa 30913, ha aprobado recientemente el Convenio sobre la Ciberdelincuencia. No es sorprendente que este tratado haya sido auspiciado por el Consejo de Europa, ya es este continente el que ha adoptado las principales medidas para poder atacar esta clase de delitos. Puede advertirse que la aprobación de este instrumento internacional es posterior a la adopción de la Ley 30096, por lo que es bastante probable que deban incorporarse o modificarse diversas disposiciones de derecho interno para hacerlas compatibles con dicho convenio[21].

De hecho, ya existen algunas iniciativas legislativas dirigidas a implementar el tratado. Por ejemplo, el Proyecto de Ley 5630-2020-CR (presentado por la congresista Robertina Santillana Paredes) propone la creación de una ley de seguridad informática y de represión de delitos informáticos a fin de dar cumplimiento al Convenio sobre la Ciberdelincuencia. Dentro de las medidas llamativas, se sugiere la aprobación de Fiscalías Especializadas en Delitos Informáticos[22].

El Perú, por lo general, ha carecido de una respuesta sólida y comprensiva de la verdadera magnitud de los delitos informáticos. Uno de los pocos avances en esta materia ha sido la implementación de ciberpolicías contra delitos informáticos. Es, probablemente, en esta institución donde se han elaborado importantes esfuerzos para prevenir

[21] De hecho, el Capítulo II del Convenio hace referencia a las "[m]edidas que deberán adoptarse a nivel nacional", lo cual grafica que la aprobación de este instrumento va a generar, ineludiblemente, modificaciones a las leyes nacionales.

[22] Es importante precisar que la creación de esta clase de órganos al interior del Ministerio Público ya se había propuesto en el Proyecto de Ley 4643-2019-CR, presentado por el congresista Juan Carlos Gonzáles Ardiles, el cual declaraba que debía, por interés nacional y necesidad pública, crearse esta clase de entidades.

la realización de delitos cibernéticos. Es por que, por ejemplo, puede destacarse la existencia de una División de Investigación de Delitos de Alta Tecnología dentro de la Policía Nacional del Perú. Sin embargo, dentro del Ministerio Público y el Poder Judicial no se han realizado importantes avances en esta disciplina[23].

Debería agregarse a lo anteriormente expuesto la relevancia que las autoridades que se encargan de conocer de la realización de estos delitos no solo conozcan la ley nacional, sino que además deben familiarizarse con la interacción con el derecho internacional, y particularmente con el derecho de los tratados. Es importante recordar que esta disciplina, especialmente en el Perú, ahora involucra a todas las autoridades judiciales. La clásica separación entre el derecho interno y el internacional no tiene cabida en nuestro ordenamiento, ya que, de conformidad con el artículo 55 de la Constitución, los tratados forman parte del derecho interno, lo cual supone que estos sean de aplicación inmediata.

También debe resaltarse que, a diferencia de lo que ocurría a mitad del siglo XX, el derecho internacional de la actualidad se caracteriza por involucrarse e incluso regular materias que antes solían ser de competencia exclusiva de los estados, como podía ocurrir con los aspectos relacionados con la protección de la información privada o incluso la lucha contra la delincuencia. Los avances de la globalización solo demostraron que esta visión estatocéntrica es insuficiente, ya que muchos de los peligros que en la actualidad aquejan a la persona tienen un origen extraestatal. De hecho, como bien ha señalado Andrée Nollkaemper, son los tribunales de justicia de las respectivas jurisdicciones estatales los que se convierten en la mayor fuerza institucional en la protección del *international rule of law*, ya que ellos operan en una suerte

[23] En este punto, es importante revisar la experiencia estadounidense. En ese país, el Departamento de Justicia ha implementado una Sección de Delitos Cibernéticos y Propiedad Intelectual de la División Penal del Departamento de Justicia, el cual se especializa en cuestiones informáticas. Esta área ha liderado la capacitación y formación del resto de autoridades nacionales que conocen de esta clase de delitos.

de zona mixta que no es ni enteramente nacional o internacional, y que se caracteriza por su activa participación para la implementación de los tratados a nivel interno[24].

Sin embargo -y quizás sea lo más importante- las autoridades nacionales deben de tener también sólidos conocimientos en cuestiones relacionadas con el uso de la tecnología. El conocimiento del derecho no es suficiente para conocer la verdadera magnitud de la ciberdelincuencia y el daño que ocasiona a los datos personales. Como bien refiere Julio Eduardo Tenorio Pereyra, uno de los principales desafíos a propósito de la adopción del Convenio sobre la Ciberdelincuencia es el de la reducción de las brechas tecnológicas "y capacitaciones para poder responder de manera rápida y efectiva ante diferentes situaciones relacionada a los delitos informáticos y la ciberdelincuencia"[25].

En todo caso, todo lo expuesto en esta investigación permite advertir que las estrategias estrictamente locales no son suficientes para una prolija protección de los datos personales. Las leyes internas pueden ser una importante muestra de preocupación, pero se muestran como no idóneas para poder enfrentar la verdadera magnitud de la manipulación de datos personales. Quizás uno de los modelos a imitar sea el de la Unión Europea, cuyo proceso de integración no solo ha reportado importantes beneficios en materia económica, sino también en lo que concierne al proceso de tutela de los derechos, y concretamente al de la protección de los datos personales. Como bien han referido Paul Schwartz y Karl-Nikolaus Peifer, la Unión Europea ha construido una suerte de identidad legal para sus ciudadanos en torno a la idea de los derechos, y ha promovido una cultura democrática que se fundamenta en la autodeterminación informativa.

[24] *Cfr*. NOLLKAEMPER, Andrée. *National Courts and the International Rule of Law*. Oxford: Oxford University Press, 2011, p. 1.

[25] TENORIO, Julio, "Desafíos y Oportunidades de la adhesión del Perú al Convenio de Budapest sobre la Ciberdelincuencia". *Programa de Maestría en Diplomacia y Relaciones Internacionales de la Academia Diplomática del Perú*, 2018, p. 90.

Esto implica que los países que integran la Unión poseen fuertes mecanismos constitucionales de protección que fundamentan las restricciones generales sobre el contrato y el consentimiento[26].

Es importante precisar que, además de que se trata de un derecho reconocido en la Carta de los Derechos Fundamentales de la Unión Europea, la protección de datos personales ha merecido, también, desarrollos importantes en el derecho secundario y en la jurisprudencia del Tribunal de Justicia de la Unión Europea[27]. Este último, por ejemplo, se ha encargado de brindar trazos generales sobre la esencia de este derecho. De hecho, conceptos como el del contenido esencial, la fórmula de la proporcionalidad, o las intensidades de intervención -conceptos que, en realidad, son básicamente empleados en el derecho constitucional local- han permitido precisar las obligaciones de los Estados frente a los ataques cibernéticos.

Evidentemente, para la forja de esta clase de procesos, es indispensable contar con esfuerzos de carácter colectivo, los cuales suponen, las más de las veces, dejar atrás la idea de que los estados son los principales actores en el terreno internacional. Solo una respuesta global puede enfrentar los peligros de carácter global, y la protección de los datos personales ha dado una importante muestra de ello.

La propia Organización de las Naciones Unidas comparte este entendimiento de los datos personales, ya que su Asamblea General y diversos organismos pertenecientes a ella han emitido diversos pronunciamientos y resoluciones sobre la protección de datos en la era digital, y han mostrado una notable preocupación respecto del acelerado flujo de la comercialización de datos, por lo que ha instado a los Estados a

[26] *Cfr*. SCHWARTZ, Paul y PEIFER, Karl-Nikolaus: "Structuring International Data Privacy Law". *International Data Privacy Law*, núm. 21, 2017, p. 48.

[27] Sobre ello, consultar: BRKAN, Maja: "The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way Through the Maze of the CJEUs Constitutional Reasoning". *German Law Journal.* Núm. 20, 2019.

implementar las medidas que sean necesarias para su adecuada tutela, recordando, además, que las empresas privadas también deben someterse a esta clase de estándares[28]. Es sintomática que, dentro de su seno, también se haya propiciado la creación del cargo de Relator Especial sobre el derecho a la privacidad, el cual ya ha publicado diversos informes relacionados a la tutela de esta libertad en la era digital[29].

V. Conclusiones

Los estudios sobre la protección de datos personales han tenido, particularmente en el Perú, un enfoque estatocéntrico. Esto obedece a la arraigada costumbre de estimar que es el Estado el principal defensor de los derechos fundamentales, a lo que puede agregarse de que aún no somos plenamente conscientes de la información que se despliega y manipula fuera de las fronteras nacionales.

Precisamente el enfoque nacional de los derechos también ha generado escenarios de desprotección del derecho a la autodeterminación informativa. Sin embargo, el Estado peruano ha ido asumiendo la verdadera magnitud de este problema. La aceptación del Convenio sobre la Ciberdelincuencia da fe de ello. Sin embargo, resta mucho por hacer para tratar de adaptar el aparato estatal a las nuevas amenazas que surgen de la tecnología. Este breve ensayo ha tenido el propósito de advertir estos peligros y, de esta manera, de generar espacios de reflexión sobre problemas que el Estado ya no puede resolver por sí mismo.

[28] Se puede consultar, sobre ello, la resolución de la Asamblea General de las Naciones Unidas titulada "El derecho a la privacidad en la era digital", la cual fue aprobada el 31 de octubre de 2016 durante su septuagésimo primer período de sesiones.

[29] Por ejemplo, ha elaborado informes en los que ha recomendado que tanto los Estados como los actores privados deben contribuir para brindar información a los usuarios sobre la seguridad digital, así como de la asistencia tecnológica, los servicios de soporte, aplicaciones de información, términos de servicios y otras herramientas que permitan proteger los datos personales. Ver: Reporte del Relator Especial sobre el derecho a la privacidad de las Naciones Unidas. Informe de 12 de febrero de 2020, párr. 45.

LA AUTONOMÍA DEL DERECHO FUNDAMENTAL A LA AUTODETERMINACIÓN INFORMATIVA

✍ Sebastián Linares Luna*

I. Introducción

El desarrollo tecnológico ha creado una situación en la que es bastante sencillo acumular, organizar y trasladar cantidades inconmensurables de información personal. Quien posea la tecnología informática para el tratamiento de la información de carácter personal, posee un poder informático cuyo ejercicio extralimitado pone en riesgo a la posición jurídica de la persona como fin supremo de la sociedad y del Estado. En consecuencia, surge la necesidad humana de neutralizar el ejercicio extralimitado del poder informático. Así, se traslada la cuestión inmediatamente hacia el bien humano que satisface la apuntada necesidad humana: uno que otorga a las personas el poder de controlar la cantidad y calidad de la información que de uno mismo se haya podido brindar, recolectar y archivar en los bancos de datos de terceros. Un bien humano con este significado podrá ser llamado "autodeterminación informativa".

* Abogado por la Universidad de Piura. Experto Certificado en Protección de Datos por el Institute of Audit & IT–Governance. Asociado del Estudio Hernández & Cía. Abogados. Ex asesor jurisdiccional del Tribunal Constitucional.

Una de las discusiones originadas en torno a la autodeterminación informativa es la relacionada con la falta de claridad que ha predominado sobre la identificación del concreto y singular bien humano debido sobre el cual se construye y fundamenta. Así, por ejemplo, se ha llegado a afirmar que este derecho no es más que un instrumento añadido en la defensa del derecho fundamental a la intimidad[1] y, en consecuencia, una extensión del mismo[2]. En este contexto, queda justificada la utilidad y conveniencia de demostrar que la autodeterminación informativa se constituye como un derecho autónomo y, por tanto, distinto a cualquier otro derecho fundamental.

Con este propósito, la presente investigación estudia la finalidad que persigue el derecho a la autodeterminación informativa para distinguirlo de otros derechos fundamentales en general y del derecho a la intimidad en particular. A partir de dicho estudio, se analiza si el concreto dispositivo constitucional que lo reconoce cuenta con deficiencias en su formulación y si, consecuentemente, resulta posible un mejoramiento que conlleve a una modificación en el texto de la disposición constitucional que reconoce el derecho fundamental a la autodeterminación informativa.

II. La finalidad que persigue el derecho a la autodeterminación informativa

La finalidad de todo derecho fundamental es la protección de la persona como fin supremo de la sociedad y del Estado. Siendo esto así, resulta conveniente formularse la siguiente pregunta: ¿qué es lo que hace al derecho fundamental a la autodeterminación informativa, ser reconocido como tal y no como algo distinto? La pregunta traslada la

[1] Véase DEL CASTILLO, Isabel-Cecilia, *Protección de datos: cuestiones constitucionales y administrativas*, Thomson-Civitas, Madrid, 2007, p. 304.

[2] Véase REBOLLO, Lucrecio, "Balance constitucional: artículo 18.4 CE", *en datos personales.org*, Revista de la Agencia de Protección de Datos de la Comunidad de Madrid, número 6, 2003, p. 2.

cuestión inmediatamente hacia la finalidad concreta del referido derecho fundamental. Para determinarla, es conveniente recordar, en primer lugar, que el bien humano autodeterminación informativa es el llamado a satisfacer la necesidad humana de neutralizar el peligro que corre la persona (y sus derechos) frente al ejercicio extralimitado del poder informático[3]. El bien humano debido "autodeterminación informativa", persigue satisfacer esa advertida necesidad esencial y evitar que el ejercicio extralimitado del poder informático, instrumentalice a la persona y la ponga al servicio de ese poder informático; y por el contrario, conseguir que aún con los riesgos propios de la sociedad de la información sea posible conseguir la más plena realización de la persona que sea posible.

Siendo esta la finalidad resulta razonable sostener que esta finalidad que singulariza este concreto derecho fundamental, podrá lograrse sólo en la medida que a todo individuo se le permita disponer, como crea conveniente, de la información referida a su persona, es decir, en la medida que se le permita autodeterminarse informativamente, teniendo él la facultad de decidir qué información sobre sí mismo está dispuesto a suministrar y, una vez suministrada, qué información está dispuesto a mantener en aquellos registros de terceros[4].

En este mismo sentido se ha pronunciado el Máximo Intérprete de la Constitución al señalar que "el derecho a la autodeterminación informativa consiste en la serie de facultades que tiene toda persona para ejercer control sobre la información personal que le concierne,

---

[3] Sobre la referida necesidad se ha dicho que "es preciso que el individuo recupere o mantenga el poder de control y disposición sobre las informaciones". Teniendo en consideración que "ese poder será mucho más fuerte cuando las informaciones puedan afectar al reducto más íntimo de la personalidad" (ADINOLFI, Giulio, *Autodeterminación informativa, consideraciones acerca de un principio general y un derecho fundamental*. Recuperado de: http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1405-91932007000200001).

[4] Cfr. CASTILLO, Luis, *Comentarios al Código Procesal Constitucional,* 2ª edición, Palestra Editores, Lima, 2006, p. 1053.

contenida en registros ya sean públicos, privados o informáticos, a fin de enfrentar las posibles extralimitaciones de los mismos. Se encuentra estrechamente ligado a un control sobre la información, como una autodeterminación de la vida íntima, de la esfera personal"[5].

Por lo tanto, debe afirmarse que la finalidad del derecho a la autodeterminación informativa consiste en "darle la posibilidad a todo sujeto de disponer real y efectivamente de los datos referidos a su persona, de modo que esté en condiciones de poder evitar extralimitaciones en el ejercicio de la tecnología informática aplicada a la organización y tratamiento de sus datos personales"[6]. En definitiva, el propósito de este derecho fundamental consiste en lograr un verdadero control de la información sobre uno mismo.

III. Breve referencia al derecho fundamental a la intimidad

La palabra "íntimo", "procede del término latino 'intimus' que constituye una variación de la expresión 'intumus', que a su vez es la forma superlativa del adverbio 'intus', que significa dentro. Es célebre la expresión de San Agustín de Hipona, refiriéndose a Dios, 'intimior intimo meo', en su Confesiones, 'Dios es más íntimo que mi propia intimidad'; y que remite a lo más profundo de cada hombre para entender la esencia de la intimidad" [7].

Nótese lo siguiente: "con el vocablo 'intimidad' se alude no sólo al carácter oculto o secreto de aquellas circunstancias que rodean la existencia del hombre sino que se refiere sobre todo a circunstancias internas, esenciales del individuo y que éste mantiene como núcleo de su personalidad. Así, lo íntimo no representa aquello que la persona

[5] EXP. N.° 4739-2007-HD/TC, fundamento 2.

[6] CASTILLO, Luis, *Comentarios al Código*..., ob. cit., p. 1053.

[7] HERRÁN, Ana, *La violación de la intimidad en la protección de datos personales*, Dykinson SL, Madrid, 1998, p. 2. Es preciso señalar que la autora se fundamenta, a su vez, en BLÁZQUEZ-FRAILE, Agustín, *Diccionario Latín-Español*, Barcelona, Sopena, 1967, p. 913.

quiere reservar, sino parte de su esencia individual que se encuentra en su interior y le es propia, como aspecto de su condición de ser humano, y sin la cual se vería despojada de su sustancialidad humana. Íntimo, pues, no se identifica con secreto o desconocido para terceros; va más allá, porque representa la propia esencia de cada individuo en cuanto ser humano, su propia individualidad"[8].

En el actual ordenamiento constitucional peruano, la intimidad es un derecho fundamental que se encuentra expresamente reconocido en el artículo 2, inciso 7, de la Constitución, con el siguiente enunciado lingüístico: "[t]oda persona tiene derecho: (...) 7. Al honor y a la buena reputación, a la intimidad personal y familiar así como a la voz y a la imagen propias (...)".

Al respecto, el Supremo Intérprete de la Constitución "ha hecho referencia al contenido protegido del derecho a la intimidad. Por ejemplo, en la STC 6712-2005-HC (…) delimitó sus alcances, concluyendo que [...] **la protección de la intimidad implica excluir el acceso a terceros de información relacionada con la vida privada de una persona, lo que incluye** las comunicaciones, documentos o **datos de tipo personal**. De esta forma, la intimidad se presenta como una libertad en un sentido negativo, en tanto excluye o impide que terceros –entre ellos, claro está, el mismo Estado– puedan acceder a determinados contenidos que la propia persona desea resguardar [énfasis añadido]"[9].

En ese contexto, la intimidad puede ser definida, en términos generales, como "el derecho a que nos dejen en paz"[10]. En efecto, el Supremo Intérprete de la Constitución ha establecido que "[e]n el caso

[8] Ibídem.

[9] EXP. N.° 9-2014-PI/TC, fundamento 6.

[10] MURILLO DE LA CUEVA, Lucas, *El derecho a la autodeterminación informativa y la protección de datos personales.* Recuperado de: http://hedatuz.euskomedia.org/6518/1/20043058.pdf.

concreto de la intimidad, se demanda lo que en su momento la doctrina anglosajona denominó *right to be alone*, esto es, el derecho a no ser perturbado. La consecuencia natural del ejercicio de este ámbito del derecho a la intimidad es, que la persona tenga la posibilidad de '[...] tomar decisiones relacionadas con diversas áreas de la propia vida libremente, tener un espacio de tranquilidad personal, mantener reservados ciertos aspectos de la vida privada y controlar la difusión de información personal hacia el público' [Corte Interamericana de Derechos Humanos en el Caso Fonteveechia y D'Amico vs. Argentina. Sentencia de Fondo de 29 de noviembre de 2011, párr. 48]"[11].

No obstante, debe tenerse en consideración que "la evolución de las sociedades contemporáneas, en las que es habitual la manipulación y traslado de toda clase de información a través de distintas plataformas, ha generado que esta dimensión negativa del ejercicio del derecho a la intimidad sea insuficiente. Consecuentemente, en la actualidad se reconoce, además, una dimensión de carácter positivo, a través de la cual se exige que el Estado adopte las medidas que sean indispensables para su adecuada tutela, lo cual abarca la posibilidad del titular de la información de poder resguardarla frente al accionar de terceros, incluso del propio Estado"[12]. En este escenario, resulta preciso preguntarse: ¿la referida "dimensión de carácter positivo" resulta suficiente para afirmar que el derecho a la intimidad protege a la persona de los ataques del poder

[11] EXP. N.° 9-2014-PI/TC, fundamento 7. Al respecto, Lucas Murillo de la Cueva ha señalado: "cabe establecer que el entendimiento del derecho a la intimidad que ha prevalecido antes de la difusión de las potencialidades de la informática lo identifica con la pretensión del individuo de excluir del conocimiento ajeno cuanto guarda relación con sus relaciones sexuales, conyugales, paterno-filiales y familiares, con su cuerpo, con su salud, con su muerte, con sus pensamientos, creencias, aficiones y afectos. Los distintos medios jurídicos puestos a disposición de su salvaguardia se ocupaban de ofrecer tutela penal, administrativa o civil frente a las eventuales amenazas o a las lesiones consumadas a tal derecho" (MURILLO DE LA CUEVA, Lucas, *El derecho a la autodeterminación informativa y la protección de datos personales*. Recuperado de: http://hedatuz.euskomedia.org/6518/1/20043058.pdf).

[12] Ídem, fundamento 8.

informático? La respuesta, es negativa. Los fundamentos que justifican esta posición serán estudiados a continuación.

IV. Autodeterminación informativa e intimidad

Como ya se ha mencionado, "[s]in ser el único que pueda llegar a existir, en la actualidad existe un peligro de agresión [a la posición jurídica de la persona] el cual proviene de la recogida y tratamiento informatizado de los datos o informaciones referidos a aspectos de la personalidad de un gran número de sujetos"[13]. No cabe duda de que esta actividad de recogida y tratamiento de información de carácter personal, efectuada a través de la creación, gestión y manipulación de los bancos de datos personales, pone en riesgo la intangibilidad del derecho fundamental a la intimidad de las personas. Considérese, por ejemplo, "cómo un conjunto de datos pertenecientes a la intimidad o privacidad de un sujeto, pueden ser difundidos y conocidos por muchos, al estar recogidos u organizados en un banco de datos"[14].

No obstante ello, debe tenerse presente que aunque la intimidad se constituya como el derecho fundamental que puede llegar a ser el más amenazado por la extralimitación del poder informático, no es el único. Y es que "el uso extralimitado de la información que se acumula en un banco de datos puede terminar afectando derechos como la libertad, la igualdad, el desarrollo de la personalidad y, en definitiva, el tratamiento de la persona humana como una realidad que posee una dignidad"[15].

---

[13] CASTILLO, Luis, *Comentarios al Código*..., ob. cit., p. 1054.

[14] Ibídem. De manera complementaria, HERRÁN, Ana, La violación de la intimidad..., ob. cit., p. 34, sostiene: "Las diversas definiciones consultadas respecto a los derechos de la personalidad coinciden en afirmar que se trata de bienes que garantizan el disfrute por cada persona de sus propias facultades físicas, morales e intelectuales, sin los cuales el ser humano se vería desprovisto de sus principales garantías para asegurar el pleno desarrollo de su persona. Entre los derechos de la personalidad destaca el derecho a la intimidad".

[15] Ibídem.

En efecto, "[s]e trata de evitar que con el uso de las tecnologías informáticas, en particular, de la recogida y tratamiento informatizado de datos personales, la persona humana se constituya en un mero objeto destinado a proporcionar información, la cual debidamente procesada puede servir para predecir su comportamiento futuro, y con base a esas predicciones, tomar decisiones –una entidad privada como una empresa de servicios, o una entidad pública como un hospital o, en definitiva, el mismo poder político– potencialmente discriminatorias. Por tanto, el derecho a la autodeterminación informativa no sólo está destinado a resguardar las esferas personalísimas de los particulares, sino a la persona en su totalidad de ámbitos"[16]. Y ello, precisamente, es lo que justifica que la referida "dimensión de carácter positivo" no resulte suficiente para afirmar que el derecho a la intimidad resguarda a la persona en su totalidad de ámbitos. No debe perderse de vista que "la problemática que suscita el tratamiento automatizado de la información personal es tan singular, que requiere de una solución jurídica *ad hoc*, de un nuevo instrumento de tutela y garantía de la libertad y dignidad humanas"[17].

En ese sentido, el derecho fundamental a la autodeterminación informativa tendrá la posibilidad de lograr la finalidad que se propone

[16] Ídem, pp. 1054-1055. Al respecto, Lucas Murillo de la Cueva ha señalado: "En los primeros momentos de despliegue de la informatización de la sociedad, se planteó la defensa frente a los riesgos específicos que comporta desde el baluarte que ofrecía el derecho a la intimidad. Y todavía hoy se encuentran quienes siguen viendo en ella el *nomen iuris* desde el que responder a las agresiones que se perpetran contra nuestros derechos mediante el uso incontrolado de información personal. Sin embargo, paulatinamente se ha ido estableciendo que los rasgos indicados del derecho a la intimidad no permiten responder a los riesgos que proceden de la recopilación, tratamiento, almacenamiento y transmisión de datos personales por medio de las posibilidades que ofrecen la informática y la telemática o, si se prefiere, las Tecnologías de la Información y de las Comunicaciones" (MURILLO DE LA CUEVA, Lucas, *El derecho a la autodeterminación informativa y la protección de datos personales*. Recuperado de: http://hedatuz.euskomedia.org/6518/1/20043058.pdf.).

[17] GARRIGA, Ana, *Tratamiento de datos personales y derechos fundamentales*, Dykinson SL, Madrid, 2009, p. 30.

(el control real y efectivo de los datos que le conciernen a una persona), si es que no sólo se reconoce respecto de datos o informaciones considerados como "privados o íntimos", sino también sobre aquellas que, siendo personales, pueden ser de carácter "público". Y es que "lo que ha de definir el derecho a la autodeterminación informativa no es la calidad de público o privado de la información o del dato incorporado al banco de datos; sino más bien lo decisivo para hablar del referido derecho es el tratamiento informatizado que se le pueda dar junto a otros datos (privados o no) de una misma persona o de personas distintas. Porque es precisamente de ese tratamiento informatizado de donde puede provenir las agresiones a la dignidad humana, a la igualdad, a la libertad, al libre desarrollo de la personalidad; y es sin lugar a dudas ese tratamiento informatizado el que singulariza de tal modo las posibles agresiones a la dignidad del hombre, que ha hecho necesario hablar de un nuevo derecho fundamental: el derecho a la autodeterminación informativa"[18].

Entonces, ¿el derecho fundamental a la autodeterminación informativa es más que un instrumento añadido o una mera extensión del derecho a la intimidad? El derecho fundamental a la autodeterminación informativa se constituye como un derecho autónomo y, por tanto, distinto a cualquier otro derecho fundamental[19]. Ello no significa que deba pasarse por alto la estrecha relación que existe entre intimidad y autodeterminación informativa como bienes humanos debidos que son, ambos llamados a ser conseguidos para lograr la plena realización de la persona. En efecto, aunque existen importantes diferencias entre ambos, "también hay que reseñar que tienen importantes conexiones:

[18] CASTILLO, Luis, Comentarios al Código..., ob. cit., pp. 1055-1056.

[19] Al respecto, GALÁN, Mercedes, *Intimidad. Nuevas dimensiones de un viejo derecho*, Ed. Ramón Areces, Servicio de Publicaciones de la URJC, Madrid, 2005, p. 214, se refiere a la autodeterminación informativa como "un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos".

son inherentes a la dignidad de la persona (…) y comparten el objetivo de ofrecer protección a la vida privada personal y familiar"[20].

En suma, y sin perjuicio de su estrecha conexión, debe tenerse presente que los derechos bajo comentario se diferencian en el bien humano que le da justificación a cada uno de ellos y, consecuentemente, se diferencian en su contenido constitucional y en su objeto. Por un lado, el derecho a la intimidad es un derecho de la personalidad que se sostiene en un bien humano debido que consiste en el aseguramiento de un ámbito propio y reservado de la vida frente a la acción y el conocimiento de los demás (sean estos poderes públicos o simples particulares); y un contenido constitucional conformado por un conjunto de atribuciones destinado a asegurar en la mayor medida de lo posible este ámbito de inmunidad propio y reservado, y que se concreta principalmente a través de deberes de abstención que se impone a terceros (privados y poderes públicos), deberes de no intromisión en ese ámbito de inmunidad de la persona (aunque es cierto que el derecho a la intimidad ha evolucionado hacia contenidos positivos). Todo esto permite concluir que el derecho fundamental a la intimidad tiene por objeto garantizar a toda persona, y en la mayor medida de lo posible, un ámbito reservado de su vida vinculado con el respeto de su dignidad.

Por su parte, el derecho a la autodeterminación informativa tiene por bien humano debido uno que consiste en el aseguramiento del control efectivo sobre los datos personales, privados o públicos, que se puedan generar de las relaciones humanas; y un contenido constitucional conformado por un haz de facultades consistentes en diversos poderes jurídicos que pretenden, en último término, atribuir a la persona afectada un control real y efectivo sobre sus datos personales, tengan el carácter de íntimos o no, y que se concretan principalmente en deberes

[20] HERNÁNDEZ, José Miguel, *El Derecho a la Protección de Datos Personales en la Doctrina del Tribunal Constitucional*, Aranzadi, Pamplona, 2013, p. 119.

de acción de terceros (particularmente los titulares de los bancos de datos) y que son deberes no contenidos en el derecho fundamental a la intimidad[21]. A su vez, este bien humano y consecuente contenido constitucional permiten reconocer que este derecho fundamental tiene por objeto asegurar, en la mayor medida de lo posible, un poder en el titular de la información personal para evitar un ejercicio extralimitado del poder informático del titular de las bases de datos.

Por todo esto, debe ser rechazado, de manera categórica, la identificación del derecho fundamental a la autodeterminación informativa con el derecho fundamental a la intimidad. La razón es simple: "los espacios tutelados por ambos no recaen sobre la misma realidad jurídica"[22].

V. Referencia al ordenamiento constitucional peruano

El derecho fundamental a la autodeterminación informativa se encuentra reconocido en el artículo 2, inciso 6, de nuestra Constitución. Este concreto dispositivo constitucional está redactado de acuerdo a los siguientes términos: "Artículo 2°.- Toda persona tiene derecho: (…) 6. A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar".

Sin embargo, y por los motivos antes expuestos, no es acertado que se pretenda circunscribir la protección del derecho fundamental a la autodeterminación informativa, única y exclusivamente, a la esfera íntima o privada de la persona. Y es que, aunque el artículo 2, inciso 6, de la Constitución haga referencia expresa sólo a la intimidad personal y familiar, el principio constitucional *pro libertatis* o *pro homine*, así

[21] Cfr. HERNÁNDEZ, José Miguel, *El Derecho a la Protección de Datos Personales*..., ob. cit., pp. 32-33 y 119.

[22] SERRANO, María, *El derecho fundamental a la protección de datos. Derecho español y comparado*, Civitas Ediciones, Madrid, 2003, p. 483.

como el principio de interpretación sistemática y unitaria de la Constitución, no permiten circunscribir la protección contra el ejercicio extralimitado del poder informático, solamente al derecho a la intimidad.

En efecto, en virtud del principio *pro libertatis* o *pro homine*, "se exige que frente a una disposición constitucional que permita más de una interpretación, se ha de preferir aquella interpretación que más favorezca a la persona y, por tanto, a sus derechos fundamentales. No cabe duda que si se ha admitido que el poder informático, en su modalidad de tratamiento informatizado de datos personales, genera riesgos a la existencia digna de la persona humana considerada en su totalidad y, por tanto, a sus derechos fundamentales, y si se ha afirmado también que el derecho a la autodeterminación informativa se ha constituido en el medio actual de protección frente a cualquier agresión que sobre la dignidad del hombre pueda producir el uso extralimitado e indebido de la tecnología informática, entonces, no puede concluirse que el derecho a la autodeterminación informativa sólo está destinado a proteger un ámbito de la personalidad del hombre, el vinculado a su intimidad. Por el contrario, deberá hacerse extensivo a proteger a la persona humana en unidad y totalidad. Esta interpretación favorece más la protección de la persona que aquella otra que limita la actuación del derecho sólo para proteger un ámbito de la personalidad"[23].

