DESAFÍOS DE LA PROTECCIÓN DE DATOS PERSONALES EN EL DERECHO DE LA UNIÓN EUROPEA

CHALLENGES OF PERSONAL DATA PROTECTION IN THE LAW OF THE EUROPEAN UNION

Alejandra Castillo Ara[*]

Resumen: Este artículo tiene por finalidad analizar desde una perspectiva práctica la aplicación y los desafíos que presenta el reglamento relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos de 2016. El legislador europeo ha creado una normativa marco estricta que tiende a proteger la autodeterminación informativa de las personas naturales. La pregunta que se plantea, sin embargo, es hasta qué punto esa autodeterminación informativa está dispuesta a ceder en aras del bien común y en qué medida esa tutela efectiva normativa es aplicable en la práctica, sin entorpecer de manera irremediable sustancial el tráfico cibernético y comercial al que los usuarios ya estamos acostumbrados.

Palabras clave: Datos personales, autodeterminación informativa, contratos internacionales.

Abstract: The purpose of this article is to analyze from a practical perspective the implementation and challenges presented by the General Data Protection Regulation from 2016. The European legislator has created a strict frame regulation that tends to protect the informational self-determination of natural persons. The question that arises, however, is to what extent this informational self-determination is willing to give way in the interest of the common good and to what extent this effective regulatory protection is in

[*] Abogada. Licenciada en Ciencias Jurídicas y Sociales, Universidad Adolfo Ibáñez. Legum Magister (LL.M.) y Dr. Iur. Albert-Ludwig Universität Freiburg. Legal Counsel para DKMS Alemania. castillo@dkms.de

the practice applicable without significant hindering the cybernetic and commercial traffic to which we users are already accustomed.

Keywords: Personal Data, Informational self-determination, International contracts.

Introducción

El 25 de mayo de 2016 entró en vigencia en el ámbito europeo el Reglamento General de Protección de Datos (RGPD), y su aplicación por parte de los tribunales se hizo obligatoria exactamente dos años después, el 25 de mayo de 2018. Este reglamento tiene por finalidad principal la protección de datos personales y su libre circulación. Datos que corresponden a personas naturales o en términos literales del Reglamento: "personas físicas".

El Reglamento busca en lo principal dos cosas en el ámbito marco: estandarización de reglas de tutela efectiva y sanciones acorde; y transparencia de los operadores económicos y estatales en materia de procesamiento de datos personales[1]. De manera progresiva los países europeos han ido adaptando el reglamento a su legislación interna con matices casi imperceptibles y respetando la esencia de la regulación supranacional. Sin embargo, esta implementación –en los hechos– no ha estado exenta de dificultades, ya que las pretensiones del legislador europeo se han encontrado con la dificultad práctica de la aplicación tecnológica[2]. En especial la falta de correspondencia entre las pretensiones jurídicas y la realidad cibernética y la deficiencia de conocimientos técnicos recíprocos. Los juristas poco saben de actualidad cibernética y los expertos cibernéticos poco conocen de la realidad jurídica.

Por otra parte, al ser los datos o el derecho a la protección de los mismos, un derecho fundamental relativamente nuevo, no resulta claro cuál es su peso específico ni en qué medida es admisible su ponderación respecto del interés común de la sociedad: los datos son una herramienta valiosa que permite predecir el comportamiento no solo de los individuos de manera aislada, sino que, también, de las decisiones grupales de una sociedad. De ahí su relevancia, por ejemplo, para los partidos políticos, la industria farmacéutica y cualquier empresa que quiera perfilar a sus consumidores con la finalidad de saber a quién y qué le vende, pero sobre todo cómo optimizar dichas ventas[3]. Lo cierto es que los datos son, para muchos, considerados el

[1] §13 Preámbulo del RGPD.

[2] Las multas por el no cumplimiento del RGPD pueden llegar a los veinte millones de euros.

[3] Valls (2016), p. 2.

"nuevo oro" y una suerte de moneda de transacción cuando se trata de vender y comprar información personal de los individuos.

