FORSETI
Revista de Derecho

Forseti. Revista de Derecho. Volumen 13, Nº 19, Lima, 2024, pp. 157 – 187

La legítima inquietud: ¿puedo saber cómo otros usuarios de redes sociales obtuvieron mis datos personales publicados en sus perfiles?

Gabriela G. Bolaños Vainstein*
Erick Américo Iriarte Ahon**

Resumen.- El artículo examina si el derecho a la autodeterminación informativa resultaría exigible a la actividad (tratamiento) que los usuarios de redes sociales realicen sobre datos personales ajenos. Asimismo, se responde a la inquietud sobre si un titular de los datos personales puede exigir a un tercero revelar la fuente de obtención de sus datos personales publicados por tal tercero en su perfil de usuario.

Abstract.- The article examines whether the right to informational self-determination would be enforceable in relation to the activity (processing) that social network users carry out on other people's personal data. Likewise, the concern is answered as to whether a personal data owner can require a third party to reveal the source of obtaining their personal data published by such third party in their user profile.

Palabras clave.- Datos personales - data privacy - autodeterminación informativa - redes sociales - perfil de usuario - derecho de acceso - derecho de información - excepciones al ámbito de aplicación.

Keywords.- Personal data - data privacy - informative self-determination - social networks, user profile, right of access, right to information, exceptions to the scope of application.

* Abogada por la Universidad de Lima. Especialista en materia de protección al consumidor, defensa de la competencia, protección de datos personales, seguridad de la información y nuevas tecnologías. Abogada en CMS Grau en el área de Nuevas Tecnologías y Protección de Datos.

** Abogado por la Pontificia Universidad Católica del Perú con maestría en Ciencia Política y Gobierno en por la Pontificia Universidad Católica del Perú. Doctorando en Administración de Empresas en Centrum PUCP. Delegado por Perú para coordinar el Grupo de Trabajo sobre Marco Regulatorio de Sociedad de la Información y de Internet Governance de la Plataforma eLAC. Socio Principal en Iriarte & Asociados.

I. Introducción al caso que nos motiva

El pasado 19 de mayo de 2023, la Sala Primera del Tribunal Constitucional [Tribunal Constitucional] emitió la Sentencia 291/2023[1] en la que resolvió declarando improcedente un recurso de agravio constitucional contra la sentencia de fecha 30 de noviembre de 2021, que fue expedida por la Segunda Sala Civil de la Corte Superior de Justicia de Piura [Sentencia Apelada]. Así, el Tribunal Constitucional (2023) confirmó tal Sentencia Apelada que declaró infundada la demanda de Hábeas Data y concluyó que los hechos y el petitorio de la demanda no estarían referidos en forma directa al contenido constitucionalmente protegido del derecho a la autodeterminación informativa.

En dicho caso, el petitorio del demandante consistía en que el demandado le informe el nombre completo de quién o quiénes le proporcionaron su información personal (i.e., su nombre completo, su calidad de miembro de una organización sindical, un monto dinerario sobre el cual se habría propuesto un arreglo extrajudicial y acciones desarrolladas al interior de un proceso de querella). Así, tal información personal había sido divulgada por el demandado en una publicación realizada en su cuenta personal de la red social Facebook.

A todo ello, el Tribunal Constitucional (2023) argumentó que:

> Si bien el emplazado habría hecho pública la información del demandante a través de su cuenta en la red social Facebook, esa cuenta personal no califica como un banco de datos de tratamiento de datos personales[2] en los términos establecidos en la precitada Ley de Protección de Datos Personales.

Además, se consideró que la Ley 29733, "Ley de Protección de Datos Personales" (2011) no aplicaría a las cuentas personales de usuarios de redes sociales "por expresa exclusión que hace de ellas (…) cuando establece que no afecta 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".

El Tribunal Constitucional (2023) también tuvo a bien considerar que, en virtud del pasado Expediente 0134-2003-HD/Tribunal Constitucional, el proceso constitucional de Hábeas Data "no es un proceso destinado a obligar a la revelación de fuentes de información o a impedir el ejercicio del derecho a la libertad de expresión, que es inherente a todo ser humano"[3].

---

1 Tribunal Constitucional. Expediente 01163-2022-PHD/Tribunal Constitucional, Piura, Edward Antonio Muñoz Salazar. (19 de mayo de 2023) https://tc.gob.pe/jurisprudencia/2023/01163-2022-HD.pdf

2 Así, el Tribunal Constitucional (2023) fue muy enfático al considerar que "las cuentas de los usuarios registrados en una red social como Facebook, donde estos crean o comparten contenido y envían mensajes a otras personas o se comunican entre ellas, no son bancos de datos personales".

3 Tribunal Constitucional. Expediente 0134-2003-PHD/Tribunal Constitucional, Lima, Ernesto Gamarra Olivares; 20 de septiembre de 2004).

Cabe precisar que tal tribunal contó con un fundamento de voto por parte del magistrado Monteagudo Valdez, quién precisó que "una pretensión como la planteada por el demandante solo podría ser acogida en la vía del amparo, mas no en el marco de un proceso constitucional de habeas data. De ahí que tampoco corresponda acoger este extremo concreto del petitorio"[4]. Por ello, no compartió la afirmación realizada por sus otros dos (2) colegas respecto de que, "bajo ninguna circunstancia una cuenta personal de Facebook pueda mantener información bajo las características de un banco de datos, ya que considero que ello debe ser producto de un análisis individualizado (caso por caso) y en atención a los constantes desarrollos tecnológicos"[5]

II. Objetivo del presente artículo

Con el ánimo de absolver la pregunta formulada en el título de este artículo, se pretende estudiar el contenido del derecho de la autodeterminación informativa en un plano constitucional y normativo. Ello, de la mano de las facultades de control que tal derecho brinda y también de la normativa a cargo del proceso constitucional para protegerlo, i.e., la Acción de Hábeas Data.

Lo anterior permitirá determinar si tal derecho resulta exigible a la actividad (tratamiento) que realizan los usuarios en línea dentro de sus perfiles -o cuentas- de redes sociales con respecto a los datos personales de terceras personas. Sobre todo, se estudiará bajo qué supuestos o presupuestos específicos puede configurarse la aplicación de la normativa de protección de datos personales a la actividad de usuarios.

Finalmente, de ocurrir lo anterior, este artículo adicionalmente pretenderá esclarecer si el contenido del derecho a la autodeterminación informativa, en vía constitucional y normativa, permite al titular conocer y/o acceder a la fuente de obtención de sus datos personales publicados por un tercero en una red social.

III. Una mirada crítica a los fundamentos constitucionales peruanos

Sin duda, el primer antecedente cronológico y genérico que sustenta la existencia de regímenes de protección de datos personales a nivel global es el respeto por la dignidad humana. Ello, con el paso del tiempo ha permitido la proliferación de múltiples derechos que componen la esfera de personalidad, entre ellos, la individualidad, la privacidad, la intimidad e, inclusive, más recientemente, el control sobre los datos personales. Así, hoy en día, pese a los percances técnicos, **la protección de los datos personales o la autodeterminación informativa constituye un derecho fundamental, subjetivo, autónomo y con una función facilitadora o habilitadora de otros derechos fundamentales**, tal como lo son la privacidad y la intimidad.

---

4 Tribunal Constitucional. Expediente 01163-2022-PHD/Tribunal Constitucional, Piura, Edward Antonio Muñoz Salazar; 19 de mayo de 2023

5 *Ídem.*

Prueba de ello, es que "la defensa de la persona humana y el respeto de su dignidad son el fin supremo de la sociedad y del Estado"[6]. En esa misma línea, y en palabras del Tribunal Constitucional, el derecho a la autodeterminación informativa está reconocido en el artículo 2.6 de la Constitución Política del Perú (1993), el mismo que dispone "que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar".

Ello fue justamente reconocido -por primera vez- en el fundamento 3 de la Sentencia 1797-2002-HD/Tribunal Constitucional, que resolvió la Acción de Hábeas Data interpuesta por el señor Wilo Rodríguez Gutiérrez, a fin de que se le proporcione la información denegada sobre los gastos efectuados por el expresidente Alberto Fujimori Fujimori y su comitiva, tras un viaje de ciento veinte (120) días al exterior del país durante su mandato presidencial. En dicha oportunidad, el Tribunal Constitucional concluyó que:

> El derecho reconocido en el inciso 6 del artículo 2 de la Constitución es **denominado por la doctrina de 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**. 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**.

Como se viene argumentando, por su propia naturaleza, el derecho a la autodeterminación informativa es subjetivo al igual que cualquier otro derecho fundamental y, a su vez, está sustentado en la dignidad de la persona. Lo anterior impone un inherente deber de respeto por parte de terceros. Además de ello, su naturaleza también es relacional o facilitadora (o habilitadora); lo que implica que las exigencias que demandan su respeto se encuentren muchas veces vinculadas a la protección de otros derechos constitucionales.

Esa misma perspectiva es compartida por la doctrina europea. Así, la Agencia de los Derechos Fundamentales de la Unión Europea [FRA] y el Consejo de Europa (2018) advirtieron que si bien la protección de los datos personales es un derecho moderno y activo que establece "(…) un sistema con mecanismos de control para proteger a los ciudadanos cuando sus datos personales sean objeto de tratamiento"[7] , es más amplio que el derecho al respeto de la vida privada o íntima.

---

6 Constitución Política del Perú [Constitución Política del Perú], 1993, artículo 1.

7 Agencia de los Derechos Fundamentales de la Unión Europea [FRA] y el Consejo de Europa. *Handbook on European data protection law*. Agencia de los Derechos Fundamentales de la Unión Europea, 2018, p. 21-22.

Esta protección afecta al tratamiento de datos personales, independientemente de la relación que se tenga con la privacidad -e intimidad- y sus efectos sobre ella. No obstante, si bien el tratamiento de datos personales podría violar el derecho a la vida íntima o privada, no es necesario demostrar una violación de las anteriores para aplicar la normativa sobre protección de datos personales[8]. Por ello, autores comunitarios como Oostven e Irion (2018) reconocen que es un derecho de tercera generación que, al igual que la privacidad, no es un fin en sí mismo porque su protección contribuye, de manera inherente, a promover otros derechos y libertades fundamentales individuales, es decir, poseen lo que se denomina una **enabling function** [función habilitadora o facilitadora][9].

Al respecto, autores británicos como Lynsky (2014), han añadido que la protección de datos personales y la privacidad son derechos separados, pero muy superpuestos a la vez[10]. La privacidad es solo uno de los derechos e intereses protegidos por las normas de protección de datos; sin embargo, dado el poco tiempo de aplicación en contraste con otros derechos, las funciones independientes de protección de datos aún no se han terminado de articular por completo.

En cuanto al plano local, León (2011) considera que el numeral 6 del artículo 2 de la Constitución Política del Perú "se limita, nítidamente, a la intimidad de la vida privada y familiar, que es bien distinta de ese aspecto de la personalidad revelado en la jurisprudencia del Tribunal Constitucional alemán, tres décadas atrás, con el nombre de informationelle Selbstbestimmung [autodeterminación informativa]"[11]. A continuación, se explicará cronológicamente dicha postura.

La jurisprudencia constitucional alemana dio origen a la "teoría de las esferas", influyente desde finales de la década de 1950. Tal como comenta Alexy, el Tribunal Constitucional Federal Alemán concibió una serie de círculos concéntricos, o esferas que componen el derecho a la personalidad. Para ello, se delinearon diferentes áreas basadas en distintos grados de lo privado (como se cita en González, 2014[12]): la "*Individualsphäre*", "*Privatsphäre*" e "*Intimsphäre*"[13]. Es por ello que tal teoría evolucionó y se diseminó en otros idiomas y países. Sin embargo, ello no sería más que el antecedente que sustentaría el posteriormente develado

---

8 *Ibid.*, pp. 22-23.