En ese mismo sentido, el Tribunal Constitucional ha manifestado que "la interpretación de la recurrida no resulta acorde a los principios *pro homine* y *pro libertatis*, según las cuales (*sic*), **ante diferentes interpretaciones de un dispositivo legal, se debe optar por aquella que conduzca a una mejor protección de los derechos fundamentales, descartando así las que restrinjan o limiten su ejercicio**. Vale decir, el principio *pro homine* impone que, en lugar de asumirse la interpretación restrictiva, e impedir el derecho a la efectiva tutela jurisdiccional, se opte por aquella que posibilite a los recurrentes el ejercicio de dicho

[23] CASTILLO, Luis, *Comentarios al Código...*, ob. cit., pp. 1057-1058.

derecho. La tesis interpretativa que posibilitaría este último supuesto es, justamente, la que proviene del propio tenor literal del mencionado artículo 80° del CPC [énfasis añadido]"[24].

Por su parte, vinculado a este razonamiento se encuentra el principio de interpretación unitaria y sistemática de la Constitución. Para lo que aquí importa resaltar, en virtud de este principio, la Constitución debe ser interpretada como una unidad sistemática, de manera que se eviten lagunas o interpretaciones dispares o contradictorias. "Pues bien, si la persona humana es el fin de la sociedad y del Estado (artículo 1 CP), de manera que los derechos fundamentales se colocan en la cúspide de toda realidad social o jurídica, significa que bien entendido el derecho a la autodeterminación, no podrá ser interpretado como un derecho que otorga facultades a su titular sólo para la defensa de su intimidad (personal y familiar) frente al mal uso del poder informático, sino que deberá otorgarle igualmente facultades para evitar la vulneración de otros derecho fundamentales igualmente puestos en riesgo por el tratamiento informatizado de datos"[25]. Y no podía ser de otro modo, pues la Carta Política no sólo reconoce a la intimidad como derecho fundamental, sino también a toda una amplia gama de derechos fundamentales que tienen un mismo propósito: garantizar el pleno desarrollo de la persona.

Sobre el principio de interpretación unitaria y sistemática de la Constitución, el Alto Tribunal tiene dicho: "según este criterio de interpretación, **el operador jurisdiccional debe considerar que la Constitución no es *una* norma (en singular), sino, en realidad, un *ordenamiento* en sí mismo, compuesto por una pluralidad de disposiciones que forman una unidad de conjunto y de sentido**. Desde esta perspectiva, el operador jurisdiccional, al interpretar cada una de sus cláusulas, no ha de entenderlas como si cada una de ellas fuera compartimentos estancos o aislados, sino cuidando de que se preserve la

[24] EXP. N.° 75-2004-AA/TC, fundamento 6.

[25] CASTILLO, Luis, Comentarios al Código..., ob. cit., p. 1058.

unidad de conjunto y de sentido, cuyo núcleo básico lo constituyen las decisiones políticas fundamentales expresadas por el Poder Constituyente. Por ello, ha de evitarse una interpretación de la Constitución que genere superposición de normas, normas contradictorias o redundantes [énfasis añadido]"[26].

Argumentada la necesidad de interpretar a la autodeterminación informativa como un derecho fundamental que protege a la persona en su totalidad de ámbitos y, en consecuencia, a sus derechos fundamentales (vigentes y exigibles en nuestro ordenamiento constitucional), ¿qué sentido tiene que el Constituyente (a través de la fórmula lingüística del artículo 2, inciso 6) sólo haya mencionado expresamente a la intimidad personal y familiar? Para responder este cuestionamiento, resulta conveniente recordar las conexiones existentes entre autodeterminación informativa e intimidad: son inherentes a la dignidad de la persona y comparten el objetivo de ofrecer protección a la vida privada, personal y familiar.

A partir de tales vínculos inescindibles, y a partir también de la estrecha relación entre ambos derechos fundamentales y sus respectivos bienes humanos debidos, resulta razonable afirmar que el Constituyente optó por mencionar expresamente a la intimidad por ser el derecho fundamental más propenso y cercano a los riesgos derivados del poder informático. No resulta no solo lógico sino tampoco constitucional, llegar a la conclusión de que los demás derechos -de los que igualmente el Constituyente predica su vigencia efectiva- puedan quedar desprotegidos frente a las extralimitaciones del poder informático. En este sentido, y reafirmando esta lógica interpretativa, el Tribunal Constitucional consagra que el derecho a la autodeterminación informativa "garantiza que el individuo sea capaz de disponer y controlar el tipo de datos que sobre él se hayan registrado"[27]. Datos que, habrá que insistir una vez más, podrán tener carácter íntimo o no.

[26] EXP. N.° 5-2003-AI/TC, fundamento 23.

[27] EXP. N.° 1797-2002-HD/TC, fundamento 3.

VI Una propuesta de cambio al artículo 2, inciso 6, de la Constitución

Si el empeño por dotar de estabilidad y firmeza a nuestra Carta Política es una constante histórica del constitucionalismo, es también cierto que tan antigua como ella es la idea de que la Constitución no puede ser entendida como una ley eterna, sino que ha de ser necesariamente modificable. Junto a este argumento, existen, fundamentalmente, otras dos razones que, de forma tradicional, se han alegado en favor de la variabilidad constitucional: (i) porque ha sido concebida y justificada como medio idóneo para subsanar los errores, políticos o técnicos, en los que hubiera podido incurrir el Constituyente; y (ii) porque la realidad política y social no es estática, sino que se encuentra en continuo movimiento (y, en consecuencia, la única manera posible de evitar el desfase entre ésta y la realidad normativa será la de permitir la modificación, formal o no, del Texto Constitucional)[28].

Pues bien, una vez justificada la necesidad de protección de la persona en todos sus ámbitos, y no solo en el referido a la intimidad, frente a ejercicios extralimitados del poder informático, conviene preguntarse si es posible un mejoramiento que conlleve a una modificación en el texto de la disposición constitucional que reconoce tal derecho fundamental a fin de recoger, lo más acabadamente posible, los elementos esenciales de su contenido constitucional.

La pregunta se debe responder afirmativamente una vez que se comprueba que el citado artículo 2, inciso 6, de la Constitución tiene al menos dos deficiencias (consecuencia de los errores técnicos o dogmáticos en los que pudo incurrir el Constituyente). La primera es que hace referencia expresa sólo a alguno de los referidos elementos esenciales, a saber, la difusión de información personal; y la segunda es que sólo hace expresa referencia al ámbito de protección de un derecho fundamental, a saber, la intimidad personal y familiar de las personas.

---

[28] Cfr. RUIPEREZ, Javier, "Algunas consideraciones sobre la reforma constitucional", en *Revista de Estudios Políticos (Nueva Época)*, número 75, 1992, pp. 234-238.

En este escenario, resulta conveniente proponer un enunciado lingüístico que refiera más acabadamente, aquello que hace a la autodeterminación informativa ser lo que es. Un tal enunciado lingüístico puede ser el siguiente:

> "Artículo 2°.- Toda persona tiene derecho: (…) 6. ***A la autodeterminación informativa, de modo que ella logre un efectivo control de los datos que le conciernen***".

Se trata de un enunciado que menciona expresamente el nombre del bien humano debido, a saber, la autodeterminación informativa; y que expresamente menciona una concreción del mismo, de la mano de la finalidad que persigue: el efectivo control que la persona debe tener sobre la información personal. Con estos dos elementos se construye un enunciado normativo desde el cual se permite concluir las atribuciones que razonablemente, en cada caso concreto, se deben reconocer para asegurar un tal control efectivo de la información personal; y permite concluir también la protección de la persona como una unidad, y no solo el ámbito de su intimidad.

De modo que el enunciado normativo propuesto lejos de resultar un enunciado menos protector por no mencionar las atribuciones o los derechos protegidos, resulta relevantemente conveniente, porque su enunciado abierto y genérico resulta adaptable al cambio de las circunstancias que pueda ser operado en cada momento histórico, adaptación que se manifestará a través de las concreciones que del bien humano debido pueda decidir tanto la ley de desarrollo constitucional, como las sentencias del intérprete supremo de la Constitución. Naturalmente, las concreciones legislativas y jurisprudenciales que se hagan del enunciado normativo aquí propuesto, necesitarán de la ayuda de la mejor dogmática constitucional que la academia pueda ir formulando para justificar la oportunidad y conveniencia de las mencionadas concreciones.

Consecuentemente, a partir de la modificación propuesta en el actual texto constitucional del mencionado artículo 2, inciso 6, quedan salvadas las dos deficiencias arriba apuntadas, y se brinda la posibilidad

de que toda persona logre una mejor y mayor comprensión de la verdadera esencia del contenido constitucional de su derecho a través del concreto dispositivo que lo recoge. Y es que las grandes mejoras pueden ser consecuencia de pequeños cambios.

VII. Reflexiones finales

- **Primera.** En términos generales, la autodeterminación informativa atribuye al titular del derecho la facultad para mantener el control de los datos que le conciernen, pero que, de manera voluntaria o necesaria, han devenido en parte de registros o bases de datos y en objeto de tratamiento informático por parte de terceros. En tal sentido, la finalidad de este derecho fundamental consiste en lograr un verdadero control de los datos que nos conciernen, de modo que la persona esté en condiciones de poder evitar el ejercicio extralimitado del poder informático o de neutralizarlo una vez que surja.

- **Segunda.** El artículo 2, inciso 6, de la Constitución recoge una atribución que consiste en la facultad de toda persona a exigir que los servicios informáticos, computarizados o no, públicos o privados, no suministren información que afecte la intimidad personal y familiar. Sin embargo, debe precisarse que el contenido constitucional de este derecho no se agota en dicha facultad constitucionalizada expresamente, sino que también deben ser consideradas todas aquellas otras facultades necesarias para conseguir la finalidad que persigue el referido derecho, es decir, para mantener el control real y efectivo de los datos personales que nos conciernen, sean estos de carácter íntimo o no.

- **Tercera.** El derecho fundamental a la autodeterminación informativa se constituye como un derecho autónomo y, por tanto, distinto a cualquier otro derecho fundamental. Aunque la intimidad se constituya como el derecho fundamental

que puede llegar a ser el más amenazado por la extralimitación del poder informático, no es el único. Y es que el uso extralimitado de la información que se acumula en un banco de datos puede terminar afectando a la persona en su totalidad de ámbitos.

- **Cuarta.** No es acertado que se pretenda circunscribir la protección del derecho fundamental a la autodeterminación informativa, única y exclusivamente, a la esfera íntima o privada de la persona. El principio constitucional pro libertatis o pro homine, así como el principio de interpretación sistemática y unitaria de la Constitución, no permiten esa interpretación restrictiva.

- **Quinta.** El Constituyente optó por mencionar expresamente a la intimidad en el concreto dispositivo constitucional que recoge el derecho fundamental a la autodeterminación informativa, por ser el derecho fundamental más propenso y cercano a los riesgos derivados del poder informático. No resulta lógico ni constitucional llegar a la conclusión de que los demás derechos puedan quedar desprotegidos frente a las extralimitaciones del poder informático.

- **Sexta.** ¿Es posible un mejoramiento que conlleve a una modificación en el texto de la disposición constitucional que reconoce el derecho fundamental a la autodeterminación informativa? La pregunta se debe responder afirmativamente. En este escenario, se propone un enunciado lingüístico que abarca, de manera concisa pero acabada, aquello que hace a la autodeterminación informativa ser lo que es, es decir, aquello que refleja la verdadera esencia de su contenido constitucional: "Artículo 2°.- Toda persona tiene derecho: (…) 6. A la autodeterminación informativa, de modo que logre un efectivo control de los datos que le conciernen".

HÁBEAS DATA Y DERECHO AL OLVIDO

La ponderación entre el derecho a la autodeterminación informativa y la libertad de información

✍ Enrique Pestana Uribe*

I. Notas Preliminares

La Constitución peruana de 1993 trajo como novedad un nuevo proceso constitucional con el cual no contábamos en la Carta de 1979 y cuyo mayor influjo lo recibió de la Carta brasileña de 1988, aunque en nuestro caso mejorada y con mayor ámbito de protección. Se trata del hábeas data, *nomen iuris* que recibió para diferenciarlo del hábeas corpus, del proceso de amparo y del proceso de cumplimiento, cada uno de los cuales tiene asignada la protección de un determinado número de derechos fundamentales según su naturaleza y finalidad. No cabe duda que bien se pudo optar por proteger los derechos que actualmente protege el hábeas data mediante el proceso de amparo, tal como ocurre en algunos países; sin embargo el constituyente prefirió configurar un mecanismo destinado especialmente a proteger el derecho a la autodeterminación informativa y además –no menos importante– el derecho de acceso a la información pública, aspecto este que por cierto no ampara el hábeas data en otras latitudes.

* Abogado especializado en Derecho Constitucional y Derecho Internacional Público. Docente y capacitador. Miembro de la Asociación Peruana de Derecho Constitucional.

El propósito de este trabajo es ir más allá de lo que tradicionalmente ha comprendido el proceso de hábeas data, tratando de indagar hasta qué punto este mecanismo procesal constitucional podría servir para que la información referida a una persona pudiese ser literalmente "borrada" de los sitios que aparecen en la web a través de los motores de búsqueda o portales que dominan la internet. Creemos que analizar esta posibilidad desde la doctrina podría contribuir, de algún modo, a esclarecer el actual y aún incipiente avance del denominado "derecho al olvido" en una época donde las redes sociales y la información que abunda en la red se encuentra omnipresente en la vida diaria de nuestra sociedad, por cierto cada vez más globalizada e interconectada.

Es necesario tener en cuenta que el derecho avanza a pasos agigantados y cada vez aparecen nuevos derechos o nuevas dimensiones de algún derecho "viejo". Particularmente creemos que el derecho al olvido constituye una nueva dimensión del derecho a la autodeterminación informativa que requiere de desarrollo tanto en el ámbito de la doctrina como a nivel jurisprudencial. No obstante, sería importante que la legislación también se ocupe de esta figura de manera específica, delimitándola de tal manera que los ciudadanos sepan cuáles son sus alcances y en qué circunstancias puede ser utilizada sin afectar otros derechos fundamentales o bienes jurídicos constitucionalmente protegidos.

En tal sentido, nuestro propósito estará esencialmente encaminado a ensayar los alcances y límites que debiera tener el derecho al olvido y hasta qué punto su utilización podría enfrentar ponderadamente al derecho a la información o a la libertad de expresión, pues es un hecho innegable que siempre habrá de existir una constante tensión entre el derecho a la privacidad y el interés público que se nutre de la libertad de prensa a través de los medios de comunicación masivos, pese a que muchas veces estos incurren en excesos que terminan afectando derechos humanos de primerísimo orden.

II. La naturaleza procesal del Hábeas Data.

Como bien refiere Castillo Córdova[1] , aludiendo a Sagüés, se puede afirmar que el hábeas data resulta siendo un amparo especializado, en la medida que estos derechos podrían haber sido protegidos por el amparo. Tan cierto es ello que desde que se dictó la hoy derogada Ley N° 26301[2], Ley de hábeas data y de acción de cumplimiento, hasta que se promulgó el actual Código Procesal Constitucional[3], ambos procesos constitucionales, hábeas data y amparo, se rigen por las mismas reglas de trámite. No obstante lo antes señalado, consideramos que a diferencia del proceso de amparo, que procede contra el hecho u omisión, por parte de cualquier autoridad, funcionario o persona, que vulnera o amenaza los demás derechos reconocidos por la Constitución (distintos a la libertad personal), el de hábeas data, en cambio, persigue otras finalidades, pues su objeto por una parte es acceder a la información pública y, por la otra, proteger la información personal que se encuentra en bases de datos informatizados o no, de tal modo que no sean objeto de tráfico sin la autorización del titular de dicha información. Asimismo, se puede recurrir a una demanda de hábeas data sin que ello se deba necesariamente a una acción u omisión. Este sería el caso, por ejemplo, de quien desea modificar o actualizar datos sobre su persona. Claramente allí no estamos ante la afectación de un derecho fundamental ya sea por el accionar o la omisión de algún funcionario, autoridad o persona,

[1] CASTILLO CÓRDOVA, Luis "Hábeas corpus, amparo y hábeas data". ARA editores, Lima, 2004, p, 368.

[2] LEY N° 26301, Ley de Hábeas Corpus y Acción de Cumplimiento. Artículo 3o.- Para la tramitación y conocimiento de la Garantía Constitucional de la Acción de Hábeas Data serán de aplicación, en forma supletoria, las disposiciones pertinentes de la Ley 23506, 25011, 25315, 25398 y el Decreto Ley 25433, en todo cuanto se refiera a la Acción de Amparo; con excepción de lo dispuesto en el artículo 11o. de la Ley 23506.

[3] CÓDIGO PROCESAL CONSTITUCIONAL. Artículo 65.- Normas aplicables

El procedimiento de hábeas data será el mismo que el previsto por el presente Código para el proceso de amparo, salvo la exigencia del patrocinio de abogado que será facultativa en este proceso. El Juez podrá adaptar dicho procedimiento a las circunstancias del caso.

a no ser que habiéndosele solicitado hacer la rectificación esta se haya negado a hacerlo. No obstante, para que proceda el hábeas data primero tiene que haberse pedido a quien posea la información que actúe conforme a lo solicitado, y solo ante la negativa o inacción se puede incoar la demanda, cosa que no es necesario en el proceso de amparo. Por lo tanto, la naturaleza procesal del hábeas data es distinta a la del amparo, aun cuando comparten similares enunciados lingüísticos al inicio de los incisos 2 y 3 del artículo 200 de la Constitución.

Desde luego, es menester mencionar que el legislador, a través de la norma de desarrollo constitucional, vale decir, el Código Procesal Constitucional, ha ido mucho más allá de lo que prescribe la Constitución como contenido esencial del derecho a la autodeterminación informativa y los alcances del hábeas data, ya que además habilita su uso para conocer, actualizar, incluir y suprimir o rectificar la información o datos referidos a su persona que se encuentren almacenados o registrados en forma manual, mecánica o informática, en archivos, bancos de datos o registros de entidades públicas o de instituciones privadas que brinden servicio o acceso a terceros. Asimismo, se puede recurrir a él para hacer suprimir o impedir que se suministren datos o informaciones de carácter sensible o privado que afecten derechos constitucionales.

Dicho lo anterior, podríamos afirmar que el Código Procesal Constitucional ha desarrollado sustancialmente lo establecido por la Constitución, ampliado el ámbito de protección que brinda el derecho a la autodeterminación informativa que se encuentra recogido en los incisos 5 y 6 del artículo segundo de la Constitución, estableciendo una variedad de medidas que el interesado puede adoptar a través de los órganos jurisdiccionales para decidir sobre el manejo de la información que le atañe y cuya utilización por terceros pudiese afectarlo.

En consecuencia, nos encontramos frente a uno de los denominados procesos constitucionales de la libertad, siendo un mecanismo procesal único y especial de carácter *plurifuncional*, toda vez que puede ser utilizado con distintos fines, ya sea que se trate de acceder a

la información pública que producen, generan, procesan o poseen las entidades del Estado, incluyendo aquella que se encuentre en manos de corporaciones privadas que brindan servicios públicos o de impedir que se suministre información privada que se encuentra en manos de bancos de datos informatizados o no.

Respecto a la parte procedimental, como ya lo habíamos adelantado, la norma exige que antes de presentarse la demanda, el accionante debe haber compelido al obligado mediante documento de fecha cierta el respeto de sus derechos, ya sea a la autodeterminación informativa o de acceso a la información pública, y que el demandado se haya ratificado en su incumplimiento o no haya contestado dentro de los diez días útiles siguientes a la presentación de la solicitud tratándose del derecho reconocido por el artículo 2 inciso 5) de la Constitución[4], o dentro de los dos días si se trata del derecho reconocido por el artículo 2 inciso 6) de la Constitución[5].

III. El derecho fundamental a la autodeterminación informativa a nivel constitucional y convencional.

Si bien es cierto los derechos que dan lugar a la interposición de una demanda de hábeas data se encuentran expresamente estipulados en la Constitución y el Código Procesal Constitucional, los alcances de esta figura y sobre los derechos fundamentales que el hábeas data protege, el Tribunal Constitucional ha sostenido que:

> (….) "*Queda claro, entonces, que la Constitución protege a través del proceso de hábeas data prima facie tanto el derecho de todo ciudadano al*

[4] Const. Art. 2° inciso 5) A solicitar sin expresión de causa la información que requiera y a recibirla de cualquier entidad pública, en el plazo legal, con el costo que suponga el pedido. Se exceptúan las informaciones que afectan la intimidad personal y las que expresamente se excluyan por ley o por razones de seguridad nacional…".

[5] Const. Art. 2° inciso 6) A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar.

> *acceso a la información pública, como el derecho a mantener en reserva la información que pueda afectar su intimidad personal y familiar (autodeterminación informativa)*[6].

De manera más específica, el Tribunal Constitucional se ha referido a la autodeterminación informativa en el caso Rodríguez Gutiérrez[7] señalando que esta:

> "(…) *tiene por objeto proteger la intimidad, personal o familiar, la imagen y la identidad frente al peligro que representa el uso y la eventual manipulación de los datos a través de los ordenadores electrónicos. Por otro lado, aunque su objeto sea la protección de la intimidad, el derecho a la autodeterminación informativa no puede identificarse con el derecho a la intimidad, personal o familiar, reconocido, a su vez, por el inciso 7) del mismo artículo 2° de la Constitución. Ello se debe a que mientras que este protege el derecho a la vida privada, esto es, el poder jurídico de rechazar intromisiones ilegítimas en la vida íntima o familiar de las personas, aquel garantiza la facultad de todo individuo de poder preservarla controlando el registro, uso y revelación de los datos que les conciernen".*

En esta sentencia el Tribunal también opta por diferenciar entre el derecho a la autodeterminación informativa con el derecho a la imagen, señalando que:

> (….) *"Tampoco el derecho a la autodeterminación informativa debe confundirse con el derecho a la imagen, reconocido en el inciso 7) del artículo 2° de la Constitución, que protege, básicamente la imagen del ser humano, derivada de la dignidad de la que se encuentra investido; mientras que el derecho a la autodeterminación informativa, en este extremo, garantiza que el individuo sea capaz de disponer y controlar el tipo de datos que sobre él se hayan registrado, a efectos de preservar su imagen derivada de su inserción en la vida en sociedad*".

Finalmente, el supremo intérprete de la Constitución acota que:

---

[6] STC Exp. N.º 05952-2006-HD/TC, fj, 3.

[7] STC Exp. N° 1797-2002-HD/TC, fj, 3.

(…) *"por su propia naturaleza, el derecho a la autodeterminación informativa, siendo un derecho subjetivo tiene la característica de ser, prima facie y de modo general, un derecho de naturaleza relacional, pues las exigencias que demandan su respeto, se encuentran muchas veces vinculadas a la protección de otros derechos constitucionales".*

En efecto, la posibilidad de que cada quien decida qué información respecto a sí mismo debe ser de conocimiento público, tiene una estrecha vinculación con el derecho a la intimidad personal, encontrándose esta última expresamente contenida en el artículo 2° inciso 7 de la Constitución política del Perú.

A nivel convencional, tenemos que el artículo 13 inciso 1 del Pacto de San José de Costa Rica señala que:

"*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".*

Respecto a este derecho, la Corte Interamericana de Derechos Humanos se ha pronunciado en el caso Claude Reyes y otros vs. Chile, del 19 de setiembre de 2006, al señalar que:

(…) *"En este sentido la Corte ha establecido que, de acuerdo a la protección que otorga la Convención Americana, el derecho a la libertad de pensamiento y de expresión comprende "no sólo el derecho y la libertad de expresar su propio pensamiento, sino también el derecho y la libertad de* ***buscar, recibir*** *y difundir informaciones e ideas de toda índole". Al igual que la Convención Americana, otros instrumentos internacionales de derechos humanos, tales como la Declaración Universal de Derechos Humanos y el Pacto Internacional de Derechos Civiles y Políticos, establecen un derecho positivo a buscar y a recibir información.."* [8]

[8] Caso Claude Reyes y otros vs. Chile. Fj. 76.

Pero el derecho a las libertades informativas no solo ha sido recogido en la Convención Americana sobre Derechos Humanos, sino también en el Pacto Internacional de Derechos Civiles y Políticos, cuyo artículo 19 inciso 2 señala que:

> (…) "*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".*

En tal sentido, el derecho a obtener o buscar información se encuentra garantizado por el derecho convencional al cual está vinculado el Perú y, por lo mismo, cualquier persona que se vea impedida de ejercerlo, podría no solo recurrir a la jurisdicción constitucional interna, sino también a los tribunales supranacionales una vez agotada la jurisdicción en sede nacional. De igual modo, tanto el Pacto Internacional de Derechos Civiles y Políticos[9] como la Convención Americana sobre Derechos Humanos protegen, prácticamente de manera idéntica, el derecho a la intimidad.[10]

Ahora bien, al igual que en el caso del amparo internacional, es un hecho indiscutible que, independientemente de los derechos reconocidos en las constituciones nacionales o en la legislación procesal constitucional de los países signatarios, cualquier individuo podría recurrir directamente a los jueces nacionales invocando los instrumentos internacionales antes mencionados, los mismos que deberán ser restituidos y debidamente protegidos en virtud al carácter vinculante que estos tienen. Si bien es cierto que el actual ámbito de

[9] PIDCP Art. 17 inciso 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.

[10] CADH Art. 11 inciso 2. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación.

protección del derecho a la autodeterminación informativa es mucho más amplio que el reconocido por las normas convencionales, sin embargo garantizan que el derecho de acceder a la información en ningún caso podrá ser menoscabado en la legislación nacional a través de limitaciones irrazonables o arbitrarias mediante reformas constitucionales o legales ordinarias, pues siempre habrá de prevalecer la norma supranacional conforme al principio del *pacta sunt servanda,* recogido en el artículo 27 de la Convención de Viena sobre el Derecho de los Tratados de 1969.

Por otra parte, debemos tener en cuenta que una vez aprobado y ratificado un tratado sobre derechos humanos, no es factible que la normativa interna de los Estados signatarios limiten en mayor medida los derechos y libertades que aquél reconoce o garantiza. Además, tanto en el Pacto Internacional de Derechos Civiles y Políticos como en la Convención Americana sobre Derechos Humanos, el ámbito de protección va más allá de lo estipulado en los mencionados Tratados, pues garantizan que tampoco se puedan desconocer, limitar o menoscabar derechos que se encuentran recogidos en otros instrumentos internacionales de los cuales el Estado sea parte, de tal modo que se extiende una suerte de manto protector muy amplio al comprometer a los Estados a respetar, no solo los derechos reconocidos en el Pacto Internacional o la Convención Americana, sino en cualquier otro instrumento convencional[11]. De allí que hoy en día ya no hablemos de un sistema de protección de los derechos humanos, sino de un auténtico derecho convencional, que

[11] Conforme al Art. 5 numeral 1 del Pacto Internacional de Derechos y Políticos "Ninguna disposición del presente Pacto podrá ser interpretada en el sentido de conceder derecho alguno a un Estado, grupo o individuo para emprender actividades o realizar actos encaminados a la destrucción de cualquiera de los derechos y libertades reconocidos en el Pacto o a su limitación en mayor medida que la prevista en él".

Según el artículo 29 literal a) de la Convención Americana sobre Derechos Humanos "Ninguna disposición de la presente Convención puede ser interpretada en el sentido de:

a) permitir a alguno de los Estados Partes, grupo o persona, suprimir el goce y ejercicio de los derechos y libertades reconocidos en la Convención o limitarlos en mayor medida que la prevista en ella;

ha alcanzado autonomía propia como tal, y desde luego va de la mano con el derecho internacional y específicamente con el derecho de los tratados.

IV. La protección de los datos personales y su desarrollo legislativo

En el ámbito administrativo, la legislación peruana ha desarrollado el derecho a la autodeterminación informativa al expedir la Ley N° 29733, Ley de Protección de Datos Personales, expedida en julio del 2011, cuyo artículo 1 establece que esta tiene el objeto de garantizar el derecho fundamental a la protección de los datos personales, previsto en el artículo 2 numeral 6 de la Constitución Política del Perú, a través de su adecuado tratamiento, en un marco de respeto de los demás derechos fundamentales que en ella se reconocen. Sin embargo, los mecanismos que dicha normativa prevé no impiden el ejercicio de los procesos constitucionales como el de hábeas data, conforme lo señala la sexta disposición complementaria final al prescribir que:

> (…) "*Las normas establecidas en el Código Procesal Constitucional sobre el proceso de hábeas data se aplican en el ámbito constitucional, independientemente del ámbito administrativo materia de la presente Ley. El procedimiento administrativo establecido en la presente Ley no constituye vía previa para el ejercicio del derecho vía proceso constitucional".*

Ahora bien, para efectos del tema que nos interesa en particular, como lo es el derecho al olvido, resulta siendo relevante lo previsto en el artículo 20 de la Ley N° 28733,cuyo primer párrafo establece que:

> *" El titular de datos personales tiene derecho a la actualización, inclusión, rectificación y* ***supresión*** *de sus datos personales materia de tratamiento, cuando estos sean parcial o totalmente inexactos, incompletos, cuando se hubiere advertido omisión, error o falsedad, cuando hayan dejado de ser necesarios o pertinentes a la finalidad para la cual hayan sido recopilados o cuando hubiera vencido el plazo establecido para su tratamiento*"(el resaltado es nuestro).

Sin embargo, esta regla sólo opera cuando se trata de bases de datos administradas por privados o entidades particulares, ya que la

supresión de datos personales contenidos en bancos de datos personales de administración pública se sujeta a lo dispuesto en el artículo 21 del Texto Único Ordenado de la Ley 27806, Ley de Transparencia y Acceso a la Información Pública, o la que haga sus veces. Así, el mencionado artículo 21 establece que:

> "*Es responsabilidad del Estado crear y mantener registros públicos de manera profesional para que el derecho a la información pueda ejercerse a plenitud. En ningún caso la entidad de la Administración Pública podrá destruir la información que posea.*
>
> *La entidad de la Administración Pública deberá remitir al Archivo Nacional la información que obre en su poder, en los plazos estipulados por la Ley de la materia. El Archivo Nacional podrá destruir la información que no tenga utilidad pública, cuando haya transcurrido un plazo razonable durante el cual no se haya requerido dicha información y de acuerdo a la normatividad por la que se rige el Archivo Nacional".*

Por lo que podemos advertir, existe la prohibición expresa de destruir la información que posean las entidades de la administración pública; no obstante, habría que analizar si dicha disposición implicaría tan solo el deber de conservar la información, más no necesariamente de hacerla pública de manera perenne, pues tratándose de condenas y antecedentes policiales, judiciales o sanciones administrativas, el acceso a ellas solo podría hacerse por autoridad competente y por razones plenamente justificadas, pero no podrían ser de acceso libre –por ejemplo– a través de portales web de la institución que posea dicha información. Tendría que determinarse también en qué casos el Archivo Nacional podría destruir información que no tenga utilidad pública y cuáles serían los criterios para establecer qué información la tiene y cual no.

Debemos, pues, distinguir entre la posesión del dato y su publicidad o difusión por cualquier medio que lo haga de acceso público. Vale decir, se puede conservar el dato pero no así hacerse público, cuando éste no sea de interés público o carezca de relevancia. En cuanto a la Ley de Transparencia y Acceso a la Información Pública, el artículo 5 de la misma establece taxativamente qué tipo de información debe

ser publicada y difundida a través de internet, la mayoría de la cual está relacionada a los ingresos de los funcionarios del Estado, gastos, ejecución presupuestal y contratación pública, de tal manera que en ninguno de los incisos del referido artículo se menciona información de carácter personal o privada. Sin embargo, el inciso 5° de la indicada norma contiene un *numerus apertus* cuando dice *"La información adicional que la entidad considere pertinente",* con lo cual queda abierta la posibilidad para que cada entidad del Estado incorpore cualquier otra información que estime conveniente y bajo el criterio evidentemente subjetivo de quién la dirija, lo cual consideramos peligroso en un país donde no existe una cultura de respeto a los derechos fundamentales y en el que algunas veces la información se suele utilizar para fines insospechados.