Pero sobre todo, los datos pueden ser una forma valiosa en lo relativo a la prevención de la criminalidad[4]. Las empresas proveedoras de Internet podrían fácilmente monitorear las búsquedas en la red de los individuos e identificar quienes tienen tendencias pederastas, homicidas, etc. Relevancia especial en este sentido, cobra la criminalidad organizada. El problema, sin embargo, es no solo hasta qué punto se permite adelantar la punición de alguien que aún se encuentra en un acto que de manera dudosa podría calificarse de preparatorio, sino que hasta qué punto es admisible la afectación de la privacidad individual en beneficio del bien común. En otras palabras, hasta qué punto este derecho a la autodeterminación informativa se ve limitado por la seguridad pública[5].

La autodeterminación informativa es, en definitiva, un derecho derivado del derecho a la privacidad y del llamado derecho al libre desarrollo de la personalidad[6], aunque también se le interpreta como parte integrante de la dignidad humana, consagrada en el art. 1 de la Constitución Política de la República Federal Alemana (Grundgesetz/GG), por lo que –según alguna doctrina– no sería en realidad un derecho nuevo[7]. De cualquier manera, es evidente que el bien común puede justificar una limitación al ejercicio de este derecho, sin embargo, la pregunta es, ¿cuáles son los límites de esos límites?[8]. Mal que mal, tal como señala el Reglamento en el § 4 del preámbulo: "el tratamiento de datos personales debe estar concebido para servir a la humanidad" y este se rige por el "principio de proporcionalidad". El problema es determinar hasta qué punto están dispuestos los individuos a sacrificar su autodeterminación informativa, en tanto concesión de esferas de privacidad, por el bien común. Esa respuesta, lamentablemente, excede los límites de este trabajo.

El presente artículo tiene como referencia legal principal el Reglamento General de la Protección de Datos (RGPD o Reglamento) y toma como base de análisis la legislación alemana que fue, sin lugar a dudas, la que inspiró la regulación en el ámbito europeo[9] y la que se encuentra más desa-

[4] Valls (2016), p. 1.

[5] *Op. cit.*, p. 3.

[6] En la jurisprudencia, véase BVerfGE 65, 1 (42). En la doctrina, véase Hermstrüwer (2016), p. 32.

[7] Franzius (2015), p. 260.

[8] Pieroth, Schlink, Kingreen, Poscher (2016), p. 71 s.

[9] El concepto de protección de datos de la manera en que hoy se comprenden según el Reglamento, apareció por primera vez en Europa, en la legislación local federal del Estado de Hessen en Alemania en 1970. La primera versión de la Ley Federal Alemana de Protección

rrollada jurisprudencial y doctrinariamente en esta área. Este artículo tiene una pretensión especialmente práctica y se divide en cuatro apartados: el primero, analiza de manera breve la consagración de la protección de datos como un derecho fundamental. El segundo, analiza el ámbito de regulación y los principios generales del Reglamento. El tercer apartado hace referencia específica a los problemas y desafíos prácticos que presentan las exigencias del legislador europeo. Por último, se agregan consideraciones finales de cara a una eventual solución a las dificultades ya mencionadas.

1. La autodeterminación informativa como derecho fundamental

La protección de datos es –evidentemente– la referencia instrumental y, en cierta medida, el contrapunto del posible objeto de ataque de los derechos fundamentales; mientras que la autodeterminación informativa[10] hace referencia al objeto de protección y, por tanto, al aspecto sustantivo del derecho, en especial al procesamiento de datos personales[11]. El art. 8 de la Carta Europea de Derechos Humanos (CEDH) si bien consagra el derecho a la autodeterminación informativa, no lo define como tal[12]. Según el Tribunal Constitucional Federal alemán , el derecho a la autodeterminación informativa es el derecho de la persona a decidir sobre la divulgación y el uso de sus datos personales[13]. El término 'autodeterminación informativa' fue acuñado por el Tribunal Constitucional Federal alemán, en el denominado fallo Volkszählungsurteil (fallo sobre el censo nacional) de 15 de diciembre de 1983[14], concretando así

de Datos (BDSG) en el ámbito nacional fue aprobada el 27 de enero de 1977 con el título "Ley de Protección contra el Uso Indebido de Datos Personales en el Tratamiento de Datos".

[10] Alguna doctrina latinoamericana se refiere al derecho a la autodeterminación informática como el *habeas data*. Véase Nogueira (2005), p. 449 ss.

[11] Bieber (2012), p. 36 s.

[12] Art. 8. Protección de datos de carácter personal.

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.

[13] BVerfGE 65, 1 (42), sentencia de 15 de diciembre de 1983.