9 OOSTVEEN, M., & IRION, K. (2018). *The Golden Age of Personal Data: How to Regulate an Enabling Fundamental Right?* In M. Bakhoum, B. Conde Gallego, M-O. Mackenrodt, & G. Surblytė-Namavičienė (Eds.), Personal Data in Competition, Consumer Protection and Intellectual Property Law: Towards a Holistic Approach? (pp. 7-26). Vol. 28. Springer.

10 LYNSKEY, O. (2019). *Grappling with "data power": normative nudges from data protection and privacy*. Theoretical Inquiries in Law. 20(1), 189-220.

11 LEÓN, Leysser. *Manipulación de Información Personal y Derechos Fundamentales*, 2011, p.2.

12 GONZÁLEZ, G. (2014). *The emergence of Personal Data Protection as a fundamental right of the EU.* Springer.

13 Como señala León (2011), la teoría de la personalidad a su vez cuenta con un debate dicotómico. Por un lado, la versión pluralista de esta teoría considera que existe un elenco de derechos de la personalidad (intimidad, imagen, nombre, honor, etc.). Por el otro lado, la pugna monista de creación alemana y reinante en la experiencia germana defiende que mediante la protección constitucional de la dignidad de la persona y del libre desenvolvimiento de la personalidad permiten deducir de esta, en el nivel aplicativo, y según las exigencias del momento, múltiples "aspectos" individuales a tutelar (p.17).

"*Informationelle Selbstbestimmung*" [autodeterminación informativa], mediante una sentencia del "*Bundesverfassungsgericht*" en el año 1983: Así, "¿cómo –me pregunto– un derecho recogido en la Constitución española de 1978, importado a nuestro ordenamiento jurídico desde 1993, va a ser el mismo derecho reconocido por el Bundesverfassungsgericht solo en 1983?[14]"

Con ello, la teoría alemana de las esferas fue la primera base cronológica y conceptual para lo que la evolución actual reconoce en la Carta de los Derechos Fundamentales de la Unión Europea[15], con estatus de ley primaria en todos sus países miembros, como el derecho a la privacidad[16] y el derecho a la protección de datos[17]. Por otro lado, en el caso peruano, también tal teoría de las esferas habría arribado por medio de la influencia española a fines de la década de los '70. En España, el artículo 18.4 de la Constitución Española de 1978 dictaminó que: "La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de sus derechos"[18]. Este hecho, como León (2006) advierte, incidió en cómo el Tribunal Constitucional peruano reconoció el derecho a la autodeterminación informativa, pues la Constitución Política del Perú vigente desde 1993 curiosamente mantiene gran similitud con la redacción de su predecesora del año 1979, momento desde el cual se incorpora constitucionalmente en el Perú la protección de la intimidad personal y familiar frente a los servicios informáticos. Es decir, la versión peruana se habría inspirado, a su vez, en la entonces reciente Constitución Española que, más allá de reconocer la autodeterminación informativa, velaba por la intimidad personal y familiar frente al avance de la tecnología.

Muchos años han pasado desde que en 1978 la Constitución Española adoptó predominantemente el término intimidad que, como se vio, sería a su vez importado a varios otros ordenamientos latinoamericanos como el peruano. Sin embargo, en la actualidad, el panorama español ya es otro: uno más comprensivo

---

14 LEÓN, L. (2006). Derechos de la personalidad y medios de comunicación [Tesis de doctorado, Scuola S. Anna di Pisa].

15 Redactada en 2000 y modificada en 2007. Así, tal documento entró en vigor el 1 de diciembre de 2009 gracias a la firma del Tratado de Lisboa suscitada el 13 de diciembre de 2007. La importancia de tal documento en la materia es su introducción de una base legal explícita para la legislación de protección de datos en el artículo 16º del Tratado de Funcionamiento de la Unión Europea [TFUE].

16 "Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones" (Carta de los Derechos Fundamentales de la Unión Europea, Artículo 7º, 2009).

17 "1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.
2. Estos datos se tratarán de modo leal para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación.
3. El respeto de estas normas estará sujeto al control de una autoridad independiente." (Carta de los Derechos Fundamentales de la Unión Europea, Artículo 8º, 2009).
En esencia, tal artículo 8 de la Carta se formula varios años después de la entonces vigente Directiva 95/46/CE, Directiva sobre protección de datos personales. En ese sentido, el primero incorporó o reconoció a nivel fundamental, la normativa preexistente en dicha Directiva (FRA y Consejo de Europa, 2018).

18 Al respecto, Murillo y Piñar (2009) detallan cómo el Tribunal Constitucional de España ha señalado en múltiples ocasiones desde el último siglo, que el fundamento constitucional para la protección de datos personales no solo sería tal artículo 18.4º de la Constitución, sino también su artículo 10.2º junto con la Carta de los Derechos Fundamentales de la Unión Europea (p.94-98).

y relacional que sigue la línea de la Carta de los Derechos Fundamentales de la Unión Europea. Así, como bien señalan los autores españoles Murillo y Piñar (2009), para el Tribunal Constitucional de España "la facultad de controlar la información es un derecho fundamental nuevo, autónomo e independiente del derecho a la intimidad"[19]

Ante tal panorama, algunos autores como León (2011) son más escépticos y rechazan incluso que el artículo 2.6 pueda configurar un reconocimiento expreso de la autodeterminación informativa. Por ello, consideran que la única vía constitucional correcta para reconocer esta tutela sería el "artículo 3 de la Carta Política, que permite deducir de la dignidad de la persona la necesidad de proteger a esta última frente a los riesgos propiciados por las nuevas tecnologías, (…) el almacenamiento y circulación de la información personal"[20]

Por su lado, autores como Castro critican directamente varios puntos de la redacción constitucional, esencialmente por la interdependencia de protección de datos de carácter personal y el derecho a la intimidad. Además, advierten que la referencia se realiza solo a una de las múltiples facultades del derecho de autodeterminación informativa[21] y la circunscripción como sujetos obligados solo ante los servicios informáticos[22], desconociendo todos aquellos que no lo sean (como se cita en Castillo, 2009).

En esa misma línea, Eguiguren (2004) señala que tal redacción abarca a la autodeterminación informativa "en forma defectuosa e insuficiente, pues solo autoriza expresamente al titular a oponerse a que se suministren informaciones que afecten su intimidad personal y familiar"[23].Por ello, indica que una interpretación literal debe descartarse porque "no incluiría el derecho de la persona a acceder (conocer y recibir) (…) sin esta facultad, mal pueden ejercitarse acciones como solicitar y exigir la rectificación o actualización de datos inexactos

---

[19] MURILLO, P. & PIÑAR, J. (2009). El derecho a la autodeterminación informativa. Fundación Coloquio Jurídico Europeo. https://www.fcjuridicoeuropeo.org/wp-content/uploads/file/Libros_Publicados/Cuadernos_Fundacion/EL%20DERECHO%20A%20LA%20AUTODETERMINACION%20INFORMATIVA.pdf

[20] León, L. Manipulación de Información Personal y Derechos Fundamentales. , 2011, p. 2.

[21] La redacción del artículo 2.6º de la Constitución Política del Perú dispone que "no suministren informaciones que afecten la intimidad personal y familiar". Ello alude a facultades de control sobre, negarse u oponerse, bloquear, cancelar o hasta denegar cierto tratamiento de datos personales. Sin embargo, hay varias otras facultades de control relativas al acceso y uso, actualización, rectificación, u otras que se dejarían de mencionar en dicha fórmula constitucional.

[22] A su vez, la interdependencia en la fórmula legislativa entre intimidad y servicios informativos podría tender a interpretaciones sesgadas que deriven en una discriminación subjetiva violando estándares y principios internacionales en torno al respecto del principio de neutralidad y no discriminación de entornos sistemáticos frente a aquellos que no lo sean, i.e. espacios físicos. Como bien señala la Red Iberoamericana de Protección de Datos (RIPD) la aplicación del principio de neutralidad tecnológica en el tratamiento de datos implica "*que la regulación sea neutral y temáticamente, es decir, que aplica a cualquier tratamiento de datos con independencia de las técnicas, procesos o tecnologías actuales o futuras que se utilicen para dicho efecto*". La existencia del derecho a la intimidad, la privacidad y la autodeterminación informativa, así como cualquier otro derecho fundamental que deriva de la personalidad existe con independencia del entorno físico, digital o sistema informático ante el que se encuentre una persona.

[23] EGUIGUREN, F. (2004). *El nuevo Código Procesal Constitucional peruano*. Derecho PUCP (Revista de la Facultad de Derecho PUCP), (57), p. 177.

o falsos ni, mucho menos, la supresión"[24]. Sin embargo, para el autor, esta contingencia podría ser posteriormente subsanada con la redacción del código procesal de la materia.

Con ello, posteriores sentencias como la Sentencia 04227-2009-PHD/Tribunal Constitucional, 06164-2007-PHD-Tribunal Constitucional[25], o 238/2022-PHD/Tribunal Constitucional de recurso de agravio constitucional de Hábeas Data permitirían aclarar con más detalle el contenido y núcleo de la autodeterminación informativa. Al respecto, este derecho:

> 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. (…) 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.[26]

Además, en la Sentencia 00693-2012-PHD/Tribunal Constitucional, el Tribunal Constitucional (2012) estableció que toda persona tiene derecho a hacer uso, por sí misma, de los datos personales que terceros públicos o privados tengan en su poder. Por ello, la autodeterminación informativa también implica el obtener copia de los datos personales:

> El derecho a la autodeterminación informativa también **supone que una persona pueda hacer uso de la información privada que existe sobre ella**, ya sea que la información se encuentre almacenada o en disposición de entidades públicas, o sea de carácter privado. En ese sentido, parece razonable afirmar que **una persona tiene derecho a obtener copia de la información particular que le concierne, al margen de si ésta se encuentra disponible en una entidad pública o privada**.[27]

Por todo lo anterior, Eguiguren (2015) afirma que esta protección constitucional tendría dos (2) dimensiones: (i) una negativa, "facultad que asiste al titular del derecho de prohibir el registro, la difusión y transmisión de datos referidos a información de carácter personal sensible" ; y, (ii) una positiva, "facultad del titular del derecho de poder controlar los datos concernientes a la propia persona"[28], que comprende el inspeccionar, verificar, actualizar, corregir y cancelar los datos o informaciones referidas a su persona[29].

---

[24] *Ibid* p. 177-178

[25] Mediante dicha sentencia, el Tribunal Constitucional (2007) en una función pedagógica, dictaminó los distintos tipos de hábeas data existentes.

[26] Tribunal Constitucional. Expediente 4739-2007-PHD/Tribunal Constitucional, Lima, Pesquera Virgen del Valle S.A.C.; 15 de octubre de 2007

[27] Tribunal Constitucional. Sala Primera. Expediente 00693-2012-PHD/Tribunal Constitucional, Lambayeque, José Manuel Curipuma Alburqueque. (24 de julio de 2012). https://www.tc.gob.pe/jurisprudencia/2013/00693-2012-HD.html, pág. 133

[28] EGUIGUREN, F. (2015). El derecho a la protección de los datos personales. Algunos temas relevantes de su regulación en el Perú. Themis, 131-140.