Por otra parte, Oscar Puccinelli[12] nos recuerda que (…)

"las normas destinadas a la protección de los datos personales contienen una serie de principios generales relativos al tratamiento de estos y también establecen algunos derechos concretos que le asisten a quienes esos datos se refieren, los cuales son conocidos vulgarmente como «derechos arco» (por acceso, rectificación, cancelación y oposición al tratamiento), aunque su elenco es bastante mayor a los enunciados en esta convencional denominación (por ejemplo, actualización, confidencialización, desindexación, adición, encriptación, etc.).

El destacado profesor argentino también afirma que (…)

Este «derecho a ser olvidado» arranca –como las leyes de protección de datos y la construcción del «derecho a la autodeterminación informativa»– en suelo alemán, en concreto en el caso «Lebach», resuelto por el Tribunal Constitucional alemán, y generado cuando en un canal de televisión se pretendió pasar el documental Der *Soldatenmord von Lebach, relativo a un hecho ocurrido en 1969 en la ciudad de Lebach, cuando cuatro soldados que custodiaban un depósito de municiones fueron asesinados mientras*

[12] PUCCINELLI, Oscar. "El «derecho al olvido» en el derecho a la protección de datos. Con especial referencia a su vigencia en Internet". Pensamiento Constitucional N° 21, 2016, p, 237.

> *dormían. El Tribunal hizo lugar a la pretensión de uno de los condenados por este crimen que estaba a punto de salir de la prisión que se oponía a la difusión televisiva de ese documental, entendiendo que tal reproducción lo estaría obligando a revivir tiempos pasados, y más específicamente hechos de su vida que eran un verdadero fastidio para él, y que ya resultaban irrelevantes para la sociedad. Consideró además especialmente que, en la tensión entre el derecho fundamental a la protección de la personalidad (más específicamente la privacidad y la intimidad) y el derecho fundamental a la libertad de información, debía prevalecer el primero, porque con la reproducción televisiva de información sin ningún tipo de relevancia actual se pondría en riesgo la posibilidad de la rehabilitación del convicto*[13].

En el caso mencionado por Puccinelli podemos advertir la existencia de una tendencia por privilegiar el derecho a la privacidad y la intimidad personal antes que el de la libertad de información, revelando que no en todos los países se ha venido resolviendo de la misma manera al momento de ponderar los derechos en juego, labor que por cierto consideramos particularmente compleja y delicada y sobre la cual trataremos en el acápite correspondiente.

V. El derecho al olvido en los portales web.

Debido al inmenso desarrollo de las redes digitales a través del internet, cuyo tráfico en un solo día puede superar varios miles de millones de búsquedas, la sociedad de la información se ha tornado sin duda en un recurso valiosísimo para millones de personas, pero también supone una amenaza para la intimidad personal, o incluso otros derechos fundamentales conexos como los de la imagen personal, la buena reputación y el honor. Por una parte, el acceso a la información constituye un derecho reconocido no solo por las Constituciones nacionales, sino también por varios de los tratados, pactos y convenios internacionales sobre derechos humanos; mientras que por otra, esas mismas normas e instrumentos convencionales garantizan el derecho a la intimidad, a

[13] Ob. Cit. p, 241, 242.

la imagen (frente a los demás) y al honor, lo cual muchas veces supone un enfrentamiento entre derechos y principios fundamentales que inevitablemente deben ponderarse en cada caso, determinándose cuál de ellos debiera prevalecer en función a lo que está en juego: ya sea el interés público, la libertad de prensa, o la vida privada de las personas afectadas a consecuencia de informaciones irrelevantes, inexactas, injuriosas, difamatorias o discriminatorias. Pero de dichas dilucidaciones nos habremos de ocupar más adelante.

Tal como lo sostiene Mesa Quesada[14]:

(….) "*Centrando más la definición del derecho al olvido, este consiste en limitar por parte del titular de los datos personales, la difusión descontrolada de datos de carácter personal, en diferentes servidores de la Red cuando la información ya esté obsoleta, o que ya no tenga ninguna relevancia ni ningún interés para la opinión pública, aunque la publicación original sea legítima".*

En cambio, Torres Manrique[15], aludiendo a Acha, refiere que:

"El derecho al olvido se define de tres formas: "i) un término ficticio cuyo núcleo es el derecho a acceder, rectificar y cancelar nuestros datos personales que estén en bases ajenas; ii) obligaciones especiales de eliminación de datos financieros y penales después de cierto tiempo; iii) la desindexación de información en buscadores, es decir, que no se elimine la información, sino que simplemente deje de aparecer en el buscador".

Carlos Cortés[16] nos dice que:

[14] MESA QUESADA, Francisco. "Dimensión constitucional del derecho al olvido". p, 9. https://www.derechoycambiosocial.com/revista049/DIMENSION_CONSTITUCIONAL_DEL_DERECHO_AL_OLVIDO.pdf

[15] TORRES MANRIQUE, Jorge. "Elucubraciones acerca del derecho fundamental al olvido en el Perú y en el derecho comparado, a propósito de su reconocimiento y evolución". INNOVARE. Ciencia y Tecnología, 2017, p, 38.

[16] CORTÉS, Carlos. "Derecho al olvido: entre la protección de datos, la memoria y la vida personal en la era digital". CELE. Universidad de Palermo, Facultad de Derecho, p,

(…) *"Siguiendo de alguna manera el enfoque de Mayer-Schönberger sobre la necesidad humana de olvidar, la Comisión Nacional de Informática y Libertades de Francia –el ente autónomo que protege el procesamiento de datos en ese país–, considera que el derecho al olvido (o a ser olvidado) es el derecho a cambiar, evolucionar y contradecirse. La Comisión lo concretiza en el "Principio de duración limitada de la retención de datos", según el cual la información no puede conservarse en ficheros digitales indefinidamente, sino únicamente por el tiempo necesario para cumplir con el propósito para el cual fue recogida".*

Leturia[17] define el derecho al olvido:

(…) "*como el fundamento jurídico que permite que ciertas informaciones del pasado no sean actualmente difundidas cuando son capaces de provocar más daños que beneficios. Ello es consecuencia de un juicio de valor que considera que, atendidas determinadas circunstancias, el beneficio del ejercicio de la libertad de expresión es inferior a los daños provocados en otros bienes jurídicos".*

El referido autor nos recuerda que el tratamiento jurisprudencial del derecho al olvido es sustancialmente distinto según el sistema jurídico en el que se aborde. Así, el mayor nivel de protección se ha alcanzado en Europa a través del Tribunal Europeo de Justicia y especialmente en Francia, ámbito del sistema romano germánico o del *civil law,* mientras que en los Estados Unidos, país donde impera la tradición jurídica del *common law,* los tribunales han sido especialmente reacios a amparar demandas destinadas a suprimir información que se encuentra en los motores de búsqueda de las grandes corporaciones que brindan el servicio de internet. Los americanos tradicionalmente han optado por proteger las libertades informativas por sobre el derecho a la intimidad. Al respecto señala que:

[17] LETURIA, Francisco. "Fundamentos jurídicos del derecho al olvido. ¿un nuevo derecho de origen europeo o una respuesta típica ante colisiones entre ciertos derechos fundamentales?". Revista Chilena de Derecho. Vol. 43 N° 1, 2016, p, 96.

(…) "*Producto de ello, el derecho al olvido presenta alcances y dinámicas muy diferentes según el país y la tradición jurídica que se observe. La comprensión de la libertad de expresión y del derecho a la privacidad en EE.UU. y en Europa, por ejemplo, difiere lo suficiente como para augurar un mayor desarrollo del derecho al olvido en los países del viejo continente, lo que dará espacio para tensiones y conflictos permanentes, como los ya observados en el caso Google*"[18].

Para Carlos Guerrero[19]:

(…) "*Posiblemente el caso más famoso es el de Mario Costeja contra Google, en el que el Tribunal de Justicia de la Unión Europea determinó que los ciudadanos europeos tienen derecho a solicitar la desindexación de contenidos que no sean actuales, sean inexactos o no revistan interés público por aplicación directa de la legislación sobre protección de datos personales. A partir de allí, este derecho está reconocida en la Unión Europea y diferentes países de todo el mundo lo han reconocido como parte de su normativa de protección de datos personales a través de modificaciones legislativas o sentencias".*

Conforme ya lo hemos visto en el capítulo anterior, nuestra reciente legislación nacional no ha regulado de manera expresa el denominado "derecho al olvido", aun cuando sí permite solicitar la supresión de los datos personales cuando estos hayan dejado de ser necesarios o pertinentes a la finalidad para la cual hayan sido recopilados. Desde luego no hay una mención especial a aquellos datos que están en la red del internet y que pueden emerger a través de los motores de búsqueda más importantes (Google, Yahoo, Bing, Altavista, entre otros más), con tan solo digitar el nombre y apellido de una persona.

Lamentablemente nuestro Tribunal Constitucional no se ha ocupado del tema en ninguna de sus sentencias relativas al proceso de hábeas data y como quiera que este derecho no se encuentra explícitamente

[18] LETURIA. Ob. Cit. p, 93.

[19] GUERRERO, CARLOS. HIPERDECHO. Recuperado de: https://hiperderecho.org/2020/03/derecho-al-olvido/.

recogido en nuestra Norma Fundamental, creemos que ello no es óbice para en algún momento pueda tener reconocimiento a través de la jurisprudencia constitucional. Particularmente creemos que podría ser considerado como parte del derecho a la autodeterminación informativa en su fase o dimensión supresiva, de tal modo que sin tener que recurrir a la cláusula abierta del artículo 3 de la Constitución, bastaría con reconocer que el derecho al olvido se encuentra comprendido dentro de la capacidad que tiene el individuo para decidir qué información respecto a él debe ser olvidada, o mejor dicho, suprimida de la internet y medios digitales en general.

En relación a nuestro país, Murrugarra[20] señala que:

> (…) *"Por su parte, el Perú no ha sido ajeno a la llegada del derecho al olvido en internet, debido a que la Dirección General de Protección de Datos Personales (vía administrativa), por primera vez, emitió un fallo en el que amparaba este derecho (Resolución Directoral Nº 045-2015-JUS-DGPDP). El caso era referido a un ciudadano peruano quien solicitó a Google Perú S.R.L. y a Google Inc. que eliminen de los resultados de búsqueda de su nombre información respecto a la supuesta comisión de un delito, debido a que se trataba de una denuncia falsa de la cual fue absuelto en el respectivo proceso".*

Aun cuando en la referida resolución no se desarrolla el denominado "derecho al olvido", limitándose tan solo a exponer los hechos por los cuales el reclamante exigía que Google Inc. y Google Perú S.R.L cancelaran de sus motores de búsqueda toda mención a su persona, lo cierto es que ha sido hasta ahora el único caso que se ha dado en nuestro país. Por todo ello, hay todavía mucho por desarrollar en cuanto a esta figura jurídica, tanto a nivel normativo como jurisprudencial, e incluso doctrinario. No obstante, consideramos que en casos como el expuesto

[20] MURRUGARRA, Brenda. "El Derecho al Olvido en Internet: Perspectivas a partir de la Ley de Protección de Datos Personales y los casos de Google. IUS360. Recuperado de: https://ius360.com/articulos-de-estudiantes/el-derecho-al-olvido-en-internet-perspectivas-partir-de-la-de-proteccion-de-datos-personales-y-los-casos-de-google/

en el párrafo anterior, el pedido está plenamente justificado, ya que no se puede condenar ni exponer a una persona inocente a un permanente reproche social, además de la afectación de otros derechos fundamentales como al honor, al buen nombre y reputación, y otros más que indirectamente también podrían verse afectados, como el derecho al trabajo, por solo citar un ejemplo.

Conforme lo refiere Moreno Bobadilla[21]

> (...) *"En Francia, la Commission Nationale de l'Informatique et les Libertés también reconoció de forma expresa la existencia del derecho al olvido, con una amplia interpretación de lo que comprende el poder solicitar una segunda oportunidad. Fue precisamente en este país, donde ya en el año 1965 se dicta una pionera sentencia que comienza a reconocer el derecho de los ciudadanos a tener una segunda oportunidad. El Tribunal de Gran Instancia de Sena, en sentencia dictada el 4 octubre del mencionado año, resolvió una demanda de una de las amantes del famoso asesino en serie Henri Landru, por haber sido representada en una película después de haber transcurrido muchos años desde la relación sentimental que mantuvo con el homicida. A pesar de que finalmente el órgano jurisdiccional francés rechaza la demanda, ya que la actora había publicitado su relación con el señor Landru, se comienza a hablar del "droit a l'oublie", sembrándose los orígenes europeos del derecho al olvido previo a la era digital".*

Consideramos que los motivos para que se solicite eliminar cierta información tendrían que estar justificados en que la data pudiese perjudicar al interesado, afectando su reputación y trayectoria personal, su imagen pública o incluso privada, o que podría estigmatizarlo para siempre, impidiéndole rehacer su vida sin que haya tenido mayor culpa en la generación de la información que pide sea olvidada. Estas situaciones podrían darse, por ejemplo, con una persona que fue víctima de violación y los medios de comunicación divulgaron su identidad, o

[21] MORENO BOBADILLA, Angela. "El derecho al olvido digital: una brecha entre Europa y Estados Unidos". Revista de Comunicación. vol.18 no.1 Piura ene./jun. 2019. http://dx.doi.org/10.26441/RC18.1-2019-A1

de alguien que en razón a su cargo fue imputado falsamente de algún delito o conducta que sea socialmente reprochable y que, pese a habérsele exonerado judicialmente de los cargos, no obstante la información sigue apareciendo en la red. Lo mismo sucedería en el caso de aquella información referida a un personaje público, pero que sin embargo forma parte de su vida íntima y estrictamente personal que revele ciertas preferencias sexuales, manías o costumbres, vale decir, aquello que se considera "información sensible". Encontrándonos en una sociedad que suele juzgar ligeramente y que es bastante prejuiciosa, el derecho al olvido se erige como una herramienta eficaz para evitar afectar derechos fundamentales reconocidos por la Constitución. Después de todo, el honor y el buen nombre son valores esenciales para todo ser humano dentro del medio social en el cual se desempeña. La era digital y el acceso a internet en forma masiva y estando al alcance de millones de personas, torna mucho más vulnerable el derecho a la intimidad personal, pues las redes sociales son una vía que se entrecruza de manera masiva y sin mayor control, puesto que algunos aplicativos multiplican el acceso a la información, ya que basta que uno de los usuarios expanda su red de contactos para que los datos de un individuo termine en manos de centenares o miles de personas más, sin que aquél lo sepa o esté consciente de ello.

V. Ponderación entre el derecho al olvido frente a la libertad de información

No cabe duda que la protección al derecho a la autodeterminación informativa mediante el derecho al olvido, podría a su vez colisionar con otros derechos igualmente iusfundamentales, esencialmente con aquellos relacionados a la libertad de acceso a la información y a difundirla a través de los medios de prensa. Determinar cuándo el derecho a la intimidad debe prevalecer frente al derecho a las libertades informativas, es algo que definitivamente no se puede regular ni preestablecer normativamente, pues se trata de valores y principios constitucionales, respecto a los cuales sólo en cada caso concreto podría optarse

por preferir uno a costa del sacrificio del otro. Como siempre lo hemos sostenido, creemos que todo dependerá de las circunstancias especiales que se presenten en cada caso en particular, debiendo ser el operador jurídico quien deba ponderar los derechos en juego; analizando una serie de factores determinantes, tales como: a) la naturaleza de la información; b) la trascendencia social que la información haya tenido y que actualmente tenga, c) la posición social del afectado con la difusión de la información; d) los hechos y circunstancias que dieron lugar a la generación de la información; e) la necesidad de preferir el interés público por encima del interés particular, entre otros elementos de juicio.

Sin lugar a dudas, uno de los mayores inconvenientes que en el caso del Perú podría encontrar el derecho al olvido es la reciente legislación dictada por el Congreso de la República, como ocurre con la Ley Nº 29988, norma que establece medidas extraordinarias para el personal docente y administrativo de instituciones educativas públicas y privadas, implicados en delitos de terrorismo, apología del terrorismo, delitos de violación de la libertad sexual y delitos de tráfico ilícito de drogas, a raíz de lo cual se ha creado el registro de personas condenadas o procesadas por delito de terrorismo, apología del terrorismo, delitos de violación de la libertad sexual y tráfico ilícito de drogas, y se modifican los artículos 36 y 38 del Código Penal. Posteriormente, por Decreto de Urgencia N° 019-2019 se modificó la Ley 29988 y se agregaron otros delitos, como los de proxenetismo, pornografía infantil, trata de personas, explotación sexual, esclavitud, homicidio doloso, parricidio, sicariato, secuestro, genocidio, desaparición forzada, tortura, violación de la intimidad mediante la difusión de material con contenido sexual, entre otros. Así, las personas condenadas por tales delitos están perpetuamente impedidas de ejercer funciones docentes o administrativas en los centros educativos públicos y privados de todo nivel, independientemente de que hayan sido rehabilitadas. Esta norma incluso ha sido convalidada por el Tribunal Constitucional cuando fue cuestionada en cuanto a su constitucionalidad, de tal forma que en dichos casos los antecedentes penales de quienes incurrieron en tan graves

delitos jamás podrán ser retirados del registro creado por el Decreto Supremo 004-2017-MINEDU, aun cuando ello pudiese significarles un serio problema para acceder a puestos de trabajo o los estigmatice socialmente. Queda claro que aquí se privilegia el interés público y la seguridad de la población por encima de la vida íntima y el derecho a la resocialización del condenado, algo que consideramos plenamente justificado por la gravedad de los delitos incurridos y sobre todo por la labor que tendrían los condenados al ejercer labores docentes.

Es posible que en algún momento se presenten demandas constitucionales de amparo o de hábeas data contra los efectos de la Ley 29988 y su Reglamento, sustentadas en supuestas vulneraciones al derecho del condenado a ser rehabilitado y reinsertado a la sociedad, consagrado en el artículo 139 inciso 22 de la Constitución, o la afectación al derecho al trabajo recogido en el artículo 22 de la misma; sin embargo, creemos que en todos los casos dichas pretensiones tendrían que ser desestimadas, no solo porque los derechos no son absolutos y admiten excepciones, sino además porque el juez debe ponderar el interés superior de los estudiantes, que es de carácter general, por encima de cualquier otro que sea de carácter individual, con el agregado que, en estricto, no hay una vulneración al contenido esencial o núcleo duro de tales derechos fundamentales, en la medida que si bien la referida ley 29988 restringe el acceso a la función docente en los centros educativos de todos los niveles, ello no impide que el afectado pueda trabajar en cualquier otro campo o actividad que no sea la educativa, aun cuando se hubiese preparado profesionalmente para ello.

No está de más decir que para quienes consideran que tales medidas restrictivas son excesivas y demasiado severas y podrían vulnerar derechos fundamentales, deberían saber que los alemanes, que ostentan unos de los niveles más elevados de desarrollo en el ámbito del derecho constitucional a nivel mundial, han establecido que una persona puede perder ciertos derechos y libertades constitucionales consagrados expresamente en la Ley Fundamental de Bonn, cuando a través de sus

actos ésta hace un uso abusivo de ellos. En efecto, el artículo 18 de la Constitución alemana estipula lo siguiente:

> "Quien, para combatir el régimen fundamental de libertad y democracia, abuse de la libertad de expresión de opinión, particularmente de la libertad de prensa (artículo 5, apartado 1), de la libertad de enseñanza (artículo 5, apartado 3), de reunión (artículo 8), de asociación (artículo 9), del secreto de las comunicaciones postales y de las telecomunicaciones (artículo 10), así como del derecho de propiedad (artículo 14) y del de asilo (artículo 16a) pierde estos derechos fundamentales. La privación y su alcance serán declarados por la Corte Constitucional Federal".

Ahora bien, el Decreto Legislativo 1295, que introduce modificaciones a la Ley del Procedimiento Administrativo General N° 27444, también establece la prohibición para que los condenados con sentencia condenatoria consentida y/o ejecutoriada por delitos de concusión, cobro indebido, colusión, peculado, malversación, cohecho, negociación incompatible, tráfico de influencias y enriquecimiento ilícito laboren en la administración pública. Para tal efecto se crea un Registro Nacional de Sanciones contra Servidores Civiles, que además es de acceso público. De esta manera, será imposible que en temas penales, salvo que se trate de información referida a procesados que fueron absueltos o cuyas investigaciones fueron sobreseídas, se puedan dictar mandatos, ya sean administrativos o jurisdiccionales, que ordenen suprimir información referida a las personas condenadas por alguno de los antes mencionados delitos. No sobra decir que todos los registros que hemos mencionado son accesibles mediante la web a través de los portales de las instituciones públicas responsables de administrarlos.

VI. Reflexiones finales

Como hemos podido observar, el derecho al olvido es solo una manifestación o dimensión del derecho a la autodeterminación informativa, la cual se enmarca esencialmente en el ámbito de aquella información que se encuentra recogida en la internet a través de los principales motores de búsqueda. Es cierto que estos motores de búsqueda sólo

replican lo que se encuentra contenido en las páginas web de las cuales se nutren, pero también lo es que sí están en la posibilidad de bloquear cualquier referencia, ya sea a un tema en particular o a una persona cuando dicha información vulnera algunas políticas de los grandes buscadores como Google, Yahoo, Altavista, etc. La mayor demostración de ello es que no es factible difundir a través de los buscadores de aquella información que haga apología del racismo, terrorismo y políticas extremistas que induzcan a crímenes de odio. Existe por lo tanto una política de censura que cada uno de estos grandes buscadores administra según sus propias políticas de uso.

Por otra parte, hay que tener en consideración hasta qué punto debe admitirse un pedido de supresión de la información que aparezca en base de datos mediante las páginas web, cuando ello podría terminar por afectar otros derechos y valores superiores, o incluso el derecho a la información y a su difusión a través de los medios de prensa. En tal sentido, creemos que en todos los casos deberá ponderarse adecuadamente los derechos en juego, siempre teniendo en cuenta determinados parámetros básicos, como la trascendencia e importancia vital de la información, si ésta concierne o no a los demás, su grado de utilidad actual, si hay derechos colectivos en juego, el aporte que dicha información podría brindar a la historia, la ciencia, la cultura o la investigación, así como la condición personal y social del afectado.

Lo cierto es que queda mucho por investigar desde el derecho comparado, puesto que en el Perú, salvo un caso que solo se vio en sede administrativa, no se ha ventilado el derecho al olvido en sede jurisdiccional y por lo tanto no tenemos mayor desarrollo jurisprudencial respecto a este importante tema. Por otra parte, la doctrina es aún muy limitada e incipiente, y lamentablemente la mayoría de los artículos publicados convergen en los mismos hechos y datos, sin ahondar más en el núcleo mismo de este derecho al olvido, dando la impresión, paradójicamente, que éste ha sido víctima de su propia denominación. Esperemos pues, que desde la academia y los tribunales de justicia pronto tengamos un mayor desarrollo de esta figura.

LA INFORMACIÓN COMO PROBLEMA.

El derecho al olvido y su protección por el *Hábeas Data*.

✍ Alfredo Orlando Curaca Kong*

"*No quiero vivir en un mundo*
donde se registra todo lo que hago y digo"

Edward Snowden

1. Presentación

Internet, "*…el gran foro público a través del cual millones de personas se expresan y se informan*"[1], se ha convertido en el abanderado del progreso tecnológico. En gran parte gracias a esta herramienta vivimos hoy en día en la denominada sociedad de la información, caracterizada por el rol preponderante que tiene el uso de la información en las diversas actividades del ser humano, tanto sociales, culturales, económicas, recreativas, como de otra índole.

Sin embargo, el tránsito a esta era no ha estado exento de problemas. La vorágine desplegada por el deseo de información, a la par

* Abogado por la Universidad de Lima, con estudios de Maestría en Derecho Procesal Constitucional por la Universidad Nacional de Lomas de Zamora de Argentina y discente de Maestría en Derechos Humanos por la Pontificia Universidad Católica del Perú. Asesor Jurisdiccional del Tribunal Constitucional. Director de Estudios e Investigación del Centro de Estudios Constitucionales. Miembro de la Asociación Peruana de Derecho Constitucional.

[1] MIERES MIERES, Luis Javier. "El derecho al olvido digital". Fundación alternativas. Documento de trabajo186/2014. p. 6.

que satisfacer el apetito de consumo, ha conllevado a una problemática que afecta la esfera misma del individuo, especialmente la relacionada con su dignidad, su honor, su imagen, su buena reputación y sus datos personales.

Los problemas generados por el avance de la tecnología no son nuevos. Como recuerda Luis Mieres ya en el siglo XIX Warren y Brandeis advertían la afectación del derecho a la privacidad a causa del progreso tecnológico: "*Las instantáneas fotográficas y las empresas periodísticas han invadido los sagrados recintos de la vida privada y hogareña; y los numerosos ingenios mecánicos amenazan con hacer realidad la profecía que reza: lo que susurre en la intimidad, será proclamado a los cuatro vientos*".[2] En su conocidísimo trabajo "*The right of privacy*", aparece así la privacidad como nuevo derecho protegido por el "*Common law*".

En tiempos actuales, el internet, aunque herramienta útil en muchos sentidos, es el que trae complicaciones debido a la cantidad de datos que se acumulan a un ritmo vertiginoso. Estos, como bien mencionan Mayer-Schönberger y Cukier, crecen tan deprisa que desbordan, "*…no solo nuestras máquinas, sino también nuestra propia imaginación*".[3]

Y es que no es fácil imaginar, por ejemplo, que Google recibe más de 3,000 millones de visitas diarias[4] y procesa más de 24 "petabytes"[5] de datos al día; que Facebook almacena diariamente más de 100,000 Gb, sus usuarios, apuntan los autores recientemente citados, hacen *click* en el botón de "me gusta" o insertan un comentario casi tres mil millones de veces diarias, dejando un rastro digital que la compañía explota para

---

[2] WARREN, S. y BRANDEIS, L. "El derecho a la intimidad". Citado por MIERES MIERES, Luis Javier. Op. Cit., p. 7.

[3] MAYER SCHONBERGER, Víctor y KENNETH, Cukier. "Big data. La revolución de los datos masivos". Turner. Madrid. 2017, p. 19.

[4] ÁLVAREZ CARO, María. "Derecho al olvido en internet: el nuevo paradigma de la privacidad en la era digital". Editorial Reus. Madrid. 2015, p. 15.

[5] Según lo averiguado, un "petabyte" es una unidad de almacenamiento de información que equivale a 1 000 000 000 000 000 de bytes.

descubrir sus preferencias.;[6] [7] que en un día se realizan 72 millones de descargas en la tienda online Appstore;[8] que los ochocientos millones de usuarios mensuales del servicio YouTube suben más de una hora de vídeo cada segundo;[9] que *Twitter* aumenta alrededor de un 200% al año y en 2012 se superaron los cuatrocientos millones de *tuits* diarios.[10]; que *Wallmart*, nos dice Puyol, almacena más de un millón de transacciones comerciales cada hora, identificando los productos que compran sus clientes;[11] y así, rápidamente, cada fracción de segundo seguimos y seguimos subiendo información alimentando a este insaciable monstruo llamado internet, que no tiene reparos en devorar todo lo que se le ofrece.

Esa apabullante y desordenada ingesta de datos, que se relaciona con el *big data*[12], ha traído consigo no pocos problemas para el ser humano que el Derecho ha resuelto en parte. Y es que si bien los beneficios que te ofrece internet pueden ser muchos y muy variados también hay aspectos perjudiciales y no son pocos. Ejemplo de esto es la aparición

[6] PUYOL MONTERO, Javier. "Big Data". En: PÉREZ BES, Francisco (coord.). "El derecho de internet". Atelie libros jurídicos. Barcelona. 2016, p. 73.

[7] MAYER-SCHÖNBERGER, Viktor y CUKIER, Kenneth. "Big data. La revolución de los datos masivos". Turner publicaciones. Madrid. 2017, p. 19.

[8] PUYOL MONTERO, Javier. Op. Cit., p. 73.

[9] MAYER-SCHÖNBERGER, Viktor y CUKIER, Kenneth. "Big data. La revolución de los datos masivos". Turner publicaciones. Madrid. 2017, p. 19.

[10] MAYER-SCHÖNBERGER, Viktor y CUKIER, Kenneth. "Big data. La revolución de los datos masivos". Turner publicaciones. Madrid. 2017, p. 19.

[11] PUYOL MONTERO, Javier. "Big Data". En: PÉREZ BES, Francisco (coord.). "El derecho de internet". Atelie libros jurídicos. Barcelona. 2016, p. 73.

[12] "Denominaremos Big Data a la gestión y análisis de enormes volúmenes de datos que no pueden ser tratados de manera convencional, ya que superan los límites y capacidad de las herramientas de software habitualmente utilizadas para la captura, gestión y procesamiento de datos. Dicho concepto engloba infraestructuras, tecnologías y servicios que han sido creados para dar solución al procesamiento de enormes conjuntos de datos estructurados, no estructurados o semi-estructurados (…) que pueden provenir de sensores, micrófonos, cámaras, escáneres médicos, imágenes." PUYOL MONTERO, Javier. "Big data". Op. Cit., p. 70.

de nuevas figuras relacionadas de algún modo con la manipulación de la información, como *phishing*[13], *pharming*[14], *ciberbullying*[15], *deep web*[16],

[13] El "phishing" es una técnica utilizada en internet, usualmente tipificada como delito informático, mediante la cual, a través del engaño, se pretende obtener información que es confidencial como claves, contraseñas o números de tarjetas de crédito. Es frecuente que se remitan a la víctima mensajes de fuentes que parecen de confianza, como bancos o empresas de servicios, diciéndoles que hay determinado problema, que hay una promoción u otro, para finalmente obtener información que después será utilizada en su contra. Según Adam Kujawa Director de Malwarebytes Labs, "el *phishing* es la forma más sencilla de ciberataque y, al mismo tiempo, la más peligrosa y efectiva. Eso se debe a que ataca el ordenador más vulnerable y potente del planeta: la mente humana". Fuente: https://es.malwarebytes.com/phishing/ Consulta: 19/09/2020.

[14] El conocido sitio web Kaspersky define el *pharming* de la siguiente manera: "El *pharming*, una combinación de los términos '*phishing*' y '*farming*', es un tipo de cibercrimen muy semejante al *phishing*, en el que el tráfico de un sitio web es manipulado para permitir el robo de información confidencial. El *pharming* aprovecha los principios con los que funciona la navegación por Internet, es decir, la necesidad de convertir una secuencia de letras para formar una dirección de Internet, como www.google.com, en una dirección IP por parte de un servidor DNS para establecer la conexión. El *exploit* ataca este proceso de dos maneras. En primer lugar, un hacker puede instalar un virus o un troyano en la computadora de un usuario que cambia el archivo de hosts de la computadora para dirigir el tráfico fuera de su objetivo previsto, hacia un sitio web falso. En segundo lugar, el hacker puede envenenar un servidor DNS para que los usuarios visiten el sitio falso sin darse cuenta. Los sitios web falsos se pueden utilizar para instalar virus o troyanos en la computadora del usuario, o pueden ser un intento de recopilar información personal y financiera para usarla en el robo de identidad." Fuente: https://latam.kaspersky.com/resource-center/definitions/pharming Consulta: 19/09/2020.

[15] Pablo Corona de la asociación de internet MX nos dice que el "*Ciberbullying* es un término que se utiliza para describir cuando un niño o adolescente es molestado, amenazado, acosado, humillado, avergonzado o abusado por otro niño o adolescente, a través de Internet o cualquier medio de comunicación como teléfonos móviles o *tablets*." Fuente: https://www.gob.mx/ciberbullying/articulos/que-es-el-ciberbullying Consulta: 19/09/2020.