[14] Véase al respecto, el comentario de Bernhard Schlink sobre la evolución del concepto autodeterminación informativa luego de la decisión del Tribunal Federal. Schlink (1986), pp. 233-250.

la protección de la intimidad con respecto a los datos personales. El Tribunal Constitucional Federal lo entendió en ese entonces como un derecho que emanaba del libre desarrollo de la personalidad consagrado en el art. 2.1. del GG[15], y señaló al respecto:

> "El libre desarrollo de la personalidad en las condiciones modernas de procesamiento de datos requiere la protección del individuo contra la recopilación, almacenamiento, uso y divulgación ilimitada de sus datos personales. Esta protección está, por tanto, cubierta por el derecho fundamental del artículo 2.1 en relación con el artículo 1.1 de la Ley Fundamental. A este respecto, el derecho fundamental garantiza el derecho de la persona a decidir sobre la divulgación y el uso de sus datos personales"[16].

El Tribunal Constitucional Federal alemán interpreta la autodeterminación informativa como un derecho derivado del derecho general de la personalidad y de la dignidad humana, pero, a su vez, autónomo en tanto derecho fundamental, y ciertamente sienta las bases para la futura regulación legal de la protección de datos, en especial, el Reglamento que aquí se analiza.

2. Ámbito de regulación y los principios generales del Reglamento

a) Aplicación material y territorial

El RGPD regula el tratamiento de los datos personales de las personas físicas, por parte de otras personas físicas, empresas u organizaciones de la Unión Europea (UE) o empresas que recojan, procesen y utilicen datos personales de personas (físicas) que vivan en la UE[17]. No se aplica al tratamiento de datos personales de personas fallecidas o entidades jurídicas. Tampoco tiene

[15] Art 2. (1) Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt. (2) Jeder hat das Recht auf Leben und körperliche Unversehrtheit. Die Freiheit der Person ist unverletzlich.

Art. 2 1) Toda persona tiene derecho al libre desarrollo de su personalidad, siempre que no viole los derechos de los demás y no atente contra el orden constitucional o la ley moral. (2) Toda persona tiene derecho a la vida y a la integridad física. La libertad de la persona es inviolable [traducción de la autora].

[16] BVerfGE 65, 1, sentencia de 15 de diciembre de 1983 [traducción de la autora].

[17] Arts. 1, 2 y 3 del RGPD.

aplicación a los datos tratados por motivos exclusivamente personales o para actividades familiares, siempre que no exista una relación con una actividad profesional o económica[18].

Por ejemplo, sí entra en el ámbito de regulación del Reglamento el caso de una persona que compra un pantalón en la tienda Zara (en Alemania), cuyos datos serán procesados tanto por la empresa que vende dicho artículo (en España) como por la empresa que lo traslada (en Turquía). Los datos que se verán involucrados son: nombre, fecha de nacimiento, domicilio, talla, datos bancarios, etcétera.

El reglamento no resulta aplicable, por ejemplo, cuando una persona emplea los datos de amigos y familiares para celebrar el cumpleaños de su madre, utilizando nombres, números telefónicos, direcciones de domicilio, direcciones de correo electrónico, etc. Si bien aquí también hay datos personales involucrados, no tienen un carácter ni comercial ni estatal en su tratamiento, sino que son datos que operan en el ámbito absolutamente privado-familiar[19].

En el ejemplo recién citado, sobre la compra en la tienda Zara, se podría entender que quien compra también se encuentra sujeto por la normativa, pues igual recibe "datos" por parte de la tienda. Sin embargo, la tienda es persona jurídica y no física, y, por lo mismo, no se encuentra protegida por el Reglamento.

b) Ámbito de regulación: ¿qué son en definitiva los datos y en qué consiste su tratamiento?

Según el art. 4.1. del RGPD, se entiende por datos personales:

> "toda información sobre una persona física identificada o identificable ('el interesado'); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona".