[29] *Idem.*

IV. Otra mirada a la acción de hábeas data

Como se ha esbozado, el derecho a la autodeterminación informativa comprende una serie de facultades para justamente garantizar su pleno ejercicio. Sin embargo, tales facultades específicas no se encuentran del todo claras o concretizadas en las sentencias estudiadas, ni tampoco en la fórmula constitucional que, a criterio del Tribunal Constitucional, ampara tal derecho. Sin embargo, habiendo zanjado algunos percances técnicos en el reconocimiento constitucional del derecho a la protección de datos personales, vale la pena ahondar en la normativa a cargo del proceso constitucional para proteger tal derecho, que es la Acción de Hábeas Data.

Tal recurso de agravio constitucional 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)[30] y 6)[31] de la Constitución" (Constitución Política del Perú., 1993, Numeral 3 del artículo 200º). Aquí cabe advertir que el artículo 59° de la Ley 31307, "*Nuevo Código Procesal Constitucional*" [Código Procesal Constitucional] (2021) ha dispuesto que "el Hábeas Data procede en defensa, no solo del derecho a la autodeterminación informativa, sino también ante el derecho de acceso a la información pública reconocido en el inciso 5) del artículo 2 de la Constitución".

Para ello, existen concretamente dieciséis (16) modalidades enunciadas en tal artículo 59º[32]. Sin embargo, destacan las siguientes modalidades por ser afines a la

---

30 Tal inciso faculta a lo siguiente:
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. 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. (Constitución Política del Perú, 1993, inciso 5 del artículo 2º).

31 "A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar" (Constitución Política del Perú., 1993, inciso 6) del artículo 2).

32 Siendo las demás modalidades las siguientes:

- Reparar agresiones contra la manipulación de datos personalísimos, almacenados en bancos de información computarizados o no.
- A modificar la información contenida en el banco de datos, si se trata de información falsa, desactualizada o imprecisa.
- A incorporar (i) en el banco de datos información que tengan como finalidad adicionar una información cierta, pero que, por el transcurso del tiempo, ha sufrido modificaciones; (ii) información que tiene como objeto aclarar la certeza de un dato que ha sido mal interpretado; y, (iii) al banco de datos una información omitida que perjudica a la persona.
- A eliminar de los bancos de datos información sensible que afecte la intimidad personal, familiar o cualquier otro derecho fundamental de la persona.
- A impedir (i) que las personas no autorizadas accedan a una información que ha sido calificada como reservada; y, (ii) la manipulación o publicación del dato en el marco de un proceso, con la finalidad de asegurar la eficacia del derecho a protegerse.
- A que el dato se guarde bajo un código que solo pueda ser descifrado por quien está autorizado para hacerlo.
- A solicitar el control técnico con la finalidad 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.

facultad de acceso y, por ende, también a la presente investigación: (i) conocer y supervisar 1. la forma en que la información personal viene siendo utilizada, 2. el contenido de la información personal que se almacena en el banco de datos, 3. el nombre de la persona que proporcionó el dato y 4. el lugar donde se almacena el dato con la finalidad de que la persona pueda ejercer su derecho; y, (ii) esclarecer los motivos que han llevado a la creación de la base de datos.

Ante ello, el Tribunal Constitucional considera que se permite la acumulación de "pretensiones de acceder y conocer informaciones de una persona, con las de actualizar, rectificar, incluir, suprimir o impedir que se suministren datos o informaciones[33]". Igualmente, con respecto a la posibilidad de si únicamente pueden ejercerse, mediante el Hábeas Data, pretensiones que estén expresamente contenidas en las dieciséis (16) modalidades jurisprudencialmente previstas (y legalmente recogidas en el Código Procesal Constitucional), debe advertirse que las mismas "no tienen por qué entenderse como limitadas a los casos que establece la ley. Hay posibilidad de extender su alcance protector a otras situaciones o alternativas (…). La propuesta del artículo 60 [actual artículo 61] es simplemente enunciativa"[34]

Es decir, en vía jurisprudencial se habría abierto dicha posibilidad de ampliar el alcance protector a otras alternativas no contempladas en el Código Procesal Constitucional para proteger la autodeterminación informativa. No obstante, aún con esa cláusula abierta, se advierte que las modalidades previstas en el Código Procesal Constitucional ya contemplan múltiples disposiciones en torno a garantizar la facultad de acceso de la autodeterminación informativa.

No debe perderse de vista que el recurso de Hábeas Data tiene como finalidad proteger los derechos constitucionales amparados en el artículo 2, incisos 5 y 6) de la Constitución Política del Perú, es decir el: "reparar las cosas al estado anterior a la violación o amenaza de violación de un derecho constitucional, o disponiendo el cumplimiento de un mandato legal o de un acto administrativo". Por ello, como requisito especial para interponer la demanda de Hábeas Data el artículo 57.2 del Nuevo Código Procesal Constitucional (2021) dispone que deben indicarse por qué razones "en el archivo, registro o banco de datos individualizado obra información referida al agraviado; los motivos por los cuales considera que la información que le atañe resulta discriminatoria, falsa, inexacta o violatoria de la intimidad personal o familiar".

Con ello, —y como bien se ha dicho— tal Acción de Hábeas Data también procede contra el hecho u omisión por parte de cualquier autoridad, funcionario o persona jurídica o natural que vulnera o amenaza los derechos contemplados en el artículo 2, incisos 5) y 6), de la Constitución Política del Perú.

- A impugnar las valoraciones o conclusiones a las que llega el que analiza la información personal almacenada.

33 Tribunal Constitucional. Expediente 06164-2007-HD/Tribunal Constitucional, Arequipa, Jhonny Robert Colmenares Jiménez; 21 de diciembre de 2007

34 *Idem.*

Así, ya va quedando claro que en vía constitucional el derecho a la autodeterminación informativa sí comprende el conocer y supervisar la forma en que la información personal viene siendo utilizada por parte de otros terceros (incluyendo personas naturales), el contenido de la información personal que se almacenaría en tal banco de datos, el nombre de la persona que proporcionó el dato, el lugar donde se almacena el dato, así como el esclarecer los motivos (finalidades) que han llevado a la creación de la base de datos en donde se almacenan los datos personales. **Es decir, la facultad de acceso a los datos personales en vía constitucional, mediante la Acción de Hábeas Data, cuenta con una función de información amplia e integral.** Además, tal facultad de control no se limita necesariamente a la fórmula legislativa del Código Procesal Constitucional y puede extenderse en vía interpretativa en favor del titular de tales datos personales. Por supuesto, sin perjuicio de los límites o excepciones que podrían surgir frente a otros derechos o bienes jurídicos tutelados, como los que se pretenden estudiar en la sección siguiente.

V. Límites ¿o interacciones? Constitucionales de la autodeterminación informativa

Tal como se argumentó, el derecho constitucional de la autodeterminación informativa es un derecho autónomo que posee una naturaleza subjetiva y relacional frente a otros derechos fundamentales. Así, a veces la protección y/o ejercicio del derecho a la autodeterminación informativa puede contribuir a la protección de otros derechos constitucionales (e.g. el honor, la voz, la intimidad, privacidad u otros); pero, también debe advertirse que en otros casos podría más bien contraponerse al ejercicio de estos[35]. Ello ha sucedido en recurridas sentencias frente a derechos o principios fundamentales como la libertad de expresión y de información, por lo que determinar el interés público y otros bienes constitucionales en juego termina siendo clave para identificar, de ser el caso, qué facultades de control de la autodeterminación informativa debieran verse limitadas en su totalidad o parcialmente frente a los mismos.

Por ejemplo, en la Sentencia 01163-2023-PHD/TC el Tribunal Constitucional (2023) reiteró, con base en una cita de la Sentencia 0134-2003-PHD/TC, que el Hábeas Data "no es un proceso destinado a obligar a los periodistas o empresas periodísticas a revelar sus fuentes de información, que, por lo demás, se encuentran protegidas por el artículo 2, inciso 18, de la Constitución, y menos a impedir el libre ejercicio de la libertad de comunicar."[36] .

---

35 Por ejemplo, recientemente el Tribunal Constitucional ha reconocido que "el avance vertiginoso de la tecnología ha generado la proliferación de información y datos de toda índole mediante diversos motores de búsqueda, sistemas informáticos, bases de datos o dispositivos tecnológicos que se encuentran al alcance de toda persona de forma global. Esta hipervisibilización de data, en ocasiones, puede intervenir en el contenido protegido del derecho a la protección de datos personales, en conexidad con otros derechos fundamentales" (Tribunal Constitucional. Expediente 03041-2021-HD/Tribunal Constitucional, San Martín, Miguel Arévalo Ramírez; 17 de junio de 2022).

36 Tribunal Constitucional. Expediente 0134-2003-PHD/Tribunal Constitucional, Lima, Ernesto Gamarra Olivares; 20 de septiembre de 2004

Sin embargo, tal cita debe ser contextualizada para un mayor entendimiento. En dicha oportunidad, si bien el Tribunal Constitucional (2003) se pronunció con respecto al Hábeas Data, el derecho cuestionado no era en estricto y únicamente la autodeterminación informativa. Así, el petitorio del demandante, entre otras cosas, versaba sobre que la información —fotografía en su ficha de identificación policial en donde se le implicaba en casos de corrupción- que había sido difundida por los medios de comunicación demandados violaron sus derechos constitucionales a la presunción de inocencia, a la intimidad personal y a su dignidad personal. A ello, el Tribunal Constitucional (2003) curiosamente se pronunció con respecto a una posible violación al derecho de acceso a la información pública previsto en el inciso 5 del artículo 2 de la Constitución Política del Perú[37] ante la negativa de los ministerios emplazados a brindar la información requerida en tanto que, como se ha visto, tal derecho también es amparado vía el Hábeas Data. Además, el Tribunal Constitucional (2003) también se pronunció sobre el requisito procesal relativo a que la información pública solicitada en vía de dicho proceso debe "ser cierta, completa, clara y, además, actual"[38]

A la luz de lo detallado, resulta cuestionable si efectivamente el Tribunal Constitucional (2003) hubiese querido sentar un límite irrestricto por parte del Hábeas Data contra ambos derechos protegidos, i.e. la autodeterminación informativa y el acceso a la información pública. En todo caso, es de resaltar que el ejercicio de los periodistas o empresas periodísticas efectivamente se encuentran protegidas por el artículo 2, inciso 18, de la Constitución, al igual que el libre ejercicio de la libertad de comunicar. No obstante, ello no siempre será un límite irrestricto a la autodeterminación informativa. Por el contrario, dicha determinación pasa más por una evaluación ad hoc, caso por caso, a fin de determinar qué interés público protegido primaría en caso de existir un conflicto de intereses.

Ante ello, en la Sentencia 0442-2017-PA/TC[39], el voto en mayoría del Tribunal Constitucional reconoció que, porque un ciudadano ingrese al ámbito de

---

37 Así en la Sentencia, el Tribunal Constitucional (2003) consideró que:
"El derecho reconocido en el inciso 5, artículo 2, de la Constitución señala 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 relativas a la intimidad personal y las que expresamente se excluyan por ley o por razones de seguridad. Según el demandante, los codemandados ministerios de Justicia y del Interior supuestamente habrían violado este derecho al negarse a informarle quiénes entregaron la fotografía a Caretas."