[16] La "*deep web"* o internet profunda hace alusión a todo lo que está en internet pero no está indexado. Vale decir, que los motores de búsqueda comunes o convencionales no pueden encontrar estos sitios por distintas razones que no necesariamente tienen que ser ilegales. Los entendidos señalan que dentro de la Deep Web hay una "Dark Web" que si tiene contenidos que usualmente son ilícitos. Se calcula que en la Deep Web está el 96% del contenido de internet. Es decir, que en el internet superficial o surface web, que es el que todos conocemos, solo está el 4% de la información. Por eso, algunos autores mencionan "Si Internet fuera un iceberg, solo la parte visible que emerge por encima de la superficie del mar sería 'lo que Google ve'". CERVANTES, Pere y TAUSTE, Oliver. "Internet negro.

ataques *insiders*[17] y un cúmulo de nuevos términos informáticos a los que ahora tenemos que acostumbrarnos, muchos de los cuales se condicen con supuestos que han sido tipificados como delitos, encargándose de ellos por tanto el Derecho Penal, aunque no siempre son regulados al mismo ritmo en que aparecen, ya que, como afirma Lawrence Lessig, "… primero viene la tecnología y luego el Derecho intenta adaptarse a ella"[18].

Pero no todo queda o debe quedar en el ámbito del Derecho Penal ante esta creciente ola de nuevos retos informáticos, pues frente a este embate de información hay problemas que a otras ramas del Derecho les corresponde resolver, como la referida a la aparición del denominado "derecho al olvido", tema emergente en el Derecho Constitucional desde algunos años ya, como afirma Artemi Rallo, y que se refiere a la posibilidad de eliminar los datos que nos afectan, no solo del internet pero si en gran medida de este.

Si bien en el mundo real olvidar o enterrar aquello que nos hace daño es frecuente y es parte de nuestra naturaleza humana, en el mundo cibernético ocurre todo lo contrario: la información tiene vocación de permanencia, aunque muchas veces tal información sea atemporal, denigrante, falsa u obsoleta. En el mundo informático, lo que quedó en el pasado sigue estando en el presente a solo un *click* de distancia, por cuanto los datos quedan accesibles indefinidamente. Por ello es que se

El lado oscuro de la red". Ediciones temas de hoy. Barcelona. 2015, p. 23. Fuente: https://www.bbva.com/es/deep-web-cinco-datos-curiosos-que-no-conocias/ Consulta: 19/09/2020.

[17] La página randed.com nos da una definición muy apropiada de los ataques insiders: "Los ataques insiders son aquellos lanzados contra una empresa y organización desde el interior de la misma. El perfil del responsable es muy variado, un espía infiltrado por la competencia o por un gobierno, un empleado descontento, un antiguo trabajador con ansias de venganza o un terrorista que busque colapsar una infraestructura crítica. En general, el autor de estos ataques es un trabajador o extrabajador de la empresa con acceso privilegiado y gran conocimiento de la misma." Fuente: https://randed.com/ataques-insider/ Consulta 25/09/2020.

[18] ÁLVAREZ CANO, María. "El derecho al olvido en internet: el nuevo paradigma de la privacidad en la era digital". Editorial Reus. Madrid. 2015, p. 17.

ha dicho que "La tecnología lleva a la humanidad a la memoria como principio general y al olvido solo por defecto".[19]

Partiendo de esta premisa, se hace necesaria una protección frente a los datos que nos afligen, para que así caigan en el llamado olvido digital. Este es, pues, un creciente problema que tenemos que afrontar.

Sean los siguientes párrafos, entonces, para referirnos a este tema que es muy interesante pero además complejo y multidisciplinario. Dada esa complejidad, desde ya decimos que en las breves líneas de las que disponemos no le hacemos justicia en su abordaje, circunscribiéndonos en el presente trabajo a colocar algunas reflexiones y conclusiones iniciales que dejamos para el debate académico, siempre necesario y constructivo.

Sentado esto, precisamos que luego de tocar algunos antecedentes del derecho al olvido y esbozar una definición, nos centramos finalmente en ventilar si el mismo ha merecido o puede merecer una protección en el ordenamiento jurídico nacional. Se trata entonces de determinar si nuestra regulación es o no deficitaria.

Hechas estas precisiones, proseguimos.

2. Antecedentes del derecho al olvido:

Para tratar sobre el derecho al olvido hay que tratar sobre el derecho a la protección de datos y para tratar el derecho a la protección de datos hay que tratar previamente el derecho a la privacidad[20], que es de donde deriva. Esto nos permitirá entender cómo ha ido desarrollándose la protección de la persona en esta materia, pues pasó de ser una defensa cerrada de la intimidad como derecho autónomo a una defensa de los derechos que podrían verse afectados por la manipulación de

[19] RALLO, Artemi. "El derecho al olvido en internet. Google versus España". Centro de Estudios Políticos Constitucionales. Madrid. 2014, p. 17.

[20] A partir de acá, al margen de diferencias doctrinarias existentes, se utilizarán los términos privacidad e intimidad como sinónimos.

la información relativa a las personas, con un sustento constitucional. Un derecho se desprendió de otro y ahora el olvido parece desprenderse del derecho desprendido para alcanzar una autonomía y un contenido propios.

A continuación veremos cómo fue evolucionando todo esto.

2.1. Orígenes de la *privacy* y la protección de datos en el *Common Law*:

El derecho a la privacidad se fue gestando en el siglo XIX a raíz de los aportes de la doctrina y la jurisprudencia. El caso del príncipe Albert (*Prince Albert v. Stranger*), resuelto 1849 en Inglaterra, fue uno de los primeros en que se protege de alguna manera este derecho[21]. El príncipe, al igual que la reina Victoria, realizaban grabados mediante la técnica del aguafuerte como un pasatiempo y los compartían privadamente. Vale decir, no tenían intención de publicarlos ni lucrar con ellos, sin embargo algunos de estos grabados fueron sustraídos indebidamente e iban a ser mostrados en una exhibición pública. Entre los grabados habían retratos de la Reina, el Príncipe de Gales, la Princesa Real y otros miembros de la familia real británica, por lo que frente a la inminente exhibición de imágenes personales, el príncipe presentó una demanda para impedir la muestra, la que fue resuelta por la *High Court of Chancery*, que le dio la razón. La particularidad de este caso es que por primera vez se determinó expresamente que la privacidad "era el derecho invadido".

En 1879, el juez norteamericano Thomas M. Cooley publicó su obra denominada "*A Treatise on the Law of Torts or the Wrongs Which*

[21] La misma sentencia señala otros antecedentes*: Gee v. Pritchard, Abernethy v. Hutchinson, Spottiswoode v. Clarke, Rigby v. The Great Western Railway Company; Wilkin v. Aikin, Saunders v. Smith, Gyles v. Wilcott, Carr v. Hood, Youatt v. Winyar, Green v. Folgham, Macklin v. Richardson, Murray v. Elliston, Tipping v. Clarke, Chandler v. Thompson, Southey v. Sherwood*, entre otros. Fuente: https://www.casemine.com/judgement/uk/5a8ff8d260d03e7f57ecdced Consulta 31/10/2020

Arise Independently of Contract"[22], un tratado de los contratos de más de 850 páginas. En el capítulo II de este libro, que lleva por título "*General Classification of Legal Rights*" (clasificación general de los derechos legales), describió el derecho denominado "*personal immunity*" (inmunidad personal) y señaló que "*The right to one's person may be said to be a right of complete immunity: to be let alone.*"[23] (Se puede decir que el derecho de una persona es el derecho a una completa inmunidad: el ser dejado solo), del que desprende un deber general de no infligir daño y mantenerse alejado si esa es la intención. De no ocurrir, agregaba este autor, "Es muy probable que haya un shock en los nervios y la paz y la tranquilidad del individuo sea perturbada".[24]

En el "derecho a ser dejado solo" se aprecia así una incipiente necesidad de no perturbar la paz ni la tranquilidad de las personas, que fue desarrollada años después por los citados Warren y Brandeis, como veremos más adelante. La profesora María Nieves Saldaña, autora que ha estudiado con prolijidad la evolución del derecho a la privacidad en los Estados Unidos, expresa sobre las ideas de Cooley lo siguiente: "Sin duda, en la concepción de Cooley está presente el principio básico heredado del Derecho inglés «*a man's house as his castle*» (la casa de cada uno es su castillo), que confiere al hogar del individuo la máxima protección personal."[25]

En el caso *Marion Manola v. Stevens and Mayers*, ya resuelto en los Estados Unidos de Norteamérica en 1890, se protegió la intimidad

[22] COOLEY, Thomas. *A Treatise on the Law of Torts or the Wrongs Which Arise Independently of Contract*. Callagahn and Company. Chicago, 1879. Fuente: https://repository.law.umich.edu/cgi/viewcontent.cgi?article=1010&context=books Consulta: 31/10/2020

[23] Op. Cit., p. 29.

[24] Loc. Cit. (traducción libre).

[25] SALDAÑA, María Nieves. "El derecho a la privacidad en los Estados Unidos: aproximación diacrónica a los intereses constitucionales en juego". UNED. Teoría y Realidad Constitucional, núm. 28, 2011, p. 282. Fuente: file:///C:/Users/Usuario/Downloads/Dialnet-ElDerechoALaPrivacidadEnLosEstadosUnidos-3883001%20(2).pdf Consulta: 31/10/2020.

de una actriz y cantante de ópera de *Broadway* que había sido fotografiada en mallas sin su consentimiento durante una presentación en el teatro llamado también *Broadway*,[26] por el señor Benjamin Stevens, gerente de la empresa "*Castle in the Air*" y un fotógrafo de apellido Mayers, cuyo nombre no hemos ubicado. Esta artista logró mediante una orden judicial que no se divulgue la fotografía por atentar contra su intimidad. Dorothy Glancy señala que para el *Common Law* de los Estados Unidos de Norteamérica este es el "…primer ejemplo específico de una persona viva (…) que reivindicó el derecho a la privacidad".[27]

Pero fue con el artículo de Samuel Warren y Louis Brandeis que se le dio forma y contenido a este derecho, al punto que a estos autores se les reconoce su paternidad. Su influyente ensayo, publicado en la "*Harvard Law Review*" en diciembre de 1890[28], fue la respuesta al acoso que el propio senador Samuel Warren sufrió por la prensa de Boston.[29]

[26] El *New York Times* relata que cuando la señorita Manola se dio cuenta de que la fotografiaron en plena actuación se tapó el rostro y salió corriendo del escenario. Sin embargo, regresó para terminar su actuación. A la semana siguiente obtuvo la restricción judicial. Véase: GLANCY, Dorothy. "Privacy and the other miss M". Symposium on the Right to Privacy: After One Hundred Years Northern Illinois University Law Review, Summer 1990, 10 N. Ill. U. L. Rev. 401, p. 7. Fuente: http://1x937u16qcra1vnejt2hj4jl-wpengine.netdna-ssl.com/wp-content/uploads/miss_m.pdf Consulta: 31/10/2020.

[27] Op. Cit., p. 1 (traducción libre).

[28] WARREN, Samuel y Louis BRANDEIS. "*The right of privacy*. *Harvard Law Review*." Vol. 4, No. 5. (Dec. 15, 1890), pp. 193-220. Fuente: https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf Consulta: 31/10/2020.

29 La impresión que sobre la prensa tenían los autores no era de las mejores: "La prensa sobrepasa en todas direcciones los límites obvios del decoro y la decencia. El chisme ya no es el recurso de los ociosos y los viciosos, sino que se ha convertido en un oficio que se persigue con industria y con descaro. Para satisfacer un gusto lascivo, los detalles de las relaciones sexuales se difunden en las columnas de los diarios. Para ocupar a los indolentes, columna tras columna se llena de chismes ociosos, que solo pueden conseguirse mediante la intromisión en el círculo doméstico." Op. Cit. p. 200. (traducción libre). Ahora bien, hay autores, como Ekmekdjian y Pizzolo, que señalan que esta incomodidad provino por el acoso de la prensa a raíz del matrimonio de la hija de Warren. Véase al respecto: EKMEKDJIAN, Miguel Ángel y Calogero PIZZOLO. "Hábeas data. El derecho a la intimidad frente a la revolución informática". Depalma. Buenos aires. 1996, p. 8. De otro lado, - y esto debe ser lo más probable por la edad de Warren en 1890

Acudió entonces a su amigo y socio Louis Brandeis, quien años después asumiría como *justice* de la Corte Suprema Federal de los Estados Unidos, para ver si el *Common Law* le ofrecía algún tipo de protección frente a la divulgación de datos.

Como se dijo, Warren y Brandeis desarrollaron el derecho a "ser dejado solo" de Cooley y sostuvieron al respecto que la protección que se otorga a los pensamientos, sentimientos y emociones, expresados a través de la escritura o del arte, que consiste en impedir la publicación si no hay consentimiento, es meramente una instancia de aplicación del derecho más general del individuo a ser dejado solo.[30]

De ahí desembocó la noción de que el *Common Law* proporcionaba un principio que se puede invocar para proteger la privacidad del individuo de la invasión, ya sea por la prensa, el fotógrafo o el poseedor de cualquier otro dispositivo moderno para reformular o reproducir escenas o sonidos.[31] Así, decantaron que cuando hay invasión de la intimidad, la que consideraban una injuria legal, existían los elementos para exigir

(38 años) y la fecha de su matrimonio (1883 o 1884)-, Saltor, apoyándose en Urabayen, señala que la mortificación se debía al embate de la prensa que era atraída por las fiestas que realizaba la esposa de Warren: "En 1884, Warren se casó con Mabel Bayard, hija de un senador, miembro de la clase social más distinguida de Boston. Mabel Bayard tenía por costumbre ofrecer fastuosas fiestas que interesaban mucho a la prensa de Boston, en particular al semanario *Saturday Evening Gazette*, que cubría la noticia con detalles que irritaron profundamente a Warren y llevaron su atención sobre la legitimidad o ilegitimidad de tales informaciones. Este hecho social fue la causa directa que llevó a los autores a escribir, luego de seis años de estudio, sobre el derecho a la privacidad junto con su compañero y socio Brandeis (más tarde juez del Tribunal Supremo de los EEUU)". SALTOR, Carlos Eduardo. "La protección de datos personales: Estudio comparativo Europa-América con especial análisis de la situación argentina". Tesis para optar al grado de doctor en la Universidad Complutense de Madrid. 2013, p. 32. Cita a: URABAYEN, Miguel. "Vida Privada e Información". EUNSA. Zaragoza. 1977, p. 90. María Álvarez Cano, por su parte, señala que fue por ambas razones. Esta autora agrega: "En las crónicas de los periódicos se daban detalles personales, sensibles o escabrosos, encaminados a infundir en el lector la idea de despilfarro, derroche y amoralidad de la elevada clase social." Op. Cit., p. 50.

30 WARREN, Samuel y Louis BRANDEIS. Op. Cit., p. 205.

31 Loc. Cit.

reparación, ya que el valor del sufrimiento psíquico, causado por un hecho ilícito en sí mismo, es reconocido como base para la indemnización.[32]

Las bases doctrinarias de la *privacy* proporcionadas por Warren y Brandeis, fueron el punto de partida para desarrollar este derecho a lo largo del siglo XX. María Nieves Saldaña nos cuenta que este derecho fue evolucionando por virtud de la jurisprudencia de inicios de ese siglo: "Desde entonces y a lo largo de todo el siglo XX, la protección de la esfera privada en los Estados Unidos ha pasado del ámbito del *common law* al propio del Derecho constitucional, como consecuencia de su evolución desde una noción propietaria de la privacidad (*privacy-property*) a una concepción estrechamente relacionada con la dignidad de la persona, consolidándose como un bien jurídico fundamental merecedor de la máxima protección en el sistema constitucional norteamericano."[33]

Así, siguiendo a esta autora, gradualmente la jurisprudencia norteamericana decantó que la *privacy* tenía fundamento directo en la libertad de asociación garantizada en la primera enmienda de la Constitución norteamericana, que faculta a las personas a no revelar la pertenencia a una organización o grupo; en la prohibición del gobierno de realizar requisas arbitrarias, que incluye no solo la invasión material sino también la vigilancia electrónica, prevista en la cuarta enmienda; en la reserva de derechos reconocida en la novena enmienda; y en el derecho de la persona a adoptar por sí misma las decisiones fundamentales que configuran su vida personal y familiar sin injerencia estatal alguna, que

32 Op. Cit., 206. Cabe advertir que Warren y Brandeis también tuvieron presente el viejo adagio inglés, pues refieren al final en su trabajo que: "El *Common Law* siempre ha reconocido la casa de un hombre como su castillo". En puridad esta noción es de 1763 y se le atribuye a William Pitt, Conde de Chatham, que dijo lo siguiente sobre el derecho a vivir tranquilos en nuestra casa sin injerencia del poder regio: «El hombre más pobre, en su cabaña, desafía todas las fuerzas de la Corona. [Su cabaña] puede ser frágil, su techo tal vez es inestable, el viento se cuela por él, la tempestad lo penetra, no impide el paso de la lluvia, pero el Rey de Inglaterra no puede entrar en ella; ni con todo su poder se atreve a cruzar el umbral de esa ruinosa morada».

33 Op. Cit., p. 80.

deriva del concepto de libertad sustantiva que la Corte Suprema ha desarrollado a partir de la cláusula del debido proceso legal (*due process of law*), contemplada en la decimocuarta enmienda.[34]

La evolución de esta categoría, apuntalada por la doctrina que desde los años sesenta reconocía un derecho llamado "*informational privacy*"[35], ocasionó que finalmente se aprobara en 1974 la Ley de Privacidad o *Privacy Act*, que regula las practicas del uso de la información de las personas que se encuentra en los archivos federales, denominados *System of records*. Esta norma señala que ninguna agencia divulgará ningún registro que esté contenido en un sistema de registros por ningún medio de comunicación a ninguna persona, ni a otra agencia, excepto de conformidad con una solicitud por escrito o con el consentimiento previo por escrito de la persona a quien el registro corresponde; que cada agencia, con respecto a cada sistema de registros bajo su control, debe mantener un registro de la fecha, naturaleza y propósito de cada divulgación de un registro a cualquier persona u otra agencia; que, a su solicitud, cualquier individuo podrá obtener acceso a su registro o a cualquier información relacionada con él que esté contenida en el sistema, y permitirle a él y a su solicitud, una persona de su elección que lo acompañe, revisar el registro; que la persona solicite la enmienda de un registro que le pertenece; entre otros aspectos.

2.2. La protección de datos en Europa: su consagración constitucional

No solo en los Estados Unidos de Norteamérica hubo esta inquietud por proteger los derechos de las personas que podían verse

[34] Op. Cit., pp. 280 y 281. La autora que hemos parafraseado aquí sustenta tal evolución en una serie de sentencias que cita en su interesante y bien elaborado artículo.

[35] María Nieves Saldaña, citando a Fried y Westin, señala que "Bajo esta nueva dimensión, se ha definido el derecho a la privacidad como el poder de controlar el flujo de información personal y como el derecho a decidir cuándo, cómo y en qué medida la información personal es comunicada a otros, proceso de autodeterminación personal que ha de integrarse asimismo en los procesos comunicativos y participativos en los que interviene el individuo" Op. cit., p. 302.

afectados debido a la manipulación de sus datos.[36] En Europa, específicamente en Inglaterra, hubo proyectos por regular esta materia desde 1961, aunque no fue hasta 1979 que se regula por primera vez en este país. En Italia, como nos explica Vittorio Frosini, se aprobó en mayo de 1970 el Estatuto del Trabajador (*Statuto dei lavoratori*), cuyos artículos 4, 5 y 6 protegían la privacidad del trabajador frente a las nuevas posibilidades ofrecidas por la tecnología. Así, se proscribía la "video vigilancia" para controlar su actividad; la indagación sobre sus convicciones políticas, religiosas, sindicales; entre otras actividades.[37]

Pero fue en Alemania que, en octubre de 1970 y por influencia de Spiros Simitis, quien es considerado como el hombre que inventó la protección de datos, se aprobó una ley de protección de datos (*Datenschtzgesetz*) en el *Land* de Hesse. Esta ley regulaba la reserva en el uso de datos personales, el derecho al control sobre los datos e instituía a un funcionario como comisario para la protección de datos. Fue tan bien acogida que sobrepasó los límites del estado de Hesse y fue replicada en otros *lander* alemanes, como el *Land* del Rin-Palatino en 1974, hasta que

[36] No nos detenemos en esta parte en el desarrollo jurisprudencial europeo en relación con el derecho a la intimidad y a la protección de datos por razones de espacio. Pero eso no quiere decir no lo hubo, pues, por ejemplo, desde la década de los años sesenta en Alemania el Tribunal Constitucional acogió la teoría de las tres esferas de Hubmann y Seidel, la que María Álvarez Cano explica muy bien: "De la jurisprudencia del Tribunal Constitucional alemán surge la teoría de las tres esferas; según la cual habrá una esfera íntima (*Intimsphäre*), que iría referido a lo más secreto del individuo; la esfera privada (*Privatsphäre*), similar a la *privacy* anglosajona y similar a nuestro derecho a la intimidad, conteniendo la vida privada y las relaciones familiares y personales; y, por último, la esfera individual (*Individualsphäre*), que hace alusión a aspectos ligados a la intimidad pero incluidos dentro de ella como el honor y la propia imagen. Partiendo de esta teoría, se puede hablar de tres esféricas concéntricas, como son la de lo íntimo, la de lo privado y la de lo público." ÁLVAREZ CANO, María. Op. Cit., p. 28. En España también hubo una evolución jurisprudencial del derecho a la protección de datos, que se dio desde la regulación constitucional de 1978. Al respecto puede verse la sentencia del 20 de febrero de 1989 del Tribunal Supremo Español o la sentencia 292/2000 del Tribunal Constitucional español, de fecha 30 de noviembre, en la que se ha reconocido el derecho fundamental a la protección de datos.

[37] FROSINI, Vittorio. "Bancos de datos y tutela de la persona". Revista de Estudios Políticos. Nº 30. 1982, p. 25.

en 1978 se expidió una ley de protección de datos para toda Alemania (federal), llamada "Ley sobre la protección de los datos contra la utilización ilícita de los datos personales", más completa que la originaria y que también propició que los *lander* germanos la siguieran.[38] Se dice que esta ley es la primera que hace mención al término "protección de datos" (*Datenschutz),* para hacer referencia a las obligaciones de que los registros, los datos y los resultados obtenidos por su procesamiento, se obtengan, transmitan y almacenen de tal manera que no puedan ser consultados, alterados, extraídos o destruidos por una persona no autorizada.[39]

Ahora bien, fue Portugal en 1976 el primer país que consagró en la Constitución de aquel año el que ahora conocemos como el derecho a la protección de datos. Su artículo 31, titulado "Utilización de la informática", reconoció así el derecho de los ciudadanos portugueses a tener acceso a todos los registros informáticos que le conciernen, así como a solicitar que sean rectificados y actualizados y a requerir que se les informe la finalidad por la que obran estas informaciones, dotándolo de un contenido. Y aquí vale precisar que la regulación constitucional portuguesa se vio impulsada en gran medida por el decurso de los acontecimientos sociopolíticos: Portugal salió en 1974 de una dictadura de 48 años, el llamado "Salazarismo" o "*Estado Nuovo*", régimen que acabó con la denominada "Revolución de los claveles" y que trajo, como primera medida, un cambio de la Constitución.

[38] Cfr. FROSINI, Vittorio. Op. Cit. pp. 27 y 28. Frosini sugiere en su trabajo que la Ley de Hesse influyó en la creación de la *Privacy Act* norteamericana de 1974: "A pesar de sus límites de territorio y de contenido, la misma ley de Hesse suscitó mientras tanto un fuerte interés en el mundo del derecho, que había tomado forma concreta en las nuevas iniciativas de ley, fuera de Alemania Federal también. En 1972, se nombró en los Estados Unidos el DHEW (Health, Education and Welfare) Secretary's Advisory Committee on Automated Personal Data Systems con la tarea específica de llevar a cabo una investigación sobre «the impact of computers on record keeping about individuals», cuyos resultados, publicados en julio de 1973, fueron determinantes para el Privacy Act de 1974". Op. Cit. p. 28.

[39] Ley de protección de dato del Land de *Hesse*, de 1970, Sección 2.

En tal sentido, frente a la recopilación de datos y la generación de archivos de aquellos que habían sido opositores al régimen, los constituyentes reconocieron el derecho de los ciudadanos a conocer y controlar la información de estos archivos. Dalmo de Abreu Dallari, citado por Óscar Puccinelli, explica que estas disposiciones "…fueron establecidas, en gran medida, con el fin de permitir el acceso a las informaciones que se encontraban en poder de la arbitraria y violenta policía política, creada por Oliveira Salazar."[40] España vivió una experiencia parecida y consagró también este derecho en el artículo 18, numeral 4, de la Constitución de 1978.

Finalmente, el 28 de enero de 1981, la comunidad europea aprobó en Estrasburgo el "Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal", cuyo artículo 8, rotulado "Garantías complementarias para la persona concernida", señalaba que cualquier persona deberá poder obtener, llegado el caso, la rectificación de dichos datos o el borrado de los mismos, cuando se hayan tratado con infracción de sus disposiciones. Se hace alusión así a la facultad de "borrar" los datos cuando infringían las estipulaciones del convenio. Este es un primer claro antecedente del derecho al olvido que nos ocupa.

2.3. La protección de datos en los organismos internacionales: un reconocimiento de las posibles implicancias de la informática en los derechos fundamentales de las personas.

Del 22 de abril al 13 de mayo de 1968, por invitación de la Asamblea General de las Naciones Unidas, se realizó la primera Conferencia Internacional de Derechos Humanos en la ciudad de Teherán,

[40] PUCCINELLI, Óscar. "Evolución histórica y análisis de las diversas espe¬cies, subespecies, tipos y subtipos de habeas data en América Latina". p. 479. Fuente: file:///C:/Users/Usuario/Downloads/14792-Texto%20del%20art%C3%ADculo- 52444-1-10-20151119%20(2).pdf Consulta: 28/10/2020.

capital de Irán. A la misma acudieron representantes de 120 países, los que aprobaron por consenso la denominada "Proclamación de Teherán", en la que se evaluaron los progresos realizados desde la aprobación de la Declaración Universal de los Derechos Humanos, del 10 de diciembre de 1948, y se estableció un programa para el futuro.[41]

En el punto 18 de este importante instrumento internacional se denota ya una preocupación por la posible afectación de los derechos y libertades como como consecuencia del avance tecnológico: "Si bien los recientes descubrimientos científicos y adelantos tecnológicos han abierto amplias perspectivas para el progreso económico, social y cultural, esta evaluación puede, sin embargo, comprometer los derechos y las libertades de los individuos y por ello requerirá una atención permanente.". Y aunque el internet estaba aún en ciernes[42] se

[41] Cfr. MOMTAZ Djamchid. "La proclamación de Teherán". United Nations Audiovisual Library of International Law. Fuente: https://www.unfpa.org/sites/default/files/event-pdf/proclamation%20sp.pdf Consulta: 30/10/2020. La Proclamación de Teherán, en cuya parte considerativa se pueden observar esos objetivos, puede visualizarse en el siguiente enlace: https://www.acnur.org/fileadmin/Documentos/BDL/2002/1290.pdf

[42] La red galáctica (*galactic network*) fue el nombre que utilizó el informático estadounidense, Joseph C.R. Licklider, "Lick", del MIT, en sus memorandos de principios de los 60's, para denominar la visión que tuvo de crear una red de ordenadores mundial, capaz de comunicar usuarios en diferentes computadoras. Este científico fue reclutado por la Agencia de Proyectos de Investigación Avanzados, ARPA por sus siglas en inglés, creada en 1958 por el presidente Dwight Eisenhower para realizar estudios acerca del material bélico y de comunicaciones de los Estados Unidos. Recordemos que el mundo vivía en ese momento un clima de suma tensión. Dos viejos aliados en la segunda guerra mundial, los Estados Unidos y la Unión Soviética, fueron los principales antagonistas de la llamada Guerra Fría, que culminó décadas después, recién el 9 de noviembre de 1989, con la caída del muro de Berlín en Alemania. Este último, el símbolo más claro del enfrentamiento que dividió al bloque capitalista, liderado por el primero, del bloque socialista, encabezado por el segundo. Había, pues, una carrera armamentista entre estos dos países y el mayor miedo de Norteamérica era que los soviéticos lancen un ataque nuclear que pueda inutilizar el ordenador central de sus lanzamisiles. La solución, pensada por otro científico, el polaco-estadounidense Paul Baran, era que todas las computadoras sean ordenadores centrales o ninguna lo sea. Vicente Trigo Aranda explica con claridad esta solución: "…si un misil acertaba en el lugar donde estaba el ordenador central y lo destruía, la red quedaría inoperante. ¿Y por qué no colocar dos ordenadores centrales y así se disponía de más seguridad? Desde luego que sí, pero, ¿por qué no tres o cuatro? ¿En realidad, por qué no hacer que todos los ordenadores sean centrales? Dicho con otras palabras,

exhortaba a los países a redoblar esfuerzos para proteger los derechos de las personas.

Unos años después, el 10 de noviembre de 1975, la Asamblea General de las Naciones Unidas emitió la "Declaración sobre la utilización del progreso científico y tecnológico en interés de la paz y en beneficio de la humanidad"[43]. En esta declaración, la ONU reiteró su preocupación, pues señaló en el punto 2 que "Todos los Estados tomarán medidas apropiadas a fin de impedir que los progresos científicos y tecnológicos sean utilizados, particularmente por órganos estatales, para limitar o dificultar el goce de los derechos humanos y las libertades fundamentales de la persona consagrados en la Declaración Universal de Derechos Humanos, en los Pactos Internacionales de Derechos Humanos y en otros instrumentos internacionales pertinentes".

Recordemos que cuatro años atrás de emitida esta declaración Intel ya había presentado su primer microprocesador comercial. El mismo año de la declaración, Bill Gates y Paul Allen fundaron Microsoft en Alburquerque, Nuevo México. Un año después, en 1976, Steve Jobs, Steve Wozniak y Ronald Wayne[44] hicieron lo mismo con Apple en Cupertino, California. Al año siguiente presentaron el Apple

¿no sería más efectivo hacer que la red careciese de nodos centrales? De esta forma, aunque algún equipo fuese dañado, la información podría circular entre los restantes… ¡Y ésa, precisamente, es la medida que se adoptó!" TRIGO ARANDA, Vicente. "Historia y evolución del internet". Fuente: https:// www.acta.es/medios/articulos/comunicacion_e_informacion/033021.pdf. Consulta: 1/11/2020. Las ideas de Licklider, Baran y otros dieron paso a "Arpanet", la red de computadores interconectados, que es el antecedente directo del internet tal como hoy lo conocemos. La guerra fría, entonces, fue decisiva para el avance de esta tecnología.

[43] Aprobada por Resolución 3384 (XXX). El texto de esta declaración puede verse en: https://www.ohchr.org/SP/ProfessionalInterest/Pages/ScientificAndTechnologicalProgress.aspx Consulta: 30/10/2020.

[44] 12 días después de fundada la empresa, Ronald "Ron" Wayne vendería sus acciones por 800 dólares. Los que lo recuerdan, que son pocos, lo recuerdan por eso y porque creó el primer logo de Apple: Isaac Newton debajo de un manzano, lo que no gustó mucho a Steve Jobs quien al poco tiempo ordenó diseñar uno nuevo. Fue así que quedó la manzana mordida que todos reconocemos hoy.