Esta determinación viene, sin embargo, condicionada por el contexto. No es lo mismo hacer referencia a "una mujer, morena, de aproximadamente 30 años" en el contexto de una empresa española de novecientos trabajadores, pues mujeres de esas características hay muchas y no se puede saber a quién

[18] Art. 2 a), b), c) y d) del RGPD.
[19] Art. 2.1.d) del RGPD.

se hace referencia. Si se hace la misma referencia en el contexto de una pequeña empresa de cinco trabajadores en Suecia, donde la población morena no abunda, la situación cambia. En el primer ejemplo, esta descripción no presenta mayores problemas, pues las posibilidades de identificar a esa persona son casi nulas. En una empresa española de novecientas personas trabajan a lo menos quinientas con esas características; sin embargo, en el segundo, sería inadmisible, pues la persona sería fácilmente identificable.

Dentro de los datos personales, la normativa destaca una subcategoría; los llamados datos en especial sensibles. Estos datos constituyen una categoría especial de datos (art. 9 del RGPD), y se denominan sensibles, pues permiten revelar el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas o la afiliación sindical, datos relativos a la salud o a la vida sexual, etc., de las personas físicas. Estos datos solo podrán ser utilizados por los cuerpos y fuerzas de seguridad, cuando sea estrictamente necesario y solo si el derecho nacional establece garantías adecuadas para su resguardo[20].

Luego, el tratamiento de datos es definido por el art. 4.2. del RGPD como

> "cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción".

En definitiva, cualquier acción (por ejemplo: almacenar) y básicamente toda omisión (por ejemplo: no borrar), pueden constituir un tratamiento de datos personales.

[20] Art. 9 RGPD. A raíz de la pandemia desatada por COVID-19, el Parlamento alemán ha dictado una serie de leyes para sortear la situación de manera eficiente, entre ellas una ley sobre protección de la población en casos de situación de epidemia de relevancia nacional (Gesetz zum Schutz der Bevölkerung bei einer epidemischen Lage von nationaler Tragweite vom 27. März 2020), Reglamento sobre la reducción laboral (Kurzarbeitergeldverordnung vom 25. März 2020, etc. Y en la actualidad se discute si en aras del art. 9 i) del RGPD, se podría dictar una ley de excepción a la prohibición general de tratamientos de datos sensibles, basados en la causal i). Es decir, el tratamiento de datos resulta "necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios (...)", con la finalidad de establecer el llamado Corona-Tracking a través de una aplicación en los aparatos celulares, siguiendo el ejemplo exitoso de Singapur. Véase sobre la discusión en www.zeit.de/politik/deutschland/2020-03/coronavirus-massnahmen-einschraenkungen-bundesregierung-helge-braun [fecha de consulta: 29 de abril de 2020].

c) La minimización de datos o el principio de economía de datos

Tanto la economía de datos, como la minimización de los mismos, se puede decir que son los principios rectores de la normativa que aquí se analiza y la base que subyace a la regulación ulterior del Reglamento, en especial en el art. 5 1 a)-f). La idea constitutiva de la regulación en materia de datos personales, es que en el procesamiento de datos solo se recogen tantos datos personales como sean indispensables para la aplicación respectiva, porque es precisamente la recopilación innecesaria de datos personales –sensibles o no– por parte de organismos públicos y privados lo que va en contra del derecho fundamental a la autodeterminación informativa.

La minimización y el principio de economía de datos, se encuentran también regulados en el art. 3a del Reglamento Federal de Protección de Datos alemán (Bundesdatenschutzgrundverordnung/BDSG), según el cual los organismos públicos y privados que manejan datos personales deben trabajar siempre con la condición de que solo almacenen, utilicen o procesen la cantidad de datos que sea necesaria para el propósito respectivo. Además, estos datos deberían ser, en la medida de lo posible, anonimizados o pseudonimizados[21].

En este contexto, entra en juego otro principio básico de la protección de datos: la subordinación a la finalidad (*Zweckbindung*). Las autoridades y las empresas deben determinar primero el propósito para el que se van a recopilar los datos personales y, respecto de ese propósito, tratar los datos indispensables que se requieran para alcanzarlo. Entonces, recién sabiendo con claridad cuál es el propósito, se puede decidir qué datos son en realidad necesarios para su cumplimiento. Solo los datos personales que realmente tienen sentido en función de dicho propósito pueden ser almacenados, uti-

[21] § 3a Datenvermeidung und Datensparsamkeit

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten und die Auswahl und Gestaltung von Datenverarbeitungssystemen sind an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Insbesondere sind personenbezogene Daten zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verwendungszweck möglich ist und keinen im Verhältnis zu dem angestrebten Schutzzweck unverhältnismäßigen Aufwand erfordert.