38 Tribunal Constitucional. Expediente 0134-2003-PHD/TC, Lima, Ernesto Gamarra Olivares; 20 de septiembre de 2004

39 Si bien en dicha oportunidad el recurso interpuesto fue un amparo y no un Hábeas Data para proteger el derecho a la libertad de información y expresión del demandante, los fundamentos permiten analizar cómo las facultades de control de la autodeterminación informativa de los usuarios en sus cuentas personales de redes sociales y otras plataformas priman frente al derecho de información de terceros. No obstante, cabe resaltar que el voto singular de dos (2) magistradas señalaron lo contrario, indicando que pese a haber sido una cuenta personal creada antes del ejercicio de la función pública incluso, la retransmisión y emisión de opiniones o juicio de valor sobre el ejercicio de las funciones públicas convertía, de facto, a tal cuenta de usuario en un canal de comunicación del Gobierno con los ciudadanos. Ante tal criterio, se concluyó que sí debió haberse compelido el desbloqueo del usuario. Finalmente, en tal oportunidad el Tribunal

funcionario público o a la arena política, no implicará el renunciar a su intimidad o su vida privada, ni mucho menos una sobreexposición de la misma. Por ello, "aquello no involucra que jurídicamente todo funcionario(a) público(a) está obligado a admitir a cualquier persona en sus redes sociales en cuentas de carácter personal[40]". Por ello, tal tribunal consideró que, como cualquier usuario: "los altos funcionarios estatales tienen la potestad de decidir, en ejercicio responsable de su capacidad de autodeterminación, qué información comparte en sus redes sociales y con quiénes comparte aquello que divulga"[41].

Así, en tal oportunidad se concluyó que no se puede compeler a una persona, incluso si es un alto funcionario público, a que desbloquee a determinada(s) persona(s) de su(s) cuenta(s) de correo electrónico o de redes sociales si las mismas tienen carácter estrictamente personal. Por tanto, la libertad de información de un tercer usuario bloqueado en la cuenta personal de una red social de un usuario, inclusive si es funcionario público, no primará frente a la autodeterminación del titular de tal cuenta personal donde justamente es este último quien debe determinar con quién se comunica o deja de hacerlo.

Para mayor análisis, en otro caso el Tribunal Constitucional consideró mediante la Sentencia 119-2022-HD/TC declarar infundado un recurso de agravio constitucional, tras una demanda de Hábeas Data exclutorio, contra distintos medios de comunicación y otros medios de difusión social como motores de búsqueda. En tal oportunidad, el demandante solicitaba ejercer su ***derecho al olvido***[42] frente a distinta información o noticias en la que se le imputa "ser narcotraficante internacional, líder de una organización dedicada al tráfico ilícito de drogas y lavado de activos, lo que afecta su honor y su buena reputación. Señala que la información publicada es falsa". Ante ello, el Tribunal Constitucional (2022) reconoció que:

> (…) como todo derecho fundamental, el derecho al olvido también está sujeto a restricciones o limitaciones derivadas, esencialmente, de la necesidad de que sea armonizado con otros derechos o bienes

Constitucional (2019) analizó y opinó a detalle sobre el funcionamiento y particularidades de las redes sociales, entre ellas, Twitter.

40 Tribunal Constitucional. Expediente 0442-2017-PA/Tribunal Constitucional, Lima, Erick Américo Iriarte Ahon; 15 de agosto de 2019

41 *Idem.*

42 Sobre el significado de tal "derecho al olvido" el Tribunal Constitucional consideró que debía entenderse lo siguiente:
"sin perjuicio de ulteriores precisiones jurisprudenciales, puede afirmarse que este garantiza la eliminación, supresión o retiro de información relacionada con datos personales que, usualmente vinculada al nombre de la persona, es posible hallarse usando motores de búsqueda o sistemas informáticos que hayan estado disponibles al público por un determinado tiempo, y que, habiendo sido ajustada a la realidad en su oportunidad, como consecuencia de nuevas condiciones fácticas y/o jurídicas relevantes, ya no lo es o no lo es plenamente, de modo tal que su difusión, ahora de contenido abiertamente inexacto, genera un perjuicio al titular de la información, en particular, respecto al contenido de su derecho fundamental al honor y a la buena reputación (artículo 2, inciso 7 de la Constitución), respecto del derecho fundamental al libre desarrollo de la personalidad (artículo 2, inciso 1 de la Constitución) o, eventualmente, respecto de su derecho a la intimidad (artículo 2, inciso 7 de la Norma Fundamental)." (Tribunal Constitucional. Expediente 03041-2021-HD/TC, San Martín, Miguel Arévalo Ramírez; 17 de junio de 2022).

> constitucionales. En particular, es evidente que dicho derecho fundamental puede ingresar en tensión con el derecho fundamental a la libertad de información, reconocido en el artículo 2, inciso 4 de la Constitución, el cual es, además, una garantía institucional crucial para el mantenimiento de un sistema democrático.

Ante ello, **el Tribunal Constitucional dejó en claro que la investigación del delito, específicamente en materia de narcotráfico y terrorismo resulta trascendental en el marco democrático de nuestra sociedad**; por ello:

> (…) toda investigación dirigida contra una persona, en cualquier nivel, acerca de sus supuestos vínculos con la supuesta comisión de los delitos de narcotráfico y terrorismo, goza de la más alta relevancia e interés público, y constituye, a todas luces, un hecho noticioso que debe ser objeto de escrutinio a través del ejercicio del derecho fundamental a la libertad de información.[43]

Además, cabe precisar que en dicha oportunidad y a criterio de los magistrados, las noticias e información objeto de análisis fueron consideradas como parte del **propio ejercicio periodístico**, es decir, se limitaban a "dar cuenta de las investigaciones que se le han realizado y que han sido publicadas o difundidas en el marco del ejercicio de la libertad de información"[44]. Por ello, tampoco se advirtió que las anteriores constituyen "en modo alguno un insulto o crítica abusiva que represente un trato que humille o degrade a la persona del recurrente"[45]

Si bien, en el caso explorado el Tribunal Constitucional determinó un claro límite en torno a la autodeterminación informativa, **sería interesante contar con mayores mecanismos o jurisprudencia en donde se observe que las limitaciones impuestas a la autodeterminación informativa gozaron de un análisis y resultado proporcional, flexible y/o parcial**. Es decir, casos en los que la decisión final no versara sobre si aplicar una decisión binaria y radical (sí o no) sobre todas las facultades de control que el contenido de dicho derecho proporciona.

Por ejemplo, Meguías (2019) comenta cómo es que en la jurisprudencia española y europea ya se han generado soluciones proporcionales al ejercicio de la autodeterminación informativa frente a otros intereses públicos o derechos fundamentales de terceros en juego: "los datos personales en principio quedan protegidos de su difusión inconsentida, pero no siempre, pues puede prevalecer

---

43 Tribunal Constitucional. Expediente 03041-2021-HD/TC, San Martín, Miguel Arévalo Ramírez; 17 de junio de 2022

44 Tribunal Constitucional. Expediente Nº 03041-2021-HD/TC, San Martín, Miguel Arévalo Ramírez; 17 de junio de 2022

45 *Idem.* Con ello, sería interesante ahondar en una investigación que determine los presupuestos de objetividad y límites a la acción periodística, como el Tribunal Constitucional (2003) señaló en su momento: "El Hábeas Data no es un proceso destinado a obligar a los periodistas o empresas periodísticas a revelar sus fuentes de información, que, por lo demás, se encuentran protegidas por el artículo 2, inciso 18, de la Constitución, y menos a impedir el libre ejercicio de la libertad de comunicar." Aunque en la misma línea y oportunidad tal tribunal reconoció que a su vez "se exceptúan las informaciones relativas a la intimidad personal y las que expresamente se excluyan por ley o por razones de seguridad" (Tribunal Constitucional. Expediente Nº 0134-2003-PHD/Tribunal Constitucional, Lima, Ernesto Gamarra Olivares; 20 de septiembre de 2004).

el derecho a la información (cuando se trata de unos hechos de interés general) o el ejercicio de la libertad de expresión y opinión"[46].

Frente a la prevalencia del derecho de información, los Meguías (2019) también rescata que los "tribunales exigen para su licitud que los datos personales difundidos sean mínimos (como puede ser el nombre y apellidos) y obtenidos de un modo legal"[47].

Mientras que, para el ejercicio de la libertad de expresión y opinión, "cuando se trata de una opinión –no información– (…) no resulta de aplicación la normativa de protección de datos personales más que para solicitar la cancelación del comentario u opinión y buscar el amparo legal a través de la protección del honor y buena fama[48]", en tanto tales derechos conexos se consideren lesionados

VI. Ámbito de aplicación de la Ley de Protección de Datos Personales ante los usos "domésticos, personales o relacionados con la vida privada o familiar"

En línea con lo anterior, a nivel normativo, el artículo 1 de Ley de Protección de Datos Personales (2011) indica que su objeto es "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".

Así, la Ley de Protección de Datos Personales (2011) es la norma aplicable a todos los datos personales contenidos (o destinados a ser contenidos) en bancos de datos personales de administración pública y privada siempre que su tratamiento se realice dentro del territorio nacional. Es decir, su ámbito de aplicación es únicamente territorial, difiriendo con otros ordenamientos jurídicos, como el RGPDP (2016), que se aplica a todo tratamiento de datos personales en el extranjero, en tanto estos pertenezcan a ciudadanos europeos. Por ello, para el ámbito de aplicación territorial deben observarse, concurrentemente, los criterios del artículo 5° del Reglamento (2013).

Adviértase que según el artículo 53 del Código Procesal Constitucional (2021) se considerará a un "archivo, registro, base o banco de datos a todo conjunto de datos organizado de información personal y que sean objeto de tratamiento o procesamiento físico, electrónico o computarizado, ya sea público o privado, y cualquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso". Ante ello, por su lado y con una redacción muy similar, la Ley de Protección de Datos Personales (2011) esboza su propia definición de banco de datos personales: "conjunto organizado de datos personales, automatizado o

---

46 Tribunal Constitucional. Expediente Nº 03041-2021-HD/TC, San Martín, Miguel Arévalo Ramírez; 17 de junio de 2022

47 *Idem.* Para más información, ver Sentencia 1960/2013 de la Sala de lo Contencioso-Administrativo de la Audiencia Nacional, de 10 de mayo de 2013 y Sentencia 594/2017 de la Sala de lo Contencioso-Administrativo de la Audiencia Nacional, de 14 de febrero de 2017.

48 *Ibid., p. 158*

no, independientemente del soporte, sea este físico, magnético, digital, óptico u otros que se creen, cualquiera fuere la forma o modalidad de su creación, formación, almacenamiento, organización y acceso" (artículo 2.1 de la Ley de Protección de Datos Personales) [49].

Ahora bien, la definición de tratamiento comprende a cualquier operación o procedimiento técnico, automatizado o no, en tanto permita "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" (numeral 19 del artículo 2, Ley de Protección de Datos Personales, 2011). Así, el tratamiento puede ser llevado a cabo por el responsable del tratamiento, el cual puede contar tanto con un encargo de tratamiento, como con una subcontratación. Además, nada impide que un titular de banco de datos personales sea el responsable o encargado del tratamiento.

Con ello, también debe mencionarse que la aplicación de tal Ley de Protección de Datos Personales (2011) ocurre con independencia de la modalidad del tratamiento de los datos personales, es decir, "ya sea efectuado por personas naturales, entidades públicas o instituciones del sector privado e independientemente del soporte en el que se encuentren" (artículo 3°, Decreto Supremo 003-2013-JUS "Reglamento de la Ley de Protección de Datos Personales" [Reglamento], 2013)[50]. Por ello, de existir normas particulares o especiales que incluyan regulaciones sobre datos personales, no excluirán el ámbito de aplicación de la Ley de Protección de Datos Personales (2011) y su Reglamento (2013) (artículo 3° del Reglamento, 2013).