II, computador personal que fue un éxito comercial. En 1981 le seguiría IBM con su IBM PC, modelo 5150, que también se vendió a gran escala. Y aunque a comienzos de la década de los 80's las pantallas de los computadores aún tenían fondo negro y letras verdes, ya se procesaban muchísimos datos en estos, lo que se aceleró drásticamente porque, entre otros factores, en 1983 ARPANET[45] pasó del uso militar al civil dando origen al Internet; en 1985 Microsoft presentó el sistema operativo Windows 1.0; y en 1990 se creó el Word Wide Web (WWW) o red informática mundial[46], que hizo más accesible todo en internet.

A comienzos de la década de los 90's las computadoras no eran una extrañeza. Una multiplicidad de empresas las comerciaban y casi todas ya venían con lectores de CD-ROM, en los que se podía guardar información adicional. Además de los particulares, muchas instituciones públicas las adquirían con la finalidad de modernizar el Estado. Lo mismo ocurría con muchas más empresas debido a sus funciones y capacidad de archivo. Si bien en 1990 solo habían 2.8 millones de personas como usuarios de internet,[47] un porcentaje mínimo de la población mundial de aquella época, estos se expandían a un ritmo acelerado, al punto que para comienzos de la década del nuevo siglo ya eran 631 millones[48] los usuarios de este servicio, los que accedían día a día a la información que se les ofrecía.

No era pues de extrañar que frente al impacto de la propagación de datos en internet surgieran los problemas que ya visionaba Naciones Unidas desde fines de los 60's; premisa que hizo poner atención a los eventuales riesgos de esta propagación.

---

[45] Véase respecto a ARPANET la nota al pie anterior.

[46] De acuerdo al sitio developer.mozilla.org: "La *World Wide Web* –comúnmente conocida como WWW, W3, o la Web– es un sistema interconectado de páginas web públicas accesibles a través de Internet (…). La Web no es lo mismo que el Internet: la Web es una de las muchas aplicaciones construidas sobre Internet."

[47] Fuente: http://archive.worldmapper.org/textindex/text_communication.html Consulta: 30/10/2020.

[48] Fuente: http://archive.worldmapper.org/textindex/text_communication.html Consulta: 30/10/2020.

2.4. Los orígenes de la protección de datos en Latinoamérica y las primeras referencias al derecho al olvido en Hispanoamérica.

Latinoamérica no fue ajena a esta efervescente ebullición que significó el reconocimiento del denominado "derecho a la protección de datos", *nomen iuris* que, como afirman muchos autores (Hondius, Puccinelli, Burkert, entre otros), en posición que compartimos, es incorrecto porque lo que se protege no son los datos sino los derechos de las personas a partir de su uso y manipulación. Existen normas que, con más propiedad, reconocen la "protección de los individuos con respecto al tratamiento de los datos personales", como la Directiva de Protección de Datos de la Comunidad Europea de 1995 y el Reglamento General de Protección de Datos de la Unión Europea de 2016, RGPD, vigente desde el 25 de mayo de 2018.[49] Sin embargo, el nombre caló y es el que usualmente se utiliza tanto en el idioma español, como en el italiano (*Protezione dei dati*), el alemán (*Datenschutz)*, el francés (*Protection des données),* entre otros.

A inicios de los años ochenta, la doctrina argentina ya mostraba una preocupación por el uso de la información personal obrante en bases de datos. En 1984, Luis Andorno, citado por Néstor Pedro Sagües, señalaba que "…resulta de todo punto de vista necesario y urgente impedir las intromisiones perturbadoras y la inadecuada difusión de datos procesados conforme a los modernos adelantos tecnológicos que pudieren afectar la esfera familiar y personal", máxime cuando "… el mero hecho de la conjunción de informaciones nominativas puede llevar a desnudar la intimidad de cada una de las personas físicas haciendo ilusorias las garantías constitucionales".[50]

---

[49] Véase al respecto: https://escueladpo.com/actualidad/origen-de-la-privacidad-como-empezo-todo/ Consulta: 29/10/2020.

[50] ANDORNO, Luis O., "La informática y el derecho a la intimidad", en La Ley 1985-A-1108, con cita de Faustina Zurich de Piatti, "La revolución informática y el derecho a la privacidad", Rosario, 1984. Citado en: SAGÜES, Néstor Pedro. "El hábeas data:

Empero, como nos relata el maestro Óscar Puccinelli, autor que es un referente obligado en esta materia, fue Guatemala el primer país que en nuestra región contempló el derecho a la protección de datos en su Constitución de 1985, cuyo artículo 31 a la letra preceptuó "Toda persona tiene el derecho de conocer lo que de ella conste en archivos, fichas o cualquier otra forma de registros estatales, y la finalidad a que se dedica. Quedan prohibidos los registros y archivos de filiación política, excepto los propios de las autoridades electorales y de los partidos políticos".[51] A esta Constitución le siguió la Nicaragüense de 1987, que señaló expresamente en su artículo 26 lo siguiente: "Toda persona tiene derecho: 1. A su vida privada y la de su familia. 2. A la inviolabilidad de su domicilio, su correspondencia y sus comunicaciones de todo tipo. 3. Al respeto de su honra y reputación. 4. A conocer toda información que sobre ella hayan registrado las autoridades estatales, así como el derecho de saber por qué y con qué finalidad tiene esa información".[52]

Tanto Guatemala como Nicaragua habían pasado por un difícil régimen dictatorial antes de aprobar estas Constituciones. De 1983 a 1985 Guatemala vivió una dura etapa represiva de dominación política y militar, que inició Efraín Ríos Montt, mientras que Nicaragua en 1987 trataba de desmantelar el orden político dejado por el régimen Somocista, instaurado desde 1936. La experiencia fue entonces parecida a la de Portugal, no siendo difícil imaginar que, a causa del contexto de persecución política antes imperante, fuera casi una obligación que los legisladores constituyentes reconocieran el derecho de las personas a conocer los archivos gubernamentales hasta entonces ocultos y controlar su uso.

---

su desarrollo constitucional". p.861. Fuente: https://archivos.juridicas.unam.mx/www/bjv/libros/1/113/39.pdf Consulta: 1/11/2020.

[51] Cfr. PUCCINELLI, Óscar. "Evolución histórica y análisis de las diversas especies, subespecies, tipos y subtipos de hábeas data en América Latina". p. 477. Fuente: file:///C:/Users/Usuario/Downloads/14792-Texto%20del%20art%C3%ADculo-52444-1-10-20151119%20(2).pdf Consulta: 28/10/2020.

[52] Loc. Cit.

Lo mismo sucedió en Brasil, cuya larga dictadura culminó en 1985, aunque este país fue un paso más allá, por cuanto contempló constitucionalmente en 1988, por primera vez en el mundo, el ahora ya conocido "*Hábeas data*", nombre que surgió desde la comisión encargada de redactar una nueva Constitución y que resulta de la conjunción de una palabra de raíz latina (*hábeas*) con una voz frecuente anglosajona (*data*), quizá haciéndonos recordar permanentemente que en materia de protección de datos tenemos tanto la influencia del Derecho europeo continental como del Derecho anglosajón, como ya se ha visto. La Constitución Brasilera de 1988, en su artículo 5, inciso LXXII establece así que:

> "*Se concederá hábeas data:*
>
> a *Para asegurar el conocimiento de informaciones relativas a la persona del impetrante que consten en registros o bancos de datos de entidades gubernamentales o de carácter público;*
>
> b. *Para la rectificación de datos, cuando no se prefiera hacerlo por procedimiento secreto, judicial o administrativo*".

Posteriormente, si bien no contempló expresamente el Hábeas data, la Constitución colombiana de 1991 reconoció el derecho a la protección de datos en su artículo 15: "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 los datos se respetarán la libertad y demás garantías consagradas en la Constitución". Jurisprudencialmente, eso sí, se ha reconocido un derecho de *Hábeas Data*.

Le siguió a la colombiana la Constitución de Paraguay de 1992, que consagró un "derecho a informarse" en su artículo 28, que tuvo la siguiente redacción: "Se reconoce el derecho de las personas a recibir información veraz, responsable y ecuánime. Las fuentes públicas de

información son libres para todos. La ley regulará las modalidades, plazos y sanciones correspondientes a las mismas, a fin de que este derecho sea efectivo. Toda persona afectada por la difusión de una información falsa, distorsionada o ambigua tiene derecho a exigir su rectificación o su aclaración por el mismo medio y en las mismas condiciones que haya sido divulgada, sin perjuicio de los demás derechos compensatorios.".

El Perú en cambio sí siguió la línea de los brasileños y fue el segundo país en regular el *Hábeas data* en la Constitución de 1993 con matices propios, lo que se detalla *infra*.

Más adelante, en 1994, Argentina reformó su Constitución Federal para asegurar el conocimiento de informaciones y la rectificación de datos. El artículo pertinente (artículo 43) hace referencia a la acción de amparo y señala que "Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquellos. No podrá afectarse el secreto de las fuentes de información periodística." (Tercer párrafo). Para nadie fue un secreto que se estaba regulando un *Hábeas Data*.

Se advierte entonces que en Latinoamérica, desde los años ochenta del siglo pasado, ya había una preocupación por proteger los derechos de las personas en esta materia, lo que fue consolidándose mediante la regulación constitucional antes descrita. Empero, fue la Corte Constitucional colombiana, que ha sido pionera en muchos aspectos, la que en 1992 hizo referencia expresa al derecho al olvido en la sentencia que resolvió el Expediente T-414-1992, Caso Arguelles Norambuena; caso que consideramos importante describir brevemente a continuación.

El 19 de diciembre de 1991, el arquitecto Francisco Gabriel Argüelles Norambuena, promovió lo que en Colombia se conoce como "acción de tutela" y que nosotros conocemos como "proceso de amparo", ante el Juzgado 110 de Instrucción Criminal de Bogotá, persiguiendo,

entre otros aspectos, que se le retire de la lista de deudores morosos y que se actualice y rectifique la información que sobre él existía en el banco de datos de la Asociación Bancaria de Colombia, entidad que administraba un registro de información del sistema financiero.

Manifestó que figuraba como deudor moroso del Banco de Bogotá en la central de información de la precitada asociación en virtud a un crédito que respaldara en su momento con un pagaré, el que venció inicialmente el 14 de julio de 1981 y fue prorrogado hasta el 14 de noviembre de 1981. Sin embargo, añadió que, en relación con esta deuda, mediante la sentencia ejecutoriada de fecha 27 de abril de 1987, el Juzgado Décimo Sexto Civil del Circuito de Bogotá declaró prescrita su obligación.[53]

No obstante ello, frente a sus solicitudes del 8 de noviembre de 1988 y del 18 de junio de 1991 de que sea rectificada la información, la Asociación Bancaria de Colombia se negó rotundamente a acceder al pedido. El 24 de junio de 1991 el peticionario elevó igual solicitud al Banco de Bogotá, el cual también la rechazó verbalmente. En virtud de todo lo anterior, el señor Argüelles aparecía como deudor moroso en el banco de datos de la Asociación Bancaria cuatro años después de ejecutoriada la sentencia que declaró extinguida su obligación.[54]

Al revisar la sentencia, se puede advertir que, como se dijo, en esta se hace mención al derecho al olvido, se reconoce una falta de legislación en Colombia y se sostiene que la justicia constitucional no puede estar ajena a las embestidas del poder informático. En cuanto al olvido en sí, el punto 5 de este pronunciamiento lleva un rótulo poético: "La cárcel del alma y el derecho al olvido" y, en este, la Corte Constitucional colombiana señaló que "El encarcelamiento del alma en la

[53] Sentencia T-414-92. Fuente: https://www.corteconstitucional.gov.co/relatoria/1992/t-414-92.htm Consulta: 20/09/2020

[54] Sentencia T-414-92. Fuente: https://www.corteconstitucional.gov.co/relatoria/1992/t-414-92.htm Consulta: 20/09/2020

sociedad contemporánea, dominada por la imagen, la información y el conocimiento, ha demostrado ser un mecanismo más expedito para el control social que el tradicional encarcelamiento del cuerpo."[55]; agregó que "Los datos tienen por su naturaleza misma una vigencia limitada en el tiempo la cual impone a los responsables o administradores de bancos de datos la obligación ineludible de una permanente actualización a fin de no poner en circulación perfiles de 'personas virtuales' que afecten negativamente a sus titulares, vale decir, a las personas reales."[56]; para concluir que "Es bien sabido que las sanciones o informaciones negativas acerca de una persona no tienen vocación de perennidad y, en consecuencia, después de algún tiempo tales personas son titulares de un verdadero derecho al olvido".[57]

Adviértase, entonces, que ya desde 1992 se hacía patente en Colombia la necesidad de resguardar a las personas frente a informaciones que las perjudiquen, concediéndoles el derecho de suprimir aquellos datos que las afecten en caso no sean rectificados o actualizados. Un verdadero derecho al olvido, reconocido ya por estas latitudes.

Estas preocupaciones también fueron tomando forma en Europa, conscientes de que "El carácter imperecedero de la información en Internet pone en jaque a la privacidad"[58]; o, cómo dijo Viviane Reding en 2010, ex vicepresidenta de la Comisión Europea e impulsora del reconocimiento del derecho al olvido, de que "Dios persona y olvida pero la Red nunca lo hace".[59]

---

[55] Sentencia T-414-92. Fuente: https://www.corteconstitucional.gov.co/relatoria/1992/t-414-92.htm Consulta: 20/09/2020

[56] Sentencia T-414-92. Fuente: https://www.corteconstitucional.gov.co/relatoria/1992/t-414-92.htm Consulta: 20/09/2020

[57] Sentencia T-414-92 Fuente: https://www.corteconstitucional.gov.co/relatoria/1992/t-414-92.htm Consulta: 05/11/2020

[58] ÁLVAREZ CANO, María. "El derecho al olvido en internet: el nuevo paradigma de la privacidad en la era digital". Op. Cit., p. 19.

[59] 30 de noviembre de 2010, en la conferencia: *Privacy Matters-Why the EU needs new personal data protection rules*. ÁLVAREZ CANO, María. Loc. Cit. En similar sentido

Pero, centrémonos en España, país respecto del cual se resolvió el caso que ha hecho famoso este derecho: el Caso Costeja. Artemi Rallo Lombarte, ex director de la Agencia Española de Protección de Datos, nos cuenta que hubieron antecedentes en relación al derecho al olvido, como el Caso "Datos personales en foros online" (TD/266/2007), el Caso Montera (PS/617/2008), el Caso Discapacitado (PS/479/200), el Caso Agresión a Menor Ecuatoriana (E/1234/2008), el Caso Conferencia de Alicante (TD/1226/2011), el Caso Opus Dei I (PS/337/2011), el Caso Opus Dei II (TD/10/2011), el Caso Tazzina-Facebook I (PS/434/2011), el Caso Magnolia-Facebook II (TD/1239/2010), entre otros.[60] Sin embargo, ha sido el precitado Caso Costeja, que llegó al Tribunal de Justicia de la Unión Europea, el que le ha dado el impulso a este derecho. Lo describimos brevemente a continuación.

Mediante sentencia de fecha 13 de mayo de 2014, el Tribunal de Justicia de la Unión Europea, que interpreta y aplica el Derecho de la Unión Europea, "resolvió" el caso Costeja, el que, como ya hemos adelantado, ha sido uno de los más emblemáticos y es considerado el más importante en lo que al derecho al olvido se refiere, al punto que en virtud de tal caso se han impuesto obligaciones al gigante Google en Europa relativas a la protección de este derecho.

Como se señala en la sentencia, la petición se presentó en el marco de un litigio contencioso administrativo entre Google Spain S.L. y Google Inc., por un lado, y la Agencia Española de Protección de Datos - AEPD y el señor Costeja González, por otro, en relación con una

---

Alejandro Platero Alcón: "El ser humano es olvidadizo y en ocasiones se enfrenta a terribles enfermedades que atacan directamente la capacidad de recodar las cosas, como es el temible Alzheimer. Sin embargo, (…) estos problemas de memoria no afectan con los mismos síntomas a las nuevas tecnologías, ni mucho menos a los motores de búsqueda de Internet, que almacenan información sin que les entre un ataque voluntario de olvido" PLATERO ALCÓN, Alejandro. "El derecho al olvido en internet. El fenómeno de los motores de búsqueda." p. 245. Fuente: file:///C:/Users/Usuario/Downloads/1726-Texto%20del%20art%C3%ADculo-6179-1-10-20160527.pdf Consulta: 27/10/2020.

[60] RALLO, Artemi. Op. Cit. pp. 55-68.

resolución de dicha agencia por la que se estimó la reclamación del señor Costeja González contra ambas sociedades y se ordenó a Google Inc. que adoptara las medidas necesarias para retirar los datos personales del reclamante de su índice e imposibilitara el acceso futuro a los mismos.

El 5 de marzo de 2010, el ciudadano español señor Costeja González presentó ante la AEPD una reclamación administrativa contra la empresa "La Vanguardia Ediciones S.L.", que publica un periódico de gran difusión en Cataluña, y contra Google Spain y Google Inc. Esta reclamación, prosigue la sentencia, se basó en que, cuando un internauta introducía el nombre del Sr. Costeja González en el motor de búsqueda de Google, obtenía como resultado vínculos hacia dos páginas del periódico "La Vanguardia", del 19 de enero y del 9 de marzo de 1998, respectivamente, en las que figuraba un anuncio de una subasta de inmuebles relacionada con un embargo por deudas a la Seguridad Social, que mencionaba el nombre del Sr. Costeja González (véase fundamento 14).

Mediante su reclamación, el Sr. Costeja González solicitó, por un lado, que se exigiese a "La Vanguardia" eliminar o modificar la publicación para que no apareciesen sus datos personales, o utilizar las herramientas facilitadas por los motores de búsqueda para proteger estos datos. Por otro lado, solicitó que se exigiese a Google Spain o a Google Inc. que eliminaran u ocultaran sus datos personales para que dejaran de incluirse en sus resultados de búsqueda y dejaran de estar ligados a los enlaces de La Vanguardia. En este marco, el Sr. Costeja González afirmaba que el embargo al que se vio sometido en su día estaba totalmente solucionado y resuelto desde hace años y carecía de relevancia actualmente (véase fundamento 15).

Mediante resolución de 30 de julio de 2010 del director de la Agencia Española de Protección de Datos, se desestimó la reclamación en relación a "La Vanguardia", al considerarse que la publicación que esta había llevado a cabo estaba legalmente justificada, dado que había tenido lugar por orden del Ministerio de Trabajo y Asuntos Sociales y

tenía por objeto dar la máxima publicidad a la subasta para conseguir la mayor concurrencia de licitadores. En cambio, se estimó la misma reclamación en la medida en que se dirigía contra Google Spain y Google Inc.

A este respecto, como se aprecia en la sentencia, la AEPD consideró en su resolución administrativa que quienes gestionan motores de búsqueda se encuentran sometidos a la normativa en materia de protección de datos, dado que llevan a cabo un tratamiento de datos del que son responsables y actúan como intermediarios de la sociedad de la información. "La AEPD consideró que estaba facultada para ordenar la retirada e imposibilitar el acceso a determinados datos por parte de los gestores de motores de búsqueda cuando considere que su localización y difusión puede lesionar el derecho fundamental a la protección de datos y a la dignidad de la persona entendida en un sentido amplio, lo que incluye la mera voluntad del particular afectado cuando quiere que tales datos no sean conocidos por terceros. La AEPD estimó que este requerimiento puede dirigirse directamente a los explotadores de motores de búsqueda, sin suprimir los datos o la información de la página donde inicialmente está alojada e, incluso, cuando el mantenimiento de esta información en dicha página esté justificado por una norma legal."[61]

Tanto Google Spain como Google Inc. interpusieron recursos contenciosos administrativos contra la resolución de la AEPD, registrados con los números 725/2010 y 257/2010, los que fueron acumulados posteriormente mediante auto de fecha 20 de julio de 2011. Sin embargo, antes de resolver, la Sala Contencioso - Administrativa, por Auto de fecha 27 de febrero de 2012 acordó plantear al Tribunal de Justicia de la Unión Europea - TJUE una cuestión prejudicial de interpretación, al amparo del artículo 267 del Tratado de Funcionamiento de la Unión Europea.

[61] Sentencia de fecha 13 de mayo de 2014 del Tribunal de Justicia de la Comunidad Europea, fundamento 17.

Con ocasión de esta cuestión prejudicial, el TJUE se pronunció sobre diversos aspectos relacionados con la aplicación de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Pero lo que interesa destacar es la respuesta a la interrogante de la siguiente pregunta:

> ¿Debe interpretarse que los derechos de supresión y bloqueo de los datos, regulados en el artículo 12.b) y el de oposición, regulado en el artículo 14.a) de la Directiva 95/46/CE comprenden que el interesado pueda dirigirse frente a los buscadores para impedir la indexación de la información referida a su persona, publicada en páginas web de terceros, amparándose en su voluntad de que la misma no sea conocida por los internautas cuando considere que puede perjudicarle o desea que sea olvidada, aunque se trate de una información publicada lícitamente por terceros?

La respuesta fue la siguiente:

> *Los artículos 12, letra b) y 14, párrafo primero, letra a), de la Directiva 95/46 deben interpretarse en el sentido de que, para respetar los derechos que establecen estas disposiciones, siempre que se cumplan realmente los requisitos establecidos en ellos, el gestor de un motor de búsqueda está obligado a eliminar de la lista de resultados obtenida tras una búsqueda efectuada a partir del nombre de una persona vínculos a páginas web, publicadas por terceros y que contienen información relativa a esta persona, también en el supuesto de que este nombre o esta información no se borren previa o simultáneamente de estas páginas web, y, en su caso, aunque la publicación en dichas páginas sea en sí misma lícita.* (el subrayado).

La resolución de caso Costeja no hace sino imponer una obligación a los motores de búsqueda como Google de eliminar los resultados de búsqueda de algunas personas cuando se afecten sus derechos. Resaltando esta sentencia, Agustín Puente Escobar señala "La sentencia, y precisamente en este punto radica su trascendental importancia, no hace sino poner de manifiesto que los principios que configuran el

derecho a la protección de datos, tal y como es concebido en el ámbito de la Unión Europea, son perfectamente aplicables a los tratamientos de datos personales llevados a cabo en el marco de los servicios de la sociedad de la información, que lógicamente no existían en su configuración actual en el momento en que las primeras normas de protección de datos fueron aprobadas."[62]

A partir de la misma, la doctrina ha puesto interés en desarrollar el derecho ahí reconocido, tratándose de dar una definición y de brindar un contenido del mismo, como veremos a continuación.

3. Definición del derecho al olvido

El mismo Artemi Rallo, señala en uno de sus trabajos que el derecho al olvido es la "…potestad del individuo de requerir la cancelación o limitación del uso de sus datos personales en un medio de comunicación"[63] Vale decir, la describe como una potestad o facultad que tienen las personas para eliminar o restringir datos. En su interesante obra "El derecho al olvido en Internet. Google Versus España", señala que si pretendemos ubicar el análisis del derecho al olvido en el de los "derechos autónomos" cuyo contenido histórico resulta perfectamente visualizable cualquiera que sea la rama del derecho que escrutemos, hoy por hoy, el derecho al olvido no existe.[64]

Y es que en ese momento, año 2014, ninguna norma reconocía ese hipotético y específico derecho, no existía un concepto jurídico pacíficamente delimitado y mal se podía amparar por el ordenamiento jurídico algo que en la realidad social no gozaba de perfiles delimitadores

[62] PUENTE ESCOBAR, Agustín. "El derecho al olvido". En: PÉREZ BES, Francisco (coord.). "El derecho de internet". Atelie libros jurídicos. Barcelona. 2016, p. 182.

[63] RALLO, Artemi. "El derecho al olvido en el tiempo de internet: la experiencia española". p 160.

[64] RALLO, Artemi. "El derecho al olvido en internet. Google versus España". Centro de Estudios Políticos y Constitucionales. Madrid. 2014, p. 23

básicos.[65] No obstante ello, en el 2018 entró a regir el antes citado Reglamento (UE) 2016/679, Del Parlamento Europeo y Del Consejo, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), antes referida, cuyo artículo 17 regula expresamente el derecho al olvido, equiparándolo al de supresión de datos y estableciendo su contenido.[66]

[65] Op. Cit., 23.

[66] "Artículo 17 Derecho de supresión («el derecho al olvido»)
1. El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales cuando concurra alguna de las circunstancias siguientes: a) los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo; b) el interesado retire el consentimiento en que se basa el tratamiento de conformidad con el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), y este no se base en otro fundamento jurídico; c) el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 1, y no prevalezcan otros motivos legítimos para el tratamiento, o el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 2; d) los datos personales hayan sido tratados ilícitamente; e) los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento; f) los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información mencionados en el artículo 8, apartado 1. 2. Cuando haya hecho públicos los datos personales y esté obligado, en virtud de lo dispuesto en el apartado 1, a suprimir dichos datos, el responsable del tratamiento, teniendo en cuenta la tecnología disponible y el coste de su aplicación, adoptará medidas razonables, incluidas medidas técnicas, con miras a informar a los responsables que estén tratando los datos personales de la solicitud del interesado de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos. 3. Los apartados 1 y 2 no se aplicarán cuando el tratamiento sea necesario: a) para ejercer el derecho a la libertad de expresión e información; b) para el cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento, o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable; c) por razones de interés público en el ámbito de la salud pública de conformidad con el artículo 9, apartado 2, letras h) e i), y apartado 3; d) con fines de archivo en interés público, fines

Ahora bien, prosiguiendo con su conceptualización por parte de la doctrina, Faustino Gudin ha dicho, por ejemplo, que el derecho al olvido se presenta pues como la consecuencia del derecho que tienen los ciudadanos a solicitar, y obtener de los responsables, que los datos personales sean suprimidos cuando, entre otros casos, estos ya no sean necesarios para la finalidad con la que fueron recogidos, cuando se haya retirado el consentimiento o cuando estos se hayan recogido de forma ilícita.[67]

Por su parte, Cecile de Terwangne[68], en su artículo "Privacidad en Internet y el derecho a ser olvidado/derecho al olvido", señala que "…es el derecho de las personas físicas a hacer que se borre información sobre ellas después de un período de tiempo determinado". Mientras que para Alejandro Touriño el olvido sería "…un derecho que exige que los datos de las personas dejen de ser accesibles en la web, por petición de las mismas y cuando estas lo decidan; como un derecho a retirarse del sistema y eliminar la información personal que la red contiene"[69] Así, para este autor, el derecho al olvido se conceptualiza como el derecho del individuo a eliminar o hacer inaccesibles ciertos datos o información publicados en el entorno digital y que se encuentren indexados por buscadores de internet.[70]

---

de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, en la medida en que el derecho indicado en el apartado 1 pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento, o e) para la formulación, el ejercicio o la defensa de reclamaciones."

[67] GUDIN RODRIGUEZ-MAGARIÑOS, Faustino. "Nuevo reglamento europeo de protección de datos versus big data". Tirant lo Blanc. Valencia. 2018, p. 126.

[68] DE TERWANGNE, Cecile. "Privacidad en Internet y el derecho a ser olvidado/derecho al olvido". Revista de los Estudios de Derecho y Ciencia Política de la UOC. Número 13 (Febrero 2012). p. 53. Fuente: http://www.crid.be/pdf/public/7166.pdf Consulta: 31/10/2020.

[69] CASTELLANO, Pere Simón. "El derecho al olvido digital en la web 2.0". Cátedra Telefónica de la Universidad de Salamanca Mario Hernández Ramos N° 11. Mayo. 2013, p. 28.

[70] TOURIÑO, Alejandro. "El derecho al olvido y la intimidad en Internet." Libros Catarata. Madrid. 2014. p. 140.

A nivel nacional, Angles Yanqui ha dicho que "El derecho al olvido enmarca la eliminación, cancelación de los hechos de nuestra vida pasada, y estos salgan del entorno virtual, y se evite su difuminación…"[71]

Nos parece muy precisa la definición de María Álvarez Caro, para quien el derecho al olvido deriva de los derechos a la intimidad y a la protección de datos personales, y "…podría definirse como el derecho a equivocarse o a que una equivocación pasada no marque y determine la vida de un individuo que, por definición, no es otra cosa que un proceso evolutivo, una secuencia de aciertos y errores, siempre en proceso de conformación, de cambio y de evolución constante."[72] Añade asimismo, "Se conoce como derecho al olvido, a un interés jurídicamente protegido de los ciudadanos que consiste en lograr efectivamente que sus datos personales no sean localizados por los buscadores en la Red."[73] En tal sentido, compartimos el criterio de que "No se trata de exigir el borrado de los datos porque éstos no son exactos o ciertos, sino porque el titular de los mismos considera que le perjudican y estima asimismo que no existe ningún fin que legitime la disponibilidad de dichos datos por parte de terceros."[74]

Teniendo en cuenta estos criterios toca analizar el caso peruano.

4. El derecho al olvido y su protección en el Perú

4.1. En primer lugar, un caso para la reflexión

En junio de 2008, en las zonas aledañas a "Larcomar", conocido centro comercial ubicado en Miraflores, fueron detenidos por la Policía

---

[71] ANGLES YANQUI, Gerard. "El derecho al olvido frente a la comercialización del derecho a la intimidad en el Perú." p. 10. Consulta: http://blog.pucp.edu.pe/blog/derechoconstitucionalperu/2017/10/30/el-derecho-al-olvido-frente-a-la-comercializacion-del-derecho-a-la-intimidad-en-peru/ Consulta: 31/10/2020.

[72] Op. Cit.

[73] Op. Cit., p. 71.

[74] Op. Cit. p. 71.

Nacional y el Serenazgo del distrito, cuatro jóvenes cuyo nombre no mencionaré para proteger sus identidades. Horas después, los presentaron enmarrocados ante los medios de comunicación escritos, radiales y televisivos, como integrantes de la banda denominada "Los Malditos de Larcomar", peligrosa organización criminal que se dedicaba principalmente al robo de los turistas que circundan la zona.

La intervención no hubiera tenido nada de extraña sino fuera porque tales jóvenes eran ciclistas que, desde el distrito de San Juan de Lurigancho, simplemente se dirigían a "Larcomar" a presenciar un evento de ciclismo de montaña. Uno de ellos incluso era campeón de "*downhill*", una modalidad de ciclismo, y poseía títulos internacionales obtenidos representando a nuestro país. Sin embargo, fueron tomados por delincuentes al parecer solo por sus rasgos. Un claro hecho vergonzoso que recuerda a las viejas y totalmente superadas teorías de Lombroso, pero que en realidad refleja un trasfondo discriminatorio y sectario en la sociedad peruana, que hasta el día de hoy persiste.[75]

El campeón de "*downhill*" manifestó a un canal de televisión el día de su captura: "He venido a presentar un evento de ciclismo y nos han confundido con delincuentes señor". Y así fue, nunca imaginaron lo que pasaría después. El maltrato sufrido no solo comprendió la exposición pública que dañó su imagen, sino también la "siembra" de drogas entre sus pertenencias, la incomunicación con su familia, sendas golpizas y el encierro por seis días, hasta que se solucionó el malentendido.

[75] Unos años después, en 2011, "Larcomar" fue escenario de otro lamentable acto discriminatorio cuando al señor Ricardo Apaza, quien vestía atuendos típicos cuzqueños, le prohibieron el reingreso a la sala del cine después de haber ido al baño. El cine fue clausurado provisionalmente por siete días. Luego de los hechos, el señor Apaza señaló "Yo vine para conocer Lima, para conocer nomás he venido. Cómo es Lima, para eso". Sin duda, conoció la peor cara de Lima, conoció a Lima racista, sin duda una nueva forma de entender el término de "Lima la horrible".

Más de doce años han pasado y aunque el hecho ya se aclaró y se relevó al entonces comandante de Miraflores, aún se pueden ver en el internet imágenes y las notas periodísticas de la captura, así como videos en los que presenta a tales personas como integrantes de la citada banda criminal, todo lo cual evidentemente afecta la reputación de los ciclistas involucrados.