§ 3a Evasión de datos y economía de datos

La reunión, el procesamiento y la utilización de datos personales y la selección y el diseño de sistemas de procesamiento de datos deben estar orientados al objetivo de reunir, procesar o utilizar la menor cantidad posible de datos personales. En particular, los datos personales serán anonimizados o seudonimizados en la medida en que ello sea posible de acuerdo con la finalidad del uso y no requiera un esfuerzo desproporcionado en relación con la finalidad de protección prevista.

lizados o procesados, si es necesario y estos solo podrán ser usados para ese propósito y no para otro. Por ejemplo, si la finalidad que se busca es hacer una transferencia bancaria. El banco solo necesita el nombre, RUT, número de cuenta y eventualmente una dirección electrónica de la persona. No se requiere ni estado civil, peso, antecedentes médicos, dirección laboral, etc. Esos datos exceden la finalidad de la transacción bancaria. La minimización de datos opera también dentro de un mismo consorcio empresarial. Por ejemplo, si recursos humanos decide amonestar a un trabajador por reiteradas faltas, y para ello reserva una sala de videoconferencia, la persona encargada del funcionamiento técnico de la sala de videoconferencia sabrá que recursos humanos reservó una sala, pero no sabrá con quién se establece la comunicación ni cuál es su contenido. Los mismos resguardos deben aplicar los trabajadores cuando imprimen documentos donde haya datos personales de externos o de los propios trabajadores. Se opera bajo un principio estricto de confidencialidad.

La economía de datos significa que el almacenamiento, procesamiento y la utilización de datos personales y la selección y el diseño de sistemas de procesamiento de datos, deben orientarse al objetivo de reunir, procesar o utilizar la menor cantidad posible de datos personales. Esto tiene especial relevancia para los consumidores, pues la economía de datos también se refiere a la renuencia del consumidor a revelar datos personales al margen de la información necesaria para una relación comercial, en especial en Internet, pero también físicamente. De ahí entonces, la obligación de tener siempre a disposición del interesado la declaración de voluntad (art. 7 del RGPD), que debe ser específica respecto de la finalidad para el tratamiento de datos[22]. Esa declaración de voluntad además de ser clara y precisa, debe señalar el propósito para el tratamiento y específicamente cuáles serán las acciones que se llevarán a cabo con dichos datos: almacenar, transferir, pseudonimizar, etc. El consentimiento también debe contener siempre la posibilidad de revocar dicho consentimiento. Ya sea a través de una dirección de correo físico o electrónico. Debe ser tan fácil retirar el consentimiento, como otorgarlo[23].

d) Pseudonimización y anonimización de datos personales

Como se señaló supra, el Reglamento protege los datos de carácter personal de toda persona física identificada o identificable. Esto significa que esta norma-

[22] Esta finalidad, sin embargo, tiene una excepción, y es la que se refiere a datos recabados con interés científico (art. 89.1. del RGPD). En la práctica qué califica como científico y qué no, suele ser decidido por un comité de ética del área en que se pretende emplear dichos datos.

[23] Art. 7.3. del RGPD.

tiva no se aplicará a datos que se encuentren anonimizados, pero sí a aquellos que estén en estado "normal", pero también a los que estén pseudonimizados. Ambos conceptos –pseudonimización y anonimización– se denominan comúnmente en conjunto "enmascaramiento de datos" (Data Masking)[24].

Datos anonimizados son aquellos respecto de los cuales no hay ningún medio de identificación de una persona física, directa o indirectamente. Un muy buen ejemplo de datos anonimizados son los votos de las elecciones típicas de sistemas democráticos. Las elecciones son secretas y –en un mundo ideal– anónimas. Es posible rastrear quién votó y quién no, pero no es posible construir mediante ese rastreo la conexión entre una determinada papeleta y un votante en particular. El factor decisivo en la anonimización es, en definitiva, que resulta imposible identificar a la persona física[25].

Las empresas recogen de manera regular datos sobre la atención y la lealtad de los clientes. Estos datos también se utilizan a menudo para analizar el comportamiento de los clientes y para identificar el contexto y los antecedentes de las compras a fin de planificar y apoyar de modo estratégico las actividades de comercialización y ventas. Sin embargo, para ello no se requieren los nombres de los interesados, y los datos anonimizados cumplen de igual forma su función.