Así, en cuanto a las excepciones al ámbito de aplicación, por un lado, se exceptúan a entidades del sector público, cuando sea "necesario para el estricto cumplimiento de competencias asignadas por ley (…) que tengan por objeto: la defensa nacional, la seguridad pública y, el desarrollo de actividades en materia penal para la investigación y represión del delito" (artículo 4 del Reglamento, 2013)[51]. Por otro lado, se exceptúan en el sector privado a los datos personales contenidos (o destinados a ser contenidos) en bancos de datos personales, creados por personas naturales siempre tal tratamiento sea realizado para **fines exclusivamente relacionados con usos domésticos, personales o relacionados con su vida privada o familiar** Sobre el particular, cabe preguntarse ¿qué debe entenderse por aquellos fines exclusivamente relacionados con usos domésticos, personales o relacionados con la vida privada o familiar de la persona natural que realiza el tratamiento?

---

[49] Un dato personal posee cuatro (4) elementos o componentes que, entre ellos, están "*estrechamente ligados y se complementan recíprocamente*" (Grupo de Trabajo del Artículo 29, 2007, p. 6).

[50] Decreto Supremo N.º 003-2013-JUS. Reglamento del Reglamento de la Ley Nº 29733, Ley de Protección de Datos Personales. https://cdn.www.gob.pe/uploads/document/file/1913756/DS-3-2013JUS.REGLAMENTO.LPDP_.pdf.pdf?v=1643315587

[51] *Idem.*

Para ello, deben tenerse en cuenta los siguientes cuatro (4) argumentos y consideraciones.

Primero, el contenido y límite inicial a la autodeterminación informativa está dada en vía constitucional, tal como se exploró en la sección anterior, este derecho aplica indistintamente a todos los "registros ya sean públicos, privados o informáticos a fin de enfrentar las posibles extralimitaciones de los mismos"[52] , pero atendiendo a las "restricciones o limitaciones derivadas, esencialmente, de la necesidad de que sea armonizado con otros derechos o bienes constitucionales"[53] con los que pueda entrar en tensión

Segundo, la fórmula legislativa es clara al reconocer que las excepciones legales (y no constitucionales) que el legislador ha decidido incorporar en tal régimen legal son aquellos **tratamientos** detallados en el artículo 4 del Reglamento (2013). Es decir, que, si bien se puede hablar de **tratamientos;** por su finalidad y carácter subjetivo —persona natural— de quien los realiza, se encuentran exceptuados de la aplicación de dicha ley[54].

Tercero, se requiere dilucidar qué debe entenderse por "fines o usos domésticos, personales o relacionados con la vida privada o familiar", los mismos que, al ser una excepción, deberán siempre interpretarse de manera restrictiva y no amplia para evitar vulneraciones no deseadas en la esfera de los posibles titulares de los datos personales afectados. Al respecto, en la jurisprudencia comparada, Meguías (2019) comenta que el Tribunal de Justicia de la Unión Europea [TJUE] también considera que:

> (…) la exclusión del ámbito de aplicación de la Directiva [ahora Reglamento][55] en relación a las actividades personales y domésticas debía ser interpretada siempre en sentido estricto, en primer lugar porque las restricciones a las garantías de los derechos fundamentales a la vida privada y a la protección de datos de carácter personal nunca deberán sobrepasar los límites de lo estrictamente necesario y, en segundo lugar, porque el propio

[52] Tribunal Constitucional. Expediente 06164-2007-HD/TC, Arequipa, Jhonny Robert Colmenares Jiménez; 21 de diciembre de 2007

[53] Tribunal Constitucional. Expediente 03041-2021-HD/TC, San Martín, Miguel Arévalo Ramírez; 17 de junio de 2022

[54] Igualmente, cabe mencionar que la Ley de Protección de Datos Personales (2013) y el RGPDP (2013) a lo largo de sus articulados también prevén otros tipos de excepciones más específicas. Por ejemplo, las excepciones al deber de consentimiento que se encuentran tipificadas en el artículo 14 de la Ley de Protección de Datos Personales, o la excepción prevista en el numeral 4 del artículo 28 de la Ley de Protección de Datos Personales (2013) relativa a "no utilizar los datos personales objeto de tratamiento para finalidades distintas de aquellas que motivaron su recopilación, salvo que medie procedimiento de anonimización o disociación".

[55] Cabe mencionar que el actual Reglamento UE 2016/679, Reglamento General de Protección de Datos Personales [RGPD] (2016) que sustituyó a la anterior Directiva UE 95/46/CE, sobre protección de datos, si bien introdujo múltiples cambios, en lo que atañe a la presente excepción, mantuvo en su artículo 2.2.c) una redacción idéntica a la del artículo 3.2 de la Directiva derogada. Así, se continúa excluyendo del ámbito de aplicación del RGPDP (2016) a todo tratamiento de datos personales "*efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas*" (literal c), del numeral 2 del artículo 2, RGPDP, 2016).

> texto normativo utilizaba el término exclusivamente para despejar las dudas que pudieran surgir en torno a la cuestión.[56]

Así, tal criterio o análisis no es ajeno a la realidad nacional. La Ley de Protección de Datos Personales (2011) curiosamente también emplea un texto similar **fines exclusivamente** y, como se viene detallando, el régimen legal de protección de datos personales peruano tiene justamente como objetivo el "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"[57].

Cuarto, ¿qué usos o supuestos específicos estarían comprendidos? Para responder a eso, puede ser de utilidad empezar analizando la doctrina comunitaria comparada para luego aterrizar en el país. Así, el considerando 18 del RGPD (2016) detalla, con relación a su artículo 2.2.c), que:

> El presente Reglamento no se aplica al tratamiento de datos de carácter personal por una persona física en el curso de una actividad exclusivamente personal o doméstica y, por tanto, sin conexión alguna con una actividad profesional o comercial. Entre las actividades personales o domésticas cabe incluir la correspondencia y la llevanza de un repertorio de direcciones, o la actividad en las redes sociales y la actividad en línea realizada en el contexto de las citadas actividades[58]. No obstante, el presente Reglamento se aplica a los responsables o encargados del tratamiento que proporcionen los medios para tratar datos personales relacionados con tales actividades personales o domésticas.

Así, por contraposición se esboza un (1) primer límite claro: la conectividad a alguna actividad ya sea profesional o comercial. A ello, la Agencia Española de Protección de Datos [AEPD] (2006) precisa que una finalidad será personal cuando "los datos tratados afecten a la esfera más íntima de la persona, a sus relaciones familiares y de amistad y que la finalidad del tratamiento no sea otra que surtir efectos en esos ámbitos" (como se cita en Loza, 2021).

Así, Meguías (2019) comenta que en aplicación de tal criterio de "exclusividad" también se debe tomar en cuenta si se está ante "ficheros mixtos", i.e., un "directorio telefónico, personal o familiar que sea utilizado simultáneamente en una actividad personal y otra no personal, como profesional, comercial, política, etc."[59] estos quedarían automáticamente sometidos a las exigencias establecidas en el RGPD (2016). Así, Loza (2021) también precisa que en algunos casos "lo personal

---

[56] MEGUIAS, J. (2019). RGPD y actividades personales en materia de protección de datos. Persona y Derecho. 80(2019/1), 147-178. http://dx.doi.org/10.15581/011.80. p. 165

[57] Ley Nº 29733. Ley de Protección de Datos Personales. (03 de julio de 2011). https://spij.minjus.gob.pe/spij-ext-web/#/detallenorma/H1034642

[58] Autores como Loza (2021) comentan que tal Considerando 18 del RGPD (2016) añadió como ejemplos de actividad personal o doméstica, a "*la actividad en las redes sociales y la actividad en línea realizada en el contexto de las citadas actividades*" gracias a la sugerencia realizada por el Supervisor Europeo de Protección de Datos (SEPD) pues la "*correspondencia y la llevanza de un repertorio de direcciones habían quedado un tanto obsoletos y debía contemplarse la realidad de internet*".

[59] MEGUIAS, J. (2019). RGPD y actividades personales en materia de protección de datos. Persona y Derecho. 80(2019/1), 147-178. http://dx.doi.org/10.15581/011.80. p. 165

y lo profesional aparece entremezclado en cuyo caso dichos tratamientos quedarían incluidos en el ámbito de aplicación de la ley al no tener como finalidad exclusiva el uso personal"[60].

En contraste a lo anterior, ¿qué pasa con aquellos datos personales generados en una esfera pública pero posteriormente empleados en una esfera privada? Aquí, Meguias (2019) opina que "el tratamiento de datos personales propios y ajenos realizado por una persona física no estará sujeto a las exigencias del RGPD cuando se trate de actividades exclusivamente personales o domésticas —aunque se hayan desarrollado en espacio público— con una finalidad privada". Un ejemplo de ello son datos personales de contacto que fueron obtenidos mediando una relación profesional por lo que tal actividad no puede ser considerada de naturaleza personal o doméstica; sin embargo, los mismos "pueden ser utilizados sin problemas posteriormente en una actividad exclusivamente personal". Ello, por ejemplo, sucede cuando un "trabajador que obtuvo lícitamente las direcciones electrónicas profesionales de sus compañeros mientras compartía trabajo con ellos en la misma empresa y que utilizó posteriormente para enviarles mensajes de carácter personal".

Además, tampoco hay que entender como un requisito que tal tratamiento sea realizado por un único individuo. La AEPD (2006) indica que "por ejercicio de una actividad personal no debe entenderse ejercicio de una actividad individual" (como se cita en Loza, 2021). Ante ello, Loza (2021) también opina que "no deja de ser personal aquella actividad de tratamiento de datos que aun siendo desarrollada por varias personas físicas su finalidad no trasciende de su esfera más íntima o familiar"[61].

En vista de lo anteriormente detallado, algunos ejemplos de exclusiones al ámbito de aplicación del RGPD, serían los directorios o agendas personales, los álbumes de fotos familiares y amistades, los registros de contabilidad familiar, los videos domésticos, los listados para invitaciones de celebraciones familiares o de amistad, etc., cuando no sean utilizados para una finalidad que exceda su cometido original. En caso de que tales ficheros fueran, por ejemplo, "difundidos en una red social sin limitación de acceso, o utilizados con fines comerciales, o en procedimientos judiciales, ya no les será de aplicación la excepción doméstica contemplada por el RGPD" (Meguias, 2019)[62].

Así, en sede local, dichos aspectos esbozados en torno al uso doméstico y personal también resultan aplicables. Autores como Morales (s.f.) detallan que "si una persona natural o jurídica, en calidad de usuario de una red social, crea su propio perfil con fines comerciales, empresariales o políticos, y en ese contexto realiza

[60] LOZA, M. (2021). Sobre la «Excepción Doméstica». Blog AEC GOVERTIS. https://dpd.aec.es/sobre-la-excepcion-domestica/

[61] *Idem.*

[62] MEGUIAS, J. (2019). RGPD y actividades personales en materia de protección de datos. Persona y Derecho. 80 (2019/1), 156. http://dx.doi.org/10.15581/011.80.147-178

tratamiento de datos personales, ya no se tratará de un uso doméstico o familiar"[63]. Así, afirma que tales usuarios "se convertirán en responsables del tratamiento" obligados a cumplir con las disposiciones de la Ley de Protección de Datos Personales (2011).

Ante ello, la misma autora comenta que "si bien no existe jurisprudencia en el Perú respecto a este caso en particular, podemos ver que la Dirección General de Datos Personales ha sancionado a varios colegios por haber subido a su página web las fotos de sus alumnos sin el consentimiento de sus padres o sus tutores"[64]. Por ende "cualquier persona natural o jurídica con un perfil comercial [o profesional] podrá ser sancionada por las mismas razones y criterios: tratar datos personales sin el consentimiento de su titular".