¿Tienen estas personas el derecho a que se eliminen del internet todas estas informaciones que si bien en su momento se publicaron al amparo de la libertad de información al día de hoy son desfasadas, obsoletas, se sabe que no son ciertas y no hacen más que afectar la dignidad, el honor y la buena reputación de un grupo de personas inocentes? Creemos que sí, toca explicar por qué.

4.2. El ordenamiento jurídico peruano en materia de protección de datos ¿protege también el derecho al olvido?

A nivel constitucional, como se dijo el Perú, después de Brasil, fue el segundo país en contemplar el *Hábeas data* como una "garantía constitucional"[76] dirigida a proteger el denominado derecho de protección de datos, aunque también sirve para cautelar el derecho de acceso a la información pública. Si se pasa revista al diario de los debates realizados al interior Congreso Constituyente Democrático, que aprobó finalmente la Constitución de 1993, observaremos las intervenciones del constituyente Carlos Torres y Torres Lara, lastimosamente desaparecido a temprana edad, en la que ya se podían vislumbrar las inquietudes y preocupaciones que traía consigo la informática:

> "*El problema de la informática, señor Presidente, tiene varios aspectos. Uno de ellos ya lo hemos tratado: el acceso de la ciudadanía a la información. El otro gran pedido que se ha abierto en la comunidad mundial es porque algunas instituciones –sean públicas o privadas, secretas o no– negocian e*

[76] El Código Procesal Constitucional se encargó de actualizar la nomenclatura por el de proceso constitucional, que es lo propio.

> *influyen sobre la comunidad en general con los datos íntimos de las personas, lo cual va contra la dignidad de éstas.*" (Comisión de Constitución del CCD, Tomo I, p. 165).

El internet estaba en ciernes en el Perú en 1993,[77] pero este legislador constituyente, muy informado, ya predecía que iba a traer no pocos inconvenientes que afectarían la dignidad de las personas:

> "*…nadie está en el derecho de ir contra la dignidad de una persona para que, a través de sistemas masivos de información, se generalicen informaciones que pertenecen solamente a su persona*" (Comisión de Constitución del CCD, Tomo I, p.166).

En ese sentido, hizo una defensa del *Hábeas Data* como medio de protección frente a la manipulación de informaciones y planteó la posibilidad de añadir este proceso a la Carta Fundamental por aprobarse. Señaló al respecto:

> *"No estamos inventando este derecho, sino que se ha recogido en los últimos diez años de las modificaciones constitucionales más modernas, como el caso de Brasil, que ha establecido precisamente el hábeas data; porque el hábeas data, al que se refería el Presidente de la Comisión, está relacionado a este caso y no al anterior. Nosotros lo estamos incorporando para los dos casos"* (Comisión de Constitución del CCD, Tomo I, p.165 y 166)

Y también que:

> "*El hábeas data es el procedimiento mediante el cual –por ejemplo, en el Brasil, en Portugal o en Italia– el ciudadano puede solicitar mayor información de la que se consigna acá; por ejemplo, que se excluya información que ya está, que se modifique información, que se cambie información, porque la información íntima es de propiedad de la persona.*

[77] Conforme relata el sitio web karlosperú.com: "El internet ingresó al Perú en el año 1992, al crearse la Red Científica Peruana (RCP). Siendo así, dos años más tarde, en 1994, se instaló a primera cabina pública de internet, la cual tuvo aproximadamente 40 computadoras para que los peruanos naveguen por la red." Fuente: https://www.karlosperu.com/internet-como-ha-cambiado-este-recurso-en-el-peru/#:~:text=El%20internet%20ingres%C3%B3%20al%20Per%C3%BA,peruanos%20naveguen%20por%20la%20red. Consulta: 01/11/2020.

> *En consecuencia, hay abundante material legislativo y teórico sobre esta materia y no tiene por qué llevar a ninguna confusión, en la medida en que seamos muy expresos, como lo estamos haciendo en estos agregados: 'A que los servicios informáticos computarizados públicos o privados, para que no suministren informaciones que afectan la intimidad personal, salvo los casos establecidos por ley'."* (Comisión de Constitución del CCD, Tomo I, 166).

Fue así que finalmente la Constitución de 1993 consagró al proceso de *Hábeas Data* en su artículo 200, numeral 3. Este numeral señala que procede contra el hecho u omisión, por parte de cualquier autoridad, funcionario o persona, que vulnera o amenaza los derechos a que se refiere el artículo 2, incisos 5 y 6, de la Constitución. Es decir, el derecho de acceso a la información pública (inciso 5) y el de protección de datos personales o también llamado jurisprudencialmente de "autodeterminación informativa" lo que proviene de la jurisprudencia alemana (inciso 6).[78]

Ahora bien, el precitado numeral 6 del artículo 2 de la Constitución resulta escueto en sus alcances, pues como se presentó y aprobó se limita solamente a señalar que toda persona tiene derecho "*A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar*". Así las cosas, si nos atenemos a la literalidad del texto podríamos concluir

[78] Cabe anotar que, inicialmente, el proceso de *hábeas data* protegía también el derecho de rectificación frente a informaciones inexactas o agraviantes propaladas por cualquier medio de comunicación, previsto en el artículo 2, numeral 7, de la Constitución, lo que fue muy criticado en su momento por la doctrina nacional. Al respecto, véase, entre otros: GARCÍA BELAUNDE, Domingo. "Garantías Constitucionales en la Constitución Peruana de 1993". En: La Constitución de 1993; análisis y comentarios. Serie Lecturas sobre Temas Constitucionales N° 10. Comisión Andina de Juristas. Lima. 1994, pp. 259-260. EGUIGUREN PRAELI, Francisco. "El hábeas data y su desarrollo en el Perú". Ius et praxis. Volumen 3. Número 1. 1997, pp. 119-135. Posteriormente, mediante el Artículo Único de la Ley de Reforma Constitucional Nº 26470, publicada en el diario oficial "El peruano" el 12 junio de 1995, se modificó el artículo constitucional citado sustrayéndose este derecho dentro del elenco de los derechos protegidos por el Hábeas Data.

que el derecho consagrado en tal numeral nos permite únicamente que obliguemos a quienes tienen la información a no suministrarla si esta afecta nuestra intimidad personal y familiar.

La Ley 26301, Ley referida a la aplicación de la Acción Constitucional de Hábeas Data, del 3 de mayo de 1994, no contempló un artículo en el que se establezcan las pretensiones que procedían plantearse en ese novel proceso constitucional. Tan solo dio luces respecto de donde pueden estar ubicados los archivos. A saber: en soportes mecánicos, telemáticos, magnéticos, informáticos o similares.

Ha sido el Código Procesal Constitucional, vigente desde diciembre del año 2004[79], el que se ha encargado de darle un mayor contenido a este derecho en su artículo 61, numeral 2. Si bien no hace mención expresa del derecho al olvido, señala que toda persona puede acudir al *Hábeas Data* para conocer, actualizar, incluir y suprimir o rectificar la información o datos referidos a su persona que se encuentren almacenados o registrados en forma manual, mecánica o informática, en archivos, bancos de datos o registros de entidades públicas o de instituciones privadas que brinden servicio o acceso a terceros. Asimismo, para suprimir o impedir que se suministren datos o informaciones de carácter sensible o privado que afecten derechos constitucionales.

En tal dirección, el proceso constitucional de *Hábeas Data* en el Perú dota a las personas un abanico de posibilidades para protegerse del uso y la manipulación de sus datos. Como se advierte, a través de este proceso estas pueden conocer, actualizar, incluir, suprimir, rectificar o impedir que suministren los datos concernientes a su persona. Asimismo, el perjudicado puede utilizar este proceso para suprimir o impedir el suministro de datos, privados o sensibles, que afecten sus derechos fundamentales.

[79] Que derogó la precitada Ley 26301.

Por consiguiente, es perfectamente posible imaginar que si el uso de la información consignada en una base de datos, pública o privada, afecta derechos reconocidos como fundamentales, tales como el honor, la imagen, la buena reputación o la propia dignidad de la persona humana, el *Hábeas Data*, al menos teóricamente, resulta totalmente idóneo para proteger el derecho al olvido, que justamente procede para suprimir la información perniciosa que en determinado momento pudo ser veraz, útil e informativa, pero que, por el paso del tiempo, se ha vuelto obsoleta, desfasada y perniciosa para la imagen del ser humano, pues, cómo "Espada de Damocles", es decir, cómo un peligro inminente, se encuentra inserta en el mundo informático y a un solo *click* de distancia para cualquier usuario de internet. Y eso ata perennemente a la persona a un pasado que quiere dejar de lado y que no viene al caso recordar.

A mayor abundamiento, la jurisprudencia del Tribunal Constitucional ha establecido una tipología del *Hábeas Data* inspirándose en clasificaciones dadas por la doctrina extranjera (Sagües, Puccinelli, entre otros). Así, en la RTC 6164-2007-HD/TC ha reconocido el denominado "Hábeas Data Supresorio", que, como dice esta resolución, busca eliminar la información sensible o datos que afectan la intimidad personal, familiar o cualquier otro derecho fundamental de la persona; y el "Hábeas Data Confidencial", que sirve para impedir que las personas no autorizadas accedan a una información que ha sido calificada como reservada. En este tipo, se incluye la prohibición de datos que por el paso del tiempo o por sentencia firme se impide su comunicación a terceros.[80]

En ambas categorías parece calzar perfectamente la pretensión de que se borren o, por lo menos, no esté al alcance de terceros (mediante procedimientos de desindexación o "anonimización", por ejemplo) aquellos datos que pueden vulnerar los derechos fundamentales. No obstante, será la casuística la que deberá resolver este tipo de

[80] RTC 6164-2007-HD/TC

controversias y, de ser el caso, establecer el contenido y delinear los criterios jurisprudenciales en relación con este derecho, para lo cual toca estar expectantes. Y es que, como señaló tempranamente Eguiguren Praeli, el *Hábeas Data* parece haber surgido para responder a las nuevas situaciones y realidades.[81] Ha sido en efecto así, conforme lo revisado a lo largo de este artículo.

Por lo demás, si bien el mismo está centrado en el derecho al olvido y su protección por el *Hábeas Data*, no debemos dejar de mencionar en la vía administrativa ya se viene protegiendo la cancelación y supresión de datos ante la Autoridad Nacional de Protección de Datos Personales - ANPDP, entidad creada por Ley 29733, Ley de Protección de Datos Personales. Esta entidad ha tenido un importante desarrollo jurisprudencial en la materia, como su par española, habiéndose interpuesto reclamaciones contra páginas web y también contra un motor de búsqueda como Google. A continuación, hacemos un rápido recuento de algunos pronunciamientos.

En el año 2013, primer año que entró en funciones, la ANPDP conoció tres casos en los que los reclamantes solicitaron la eliminación de sus datos publicados en la web. En dos de estos casos, correspondientes a los Expedientes 001-2013-PTT y 002-2013-PTT, concluyeron los procedimientos por haberse obtenido la tutela, al menos parcialmente. Se trató de los procesos reclamados contra la Asociación Movimiento Peruanos Sin Agua y contra Convergia Perú y Claro Perú, respectivamente.[82]

---

[81] EGUIGUIREN PRAELI, Francisco. "El Hábeas Data y su desarrollo en el Perú.". Derecho PUCP. 51. 1997, pp. 291 y 292. Fuente: http://revistas.pucp.edu.pe/index.php/derechopucp/article/view/6134/6155 Consulta: 30/10/2020.

[82] En el primero, la reclamante solicitó que se eliminen sus datos personales de las direcciones web http://www.lossinagua.org. y http://www.prensa.indígena, por haberse vulnerado su intimidad debido a que el presidente del Movimiento Peruanos Sin Agua difundió en diversos medios de comunicación frases ignominiosas adjuntando sus fotografías personales. La Resolución 017-2013-JUS/DGPDP, del 9 de octubre de 2013, que resolvió la cuestión dio por concluido el procedimiento trilateral de tutela como

En el año 2014, la ANPDT resolvió 14 reclamaciones referidas a la supresión de datos. Los reclamados fueron Sonico (en dos ocasiones), Hoovers, Editora el Comercio, Diario Grupo La República S.A., Personas Perú, Mercado Libre, Datos Perú Org. (en dos ocasiones también), Corporación Turística Peruana SAC, Google Perú SRL (blog verdades universitarias), páginas webs sistemas3.minjus.gob.pe/ y www.asesorempresarial.com, Facebook (Produce Lima Pesca) y Superintendencia de Banca, Seguros y AFP.

En cuatro ocasiones, en las reclamaciones contra Hoovers, Sonico, Corporación Turística Peruana SAC y Facebook, se declaró el abandono del procedimiento trilateral de tutela por no subsanarse las observaciones y se archivó la reclamación. En el caso contra Persona Perú se declaró improcedente la reclamación por incompetencia territorial. En el seguido contra Google Perú SRL se declaró improcedente la reclamación por tratarse de derechos referidos al honor que no corresponden a la vía administrativa. En el caso contra las páginas web sistemas3.minjus.gob.pe/ y www.asesorempresarial.com, se declaró improcedente la reclamación por carecer de sustento fáctico puesto que el tratamiento de datos personales había cesado.

consecuencia de haber obtenido la reclamante la tutela de su derecho de cancelación de sus datos personales del sitio web http://www.lossinagua.org. Sin embargo, desestimó la reclamación formulada por la reclamante respecto a la cancelación de los comentarios y publicación de imágenes contenidos en el foro del grupo de Yahoo, cuya dirección web es http//español.groups.yahoo.com/group/comandohaya/message/54388 y en el sitio web http://www.prensaindigena.org., por no ser el reclamado el responsable del tratamiento que en tales páginas web se dieron a sus datos personales. En el segundo caso, el reclamante solicitó la tutela directa a la ANPDP, alegando que la empresa CLARO PERU había proporcionado sus datos personales a la empresa CONVERGIA PERU sin contar con su autorización, con la finalidad de publicar dicha información personal en la guía de abonados de esta última. Al haberse verificado que la reclamada, en atención al reclamo, procedió al bloqueo y ulterior cancelación de los datos personales en el banco de datos personales alegado por el reclamante, cesando los hechos que ocasionaron la reclamación, la ANPDP, mediante la Resolución 032-2013-JUS/DGPDP, de 20 de noviembre de 2013, dio por concluido el procedimiento.

En el tercer caso, resuelto mediante Resolución 018-2013-JUS/DGPDP, de 9 de octubre de 2013, se declaró inadmisible la reclamación por incompetencia territorial.

En el caso seguido contra Mercado Libre se declaró la conclusión del procedimiento por haberse obtenido la tutela y se ordenó al responsable del sitio web el bloqueo y eliminación de los datos personales que puedan afectar al reclamante. Sucede que en este caso el reclamante solicitó la tutela directa a la Autoridad Nacional de Protección de Datos Personales y señaló que MercadoLibre Perú SRL no atendió debidamente su derecho de cancelación respecto de seis publicaciones de anuncios, ubicados en el sitio web www.mercadolibre.com.pe, y en los cuales se visualizó como número telefónico de contacto del anunciante el número telefónico del servicio móvil del reclamante. A este respecto, el reclamante sostuvo que no publicó ningún anuncio de alquiler o venta en el sitio web de la reclamada, ni realizó búsqueda alguna de compra. En este caso, la ANPDP entendió que la solicitud de supresión o cancelación implica el cese en el tratamiento de los datos personales a partir de un bloqueo de los mismos y su posterior eliminación[83], dándole un contenido al derecho de supresión.[84]

Mención aparte merecen los procedimientos administrativos trilaterales promovidos por dos reclamantes contra Datos Perú. Org., resueltos mediante las Resoluciones 074-2014-JUS/DGPDP y 075-2014-JUS/DGPDP, ambas del 24 de octubre de 2014. En estos, por primera vez se sancionó pecuniariamente a una empresa por infracción de la Ley de Protección de Datos Personales. La multa impuesta a Datos Perú. Org. ascendió a la suma total de 78,600 dólares

[83] Resolución N° 066-2014-JUS/DGPDP de 07 de agosto de 2014, fundamento 12.

[84] Las reclamaciones interpuestas contra Editora el Comercio y Diario Grupo La República S.A, dos de los más grandes medios de comunicación en el Perú, se desestimaron porque por versar sobre información de interés público y político; sin perjuicio a ello, la APDP dejó constancia que la información fue eliminada de las publicaciones online. En el segundo procedimiento promovido contra Sonico se declaró infundada la reclamación por insuficiencia de medios probatorios para acreditar actos contrarios a la LPDP. Asimismo, en la reclamación contra la Superintendencia de Banca, Seguros y AFP también se declaró infundada la reclamación por haberse acreditado que los tratamientos realizados por la Central de Riesgos de la SBS son conforme a lo establecido en la Ley de Protección de Datos Personales.

aproximadamente y fue un golpe muy duro para la empresa, que hasta tuvo que cerrar temporalmente.[85]

En el expediente resuelto mediante Resolución 074-2014-JUS/DGPDP, el reclamante solicitó la tutela directa a la Autoridad Nacional de Protección de Datos Personales y señaló que Google Perú no atendió debidamente su derecho de cancelación respecto de la publicación, ubicada en el sitio web "http://www.datosperu.org/" y en la cual se visualiza, en formato de documento portátil (PDF) y texto, una resolución administrativa del Ministerio del Interior que autorizó al Procurador Público encargado de los asuntos judiciales de la Policía Nacional del Perú a impugnar judicialmente las resoluciones supremas sobre ascenso y posterior pase al retiro por causal de renovación del reclamante.

El reclamante sostuvo que tal resolución administrativa fue dejada sin efecto mediante una resolución posterior, también del Ministerio del Interior. Sin embargo, este último documento no figura en internet perjudicando al reclamante.

Como dato resaltante la ANPDP consideró que la comunicación por transmisión, la difusión o cualquier otra forma que facilite el acceso a los datos personales por parte de terceros implica un tratamiento de datos; por lo que la conducta que consiste en publicar en un sitio web datos personales debe considerarse un tratamiento de esta índole.[86]

---

[85] En la página web www.datosperu.org se puede observar este mensaje: "El Portal de data abierta de Datos Perú, fue creado para promover la transparencia, servir de fuente de datos al periodismo de investigación y para facilitar negocios nacionales e internacionales. El portal ofrece información relativa a empresas, marcas registradas, normas y leyes peruanas así como datos de comercio exterior en detalle. Lanzado en 2011, este portal es una iniciativa de los que éramos un grupo de estudiantes peruanos en el extranjero. Este portal fue multado de manera notoria en el 2014 por la Autoridad Nacional de Protección de Datos Personales en un asombroso despliegue de pobre interpretación de la legislación en esa materia. Esta mala interpretación así como un afán de figuración y un notorio abuso de poder tuvieron como consecuencia el cierre temporal de este portal." Revisada el 08/02/2019.

[86] Resolución 074-2014-JUS/DGPDP, fundamento 14, segundo párrafo.

Añadió que cuando la LPDP desarrolla el concepto de tratamiento emplea los términos: "automatizado o no automatizado". La ANPDP considera que difundir información en un sitio web implica, conforme con los procedimientos técnicos e informáticos actuales, publicar dicha página en un servidor, así como realizar las operaciones necesarias para que resulte accesible a los usuarios de internet. Estas operaciones se efectúan, al menos en parte, de manera automatizada; por lo que la conducta que consiste en identificar a una persona por diversos tipos de información relativa, por ejemplo, a sus condiciones de trabajo, aficiones, información sindical, ideología política, o como en el caso, mediante una resolución administrativa, constituye un tratamiento total o parcialmente automatizado de datos personales.[87]Así concluyó que el tratamiento de datos personales sin consentimiento del titular constituye una afectación al derecho fundamental a la protección de datos personales, en su aspecto conocido como "autodeterminación informativa".

En la Resolución 075-2014-JUS/DGPDP, la ANPDP la resolvió un caso en el que el reclamante solicitó la tutela directa a la Autoridad Nacional de Protección de Datos Personales porque el sitio web "datosperu.org" no atendió debidamente su derecho de cancelación respecto de la publicación ubicada en el sitio web "http://www.datosperu.org/" y en la cual se visualiza en formato de documento portátil (PDF) y texto, la resolución que le impuso una sanción disciplinaria de destitución en su condición de ex funcionario de la Unidad de Tesorería del municipio donde laboraba.

El reclamante sostuvo que la referida resolución de destitución fue declarada nula en la sentencia de 20 de febrero de 2002 expedida por la Sala de Derecho Constitucional y Social Transitoria de la Corte Suprema, que dispuso un nuevo proceso administrativo disciplinario el cual concluyó con la resolución que declaró la prescripción del mismo.

[87] Resolución 074-2014-JUS/DGPDP, fundamento 14, tercer párrafo.

En este caso, la ANPDP declaró fundada la reclamación formulada contra el sitio web "http://www.datosperu.org/" por: (i) Infracción del artículo 38, numeral 2, literal a) de la Ley N° 29733, Ley de Protección de Datos Personales, tipificada como "grave", al haberse verificado que contravino los principios de consentimiento, calidad y proporcionalidad; e imponerle la sanción de multa correspondiente a quince (15) Unidades Impositivas Tributarias, conforme con lo establecido por el artículo 39 numeral 2 de la referida Ley. (ii) Infracción del artículo 38, numeral 2, literal c) de la Ley N° 29733, Ley de Protección de Datos Personales, tipificada como "grave", al haberse verificado que contravino el ejercicio de los derechos del titular de datos personales y obstaculizado el ejercicio de su derecho de cancelación; e imponerle la sanción de multacorrespondiente a quince (15) Unidades Impositivas Tributarias, conforme con lo establecido por el artículo 39 numeral 2 de la referida Ley.

En el año 2015, la ANPDP resolvió 17 casos en materia de supresión de datos. Los reclamados fueron Editora El Comercio S.A., Ministerio de Economía y Finanzas. Programa de Fondo de Cooperación para el Desarrollo Social, Superintendencia Nacional de los Registros Públicos (SUNARP), Instituto Peruano de Energía Nuclear (IPEN), Sitio web https://peru.rutificador.com/, Empresa Peruana de Servicios Editoriales S.A. Editora Perú., Hibu Perú S.A.C. y América Móvil Perú S.A.C., Unidad de Gestión Educativa Local (UGEL) N° 6., GOOGLE Inc. y Google Perú S.R.L., Diners Club Perú S.A., Club Internacional Arequipa y Diners Club Perú S.A., Superintendencia de Banca, Seguros y AFP (SBS)., Consejo Nacional de la Magistratura (CNM), Hospital Regional Manuel Núñez Butrón (HRMNB), América Móvil Perú S.A.C. y Superintendencia Nacional de Educación Superior Universitaria – SUNEDU.

El resuelto contra Google repercutió en los medios de comunicación como el primero donde se aplica el derecho al olvido en el Perú. En este caso el reclamante fue objeto de una denuncia anónima que posteriormente fue sobreseída. Sin embargo, en una página web,

aparecía la noticia si se buscaba desde Google Search. Solicitó a Google la cancelación de sus datos, pero este le respondió mediante correo electrónico que se ponga en contacto con el sitio web y que "Si emprende acciones legales contra este sitio que den lugar a la retirada del material, ese cambio se reflejará en nuestros resultados de búsqueda tras el próximo rastreo del sitio." (Resolución 045-2015-JUS/DGPDP, punto 1.7).

La ANPD, luego de hacer suyos los criterios del Caso Costeja, señaló que "…el análisis de la protección de los datos personales no puede olvidar que los robots de búsqueda o indexadores pueden agregar páginas web o enlaces, sin importar sus formatos, a la lista de resultados de los buscadores, lo que ocasiona un efecto divulgativo multiplicador en internet que puede llamarse 'hipervisibilización' de información personal de ciudadanos peruanos sin trascendencia pública, que constituyen fenómenos no tradicionales que pueden, por sí mismos, generar consecuencias indeseadas e ilegítimas, al margen de que se refieran a publicaciones legítimas."[88]

Añadió que "Al permitirse que los robots de búsqueda puedan indexar los datos personales y estos sean difundidos en los resultados de búsqueda hipervisibles, está vulnerándose el derecho del reclamante a no ser enlazado a la información materia de reclamación (que en este caso, lo relaciona con la presunta comisión de un delito, el cual ha sido archivado por la autoridad judicial competente y por lo cual incluso se borraron sus antecedentes penales y judiciales) en los resultados de los motores de búsqueda por sus 'nombres y apellidos'; información que no resulta de interés para el público; de forma que el tratamiento de indexación realizado por la reclamada debe cesar."[89]. Relacionó finalmente el caso con una vulneración del derecho a la privacidad y dispuso el bloqueo de toda noticia relacionada con la denuncia.

[88] p. 19
[89] p. 20

Advertimos así que, en el Perú, la protección del olvido digital está garantizada, siendo esto necesario para que el ser humano siga adelante y no se encuentre encadenado a un pasado que quiere dejar atrás. Mayer-Schönberger, traducido por Álvarez, apunta al respecto que "… como humanos no viajamos a través del tiempo de un modo ignorante. Con la capacidad del recuerdo somos capaces de comparar, aprender y capaces de experimentar el tiempo como un cambio. Igualmente importante es la habilidad de olvidar, de deshacernos de las cadenas del pasado y vivir en el presente".[90] Sin embargo, "…el recuerdo digital nos amenaza como individuos y como sociedad, en lo relativo a nuestra capacidad para aprender y razonar y actuar en el tiempo, así como también nos expone a la 'potencialmente devastadora' sobrerreacción humana ante nuestro pasado."[91]

Se trata entonces de que el Derecho ponga los correctivos necesarios frente al asedio tecnológico, siendo el reconocimiento del derecho al olvido una herramienta dinámica, acorde con los tiempos y muy útil en este sentido. Y es que, como dice Martín Pallín, "Un ordenador también debe olvidar; debe tener por lo menos esa faceta humana y pasar por alto algunas cosas una vez que ha pasado cierto tiempo, una vez que ya no son necesarios esos datos para el cumplimiento de los fines para los que se ha creado el archivo".[92] Se trata así, de humanizar la tecnología.

[90] Citado en ÁLVAREZ CANO. Op. Cit. p. 69.

[91] Op. Cit., p. 70.

[92] Martín Pallín, 1994. En Masciotra, 2012. Citado en SINDERLEIB, Laura. "El derecho al olvido y la persistencia de la memoria" Fuente: file:///C:/Users/Usuario/Downloads/Dialnet-ElDerechoAlOlvidoYLaPersistenciaDeLaMemoria-5985068.pdf Consulta: 30/10/2020.

EL DERECHO AL OLVIDO EN EL PROCESO DE *HÁBEAS DATA* EN EL PERÚ

Astrid Kelly Cabezas Poma*

1. Introducción

¿Existe un derecho a olvidar? En los últimos años, el crecimiento tecnológico ha facilitado la creación de bases de datos que cruzan y almacenan información personal, crediticia, judicial, etc. Asimismo, dicho crecimiento también ha permitido la proliferación de motores de búsqueda que brindan información que en muchos casos linda con lo personal. Si bien ello se realiza en el ejercicio de los derechos a la libertad de expresión e información, lo cierto es que interviene en otros derechos, como el honor, privacidad, libre desarrollo de la personalidad, vida digna, igualdad y no discriminación, entre otros.

En este escenario, el derecho al olvido surge como un límite a dicha intervención, pues garantiza que la información personal almacenada en bases de datos o motores de búsqueda de la web, pueda retirarse o eliminarse. Así, la protección de este derecho se convierte en un presupuesto importante para la efectividad de otros derechos fundamentales, pero ¿cuál sería su límite?

* Abogada por la Universidad de San Martín de Porres. Con estudios de maestría en la Pontificia Universidad Católica del Perú. Asesora del Tribunal Constitucional del Perú.

De otro lado, el derecho al olvido no se encuentra reconocido de manera expresa en nuestra Constitución. Por lo que cabe preguntarnos si ¿es posible que este derecho pueda tener protección judicial en nuestro ordenamiento jurídico? Si la respuesta es afirmativa, ¿lo sería de manera autónoma o a través de otro derecho? y ¿bajo qué tipo de proceso judicial?

El proceso de hábeas data es un proceso constitucional a través del cual se garantizan los derechos de acceso a la información pública y a la autodeterminación informativa. Teniendo en cuenta que el derecho a la autodeterminación informativa garantiza la solicitud de cambiar, modificar o eliminar la información privada almacenada en bases de datos públicos o privados, cabe preguntarnos si ¿es posible considerar que el proceso de hábeas data garantice el derecho al olvido?

Estas interrogantes serán respondidas en el presente trabajo; para lo cual se analizarán las características del derecho al olvido, sus titulares, los obligados, el contenido de las obligaciones que genera, sus límites, y finalmente, su protección judicial.

2. El derecho al olvido

El derecho al olvido es un derecho nuevo, que recientemente viene siendo reconocido en diversos ordenamientos jurídicos frente a los avances tecnológicos. En Europa, Tribunal de Justicia de la Unión Europea reconoció jurisprudencialmente este derecho, en el caso Costeja contra España, en el año 2014. Otros países recientemente también lo han venido incorporando a sus ordenamientos internos. En el Perú, este derecho no se encuentra reconocido de manera expresa en el texto constitucional vigente, sin embargo, su protección puede serlo a nivel interpretativo.

En efecto, en el ordenamiento jurídico peruano, los derechos fundamentales se encuentran reconocidos de manera expresa o vía interpretativa, apelando a la opción principista del artículo 3 de la

Constitución, a los instrumentos internacionales sobre derechos humanos, o también a través de una fórmula sistémica[1].

Los derechos reconocidos de manera expresa[2] se encuentran en el texto constitucional, y entre ellos se observan los derechos a la libertad de expresión e información (artículo 2 inciso 4), libre desarrollo de la personalidad (artículo 2 inciso 1), etc.

Por su parte, a nivel interpretativo[3], los derechos fundamentales pueden incorporarse en virtud de los derechos reconocidos en instrumentos internacionales, a partir de la IV disposición final y transitoria de la Constitución; como por ejemplo, el derecho a la alimentación, reconocido en el Pacto Internacional de Derechos Económicos, Sociales y Culturales[4]. También se incorporan a partir del artículo 3 de la Constitución, y nacen de la dignidad, los principios de soberanía del pueblo, del Estado democrático de derecho y de la forma republicana de gobierno; un ejemplo es el derecho a la verdad[5]. De otro lado, los derechos también pueden reconocerse como parte del contenido implícito de otro derecho fundamental, reconocido de manera expresa en la Constitución. Estos derechos se fundamentan en el principio de seguridad jurídica, en tanto que evitan el reconocimiento ilimitado de nuevos derechos. De esta manera, la incorporación de nuevos derechos al ordenamiento jurídico, en virtud del artículo 3 de la Constitución es excepcional. Un ejemplo es el derecho a la prueba, que se considera parte del contenido del derecho al debido proceso[6].

[1] Tribunal Constitucional, STC 6546-2006-PA/TC, 4.

[2] El reconocimiento expreso de los derechos fundamentales tiene su fundamento en el principio democrático, dado que el legislador, quien representa al pueblo, los reconoce al promulgar el texto constitucional o vía reformas constitucionales.

[3] El reconocimiento de los derechos fundamentales a nivel interpretativo tiene su fundamento en el principio de dignidad, ya que el juez, adaptándose a las nuevas circunstancias, reconoce el derecho a fin de garantizar mínimos materiales que permitan a la persona una vida digna

[4] Tribunal Constitucional, STC 1470-2016-PHC/TC.

[5] Tribunal Constitucional, STC 2488-2002-PHC/TC

[6] Tribunal Constitucional, STC 3271-2012-PA/TC.

Teniendo en cuenta lo expuesto, se observa que en el caso del derecho al olvido, este no se encuentra reconocido de manera expresa en nuestro ordenamiento jurídico; sin embargo, sí puede serlo a nivel interpretativo. A fin de determinar bajo qué modalidad, vía interpretativa, puede ser reconocido, a continuación analizaremos en qué consiste este derecho.