Por su parte, datos paseudonimizados, son según el art. 4.5. del RGPD, datos personales de una persona física, que ya no puedan atribuirse a ella sin utilizar información adicional. Siempre que esta información adicional figure por separado y esté sujeta a medidas técnicas y organizativas que garanticen que los datos personales no se atribuyan a una persona física identificada o identificable. El ejemplo más clásico sería una dirección de correo electrónico que no se corresponda con el nombre de una persona, pero que es fácilmente averiguable, por ejemplo: mm@gmx.de. No dice a quién pertenece, ni se puede averiguar con solo recibir ese dato; la dirección de correo electrónico, pero si se contacta con el proveedor de Gmx, puedo de manera eventual acceder al nombre detrás de dicho correo: Max Mustermann. Lo mismo ocurre con los números de donantes, por ejemplo, en casos de donaciones de sangre o de médula. Los datos se pseudonimizan, pero se

[24] Melnick, Everitt (2008), p. 240 s.

[25] Art 3.6. BDSG. „das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können".

Art. 3.6 de la BDSG. "la alteración de los datos personales de tal manera que los detalles individuales de las circunstancias personales o fácticas ya no puedan atribuirse a una persona física específica o identificable o sólo puedan atribuirse a una persona física específica o identificable con un gasto desproporcionado de tiempo, costo y trabajo".

puede acceder a contactar a la persona, en caso de requerir, por ejemplo, un trasplante de médula para salvarle a la vida a una persona[26].

Los principios de protección de datos, entonces, se aplican a los datos seudonimizados, pero no a los anonimizados. Tampoco se aplica a los datos convertidos en anónimos de forma que el interesado no sea identificable, o deje de serlo. Esto tiene especial relevancia cuando se trata de información anónima que suele utilizarse con fines estadísticos o de investigación científica[27].

Los conceptos de anonimización y pseudonimización son dos cuestiones que en la práctica presentan una serie de dificultades, especialmente por la falta de comprensión conceptual al respecto y, por consiguiente, la constante confusión entre qué datos se encuentran anonimizados y qué datos pseudonimizados y, por tanto, qué datos deben o no deben someterse al Reglamento.

e) La finalidad específica para el tratamiento de datos: el principio de transparencia

Según el RGPD, "todo tratamiento de datos personales debe ser lícito y leal"[28]. Esto significa que para los interesados debe ser inequívoco el fin para el cual se están recogiendo, utilizando, consultando o tratando de cualquier otra manera datos personales que les conciernen. El interesado debe tener también claridad sobre cuáles son los datos personales que se van a procesar: edad, sexo, origen, altura, dirección, etc. Esto debe estar incorporado según el art. 7 del Reglamento en la declaración de voluntad que el interesado otorga para el tratamiento de sus datos.

Según el art. 13 del Reglamento, el principio de transparencia exige que toda información y comunicación relativa al tratamiento de estos datos personales sea fácilmente accesible y comprensible, para lo cual se debe utilizar un lenguaje sencillo y claro. El principio de transparencia se refiere en especial a la información que tiene el interesado sobre la identidad del responsable del tratamiento (empresa, entidad pública u organización) y sus fines, y a la información que se entrega para garantizar un tratamiento leal y transparente de ella.

[26] Así opera, por ejemplo, el „match" en el caso de los trasplantes de médula organizados por DKMS (deutsche Knochenmarkspende Datei) o por WMDA (World Marrow Donor Association). Al respecto véase www.dkms.de o, bien, https://wmda.info/. Esto también es sin perjuicio de las normas relativas al anonimato que se debe mantener entre donante y paciente durante los años posteriores a la donación según las mismas reglas de la WMDA.

[27] §26 Preámbulo y art. 89.1 del RGPD y art. 3.6 del Bundesdatenschutzgesetz (BDSG).

[28] §39 Preámbulo, art. 12 ss. del RGPD.

Comprende, también, el derecho a obtener confirmación y comunicación de los datos personales que les conciernan a las personas físicas que sean objeto de tratamiento. Implica especialmente, que las personas físicas tengan conocimiento de los riesgos, las normas, las salvaguardias y los derechos relativos al tratamiento de datos personales, así como del modo de hacer valer sus derechos en relación con este tratamiento, y la oportunidad inequívoca de retirar su consentimiento[29]. Los fines específicos del tratamiento de datos personales deben ser explícitos y legítimos, y deben determinarse en el momento de su recogida.