Además, una aplicación práctica de tales argumentos dentro de la normativa peruana es el ámbito de aplicación material de la Directiva 01-020-JUS/DGTAIPD, "Tratamiento de Datos Personales mediante sistemas de videovigilancia". Así, la Dirección General de Transparencia, Acceso a la Información y Protección de Datos Personales [DGTAIPD] exceptúa de tal ámbito de aplicación, con base en el artículo 4º del Reglamento (2011):

> (…) al tratamiento de imágenes en el ámbito personal y doméstico, que incluye el uso de cámaras 'on board'[65] y los sistemas de videoportería, salvo que estos últimos se articulen mediante procedimientos que reproduzcan o graben imágenes de modo constante y que resulten accesibles (mediante internet o emisiones por televisión en circuito cerrado) y, en particular, cuando el objeto de las mismas alcance a las zonas comunes y/o la vía pública colindante. (numeral 6.2.2 del artículo VI, Directiva, 2020).[66]

Con ello, vale acabar este capítulo comentando que la redacción peruana es muy similar a la europea, en tanto que ambos poseen **dos (2) requisitos indispensables para la verificación de la excepción estudiada**; y, en vista de ello, su aplicación en sede local también debiera serlo, al menos en esencia:

a. El primer requisito es que el tratamiento lo realice, en principio, **una persona natural**, aunque aquí también se ha visto que puede haber casos en que una o más personas realicen el tratamiento siempre que ello no desvíe el segundo requisito.

   De igual manera, si un tercero proporcionara los "medios" empleados para el tratamiento, y tal medio comparte un fin comercial o profesional en su

---

63 MORALES, A. (s.f.). *¿Cuál es el impacto jurídico que tiene el uso de redes sociales en lo que respecta al ámbito del derecho a la protección de datos personales?*. Agnitio.

64 *Idem.*

65 Una cámara "on board" según la Directiva (2020) es aquella "*instalada dentro de un vehículo, casco o vestimenta de un conductor, que permite grabar imágenes durante el recorrido que se realiza con el mismo*" (numeral 5.5. del artículo V, Directiva, 2020).

66 Directiva Nº 01-020-JUS/DGTAIPD. Tratamiento de Datos Personales mediante sistemas de videovigilancia. (14 de febrero de 2020). https://www.gob.pe/institucion/anpd/informes-publicaciones/1938476-directiva-para-el-tratamiento-de-datos-personales-mediante-sistemas-de-videovigilancia

funcionamiento (e.g., algunas plataformas o empresas que se dedican a organizar eventos y debieran proporcionar algún servicio a una lista de invitados a un evento familiar), tal tercero y los medios empleados sí deberán cumplir con la normativa de protección de datos personales en su funcionamiento. Lo anterior, sobre todo, por cuanto la finalidad del tratamiento y, con ello, del probable encargo que realicen sí tiene una finalidad económica. Así, la excepción alcanzará estrictamente al tratamiento concreto que realice la persona natural, siempre que pueda seguirse entendiendo dentro del segundo requisito.

b. El segundo requisito va ligado a que el tratamiento que realice tal persona natural sea justamente para un **fin estrictamente doméstico o personal**. Ahora bien, en el caso peruano el legislador añade un tercer supuesto que, lejos de generar mayor predictibilidad, resulta quizás redundante "o usos domésticos, personales o relacionados con su vida privada o familiar" (artículo 4, Reglamento, 2013)[67]. Ello, por supuesto, salvo que en vía interpretativa ingeniosamente se llegasen a prever supuestos de la vida privada o familiar que no estén comprendidos en lo doméstico o personal lo cual resulta difícil de dilucidar.

VII. Redes sociales frente a los usos "domésticos, personales o relacionados con la vida privada o familiar" de sus usuarios

Los servicios de redes sociales [SRS] pueden definirse generalmente como "plataformas de comunicación en línea que permiten a los individuos crear redes de usuarios que comparten intereses comunes" (pp. 4-5, Grupo de Trabajo del Artículo 29 [GT29], 2009). Así, para el GT29 (2009) los SRS comparten determinadas características: (i) sus usuarios deben proporcionar datos personales para generar su descripción o perfil; (ii) proporcionar también herramientas que permiten a sus usuarios poner su propio contenido en línea, que es el contenido generado por el usuario como fotografías, crónicas o comentarios, música, vídeos o enlaces hacia otros sitios; y, (iii) funcionan gracias a la utilización de herramientas que proporcionan una lista de contactos para cada usuario con los que pueden interactuar[68].

Además, cabe mencionar que los SRS "generan la mayoría de sus ingresos con la publicidad que se difunde en las páginas web que los usuarios crean y a las que acceden". Por ello, "los usuarios que publiquen en sus perfiles mucha información sobre sus intereses ofrecerán un mercado depurado a los publicitarios que desean

[67] Decreto Supremo N.º 003-2013-JUS. Reglamento de la Ley Nº 29733, Ley de Protección de Datos Personales. https://cdn.www.gob.pe/uploads/document/file/1913756/DS-3-2013JUS.REGLAMENTO.LPDP_.pdf.pdf?v=1643315587

[68] Para mayo detalle sobre los distintos tipos de SRS y su impacto en la protección de datos personales, ver: Barriuso, C. (2009). *Las redes sociales y la protección de datos hoy*. Anuario Facultad de Derecho - Universidad de Alcalá II. (pp. 301-3338). https://core.ac.uk/download/pdf/58906859.pdf

difundir publicidad específica y basada en esta información" (p. 5, Grupo de Trabajo del Artículo 29 [GT29], 2009).

En ese mismo sentido, Morales (s.f.) también advierte que un SRS "social se puede acceder, compartir, consultar, reproducir la información que se encuentra en los perfiles de sus usuarios, así como la que brindan estos durante su interacción en la red social, como pueden ser hábitos, fotografías, videos, entre otros"[69]. Por ello, considera como "innegable señalar que, en una red social, se produce lo que se conoce como tratamiento de datos personales". Asimismo, el autor menciona que entre los ejemplos de SRS más utilizados se encuentran Facebook, YouTube, WhatsApp, Twitter, Instagram, LinkedIn, Snapchat, entre otras.

En el ámbito jurisprudencial, un primer caso de relevancia en relación con las actividades en línea de usuarios de SRS fue dictado por el Tribunal de Justicia de las Comunidades Europeas [Tribunal de Justicia de la Unión Europea] (2003), pronunciándose sobre la calificación de la difusión sin consentimiento previo de datos personales de terceros a través de una web[70]. En dicha oportunidad, se zanjaron dos (2) criterios importantes que hoy sirven de base para el análisis en redes sociales[71]. Primero, que el "hacer referencia, en una página web, a diversas personas y en identificarlas por su nombre o por otros medios, como su número de teléfono o información relativa a sus condiciones de trabajo y a sus aficiones, constituye un tratamiento total o parcialmente automatizado". Segundo, que tal tratamiento consistente en "la difusión de dichos datos por Internet de modo que resulten accesibles a un grupo indeterminado de personas" no puede estar comprendido dentro de la excepción de actividades exclusivamente personales o domésticas, que ocurren dentro de la vida privada o familiar de las personas naturales (Tribunal de Justicia de la Unión Europea , 2003)[72].

Del mismo modo, Meguias (2019) interpreta que para el caso concreto de imágenes o vídeos que no son difundidas fuera del ámbito familiar no revisten problema alguno porque la incidencia sobre la privacidad de los afectados es mínima o nula[73]. Sin embargo, si los anteriores datos personales terminaran a disposición del

---

69 MORALES, A. (s.f.). *¿Cuál es el impacto jurídico que tiene el uso de redes sociales en lo que respecta al ámbito del derecho a la protección de datos personales?*. Agnitio.

70 En dicha oportunidad, Bodil Lindqvist, una ciudadana europea que impartía catequesis junto a otras personas en una parroquia sueca y quiso hacer más asequible la información a los participantes, razón por la que creó una web abierta y sin restricciones de acceso. Tal web contenía los nombres, números telefónicos, aficiones y otros datos del resto de los catequistas, pero sin haberles solicitado previamente su consentimiento. Cuando los anteriores mostraron su disconformidad al respecto la ciudadana eliminó la web.

71 Adicionalmente, en tal sentencia el TJUE (2003) precisó que las actividades personales y domésticas deben quedar referidas únicamente a las actividades claramente privadas y reservadas, es decir, confinadas en la esfera personal o doméstica de los interesados. Por tanto, una actividad que presenta una marcada connotación social, como la actividad de catequesis en el seno de la comunidad parroquial no califica dentro de ello. Menos aún, si se considera que adicionalmente el tratamiento implicó la divulgación de datos personales en una página web accesible desde cualquier parte del mundo.

72 Tribunal de Justicia de las Comunidades Europeas [TJUE]. (6 de noviembre de 2003. ECLI:EU:C:2003:596.

73 MEGUIAS, J. (2019). *RGPD y actividades personales en materia de protección de datos*. Persona y Derecho. 80 (2019/1), 159.

público en Internet vía una web o una plataforma, como lo es una SRS, entonces tal tratamiento ya no estaría excluido de la aplicación de las normas de protección de datos. Lo anterior "supondría la obligación de recabar el consentimiento explícito de los terceros afectados o, como mínimo, prever un fácil ejercicio del derecho de rectificación/cancelación por esos terceros".

Con ello, una primera conclusión en esta sección es que **una plataforma, web o un blog sin limitación de acceso exceden el ámbito doméstico; por lo que, en principio, los datos de carácter personal de terceros que se difundan a través de ella quedaban protegidos por la normativa de protección de datos personales**. Por supuesto, en tanto otros derechos constitucionales no primen total o parcialmente, como podría ser la libertad de información, expresión u otro interés público, y conforme se detalló líneas arriba.

A ello, García (2011) señala que un usuario en una red social, salvo que se le aplique la exención de ámbito doméstico o personal, "podría ser considerado responsable del tratamiento de datos respecto al fichero que constituye su cuenta"[74]. Esto además deja entrever que una cuenta de usuario o perfil propio puede ser considerada un fichero o, como en otras legislaciones se denominan, "bancos de datos personales". Asimismo, tal autora enfatiza que:

> El prestador del servicio online lo es [responsable] respecto el fichero privado creado por los registros de perfiles y contactos de los usuarios e independientemente de la responsabilidad sobre los datos de tráfico, localización y conservación del proveedor de servicios de comunicación pública en Internet. Exención de ámbito doméstico en el tratamiento de datos, ficheros privados, excepciones al derecho y fuentes accesibles al público[75], son categorías que están implicadas en el complejo entramado de contactos, datos, informaciones e interacciones que son las redes sociales online.

Es por ello por lo que la FRA y Consejo de Europa (2018) reconocen que ciertamente el acceso de los ciudadanos a internet y, con ello, "la posibilidad de utilizar plataformas de comercio electrónico, redes sociales y blogs para compartir información personal acerca de sí mismos y de otras personas hace que sea cada vez más difícil distinguir el tratamiento de datos para actividades personales"[76]

---

[74] GARCIA, R. (2011). *Redes sociales online: Fuentes de acceso público o ficheros de datos personales privados (Aplicación de las Directivas de protección de datos y privacidad de las comunicaciones electrónicas).* Revista de Derecho Político. (81), 151.

[75] Para mayores detalles, la autora aborda distintas cuestiones en torno a la naturaleza funcional de todos los registros de perfiles y contactos que cataloga como ficheros privados; por supuesto, con independencia de la responsabilidad sobre los datos de tráfico, localización y conservación del proveedor de servicios de comunicación en Internet. Sin embargo, al mismo tiempo la autora discute que la vocación de fuente de información pública parece estar en la esencia de estos sitios de colaboración o SRS, aunque arguye que al mismo tiempo puedan encajar en la definición legal de ficheros privados. Para la autora, las SRS viven una constante pugna o disyuntiva en torno a la exención de ámbito doméstico en el tratamiento de datos, ficheros privados y fuentes accesibles al público. Así, todas esas categorías están implicadas en el complejo entramado de contactos, datos, informaciones e interacciones que son las redes sociales online.