2.1. El titular

La titularidad de un derecho fundamental es la atribución a favor de una persona, a partir de la cual se generan diversas posiciones jurídicas frente al poder público o los particulares. Estas posiciones jurídicas involucran obligaciones a favor de la persona[7]. Dicha persona es la titular de un derecho fundamental y puede ser física o jurídica[8].

En ese sentido, el titular del derecho al olvido es toda persona, física o jurídica, cuyos datos personales se encuentran almacenados en bases de datos o motores de búsqueda, del poder público o de particulares. Dicha información debe haber estado publicada o ser de acceso al público, en un tiempo determinado; y, debe afectarle al titular de dichos datos.

Al respecto, los datos personales son, como lo define el artículo 2 inciso 4 de la Ley 29733, Ley de protección de datos personales, "[t]oda información sobre una persona natural que la identifica o la hace identificable a través de medios que pueden ser razonablemente utilizados".

Esta información puede provenir del mismo titular, quien *motu proprio* publica la información a través de la base de datos o motores de búsqueda. O, también puede originarse en una tercera persona, quien en el ejercicio de su derecho a la libertad de información o expresión,

---

[7] Las posiciones jurídicas de derecho fundamental generan relaciones entre el titular del derecho y los obligados, de modo que surgen un conjunto de obligaciones y facultades de ambas partes.

[8] Alexy, Robert, "Teoría de los derechos fundamentales". Centro de Estudios Políticos y Constitucionales, 2da Edición, Madrid, 2012, pág. 164.

publica información relacionada con los datos personales del titular, a través de una base de datos o motor de búsqueda. A manera de ejemplo, en el primer caso, el titular publica personalmente sus datos en un sitio web que conserva la información a través de su historia; y, en el segundo supuesto, una tercera persona publica la información del titular de la información en una nota informativa o un blog difamatorio, que es accesible a través de un motor de búsqueda[9].

Asimismo, la información publicada en la base de datos o motor de búsqueda debe afectarle al titular de dicha información, dado que no se trata de la salvaguarda de simples intereses individuales que impliquen un mero deseo, por lo que el titular debe acreditar la existencia de efectos nocivos hacia su persona[10].

En síntesis, el titular del derecho al olvido es toda persona, física o jurídica, a favor de la cual se le genera, como posición jurídica, la facultad de solicitar la eliminación o el retiro de información personal, almacenada en bases de datos o motores de búsqueda en manos del poder público o los particulares, independientemente de que haya sido publicada por su propia voluntad o de terceros, y siempre que le ocasionen efectos nocivos.

2.2. Los obligados

El obligado de un derecho fundamental es todo sujeto, conformado por el poder público o los particulares, responsable de respetar y garantizar dicho derecho[11].

---

[9] Pérez Gómez, Ana María. Cuando google juega con la información privada…El derecho al olvido digital en Europa, una lucha de titanes. En Revista *La propiedad* inmaterial. Colombia, N° 22, julio - diciembre 2016, p. 179.

[10] Puccinelli, Oscar, "El derecho al olvido en el derecho a la protección de datos. Con especial referencia a su vigencia en Internet. Pensamiento Constitucional N° 21, 2016, pág. 248.

[11] Alexy, Robert, "Teoría de los derechos fundamentales". Centro de Estudios Políticos y Constitucionales, 2da Edición, Madrid, 2012, pág. 164.

En esa línea, el obligado de respetar y garantizar el derecho al olvido está constituido por cualquier autoridad o funcionario (el poder público), o también por los sujetos privados (los particulares), responsable del tratamiento de los datos personales del titular del derecho.

Al respecto, el artículo 2 inciso 19 de la Ley 29733, Ley de protección de datos personales, define al tratamiento de datos personales como "Cualquier operación o procedimiento técnico, automatizado o no, que permite la recopilación, registro, organización, almacenamiento, conservación, elaboración, modificación, extracción, consulta, utilización, bloqueo, supresión, comunicación por transferencia o por difusión o cualquier otra forma de procesamiento que facilite el acceso, correlación o interconexión de los datos personales".

Cuando el responsable es la autoridad o funcionario público, estamos ante la eficacia vertical del derecho al olvido, en la medida que la autoridad o el funcionario representan al Estado, y tienen obligaciones frente al titular de la información personal. A manera de ejemplo, los bancos de datos de los órganos jurisdiccionales que contienen sentencias judiciales de procesos concluidos pueden ser sujetos obligados del derecho, dado que poseen información que identifica o hace identificable a las personas titulares de la información. Tales sentencias judiciales, en tanto que no estén sujetos a reserva, son de acceso al público; sin embargo, con el transcurso del tiempo, dicha información podría limitar los derechos al libre desarrollo de la personalidad, proyecto de vida, trabajo, entre otros, del titular de la información. Consecuentemente, el órgano jurisdiccional, como parte del Estado, podría convertirse en el obligado a garantizar el derecho al olvido, lo cual corresponderá evaluarse en el caso concreto, teniendo en cuenta los derechos que convergen y las particularidades del caso, conforme a lo que se expondrá más adelante.

Por su parte, el sujeto obligado de respetar y garantizar el derecho al olvido también puede ser cualquier particular, siempre que sea responsable del tratamiento de datos personales. De esta forma, el sujeto obligado puede ser una persona natural que publica en la web

información personal de una determinada persona (ej. Las personas que publican informes en sus blogs de Internet). También puede ser una persona jurídica que recopila datos personales relacionados con créditos, préstamos o avales de un sujeto determinado (ej. Infocore SAC[12]).

En esta línea, se observa que los motores de búsqueda (entiéndase Google, Yahoo, Bing, etc.) también pueden ser sujetos obligados a respetar y garantizar el derecho al olvido, por cuanto son responsables del tratamiento de datos personales, al recopilar, registrar, organizar, almacenar y conservar información que podría contener datos personales, publicada en la web por terceros. De hecho, para el Tribunal de Justicia de la Unión Europea, los motores de búsqueda afectan en un grado más elevado los derechos a la vida privada y la protección de datos personales, en comparación con los particulares que editan las páginas web, debido a que con la indexación facilitan el acceso de los internautas a las páginas web que contienen la información privada, desempeñando un papel decisivo para la difusión de la información privada[13].

Sin embargo, cabe destacar que también hay sectores que consideran que los motores de búsqueda no pueden ser obligados a eliminar de su sistema información alguna, dado que solo facilitan el acceso a la información publicada. Este punto de vista fue adoptado por la Suprema Corte Federal de Brasil, en el caso Maria da Graça Xuxa Meneghel contra Google, en la que señaló que "No hay razón para demandar a quien solo facilite el acceso a este acto, que, hasta entonces, ha estado

[12] Según lo publicado en la web de la Autoridad Nacional de Protección de datos personales, Infocore SAC, recopila datos personales – de tipo económico financieros y de seguros - de los prospectos de clientes para evaluar el otorgamiento de préstamos, tarjeta de crédito y otros productos financieros.

En https://prodpe.minjus.gob.pe/prodpe_web/BancoDato_verResultado recopilado el 28 de agosto de 2020.

[13] Tribunal de Justicia de la Unión Europea, 13 de mayo de 2014, Sentencia en el asunto C-131/12, Google Spain, S.L. y Google Inc. Contra la Agencia Española de Protección de Datos (AEPD) y Mario Costeja Gonzáles, párr. 86 – 87.

disponible públicamente en la red para su difusión"[14]. Al respecto, se advierte que en la medida que los motores de búsqueda realizan el tratamiento de información (recopilan, almacenan y conectan a información publicada en otros sitios web), sí podrían ser sujetos obligados del derecho al olvido.

Ahora bien, los sujetos particulares, obligados de garantizar y respetar el derecho al olvido, son responsables, independientemente si tienen o no su sede u oficina principal en el territorio peruano. Ello es así debido a que, en virtud del modelo de Estado democrático y social de derecho (artículo 3 y 43 de la Constitución), y del deber constitucional del Estado establecido en el artículo 44[15] de la Constitución, todos los derechos fundamentales tienen vigencia efectiva, lo que involucra que los titulares de la información personal que se vean afectados, puedan reclamar su protección frente a los particulares que hayan tratado sus datos personales en el territorio nacional.

Finalmente, cuando el responsable del tratamiento de los datos personales es un particular, estamos ante la eficacia horizontal, dado que estos sujetos tienen obligaciones de respetar y garantizar el derecho al olvido, dependiendo de la posición en la que se encuentran respecto del titular del derecho.

En suma, el sujeto obligado del derecho al olvido, está conformado por el Estado o cualquier privado responsable del tratamiento de los datos personales del titular del derecho. En el caso del Estado, está conformado por todos los niveles, dado que el responsable puede

[14] Recuperado el 25 de agosto de 2020, de la página web del Supremo Tribunal Federal de Brasil: "não tem motivo para demandar contra aquele que apenas facilita o acesso a esse ato que, até então, se encontra publicamente disponível na rede para divulgação". (traducción propia)

En: http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=276284

[15] Constitución Política del Perú

Artículo 44.- Deberes del Estado Son deberes primordiales del Estado: defender la soberanía nacional; garantizar la plena vigencia de los derechos humanos (…).

ser cualquier autoridad o funcionario que trate datos personales. Y, en el caso de los particulares, está conformado por toda persona, natural o jurídica, que trate los datos personales, independientemente de que no sea el emisor directo de la publicación de la información, o tenga su sede principal fuera del territorio nacional.

2.3. El contenido de la obligación

El contenido u objeto de la obligación es el ámbito de protección del derecho fundamental. Y, está conformado por un haz de obligaciones positivas o negativas que se derivan de la posición jurídica surgida de la relación entre el titular del derecho y el obligado.[16]

En tal sentido, el derecho al olvido garantiza la obligación de que la información de índole personal que se encuentra almacenada en bases de datos o motores de búsqueda del sujeto obligado, pueda ser eliminada o retirada. Dicha información debe haber sido de acceso al público y por un tiempo determinado.

Ejemplos de información personal cubiertas por el derecho al olvido pueden ser el historial crediticio, las condenas cumplidas, información publicada en la web o las que contienen los motores de búsqueda, entre otras.

Un tema controvertido es si la información personal publicada debe carecer de interés o relevancia pública. Para el Tribunal de Justicia de la Unión Europea, la información privada del demandante debe carecer de relevancia pública para que sea retirada bajo el amparo del derecho al olvido; pues de lo contrario, si es de interés preponderante del público, debe continuar siendo de libre acceso[17]. Opinión diferente

[16] Alexy, Robert, "Teoría de los derechos fundamentales". Centro de Estudios Políticos y Constitucionales, 2da Edición, Madrid, 2012, pág. 164.

[17] Tribunal de Justicia de la Unión Europea, 13 de mayo de 2014, Sentencia en el asunto C-131/12, Google Spain, S.L. y Google Inc. Contra la Agencia Española de Protección de Datos (AEPD) y Mario Costeja Gonzáles párr. 98. En dicho caso, el Tribunal

tuvo el Instituto Nacional de Transparencia, Acceso a la Información y Protección de datos personales Tribunal de México, quien consideró en un caso que debía garantizarse el retiro de información personal vinculada con delitos de corrupción, en tanto que el sujeto obligado no había justificado que la publicación de la información fuera necesaria[18]. En este caso, la institución mexicana no evaluó directamente (de oficio) la relevancia pública de la información que se solicitaba retirar, sino la actuación del obligado.

Al respecto, se advierte que frente a la solicitud de eliminación o retiro de información personal publicada en bases de datos o medios electrónicos, resulta imperioso el análisis de la relevancia de la información. Y es que, teniendo en cuenta que el derecho al olvido, al igual que los demás derechos fundamentales, puede ser limitado, dicha restricción corresponde ser analizada en cada caso concreto, teniendo en cuenta las particularidades del asunto, como la relevancia pública de la información publicada, la misma que será analizada en el siguiente apartado.

De otro lado, el tiempo que debe transcurrir para que la información personal pueda ser retirada o eliminada, bajo el amparo del derecho al olvido, no es en estricto un número de años. Por ejemplo, para el Tribunal de Justicia de la Unión Europea, el tiempo que debe

---

consideró que la información referida al remate del bien inmueble del señor Costeja en una subasta inmobiliaria por deudas a la Seguridad Social, no era de interés preponderante del público, por lo que concluyó que el demandante tenía el derecho a que ya no se vincule su nombre en el motor de búsqueda.

[18] Instituto Nacional de Transparencia, Acceso a la Información y Protección de datos personales de México. Resolución 94/14. Caso Carlos Sánchez de la Peña contra Google México.

En este caso, el empresario Carlos Sánchez de la Peña solicitó que Google México eliminara los vínculos que permitían el acceso a información que lo identificaba y vinculaba con delitos de corrupción. En este caso, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de datos personales Tribunal de México consideró que Google México no garantizó los derechos de oposición y cancelación del tratamiento de los datos personales del empresario.

conservarse la información depende de los fines para los cuales se encuentran almacenados o tratados, lo que involucra el análisis de cada caso concreto[19]. Por su parte, el Tribunal Constitucional peruano, ha considerado que el tiempo de publicación de información referida al cumplimiento o incumplimiento de obligaciones de naturaleza civil, comercial o tributaria contenidas en un banco de datos que difunde reportes, no debe ser más allá de lo estrictamente necesario, a fin de evitar la vulneración del derecho a la intimidad y la autodeterminación informativa[20]. En todo caso, la determinación del tiempo debe obedecer a la evaluación de cada caso, siguiendo estándares de razonabilidad, donde se analicen los fines y la necesidad de la publicidad de la información personal.

Finalmente, el contenido del derecho al olvido se fundamenta en el principio de dignidad, dado que garantiza mínimos materiales, como es la eliminación o retiro de una información que limita el goce y ejercicio de otros derechos fundamentales, como a la vida privada, al libre desarrollo de la personalidad, igualdad, al trabajo, entre otros. Asimismo, también tiene como fundamentos la plena vigencia de los derechos fundamentales (artículo 44 de la Constitución) y el modelo de Estado democrático y social de derecho (artículos 3 y 43 de la Constitución), ya que contribuye con el goce efectivo de otros derechos.

[19] Tribunal de Justicia de la Unión Europea, 9 de marzo de 2017, Sentencia en el asunto C-398/15, Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce / Salvatore Manni, párr. 45. En este caso, Salvatore Manni había solicitado que se elimine del registro de la Camera di Commercio de Lecce la información que señalaba que había sido administrador de otra sociedad declarada en concurso de acreedores en 1992 y liquidada en 2005. Salvatore señalaba que dicha información ocasionaba que no pudiera vender inmuebles en un complejo turístico en Italia que había construido. El Tribunal de Justicia consideró que no correspondía el retiro de la información, toda vez que el registro de sociedades sólo contenía un número limitado de datos personales, y era justificado que las personas que deciden participar en intercambios económicos que sólo ofrecen su patrimonio social como garantía frente a terceros, estén obligadas a hacer públicos sus datos relativos a su identidad y funciones dentro de aquélla.

[20] Tribunal Constitucional del Perú, STC 0831-2010-PHD/TC, fund. 11.

2.4. Los límites

El ejercicio del derecho al olvido puede verse limitado por otros derechos fundamentales, como los derechos a la libertad de expresión, información, empresa, etcétera. A fin de analizar los límites del derecho al olvido, reconstruiremos los conflictos que se presentan a su alrededor, para lo cual aplicaremos el juicio de proporcionalidad en sentido estricto, propuesto por Robert Alexy[21], que ha sido ampliamente aplicado por el Tribunal Constitucional peruano en su jurisprudencia, el cual nos permitirá identificar el grado de intervención y optimización de los derechos involucrados.

Por lo que respecta al derecho al olvido, éste permite la garantía plena de los derechos a la igualdad y no discriminación, libre desarrollo de la personalidad, trabajo, entre otros.

En efecto, el derecho al olvido garantiza el derecho a la igualdad y no discriminación, en la medida que evita un trato diferente en perjuicio de una persona cuya información personal sobre situaciones sucedidas con anterioridad, se encuentre publicada y sea de acceso al público. De igual forma, el derecho al olvido posibilita el ejercicio efectivo del derecho al libre desarrollo de la personalidad, dado que el retiro de la información personal publicada permite que el titular de dicha información pueda realizar plenamente su proyecto de vida, sin que se le denieguen oportunidades o se le impongan obstáculos a causa de una estigmatización originada en la información personal publicada. Asimismo, el derecho al olvido coadyuva al goce del derecho al trabajo, pues el retiro de la información personal almacenada en bases de datos o motores de búsqueda de acceso al público evita que se le estigmatice y

[21] El examen del principio de proporcionalidad en sentido estricto evalúa lo siguiente: "Cuanto mayor es el grado de la no satisfacción o de afectación de uno de los principios, tanto mayor debe ser la importancia de la satisfacción del otro." En Alexy, Robert, "Epílogo a la teoría de los derechos fundamentales". Revista Española de Derecho Constitucional, Año 22, Núm. 66, setiembre-diciembre 2002, pág. 31.

deniegue el acceso a puestos de trabajo, por los antecedentes indicados en dicha información.

En cuanto al posible conflicto entre el derecho al olvido y los derechos a la libertad de expresión e información, ello es debido a que las libertades de expresión e información garantizan la difusión de opiniones, expresiones, datos o noticias, que sin embargo, el derecho al olvido garantizaría su retiro.

Al respecto, los derechos a la libertad de expresión e información se encuentran reconocidos en el artículo 2 inciso 4 de la Constitución. Así, estos derechos garantizan, en el caso del derecho a la libertad de expresión, la libre comunicación de ideas y opiniones, y en cuanto al derecho a la libertad de información, la libre comunicación de noticias y datos, incluyendo el acceso a ellos[22]. Estos derechos son considerados la piedra angular de todo Estado democrático, por lo que uno de los fundamentos de los derechos a la libertad de expresión e información es el principio de la democracia. Asimismo, conforme lo ha señalado la Corte Interamericana de Derechos Humanos, el derecho a la libertad de expresión, entendido como de información y expresión en sentido estricto, se rige bajo el principio de máxima divulgación[23], en virtud del cual se garantiza la difusión de la mayor cantidad de información, aunque con límites, los cuales deben ser evaluados de manera particular, a través de un examen de idoneidad, necesidad y proporcionalidad[24].

Para el análisis particular de los límites del derecho a la libertad de expresión, resulta relevante el tipo de información personal que se

[22] Defensoría del Pueblo, "Situación de la libertad de expresión en el Perú". Serie de Informes defensoriales, Informe N° 48, Lima, 2000, pág. 8-12.

[23] Corte Interamericana de Derechos Humanos. Caso Gomes Lund y otros vs. Brasil, 2010, párr. 199.

[24] Corte Interamericana de Derechos Humanos. Caso Fontevecchia y D'Amico vs. Argentina, 2011, párr. 51.

encuentra publicada en una base de datos o motor de búsqueda; esto es, si tiene relevancia pública o no.

Cuando la información personal publicada no tiene relevancia pública, se observa que, si bien en su momento se garantizó plenamente o en grado alto los derechos a la libertad de expresión o información; con el paso del tiempo, dicha información ya no alcanza, con el mismo grado, su fundamento, el cual es el principio democrático, en la medida que dicha información no aporta de manera significativa en el escrutinio de la población para participar en el Estado. En esa línea, para el Tribunal de Justicia de la Unión Europea, los datos personales pueden ser conservados, pero por un período no superior al necesario, de modo que reconoce que la información tiene relevancia en su momento, pero con el transcurso del tiempo, puede disminuirse[25].

No obstante, se advierte que esta información interviene en un grado elevado los derechos a la igualdad y no discriminación, libre desarrollo de la personalidad, trabajo, y otros, debido a que la persona titular de la información es tratada de manera desigual, no puede realizarse conforme a su plan de vida y su acceso a puestos laborales es obstaculizado, únicamente debido al estigma que le genera información de índole personal publicada.

De esta manera, se observa que, por un lado, la información personal publicada, y sin relevancia pública, con el paso del tiempo garantiza los derechos a la libertad de expresión e información (atendiendo a su fundamento), en un grado medio o menor. Sin embargo, por el otro, interviene en un nivel grave o alto los derechos a la igualdad y no discriminación, libre desarrollo de la personalidad y trabajo. Por lo tanto, resulta razonable y necesario el retiro o eliminación de dicha información, garantizada por el derecho al olvido. Con ello, se alcanzan

[25] Tribunal de Justicia de la Unión Europea, Sentencia en el asunto C-398/15, Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce / Salvatore Manni.

los fundamentos del derecho al olvido, los cuales son el principio de dignidad, la plena vigencia de los derechos fundamentales y la concretización del modelo de Estado democrático y social de derecho.

Por otro lado, cuando la información personal publicada sí tiene relevancia pública, dicha publicidad se encuentra garantizada plenamente (en un grado alto) por los derechos a la libertad de expresión e información. Ello en la medida que permite la comunicación de ideas, opiniones, noticias y datos, y se conecta directamente con su fundamento que es el principio democrático, al permitir el acceso a información que puede ser útil a la ciudadanía para su participación en el Estado. Y, en este escenario, la garantía del principio de la democracia se vincula con otros bienes jurídicos protegidos de la sociedad, como el presupuesto público, la justicia social, la protección de derechos fundamentales de la sociedad, etcétera, en la medida que si la información personal se refiere a la realización de delitos que tienen de por medio los recursos del Estado (como procesos judiciales por tráfico de influencias, malversación de fondos, etc.), violaciones de derechos humanos (como la comisión de esterilizaciones forzadas, crímenes de lesa humanidad, genocidios, etc.), entre otros, resulta determinante para la toma de decisiones de la población en su participación en el Estado.

Ahora bien, con el transcurso del tiempo, los derechos a la libertad de expresión e información continúan siendo garantizados con el mismo nivel, pues se sigue alcanzando el principio democrático en el mismo grado, debido a que la información publicada continúa siendo útil para la toma de decisiones de la ciudadanía en su participación en el Estado.

Sin embargo, la publicación de la información personal, de relevancia pública, interviene en un grado elevado o alto en los derechos a la igualdad y no discriminación, libre desarrollo de la personalidad, trabajo, entre otros, de la persona titular de la información privada, en el mismo tenor del escenario anterior (publicación de información personal que no es de relevancia pública).

Así las cosas, se advierte, por un lado, que la información personal publicada, y con relevancia pública, aún con el paso del tiempo, continúa garantizando en un grado alto o elevado los derechos a la libertad de expresión e información, en conexión con el principio de la democracia y los demás bienes jurídicos y derechos fundamentales colectivos que se busca proteger. Y, por el otro, se observa que interviene en un grado alto los derechos a la igualdad y no discriminación, libre desarrollo de la personalidad y trabajo de titular de la información. Por lo tanto, frente al empate, resulta razonable que se continúe con la transmisión de la información personal publicada.

La justificación de la proporcionalidad advertida es debido a que las razones de la intervención (libertad de expresión e información, principio de la democracia, derechos y bienes jurídicos de la sociedad) son tan fuertes como las razones en su contra (los derechos a la igualdad, libre desarrollo de la personalidad y el trabajo)[26], lo que apuesta por la continuidad de la intervención. Además, en términos de Hábermas, el principio de la democracia puede imponerse frente a los derechos del titular de la información personal publicada, en la medida que se justifica a la luz del principio del principio de la máxima divulgación, bienes jurídicos como el presupuesto público, y los derechos fundamentales de la sociedad[27]. Aunado a ello, ante el caso de empate surgido, el principio de máxima divulgación juega a favor de los derechos a la libertad de expresión e información, incrementando la carga argumentativa a favor de este derecho de cara a la colisión que se presenta.

[26] En casos de empate, Alexy señala "si las razones para la intervención son tan fuertes como las razones que juegan en su contra, la intervención no es desproporcionada". Alexy, Robert, "Epílogo a la teoría de los derechos fundamentales". Revista Española de Derecho Constitucional, Año 22, Núm. 66, setiembre-diciembre 2002, pág. 45.

[27] Habermas considera que un bien colectivo puede imponerse frente a un derecho, en la medida que dicho bien colectivo se justifique a la luz de principios. En Habermas, Jurgen, "Facticidad y validez", Editorial Trotta, Cuarta edición, 2005, pág. 332.

Otro límite del derecho al olvido es el derecho a la libertad de empresa. Este último se encuentra reconocido en los artículos 58 y 59 de la Constitución, y garantiza las libertades de: creación de empresa y acceso al mercado, organización, competencia y cesar las actividades[28]. En ese sentido, la publicidad de información personal permite que las personas jurídicas o naturales, traten la información en sus bases de datos o motores de búsqueda, y obtengan ingresos económicos de ello, conforme a su organización en el mercado. Empero, con el transcurso del tiempo, el grado de protección del derecho a la libertad de empresa es medio o menor que alto, debido a que el sujeto encargado de tratar la información, ya obtuvo ingresos económicos de dicha información, y su retiro no involucraría una prohibición absoluta del tratamiento de información de otros sujetos o respecto de nueva información del titular.

Por tal motivo, dado que la publicidad de la información personal en un tiempo prolongado, por un lado, afecta en un grado elevado o alto en los derechos a la igualdad y no discriminación, libre desarrollo de la personalidad, trabajo y otros, de la persona titular de la información privada; mientras que, por el otro, garantiza en un nivel medio o menor que alto el derecho a la libertad de empresa; es razonable que la información personal sea retirada o eliminada, conforme a lo garantizado por el derecho al olvido.

Sobre la base de todo lo expuesto, se puede concluir que el derecho al olvido tiene entre sus límites a los derechos a la libertad de expresión e información, empresa. De los cuales, el derecho al olvido puede ceder, dependiendo de los principios, bienes jurídicos y derechos fundamentales que se pretenda optimizar, así como de la naturaleza de la información, el carácter público del titular de la información, el examen de la máxima divulgación, entre otros aspectos, los que corresponderán ser realizados en cada caso concreto.

[28] Tribunal Constitucional, STC 03479-2011-AA/TC, STC 1405-2010-AA/TC.

3. El derecho al olvido en el proceso de *hábeas data*

3.1. El proceso de *hábeas data*

El proceso de *hábeas data* se encuentra reconocido como una garantía constitucional en el artículo 200 inciso 3 de la Constitución[29], el mismo que señala que procede contra el hecho u omisión que vulnera o amenaza los derechos de acceso a la información pública y a la autodeterminación informativa. Asimismo, el Código Procesal Constitucional regula el proceso de *hábeas data*, refiriéndose a los derechos que protege y a su procedimiento.

En cuanto al derecho a la autodeterminación informativa, el inciso 6 del artículo 2 de la Constitución, señala: "Toda persona tiene derecho: (..) A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar".

Al respecto, el Tribunal Constitucional ha señalado que el derecho a la autodeterminación informativa consiste en "la serie de facultades que tiene toda persona para ejercer control sobre la información personal que le concierne, contenida en registros ya sean públicos, privados o informáticos, a fin de enfrentar las posibles extralimitaciones de los mismos"[30].

Consecuentemente, el derecho a la autodeterminación informativa, protegido a través del proceso de *hábeas data*, garantiza al titular de la información el control de la información personal, contenida en registros públicos privados o informáticos, a fin de evitar el uso extralimitado de dicha información.

---

[29] Constitución Política del Perú
Artículo 200.- Son garantías constitucionales:
"3. La Acción de Hábeas Data, que procede contra el hecho u omisión, por parte de cualquier autoridad, funcionario o persona, que vulnera o amenaza los derechos a que se refiere el artículo 2, incisos 5 y 6 de la Constitución."

[30] Tribunal Constitucional STC 4739-2007-PHD/TC, fund. 3.

3.2. La protección judicial del derecho al olvido

Como se ha advertido, el derecho al olvido es un derecho nuevo que surge ante la innovación tecnológica. Por tal motivo, no se encuentra reconocido de manera expresa en la Constitución de 1993, ni por tratados internacionales de derechos humanos de los cuales el Perú es parte. Sin embargo, podría considerarse como parte del contenido del derecho a la autodeterminación informativa, el cual es tutelado a través del proceso constitucional del *hábeas data*.

En efecto, a fin de garantizar el principio de seguridad jurídica, corresponde verificar si el derecho al olvido puede ser tutelado, en primera instancia, por algún derecho fundamental ya reconocido en nuestro ordenamiento jurídico. En caso de que no se le pueda identificar como parte del contenido de otro derecho, podría ser reconocido a partir de la fórmula principista señalada en el artículo 3 de la Constitución.

Al respecto, como se indicó anteriormente, en líneas generales, el derecho al olvido garantiza el retiro, cancelación o eliminación de información personal que se encuentra en una base de datos o motor de búsqueda, público o privado, por un periodo determinado de tiempo, y que le genera perjuicio al titular de la información.

Mientras que el derecho a la autodeterminación informativa garantiza al titular afectado "la posibilidad de lograr la exclusión de los datos que considera 'sensibles' y que no deben ser objeto de difusión ni de registro; así como le otorga la facultad de poder oponerse a la transmisión y difusión de los mismos"[31]. Asimismo, garantiza una "serie de facultades que tiene toda persona para ejercer control sobre la información personal que le concierne, contenida en registros ya sean públicos, privados o informáticos, a fin de enfrentar las posibles extralimitaciones de los mismos"[32].

---

[31] Tribunal Constitucional, STC 4739-2007-PHD/TC, fund. 2-4.

[32] Tribunal Constitucional STC 4739-2007-PHD/TC, fund. 3.

En tal sentido, se advierte que la eliminación o retiro de la información personal contenida en una base de datos o motor de búsqueda, protegida por el derecho al olvido, calza en una de las facultades –referida al control sobre la información personal contenida en registros públicos, privados o informáticos– que tiene por finalidad enfrentar posibles extralimitaciones en el tratamiento de la información, garantizada por el derecho a la autodeterminación informativa.

Consecuentemente, se observa que si bien el derecho al olvido, es un derecho autónomo, en tanto que su objeto de protección se refiere a una información con sus particularidades propias, persigue uno de los fines del derecho a la autodeterminación informativa, el cual es el evitar el uso extralimitado de la información; asimismo, ambos derechos tienen como fines, la protección de la persona frente al tratamiento de su información personal, el principio de dignidad y la plena vigencia de derechos fundamentales conexos.

En base a lo expuesto, se puede considerar que aunque el derecho al olvido tiene un contenido propio, puede formar parte del contenido del derecho a la autodeterminación informativa.

Finalmente, dado que el derecho a la autodeterminación informativa es tutelado a través del proceso de *hábeas data*, el derecho al olvido también puede ser garantizado a través de este proceso constitucional.

4. Conclusiones

1. El titular del derecho al olvido es toda persona, física o jurídica, que tiene la facultad de solicitar la eliminación o el retiro de información personal, almacenada en bases de datos o motores de búsqueda en manos del poder público o de particulares.

2. El sujeto obligado del derecho al olvido, está conformado por el Estado o cualquier privado responsable del tratamiento de los datos personales del titular del derecho.

3. La obligación de retirar, cancelar o eliminar información personal almacenada en base de datos o motores de búsqueda, que haya sido de acceso al público, por un tiempo razonable, forma parte del contenido del derecho al olvido.

4. El derecho al olvido tiene límites, los cuales deberían ser analizados en cada caso concreto, teniendo en cuenta factores como los principios, bienes jurídicos, derechos fundamentales que se pretenda optimizar, la naturaleza de la información, el carácter público del titular de la información, el examen de la máxima divulgación, entre otros aspectos.

5. El derecho al olvido debe ser garantizado en nuestro ordenamiento jurídico a través del derecho a la autodeterminación informativa, en tanto que persiguen los mismos fines.

6. El proceso mediante el cual se puede garantizar el derecho al olvido es el proceso de *hábeas data*, en la medida que éste tutela el derecho a la autodeterminación informativa.