[76] Agencia de los Derechos Fundamentales de la Unión Europea [FRA] & el Consejo de Europa. (2018). *Handbook on European data protection law*. Agencia de los Derechos Fundamentales de la Unión Europea. http://doi.org/10.2811/343461

frente a aquellas otras no personales. Así, más pareciera ser que la consideración o determinación sobre si ciertas actividades califican como puramente personales o domésticas "depende de las circunstancias". Por ello, en una labor conciliadora, advierte que resulta "crucial que los usuarios sean conscientes de que subir información de otras personas sin obtener su consentimiento puede violar los derechos a la privacidad y la protección de datos de esas personas".

Ahora, deben tomarse en cuenta ciertos matices dentro del espectro de las redes sociales. Entre tales, la principal diferencia de una RSR frente a una web es que la primera "ofrece al usuario la posibilidad de restringir a una lista limitada de contactos el acceso a los contenidos o permitir el acceso a todos los usuarios de la red" (Meguias, 2019)[77]. De optarse por tal segunda opción, se aplicará lo detallado líneas arriba sobre las webs.

Por ello, de la mano de lo indicado por el GT (2009) y Meguias (2019) pueden irse concluyendo **tres (3) supuestos dentro de un SRS en los que no será de aplicación la excepción del uso doméstico o personal**:

- Como se vio líneas arriba, es claro que si un usuario actúa en nombre de una empresa o de una asociación o utiliza su cuenta o perfil o una actividad dentro de la misma tiene una connotación con fines principalmente comerciales, políticos o sociales.

- Si un usuario dentro de la SRS decide (o no puede) limitar su lista de contactos al ámbito familiar o de amistad, abriendo el acceso a su perfil y contenidos a personas completamente desconocidas o si los datos de tal perfil son indexables por los motores de búsqueda. En esa misma línea, si tal usuario decidiera con perfecto conocimiento de causa ampliar el acceso más allá de los amigos elegidos para cierto contenido, entonces asumirá nuevamente las responsabilidades de un responsable del tratamiento de datos.

- Si el usuario habiendo limitado su lista de contactos y, por tanto, el acceso al círculo estrictamente familiar o de amistad, incluye entre sus contenidos datos personales de carácter sensible de alguno de ellos o de terceros. Sin embargo, en este caso, la legislación europea sí podría diferir de la local, aunque no exista a la fecha un pronunciamiento concreto al respecto[78].

---

77 MEGUIAS, J. (2019). *RGPD y actividades personales en materia de protección de datos.* Persona y Derecho. 80 (2019/1), 166.

78 Al respecto, si bien no se cuenta con un pronunciamiento al respecto y no debiera distinguirse donde la ley no lo hace, salvo que medien razones que justifiquen dicha distinción razonable. La DGTAIPD (2015) en la Opinión Consultiva con Oficio 570-2015/JUS/DGPDP, opinó con respecto a las excepciones al deber de obtener el consentimiento libre, previo, expreso, informado e inequívoco de los datos personales que están contenidas en el artículo 14º de la Ley de Protección de Datos Personales (2011). En dicha oportunidad la DGTAIPD (2015) indicó que en tanto el artículo 14º no distingue entre datos personales sensibles y no sensibles, entonces dicha excepción específica al deber de obtención del consentimiento abarca por completo a cualquier tipo de dato personal (sensible o no).
Así, en la misma línea el artículo 4 del Reglamento (2013) habla de la totalidad de la aplicación de la Ley de Protección de Datos Personales (2011), por lo que ni en vía normativa, ni

Frente a lo anterior, en principio la actividad de los usuarios de redes sociales, incluyendo aquellos datos ajenos que son tratados por éste, se considera como actividad doméstica y personal si mantiene dicha actividad razonablemente en el ámbito de su lista de contactos al círculo más cercano. Sin embargo, como bien señala el GT29 (2009) siempre "habrá que analizar y ponderar cada caso concreto, pues ni todas las redes sociales son iguales, ni todas las que más o menos lo son ofrecen los mismos servicios" (como se cita en Meguias 2019)[79]. Así, siempre podrá probarse en contra y ningún argumento parece irrefutable ante tales conclusiones.

Ante los distintos matices o particularidades de las plataformas digitales, el propio Meguias (2019) pone de ejemplo que "un usuario puede publicar un tweet dirigido a sus seguidores convencido de que sus destinatarios constituyen un grupo restringido, pero la posibilidad ofrecida por la aplicación de retweetear ese mismo mensaje hace imposible que le pueda ser aplicada la excepción doméstica"[80]. De igual manera, otro debiera ser el análisis cuando "se crea un grupo de WhatsApp en el que los integrantes superan el círculo cercano del administrador y no existe relación entre ellos, pues los números de móviles suelen llevar asociados los datos de identificación (imagen y nombre) de los titulares de los terminales"[81].

VIII. ¿Qué comprende el derecho de acceso?

Como parte de la manifestación de las facultades de control previstas en el derecho a la autodeterminación informativa en vía constitución, la Ley de Protección de Datos Personales (2011) prevé que todo titular de datos personales goce de once (11) derechos. Entre ellos, los más importantes a esta investigación, el derecho de información[82] y el de acceso.

Así, el derecho de acceso se encuentra contenido en los artículos 19 de la Ley de Protección de Datos Personales (2011) y 61º del Reglamento (2013). Además, implica obtener información que sobre sí mismo sea objeto de tratamiento en bancos de datos públicos o privados; la forma en que se recopilaron sus datos; las razones que lo motivaron; a solicitud de quién se realizó tal recopilación; las

jurisprudencial se ha previsto esa salvedad con respecto a los datos sensibles que reflejan la esfera más íntima de una persona. Ahora bien, cuestión distinta es si tal matiz resultara positivo, proporcional y razonable a los titulares de datos personales peruanos frente a dicho supuesto.

79 MEGUIAS, J. (2019). *RGPD y actividades personales en materia de protección de datos*. Persona y Derecho. 80 (2019/1), 162.

80 Inclusive, el propio Tribunal Constitucional (2019) ha reconocido que Twitter es, esencialmente, una red social. Que, eventualmente, incluya contenido oficial de agencias estatales no altera dicha esencia —y, por tanto, el carácter voluntario de las interacciones que se den en ella. Igualmente, considera que "*en esta red social, predominaron las opiniones y juicios de valor, más que la información*". Pudiendo ser la información sometible a una prueba de veracidad, lo que no ocurre cuando se transmiten opiniones o juicios de valor ya que estas son eminentemente subjetivas. (Tribunal Constitucional. Expediente 0442-2017-PA/Tribunal Constitucional, Lima, Erick Américo Iriarte Ahon; 15 de agosto de 2019).

81 MEGUIAS, J. (2019). *RGPD y actividades personales en materia de protección de datos*. Persona y Derecho. 80 (2019/1), 162.

82 El alcance de derecho se encuentra definido en los artículos 18 de la Ley de Protección de Datos Personales (2011), el numeral 4 del artículo 12 y 60 del Reglamento (2013).

transferencias realizadas o previstas; la información relativa a sus datos personales[83]; y, todas las condiciones y generalidades del tratamiento a estos.

De igual manera, en la Opinión Consultiva 34-2020-JUS/DGTAIPD se ha concluido que este derecho nace de la "facultad de control que tiene el titular del dato personal sobre su información y, por ende, es un derecho personal que se basa en el respeto al derecho de protección de datos"[84]. El derecho de acceso, al igual que el resto, está concebido para materializar esa facultad de control, que la autodeterminación informativa implica.

El artículo 61 del Reglamento (2013) prevé que se tiene derecho a obtener del titular del banco de datos personales o responsable, toda la información relativa a sus datos personales, condiciones y generalidades de sus tratamientos[85]. Por ello, esta información debe ser extensa y abarcar todo el tratamiento realizado con respecto al titular de los datos personales independientemente de que se reciba un pedido; siendo su único límite los derechos de terceros.

Un caso práctico es la Resolución Directoral RD-044-2015-DGPDP. Aquí, se concluyó que "la información a la que podrá tener acceso el titular de los datos personales debe ser amplia y comprender la totalidad del registro correspondiente al titular del dato personal, aun cuando el requerimiento solo comprenda un aspecto de dichos datos". Esto comprende qué datos se vienen "utilizando, cómo y de dónde fueron recopilados, para qué finalidades se recopilaron, a solicitud de quién se realizó la recopilación, con quién comparten la información, qué transferencias se realizan, en qué condiciones están tratando los datos y cuánto tiempo". En este sentido, a pesar de que la reclamada "atendió la solicitud de acceso dentro del plazo, (…) no demuestra que cumplió con el derecho de acceso de acuerdo con la Ley de Protección de Datos Personales y su Reglamento, ya que solo indicó que la información de la reclamante la obtuvo de fuentes de acceso al público y que no realiza transferencia de sus datos personales a terceros"[86].

---

83 Probablemente, con la expresión: incluye a la información relativa a sus datos personales, se aluda a la metadata sobre los datos personales, es decir, aquellos datos sobre los datos personales, que sirven para suministrar información sobre los datos producidos y consisten en información que caracteriza a los datos, describen el contenido, calidad, condiciones, historia, disponibilidad y otras características de los datos a los que aluden. Lo anterior permite ubicar y entender los datos tratados. Para más información ver: https://www.geoidep.gob.pe/conoce-las-ides/metadatos/que-son-los-metadatos

84 Dirección de Protección de Datos Personales. Opinión Consultiva Nº 34-2020-JUS/DGTAIPD. (14 de julio de 2020). https://cdn.www.gob.pe/uploads/document/file/1745107/Sobre%20solicitud%20de%20acceso%20a%20los%20datos%20personales%20y%20acceso%20a%20la%20informaci%C3%B3n%20p%C3%BAblica.pdf.

85 Decreto Supremo N.º 003-2013-JUS. Reglamento del Reglamento de la Ley Nº 29733, Ley de Protección de Datos Personales. https://cdn.www.gob.pe/uploads/document/file/1913756/DS-3-2013JUS.REGLAMENTO.LPDP_.pdf.pdf?v=1643315587

86 Dirección de Supervisión y Control de la Dirección General de Protección de Datos Personales. Resolución Directoral Nº 044-2015-JUS/DGPDP-DS. (31 de julio de 2015). https://cdn.www.gob.pe/uploads/document/file/1365972/RD-44-2015-DS.pdf.pdf

De manera adicional, en cuanto a un límite que podría esbozarse en torno a tal derecho, en la Resolución Directoral 378-2017-JUS/DGTAIP-DPDP se afirmó que los datos personales de otros titulares de datos personales e información o documentos de terceros, inclusive si en estos se les alude o impacte, resultan un límite al ejercicio de este derecho, en tanto posee las siguientes características:

> a) La información solicitada debe corresponder exclusivamente a los datos personales del titular, ya que el derecho de acceso es la petición legítima del interesado a obtener información sobre sus propios datos personales y no de 'terceros', b) Si bien el derecho de acceso consiste en obtener información de los bancos de datos personales de administración privada o pública, esto no significa el acceso a documentos concretos que puedan contener información de 'terceros' como por ejemplo documentos de seguridad de la información.[87]

Con ello, queda en evidencia que, siguiendo la línea constitucional, **el derecho de acceso en vía legal también debe ser aplicado de manera amplia y abarcando todo el tratamiento realizado con respecto al titular de los datos personales**, incluso si tal pedido no fue pedido de manera concreta y detallada siendo en estricto el único límite, la vulneración de los derechos de terceros afectados. Así, también queda claro que en vía legal el derecho de acceso **comprende el conocer o informarse sobre la forma, fuentes y/o razones por las que se recopilaron sus datos**. Ahora bien, cuestión distinta es el determinar si ad hoc la revelación de tal información pudiera vulnerar algún derecho de un tercero en concreto. Ante lo cual, de argumentarse ello por parte de un responsable de tratamiento en la negativa a brindar tal información, siempre podrá recurrir a un procedimiento trilateral de tutela y/o a la vía judicial explorada, en ejercicio de su derecho de tutela.

IX. Conclusiones

a. Hoy en día, pese a los percances técnicos de su reconocimiento constitucional, la protección de los datos personales o la autodeterminación informativa constituye un derecho fundamental, subjetivo, autónomo, y con una función facilitadora o habilitadora de otros derechos fundamentales, tal como lo son la privacidad y la intimidad. Si bien, tal derecho comprende una serie de facultades para justamente garantizar su pleno ejercicio, tales facultades específicas no se encuentran del todo claras o concretizadas en vía jurisprudencial, ni en la fórmula constitucional del artículo 2.6 de la Constitución Política del Perú (1993). Sin embargo, mediante el recurso constitucional destinado a proteger tal derecho, el Hábeas Data, se ha enlistado de manera enunciativa más no taxativa, tanto jurisprudencial y normativamente vía el Código Procesal Constitucional, todas las

[87] Dirección de Protección de Datos Personales. Expediente Nº 004-2017-PTT. Resolución Directoral Nº 378-2017-JUS/DGTAIPD- DPDP. (1 de septiembre de 2017). https://cdn.www.gob.pe/uploads/document/file/589686/RD-378-2017-DPDP.pdf

modalidades de Hábeas Data para proteger la autodeterminación informativa.

b. La autodeterminación informativa y, con ello, el Hábeas Data permiten ejercer control sobre la información personal contenida en registros ya sean públicos, privados o informáticos. Incluso, el Código Procesal Constitucional contempla múltiples disposiciones expresas en torno a garantizar la facultad de acceso, específicamente el conocer y supervisar la forma en que la información personal viene siendo utilizada por parte de otros terceros (incluyendo personas naturales), el contenido de la información personal que se almacenaría en tal banco de datos, el nombre de la persona que proporcionó el dato, el lugar donde se almacena el dato, así como el esclarecer los motivos (finalidades) que han llevado a la creación de la base de datos en donde se almacenan los datos personales.

c. Por supuesto, la autodeterminación informativa no es un derecho irrestricto y comprende límites frente a derechos de terceros u otros bienes constitucionales en juego con los que debe armonizarse. Por ejemplo, el libre ejercicio de la libertad de información o comunicar, incluyendo el ejercicio de la función periodística, no siempre será un límite irrestricto a la autodeterminación informativa, pues pasa más por una evaluación ad hoc, caso por caso, a fin de determinar qué interés público protegido primaría en caso de existir un conflicto de intereses.

   Sin embargo, un límite sí ha quedado claro en vía jurisprudencial: "toda investigación dirigida contra una persona, en cualquier nivel, acerca de sus supuestos vínculos con la supuesta comisión de los delitos de narcotráfico y terrorismo, goza de la más alta relevancia e interés público, y constituye, a todas luces, un hecho noticioso que debe ser objeto de escrutinio a través del ejercicio del derecho fundamental a la libertad de información". Tal límite a su vez podría extenderse analógica y funcionalmente a otros delitos de igual o similar gravedad y trascendencia para el bienestar general, como lo son la corrupción, delitos de lesa humanidad, delitos de explotación sexual y contra menores, entre otros totalmente repudiables por nuestros cimientos democráticos y éticos.

d. No obstante, la conclusión anterior, para otros casos donde el interés público ni el bien protegido requiere de una imposición absoluta y radical frente a la autodeterminación informativa, sí sería interesante contar con mayores mecanismos o jurisprudencia en donde se observe que las limitaciones impuestas a la autodeterminación informativa gozaron de un análisis y resultado proporcional, flexible y/o parcial. Ello, en vez de aplicar una decisión binaria y radical (sí o no) sobre todas las facultades de control del titular de los datos personales. A ello, se ha visto cómo en algunos casos de legislación comparada sí se han esbozado algunas soluciones más proporcionales, flexibles y viables para tales casos.

e. En vía legal, la Ley de Protección de Datos Personales (2011) y su Reglamento (2013) junto con demás normativa orientativa o modificatoria constituyen el marco normativo de protección de datos personales. La anterior, posee algunas excepciones a su ámbito de aplicación previstas en su artículo 4º del Reglamento (2013), entre ellas, los bancos de datos personales creados por personas naturales siempre que tal tratamiento sea realizado para fines exclusivamente relacionados con usos domésticos, personales o relacionados con su vida privada o familiar.

f. Tal excepción, al igual que las demás previstas en tal artículo 4º del Reglamento, deberán siempre interpretarse de manera restrictiva y no amplia para evitar vulneraciones no deseadas en la esfera de los posibles titulares de los datos personales afectados. Además, tal excepción debiera verificar dos (2) requisitos indispensables para su aplicación:

- Que el tratamiento lo realice, en principio, una persona natural, aunque puede haber casos en que una o más personas realicen el tratamiento siempre que ello no desvíe el segundo requisito.

  Si un tercero proporcionara los "medios" empleados para el tratamiento, y tal medio comparte un fin comercial o profesional en su funcionamiento (por ejemplo, algunas plataformas o empresas que se dedican a organizar eventos y debieran proporcionar algún servicio a una lista de invitados a un evento familiar), tal tercero y los medios empleados sí deberán cumplir con la normativa de protección de datos personales en su funcionamiento. Lo anterior, sobre todo, por cuanto la finalidad del tratamiento y, con ello, del probable encargo que realicen sí tiene una finalidad económica. Así, la excepción alcanzará estrictamente al tratamiento concreto que realice la persona natural, siempre que pueda seguirse entendiendo dentro del segundo requisito.

- Que el tratamiento que realice tal persona natural sea justamente para un fin estrictamente doméstico, personal y/o relacionados con su vida privada o familiar.

g. Las SRS son plataformas de comunicación en línea que permiten a los individuos crear redes de usuarios que comparten intereses comunes, donde sus usuarios deben proporcionar datos personales para generar su descripción o perfil. Las SRS inclusive proporcionan herramientas que permiten a sus usuarios poner su propio contenido o generarlo en línea y funcionan gracias a la utilización de herramientas que proporcionan una lista de contactos para cada usuario con los que pueden interactuar. Ante ello, y contrariamente a lo expresado por el Tribunal Constitucional (2023), una plataforma, web o un blog sin limitaciones de acceso exceden el ámbito doméstico y personal; por lo que, en tales casos los datos de carácter personal de terceros que se difundan a través de ella debieran quedar protegidos por la normativa de protección de datos personales. Por supuesto, en tanto otros

derechos constitucionales no primen total o parcialmente, como podría ser la libertad de información, expresión u otro interés público.

h. Por ende, pese a lo indicado por el Tribunal Constitucional (2023), se ha visto que un usuario en una SRS, salvo que se le aplique la exención de ámbito doméstico o personal, sí podría ser considerado responsable del tratamiento de datos respecto al banco de datos personales que constituye su propia cuenta de usuario. Por su lado, el prestador del servicio online continuará siendo el responsable y titular del(os) banco(s) de datos personales creado(s) por los registros de perfiles y contactos de los usuarios e independientemente de la responsabilidad sobre los datos de tráfico, localización y conservación del proveedor de servicios de comunicación pública en Internet.

i. Se ha visto que deben tomarse en cuenta ciertos matices o particularidades dentro del espectro de las SRS ya que ni todas las SRS son iguales, ni todas las que más o menos lo son ofrecen los mismos servicios. No obstante, se pueden esbozar algunos criterios generales de ayuda donde se estará fuera de la excepción de uso personal, doméstico y/o privado o íntimo y será aplicable la normativa de protección de datos personales:

   - Si un usuario actúa en nombre de una empresa o de una asociación o utiliza su cuenta o perfil o una actividad dentro de la misma tiene una connotación con fines principalmente comerciales, políticos o sociales.

   - Si un usuario dentro de la SRS decide (o no puede) limitar su lista de contactos al ámbito familiar o de amistad, abriendo el acceso a su perfil y contenidos a personas completamente desconocidas o si los datos de tal perfil son indexables por los motores de búsqueda. En esa misma línea, si tal usuario decidiera con perfecto conocimiento de causa ampliar el acceso más allá de los amigos elegidos para cierto contenido, entonces asumirá nuevamente las responsabilidades de un responsable del tratamiento de datos.

   - Si un usuario habiendo limitado su lista de contactos y, por tanto, el acceso al círculo estrictamente familiar o de amistad, incluye entre sus contenidos datos personales de carácter sensible de alguno de ellos o de terceros. Sin embargo, en este caso, la legislación europea sí podría diferir de la local, aunque no exista a la fecha un pronunciamiento concreto al respecto.

j. Con ello, el derecho de acceso en vía legal también debe ser aplicado de manera amplia y abarcando todo el tratamiento realizado con respecto al titular de los datos personales, incluso si tal pedido no fue pedido de manera concreta y detallada siendo en estricto el único límite, la vulneración de los derechos de terceros afectados. Así, también queda claro que en vía legal el derecho de acceso comprende el conocer o informarse sobre la forma, fuentes

y/o razones por las que se recopilaron sus datos. Ahora bien, cuestión distinta es el determinar si ad hoc la revelación de tal información pudiera vulnerar algún derecho de un tercero en concreto. Ante lo cual, de argumentarse ello por parte de un responsable de tratamiento en la negativa a brindar tal información, siempre podrá recurrirse a un procedimiento trilateral de tutela y/o a la vía judicial explorada, en ejercicio del derecho de tutela que asiste a todo titular de datos personales.

k. Ante tal situación, algunos autores en la experiencia comparada han resaltado que resultaría deseable abordar mecanismos legales y prácticos más simples que permitieran a los usuarios de redes sociales, como responsables del tratamiento, cumplir con sus obligaciones derivadas y permitir el ejercicio de los derechos de terceros titulares de datos personales sobre todo cuando divulguen su información. Sin embargo, hasta la fecha resulta cuestionable si los usuarios de SRS siquiera conocen y/o son conscientes de la posible aplicación y obligaciones legales derivadas cuando difundan o traten datos personales de otras personas naturales. Lo anterior, sobre todo considerando que, como hemos visto, requiere de cierto nivel técnico y legal el determinar en qué supuestos específicos ello podría ocurrir. Quizás mecanismos y obligaciones más simplificadas, pero aterrizadas a las necesidades reales de usuarios en SRS y otros entornos digitales similares podrían garantizar una aplicación y protección adecuada de la autodeterminación informativa, y evitando así el incumplimiento masivo del régimen de protección de datos personales que vendría existiendo.

l. Así, respondiendo a la pregunta de este artículo, puede concluirse que los titulares de datos personales sí tienen derecho a exigir, en vía constitucional y normativa, el conocer la fuente de obtención de sus datos personales que sean publicados por usuarios de SRS en sus propias cuentas de perfil, salvo que mediaran las excepciones detalladas anteriormente. Particularmente, en el caso estudiado del Expediente 0134-2003-HD/TC, el Tribunal Constitucional debió dilucidar si la información personal de un tercero que fue difundida por un usuario de Facebook calificaba dentro del ámbito de uso doméstico o personal y/o privado o íntimo; y/o, en caso de no calificar dentro de tal excepción, si mediaba algún interés público o derecho de tercero que primara frente a la autodeterminación informativa del demandante (como podría haber sido la libertad de información u otros). Sin embargo, tal análisis nunca fue abordado.