Bibliografía

- Alexy, Robert, "Teoría de los derechos fundamentales". Centro de Estudios Políticos y Constitucionales, 2da Edición, Madrid, 2012.
- Alexy, Robert, "Epílogo a la teoría de los derechos fundamentales". Revista Española de Derecho Constitucional, Año 22, Núm. 66, setiembre-diciembre 2002.
- Corte Interamericana de Derechos Humanos. Caso Gomes Lund y otros vs. Brasil, 2010.
- Corte Interamericana de Derechos Humanos. Caso Fontevecchia y D'Amico vs. Argentina, 2011.
- Defensoría del Pueblo, "Situación de la libertad de expresión en el Perú". Serie de Informes defensoriales, Informe N° 48, Lima, 2000.

- Habermas, Jurgen, "Facticidad y validez", Editorial Trotta, Cuarta edición, 2005, pág. 332.
- Instituto Nacional de Transparencia, Acceso a la Información y Protección de datos personales de México. Resolución 94/14. Caso Carlos Sánchez de la Peña contra Google México.
- Ministerio de Justicia: https://prodpe.minjus.gob.pe/prodpe_web/BancoDato_verResultado recopilado el 28 de agosto de 2020.
- Supremo Tribunal Federal de Brasil: http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=276284
- Constitución Política del Perú
- Pérez Gómez, Ana María. Cuando google juega con la información privada…El derecho al olvido digital en Europa, una lucha de titanes. En Revista *La propiedad* inmaterial. Colombia, N° 22, julio - diciembre 2016.
- Puccinelli, Oscar, "El derecho al olvido en el derecho a la protección de datos. Con especial referencia a su vigencia en Internet. Pensamiento Constitucional N° 21, 2016.
- Tribunal de Justicia de la Unión Europea, 13 de mayo de 2014, Sentencia en el asunto C-131/12, Google Spain, S.L. y Google Inc. Contra la Agencia Española de Protección de Datos (AEPD) y Mario Costeja Gonzáles.
- Tribunal de Justicia de la Unión Europea, 9 de marzo de 2017, Sentencia en el asunto C-398/15, Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce / Salvatore Manni.
- Tribunal Constitucional del Perú, STC 2488-2002-PHC/TC.

- Tribunal Constitucional del Perú, STC 6546-2006-PA.
- Tribunal Constitucional, STC 4739-2007-PHD/TC.
- Tribunal Constitucional del Perú, STC 0831-2010-PHD/TC.
- Tribunal Constitucional del Perú, STC 3271-2012-PA/TC.
- Tribunal Constitucional del Perú, STC 1470-2016-PHC

LA JURISPRUDENCIA DEL TRIBUNAL CONSTITUCIONAL SOBRE EL DERECHO A LA AUTODETERMINACIÓN INFORMATIVA

✍ Nadia Paola Iriarte Pamo*

1. Introducción

El hábeas data es un proceso constitucional que tiene por objeto la protección de los derechos de acceso a la información pública y a la autodeterminación informativa, previstos en los incisos 5 y 6 del artículo 2 de la Constitución Política de 1993 (en adelante Constitución).

En el marco del proceso de hábeas data, el Tribunal Constitucional del Perú (en adelante Tribunal) ha expedido profusa jurisprudencia sobre la salvaguarda de ambos derechos. En ese artículo, nos centraremos en el estudio del derecho a la autodeterminación informativa a través de la jurisprudencia constitucional. Así, analizaremos y reflexionaremos sobre el ámbito de protección, la titularidad del derecho, las diferencias con otros derechos, los límites temporales de los datos negativos, los tipos hábeas data, y, la jurisprudencia del Tribunal en materia de defensa del derecho a la autodeterminación informativa a través del proceso de hábeas data.

* Abogada por la Universidad Católica de Santa María de Arequipa. Magister en Estudios Avanzados en Derechos Humanos por la Universidad Carlos III de Madrid. Asesora jurisdiccional del Tribunal Constitucional.

2. El ámbito de protección del derecho a la autodeterminación informativa

La Constitución precisa en su artículo 2, inciso 6 que toda persona tiene derecho a que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar.

La jurisprudencia del Tribunal se ha decantado por denominar a este derecho, consagrado en la Constitución, como "derecho a la autodeterminación informativa", denominación que fue acuñada por el Tribunal Constitucional Federal alemán, en su Sentencia de 15 de diciembre de 1983 sobre la Ley del Censo de 31 de marzo de 1982. La doctrina ha utilizado otros términos, por ejemplo "derecho a la protección de datos", "libertad informática"; a nuestro parecer, la denominación acogida por nuestra jurisprudencia refleja la esencia del derecho: el control de uno mismo sobre su información personal que se proyecta frente a la informática o cualquier tecnología.

El derecho a la autodeterminación informativa se ha consolidado como un derecho autónomo y con un ámbito de protección distinto al que corresponde a otros derechos. Si bien la Constitución enuncia de manera expresa sólo uno de los contenidos de este derecho, el de oposición al suministro de información que afecte la intimidad personal y familiar; éste comprende un haz de facultades, que han sido objeto de desarrollo jurisprudencial[1].

Al respecto, el Tribunal en la STC N° 0666-96-HD/TC, precisa que la protección de este derecho, a través del hábeas data, implica que cualquier justiciable pueda recurrir a este proceso constitucional con el objeto de acceder a los registros de información almacenados en centros informáticos o computarizados, cualquiera sea su naturaleza, a fin de

[1] Cfr. EGUIGUREN PRAELI, Francisco, "El Hábeas Data y su desarrollo en el Perú", en Derecho PUCP, N° 50, diciembre de 1997, pp. 291-310.

rectificar, actualizar, excluir determinado conjunto de datos personales, o impedir que se propague información que pueda ser lesiva al derecho constitucional a la intimidad[2].

En esa línea, la STC N° 01797-2002-HD/TC, uno de los principales referentes en esta materia, especifica que el acceso a los registros puede tener por objeto que se permita conocer qué es lo que se encuentra registrado, para qué y para quién se realizó el registro de información así como la (o las) persona(s) que recabaron dicha información. Además, precisa que el hábeas data puede tener la finalidad de agregar datos al registro que se tenga, ya sea por la necesidad de que se actualicen los que se encuentran registrados, o bien con el fin de que se incluyan aquellos no registrados, pero que son necesarios para que se tenga una cabal referencia sobre la imagen e identidad de la persona afectada. Asimismo, se puede rectificar la información, personal o familiar, que se haya registrado; impedir que esta se difunda para fines distintos de aquellos que justificaron su registro o, incluso, se tiene la potestad de cancelar aquellos que razonablemente no debieran encontrarse almacenados[3].

De lo expresado en los párrafos precedentes inferimos que el bien protegido por el derecho a la autodeterminación informativa es el control de la información personal. Este derecho garantiza la competencia del titular de determinar por sí mismo sobre la transmisión y utilización de sus datos personales. Además le atribuye un conjunto de facultades: acceder a los registros de información, agregar datos a los registros, rectificar la información, impedir que la información se difunda, cancelar los registros, entre otras[4].

---

[2] Tribunal Constitucional. Sentencia recaída en el Expediente N° 0666-96-HD/TC, de fecha 2 de abril de 1998.

[3] Tribunal Constitucional. Sentencia recaída en el Expediente N° 01797-2002-HD/TC, de fecha 29 de enero de 2003.

[4] Cfr. GOZAINI, Osvaldo Alfredo, *Hábeas Data*. Protección de Datos Personales, Editorial Rubinzal - Culzoni, Buenos Aires, 2003.

Por otra parte, la citada sentencia puntualiza que el derecho a la autodeterminación informativa tiene por objeto proteger la intimidad, personal o familiar, la imagen y la identidad frente al peligro que representa el uso y la eventual manipulación de los datos a través de los ordenadores electrónicos[5].

Una de las características del derecho a la autodeterminación informativa es ser un derecho de naturaleza relacional -*prima facie* y de modo general-, pues las exigencias que demandan su respeto, se encuentran muchas veces vinculadas a la protección de otros derechos constitucionales.

En suma, tal como se expone en la STC N° 04739-2007-PHD/TC, el derecho a la autodeterminación informativa consiste en la serie de facultades que tiene toda persona para ejercer el control sobre la información personal que le concierne, contenida en registros ya sean públicos o privados, a fin de enfrentar las posibles extralimitaciones de los mismos. Se encuentra estrechamente ligado a un control sobre la información, como una autodeterminación de la vida íntima, de la esfera personal[6].

3. La titularidad del derecho a la autodeterminación informativa

El derecho a la autodeterminación informativa, busca proteger a la persona en sí misma, no únicamente en los derechos que conciernen a su esfera personalísima, sino a la persona en la totalidad de ámbitos. En ese sentido, protege al titular del mismo frente a posibles abusos o riesgos derivados de la utilización de los datos, brindando al titular afectado la posibilidad de lograr la exclusión de los datos que considera "sensibles" y que no deben ser objeto de difusión ni de registro; así

[5] Tribunal Constitucional. Sentencia recaída en el Expediente N° 01797-2002-HD/TC, de fecha 29 de enero de 2003.

[6] Tribunal Constitucional. Sentencia recaída en el Expediente N° 04739-2007-PHD/TC, de fecha 15 de octubre de 2007.

como le otorga la facultad de poder oponerse a la transmisión y difusión de los mismos[7].

Con relación a la titularidad, nos preguntamos si las personas jurídicas pueden ser consideradas titulares del derecho a la autodeterminación informativa. Sobre el particular, el Tribunal se ha pronunciado en la STC N° 04972-2006-PA/TC. Menciona que dos criterios esenciales permiten justificar que toda persona jurídica tiene o retiene para sí un conjunto de derechos. En primer lugar, la necesidad de garantizar el derecho a la participación de toda persona en forma individual o asociada en la vida política, económica, social y cultural de la Nación (artículo 2, inciso 17 de la Constitución). En este marco, si a toda persona natural se la habilita para que pueda participar en forma individual o asociada, mediante diversas variantes de organización -personas jurídicas- es porque estas últimas retienen para sí una multiplicidad de derechos fundamentales.

En segundo lugar, la necesidad de que el principio del Estado democrático de derecho e, incluso, el de dignidad de la persona, permitan considerar un derecho al reconocimiento y tutela jurídica en el orden constitucional de las personas jurídicas. La existencia de un Estado democrático de derecho supone dotar de garantías a las instituciones por él reconocidas. Además, quienes integran las personas jurídicas retienen para sí un interminable repertorio de derechos fundamentales nacidos de su propia condición de seres dignos, no siendo posible que dicho estatus, se vea minimizado o, peor aún, desconocido, cuando se forma parte de una persona jurídica.

En consecuencia, siendo constitucionalmente legítimo el reconocimiento de derechos fundamentales sobre las personas jurídicas, cabe anotar que tal consideración tampoco significa ni debe interpretarse como que todos los atributos, facultades y libertades reconocidas

[7] Ibídem.

sobre la persona natural sean los mismos que corresponden a la persona jurídica. En este contexto, en la citada sentencia, el Tribunal ha señalado de manera enunciativa una serie de derechos fundamentales invocables por las personas jurídicas, entre los que se encuentra el derecho a la autodeterminación informativa (artículo 2, inciso 6 de la Constitución)[8].

Sobre la titularidad, traemos a colación lo previsto en la Ley de Protección de Protección de Datos Personales, Ley 29733, que en su artículo 19 especifica que el titular de datos personales tiene derecho a obtener la información que sobre sí mismo sea objeto de tratamiento en bancos de datos públicos o privados, la forma en que sus datos fueron recopilados, las razones que motivaron su recopilación y a solicitud de quién se realizó la recopilación, así como las transferencias realizadas o que se prevén hacer de ellos. También, conforme lo preceptúa el artículo 20 de la citada ley, el titular tiene derecho a la actualización, inclusión, rectificación y supresión de sus datos personales materia de tratamiento, cuando estos sean parcial o totalmente inexactos, incompletos, cuando se hubiere advertido omisión, error o falsedad, cuando hayan dejado de ser necesarios o pertinentes a la finalidad para la cual hayan sido recopilados o cuando hubiera vencido el plazo establecido para su tratamiento.

4. Diferencias del derecho a la autodeterminación informativa con otros derechos

El Tribunal, mediante su jurisprudencia, ha enfatizado en las diferencias del derecho a la autodeterminación informativa con otros derechos. En esa línea, advierte, en la STC N° 01797-2002-HD/TC, que si bien tiene por objeto proteger la intimidad; no puede identificarse con el derecho a la intimidad, personal o familiar (artículo 2, inciso 7

[8] Tribunal Constitucional. Sentencia recaída en el Expediente N° 04972-2006-PA/TC, de fecha 4 de agosto de 2006.

de la Constitución), pues mientras que este derecho protege el derecho a la vida privada, esto es, el poder jurídico de rechazar intromisiones ilegítimas en la vida íntima o familiar de las personas, el derecho a la autodeterminación informativa garantiza la facultad de todo individuo de poder preservarla controlando el registro, uso y revelación de los datos que les conciernen.

Diversos sectores de la doctrina se han pronunciado sobre las diferencias entre el derecho a la autodeterminación informativa y el derecho a la intimidad. Siguiendo a Pablo Lucas Murillo, manifestamos que la protección que la Constitución quiere asegurarnos ante los progresos tecnológicos no coincide con la que brinda el derecho a la intimidad; en tanto, el riesgo específico que implica la informática es el control sobre las vidas de los demás que permite la captación incontrolada de información personal; es decir, la recopilación y el tratamiento automatizado de datos sobre los más variados aspectos. En esa línea, los instrumentos de tutela jurídica de la intimidad no sirven para afrontar esos peligros. No es la intimidad lo que está en juego, sino el control del uso por terceros de la información personal que nos afecta, aunque no se refiera a aspectos íntimos de nuestra existencia[9].

El derecho objeto de nuestro estudio difiere del derecho a la imagen (artículo 2, inciso 7 de la Constitución) pues este protege, básicamente la imagen del ser humano, derivada de la dignidad de la que se encuentra investido; en cambio el derecho a la autodeterminación informativa, garantiza que el individuo sea capaz de disponer y controlar el tipo de datos que sobre él se hayan registrado, a efectos de preservar su imagen derivada de su inserción en la vida en sociedad.

Por último, se diferencia del derecho a la identidad personal, esto es, del derecho a que la proyección social de la propia personalidad

[9] MURILLO DE LA CUEVA, Pablo Lucas, "La Constitución y el derecho a la autodeterminación informativa", en *Cuadernos de Derecho Público*, núms. 19-20 (mayo-diciembre 2003) pp. 36-37.

no sufra interferencias o distorsiones a causa de la atribución de ideas, opiniones, o comportamientos diferentes de aquellos que el individuo manifiesta en su vida en sociedad[10].

5. El derecho a la autodeterminación informativa y los límites temporales de los datos negativos

El derecho a la autodeterminación informativa, tal como lo expresáramos en párrafos anteriores, protege a su titular frente a abusos o riesgos derivados del uso, manipulación, y difusión de los datos personales o familiares registrados a través de medios informáticos o electrónicos.

Siendo así, uno los ámbitos en los que se proyecta este derecho está vinculado al registro de la información financiera destinada al cálculo del riesgo crediticio. Bajo este marco, la facultad de controlar la información (legalidad de la obtención de la información; que los datos que se hallen almacenados satisfagan criterios de veracidad, integridad, utilidad y caducidad; que la información no contenga aspectos íntimos) que se encuentra compilada en las centrales de riesgo -sean públicas o privadas- salvaguarda al titular de la información de los potenciales excesos que la publicidad de sus datos crediticios y financieros pudiera ocasionarle y que, como consecuencia de ello, se incida negativamente en el goce y ejercicio de diversos derechos e intereses.

La limitación temporal del almacenamiento de la información financiera destinada al cálculo del riesgo crediticio está directamente relacionada con la facultad de que los datos que se conserven en un registro informático sean actuales y veraces. Esta temática fue abordada detalladamente por el Tribunal en la STC N° 04227-2009-PHD/TC. Según refiere, la única forma de que mediante los datos se pueda proyectar una imagen real del comportamiento de una persona en el

[10] Tribunal Constitucional. Sentencia recaída en el Expediente N° 01797-2002-HD/TC, de fecha 29 de enero de 2003.

sistema bancario y financiero es que éstos sean constantemente actualizados. Lo que presupone, una prohibición de almacenamiento *ad aeternum* de los datos. En especial, de los denominados "datos negativos", es decir, de los que registran una mala práctica en el mercado, pues también las malas historias crediticias se pueden revertir por la adopción de hábitos de honramiento de las obligaciones contraídas o, llegado el caso, incluso por efectos legales del transcurso del tiempo.

La citada sentencia, advierte que la vigencia del registro de información bancaria o financiera adversa en un banco de datos no se relaciona necesariamente con la satisfacción (extemporánea) de una obligación patrimonial. La exigencia de veracidad de este tipo de información requiere que también se registre los antecedentes financieros y la solvencia económica de las personas, principalmente en lo que se refiere a la capacidad y trayectoria de endeudamiento y pago. La información de que una obligación patrimonial se ha extinguido por su pago oportuno es tan valiosa como la información de que dicha obligación se ha extinguido fuera del plazo, por medio de una acción judicial o, en fin, como consecuencia de los efectos legales atribuidos al transcurso del tiempo sin que se haya ejercitado judicialmente los derechos del acreedor. Toda ella, llegado el caso, forma parte de la información actualizada y no desaparece o deja de existir por el hecho de que ya no se encuentra pendiente de cumplimiento, pues la historia o "imagen crediticia" de una persona está conformada por una serie de datos que en el tiempo evidencian su comportamiento en el mercado, y no se reducen sólo al último hecho.

No obstante -puntualiza la mencionada sentencia- cualquiera que fuera el caso de información adversa que se pueda haber registrado en un banco de datos, el deber que tienen de proporcionar información veraz exige que éstos sean actualizados constantemente, y reparar que ella no puede mantenerse registrada eternamente. Ello vale incluso para el caso de las obligaciones no pagadas, en concreto, cuando su exigibilidad haya superado el término de prescripción legal para poder reclamar su satisfacción. En estos supuestos, la conservación sin plazo de los

datos negativos de la persona constituye un ejercicio abusivo del poder, pues pese a que el ordenamiento jurídico ha establecido que el transcurso del plazo legal extingue la obligación insoluta, se prosigue irradiando una imagen crediticia y financiera no veraz al proyectar como actual el incumplimiento de obligaciones que se encuentran excluidas del tráfico jurídico[11].

6. El derecho a la autodeterminación informativa y los tipos de hábeas data

El Tribunal, en la STC N° 06164-2007-PHD/TC[12] -a efectos de cumplir la función pedagógica de sus resoluciones-, describe los tipos de hábeas data. Nos centraremos en aquellos que salvaguardan el derecho a la autodeterminación informativa.

I. Hábeas data puro: Este tipo de hábeas data es el que protege el derecho a la autodeterminación informativa. Comprende el hábeas data de cognición y el hábeas data manipulador.

1. **Hábeas data de cognición**: No se trata de un proceso en virtud del cual se pretende la manipulación de los datos, sino efectuar una tarea de conocimiento y de supervisión sobre la forma en que la información personal almacenada está siendo utilizada. Se subdivide en los siguientes tipos de hábeas data:

   1.1. **Hábeas data informativo**: Está dirigido a conocer el contenido de la información que se almacena en el banco de datos (qué se guarda).

   1.2. **Hábeas data inquisitivo**: Para que se diga el nombre de la persona que proporcionó el dato (quién).

[11] Tribunal Constitucional. Sentencia recaída en el Expediente N° 04227-2009-PHD/TC, de fecha 30 de mayo de 2011.

[12] Tribunal Constitucional. Sentencia recaída en el Expediente N° 06164-2007-PHD/TC, de fecha 21 de diciembre de 2007.

1.3. Hábeas data teleológico: Busca esclarecer los motivos que han llevado al sujeto activo a la creación del dato personal (para qué).

1.4. Hábeas data de ubicación: Tiene como objeto que el sujeto activo del poder informático responda dónde está ubicado el dato, a fin de que el sujeto pasivo -el accionante- pueda ejercer su derecho (dónde).

2. Hábeas data manipulador: No tiene como propósito el conocimiento de la información almacenada, sino su modificación. Comprende los siguientes tipos de hábeas data:

2.1. Hábeas data aditivo: Agrega al banco de datos una información no contenida. Esta información puede consistir: en la actualización de una información cierta pero que por el paso del tiempo se ha visto modificada; también puede tratarse de una información que tiene como objeto aclarar la certeza de un dato que ha sido mal interpretado; o incorporar al banco de datos una información omitida que perjudica al sujeto pasivo.

2.2. Hábeas data correctivo: Tiene como objeto modificar los datos imprecisos y cambiar o borrar los falsos.

2.3. Hábeas data supresorio: Busca eliminar la información sensible o datos que afectan la intimidad personal, familiar o cualquier otro derecho fundamental de la persona. También puede proceder cuando la información que se almacena no guarda relación con la finalidad para la cual ha sido creado el banco de datos.

2.4. Hábeas data confidencial: Pretende impedir que las personas no autorizadas accedan a una información que ha sido calificada como reservada. En este tipo, se incluye la prohibición de datos que por el paso del tiempo o por sentencia firme se impide su comunicación a

terceros.

2.5. Hábeas data desvinculador: Sirve para impedir que terceros conozcan la identificación de una o más personas cuyos datos han sido almacenados en función de determinados aspectos generales como la edad, raza, sexo, ubicación social, grado de instrucción, idioma, profesión.

2.6. Hábeas data cifrador: Tiene como objeto que el dato sea guardado bajo un código que sólo puede ser descifrado por quien está autorizado a hacerlo.

2.7. Hábeas data cautelar: Tiene como propósito impedir la manipulación o publicación del dato en el marco de un proceso, a fin de asegurar la eficacia del derecho a protegerse.

2.8. Hábeas data garantista: Busca el control técnico en el manejo de los datos, a fin de determinar si el sistema informativo, computarizado o no, garantiza la confidencialidad y las condiciones mínimas de seguridad de los datos y su utilización de acuerdo con la finalidad para la cual han sido almacenados.

2.9. Hábeas data interpretativo: Tiene como objeto impugnar las valoraciones o conclusiones a las que llega el que analiza la información personal almacenada.

2.10. Hábeas data indemnizatorio: Aunque no es de recibo en nuestro ordenamiento, este tipo de hábeas data consiste en solicitar la indemnización por el daño causado con la propalación de la información[13].

[13] Cfr. PUCCINELLI, Oscar Raúl, "Tipos y Subtipos de Hábeas Data en América Latina", en Cuaderno de Derecho Público, N° 1, 2006, pp. 163-176.

7. La jurisprudencia del Tribunal Constitucional en materia de defensa del derecho a la autodeterminación informativa a través del proceso de hábeas data

La jurisprudencia del Tribunal sobre esta materia es profusa. Son recurrentes aquellos casos en los que el demandante solicita se actualice la información de riesgos que figura en los registros de crédito de entidades financieras sobre deudas; y, la rectificación de la información de riesgos del actor, referida a la calificación de cliente pérdida por la calificación de cliente normal, información reportada a la Central de Riesgos Crediticios de la Superintendencia de Banca, Seguros y AFP. En estos supuestos se alega que la deuda ha sido pagada[14].

Diversos son los casos en los que el objeto de la demanda es que se corrija datos. Mencionamos la STC N° 5356-2016-PHD/TC, que declaró fundada la demanda interpuesta contra la Reniec, en la que se solicitó que se corrija el estado civil del actor en el registro respectivo de "casado" a "soltero", y, que se expida nuevo DNI con el estado civil debidamente corregido[15]. Advertimos, que en este caso, nos encontramos frente a un hábeas data manipulador.

Por otra parte, se advierte múltiples casos en los que la entidad requerida es una de carácter privado y no desempeña actividades de carácter público (empresas mineras), situación que no enerva el derecho a la autodeterminación informativa de los accionantes de poder acceder y obtener copias certificadas, por ejemplo de fichas médicas ocupacionales, exámenes audiométricos, etc. Recordemos que el derecho, objeto de nuestro análisis, supone que una persona pueda hacer uso de la información privada que existe sobre ella ya sea que la información se

[14] Tribunal Constitucional. Sentencias recaídas en los Expedientes N° 03052-2007-HD/TC, de fecha 16 de noviembre de 2007; N° 01988-2009-PHD/TC, de fecha 7 de octubre de 2009.

[15] Tribunal Constitucional. Sentencia recaída en el Expediente N° 05356-2016-HD/TC, de fecha 25 de mayo de 2017.

encuentre almacenada o en disposición de entidades públicas o de carácter privado. En esa línea, el titular tiene derecho a obtener una copia de la información particular que le concierne, al margen de si ésta se encuentra disponible en una entidad pública o privada[16].

Asimismo, se ha presentado casos cuyos actores solicitan que se ordene a las universidades la entrega de copia autenticada de certificados de estudios universitarios. Algunas de estas entidades fundamentan su negativa de entregar dicha información bajo el argumento que ésta es "financiada" con sus propios recursos. Para el Tribunal tal alegación carece de sustento constitucional porque el titular de la información en cuestión no es la universidad emplazada, sino las personas sobre las cuales se dispone de ciertos datos, en este caso, sobre el aspecto académico de los accionantes. Se subraya, que el hecho que las universidades los almacenen, sistematicen y administren, no les otorga titularidad sobre los mismos. El derecho a la autodeterminación informativa garantiza el acceso y uso de dicha información[17].

También, se ha presentado aquellos casos en los que el actor solicita se le proporcione copias del expediente coactivo iniciado por la Sunat. En este supuesto, si bien la parte demandante considera que la denegación de las copias solicitadas vulnera su derecho de acceso a la información pública, el Tribunal, en aplicación del principio *iura novit curia,* consideró que el derecho que en realidad sustenta su pretensión es el derecho a la autodeterminación informativa, pues se trata de información propia del administrado y de su representada. En esa línea, el Tribunal, en la STC N° 01508-2016-PHD/TC ha señalado que la solicitud -verbal o escrita- de copias del expediente administrativo o de cualquier otro documento referido al administrado, no debe

[16] Tribunal Constitucional. Sentencia recaída en el Expediente N° 0300-2010-HD/TC, de fecha 11 de mayo de 2010.

[17] Tribunal Constitucional. Sentencia recaída en el Expediente N° 00746-2010-PHD/TC, de fecha 20 de agosto de 2010.

tramitarse como un procedimiento de acceso a la información pública; pues, este sería respondido en el plazo de 10 días; lo cual sería totalmente inadecuado; pues en el supuesto que una persona alegue que no fue notificada con la resolución de primera instancia administrativa y que el plazo para interponer su recurso de apelación está próximo a vencer; por lo que, solicita copia de la misma con la finalidad de ser apelada; sería absurdo que la Administración tramite su pedido como acceso a la información pública y le entregue la información requerida a los 10 días, cuando el plazo para interponer su recurso de apelación se encuentra vencido.

Ponemos de relieve que se han interpuesto varias demandas de hábeas data contra la Oficina de Normalización Previsional (ONP)[18], mediante las cuales los recurrentes solicitan acceder a la información de los períodos de aportaciones efectuados al Sistema Nacional de Pensiones por sus exempleadores, y que, como consecuencia de ello, se extracte determinados periodos laborados[19]. Sobre el particular, apreciamos, que en algunos de estos casos los actores invocaron como derecho presuntamente afectado el de acceso a la información pública (artículo 2, inciso 5 de la Constitución). En estos supuestos, el Tribunal. en aplicación del principio *iura novit curia,* consideró que el derecho que se habría vulnerado es el de autodeterminación informativa (artículo 2, inciso 6 de la Constitución) y emitió pronunciamiento al respecto. Sobre esto, podemos citar las siguientes sentencias: STC N° 02324-2013-PHD/TC[20], STC N°05676-2013-PHD/TC[21], STC

[18] Cfr. GUICHOT, Emilio, *Datos personales y Administración Pública*, Agencia de Protección de Datos de la Comunidad de Madrid, Primera Edición, Editorial Aranzadi, Navarra, 2005.

[19] Tribunal Constitucional. Sentencia recaída en el Expediente N° 01846-2014-HD/TC, de fecha 11 de marzo de 2015.

[20] Tribunal Constitucional. Sentencia recaída en el Expediente N° 02324-2013-PHD/TC, de fecha 21 de agosto de 2014.

[21] Tribunal Constitucional. Sentencia recaída en el Expediente N° 05676-2013-PHD/TC, de fecha 10 de diciembre de 2015.

N° 08263-2013-PHD/TC[22], STC N° 00422-2014-PHD/TC[23], STC N° 01881-2014-PHD/TC[24], STC N° 00010-2015-PHD/TC[25], y, STC N° 00146-2015-PHD/TC[26].

Observamos, que nos encontramos frente a un hábeas data de cognición; pues se pretende el acceso a datos. La negativa de la ONP respecto de la petición de los actores no encuentra justificación alguna, como entidad pública tiene la obligación de brindar el acceso a los datos personales que resguarde en sus bancos de datos físicos o virtuales, siempre y cuando no se produzca alguna situación razonable de restricción de dichos datos, prescrita en el artículo 3 de la Ley de Protección de Datos Personales, Ley 29733.

Mediante la STC N° 4538-2015-PHD/TC el Tribunal ha realizado puntualizaciones importantes. Así, advierte que la inexistencia de la obligación de contar con cierta información no enerva la existencia de una obligación de dar respuesta a la solicitud, la cual se funda en el derecho de acceso del titular de datos contenido en la autodeterminación informativa; y, de manera relacional, en el derecho de petición. Por consiguiente, el derecho a la autodeterminación informativa también importa la obligación por parte de la entidad que guarda la información de responder oportunamente a una solicitud debidamente realizada, aun cuando se considere que no tiene asidero, evaluación que solo corresponde a un momento posterior.

[22] Tribunal Constitucional. Sentencia recaída en el Expediente N° 08263-2013-PHD/TC, de fecha 24 de agosto de 2016.

[23] Tribunal Constitucional. Sentencia recaída en el Expediente N° 00422-2014-PHD/TC, de fecha 11 de marzo de 2015.

[24] Tribunal Constitucional. Sentencia recaída en el Expediente N° 01881-2014-PHD/TC, de fecha 11 de marzo de 2015.

[25] Tribunal Constitucional. Sentencia recaída en el Expediente N° 00010-2015-PHD/TC, de fecha 25 de enero de 2017.

[26] Tribunal Constitucional. Sentencia recaída en el Expediente N° 00146-2015-PHD/TC, de fecha 21 de noviembre de 2017.

Esa situación -según el Tribunal- guarda plena concordancia con los posibles remedios que puedan presentarse frente a una solicitud que resulte insuficiente a efectos de dar lugar a la búsqueda de información. En este marco, la entidad requerida tiene diversas opciones para dar respuesta a la misma, tales como denegar motivadamente la solicitud sobre la base de lo previsto legislativamente como límite al ejercicio de la autodeterminación informativa, solicitar mayor información para que se pueda realizar la búsqueda -en una lógica de colaboración entre Administración y administrado-, informar sobre la imposibilidad de dar cobertura a la solicitud por inexistencia de la información, pérdida -destrucción-. Frente a todas estas posibilidades, lo inadmisible constitucionalmente es la denegatoria arbitraria incomunicada al solicitante que busca ejercer su derecho a la autodeterminación informativa.

Finalmente, en la citada sentencia, el Tribunal advierte que dichos pedidos no exigen a la ONP la generación de información con la que no se cuenta o no esté obligada a contar. En ese sentido, la respuesta que satisface los alcances del derecho a la autodeterminación informativa se circunscribe básicamente a la entrega de información que exista sobre el propio solicitante en la base de datos consultada, así como aquellas precisiones referidas enunciativamente en el artículo 19 de la Ley de Protección de Datos Personales[27].

[27] Tribunal Constitucional. Sentencia recaída en el Expediente N° 04538-2015-PHD/TC, de fecha 9 de diciembre de 2015.

ISBN: 978-612-4464-04-1