Los datos personales deben ser adecuados, pertinentes y limitados a lo necesario para los fines para los que sean tratados y no exceder dichos fines. Es decir, si una persona consiente en entregar datos para, por ejemplo, ser parte de un estudio de campo sobre sobrepeso, pero no para recibir *newsletter* o cualquier tipo de llamado telefónico (práctica que hasta hace poco era tan común en Chile por parte de bancos y otras entidades) ofreciendo productos para adelgazar o engordar. Los datos de la persona pueden solo ser usados para los fines respecto de los cuales esta consintió: un estudio científico respecto del sobrepeso. Si cambiara la finalidad para la cual se recogieron los datos, es necesario nuevamente obtener el consentimiento de la persona para esa nueva finalidad.

Esta finalidad específica del uso de datos, conlleva también un límite temporal en cuanto a su conservación. Los datos no pueden permanecer almacenados de manera ilimitada. Se debe garantizar su conservación a un mínimo estrictamente necesario de conservación. Por lo demás, el principio de la economía de datos lleva consigo una especie de *ultima ratio*. Es decir, existe autorización para el tratamiento de datos, siempre que su finalidad no pudiera lograrse de forma razonable por otros medios. El responsable del tratamiento, debe establecer plazos para su supresión o revisión periódica, y tomar todas las medidas razonables para garantizar que se rectifiquen o supriman los datos personales que sean inexactos. Los datos personales deben tratarse de un modo que garantice su seguridad y confidencialidad adecuadas, incluyendo medidas de carácter cibernético (uso de *software* de seguridad en el marco de programas de Compliance, por ejemplo) y físico que impidan, por ejemplo, el acceso o uso no autorizados de dichos datos y del equipo utilizado en el tratamiento[30].

[29] Art. 7 a), b), c) y d) del RGPD.

[30] Art. 32 del RGPD.

f) La licitud del tratamiento de los datos personales

La licitud del tratamiento de datos personales tiene relación con el fundamento normativo que legitima el tratamiento los mismos. Según el art. 6 del Reglamento, el tratamiento de datos puede tener solo ciertas bases legales y estas son enumeradas de manera taxativa por el legislador, no obstante –al ser el Reglamento una decisión marco de la Unión Europea– ser susceptible de especificaciones por parte de la legislación nacional.

Según el numeral 1 del art. 6 del Reglamento, el tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:

a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;
b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;
c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;
d) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física;
e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;
f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.

Lo dispuesto en la letra f) del párrafo primero no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones.

Solo el tratamiento basado en una o más de estas causales será legítimo. Si bien parece relativamente sencillo entender las bases del tratamiento de datos, en la práctica, resulta complejo limitarlo. Por ejemplo, uno de los fundamentos más comunes para el tratamiento de datos es la base contractual. Esto es, si se conceden datos a una contraparte contractual, por ejemplo, una inmobiliaria, para efectos de arrendar una casa en Ibiza, el tratamiento de esos datos será legítimo, pero con limitaciones. En este ejemplo, esta base contractual no habilita a la inmobiliaria para enviar todos los meses *newsletters* sobre otras posibles casas en Mallorca o en Ibiza misma. Los datos fueron autorizados solo para la celebración de ese contrato que tenía como finalidad arrendar una determinada casa en un determinado período en Ibi-

za y nada más. Cualquier otro uso que se le dé a esos datos escapa de esa base legal. Puede ocurrir también que en ese mismo acto de firmar el contrato se haya, a su vez, firmado un consentimiento explícito donde se autoriza a procesar datos para recibir ofertas sobre otras casas en la playa. En ese caso, estaría justificado, pero el uso de esos datos no sería lícito por la base contractual (art. 6 b) del RGPD), sino que lo sería en razón de un consentimiento expreso para esa otra finalidad: publicidad en este caso (art. 6 a) del RGPD).

g) La supresión o borrado de datos o el llamado "derecho al olvido"

El Reglamento regula no solo la supresión o borrado, sino que, también, el bloqueo y la rectificación de los datos personales (arts. 16 y 17 del RGPD). Los datos se rectifican toda vez que el interesado considere que sean inexactos o que estén incompletos. Los datos se deben borrar o suprimir, siempre que la finalidad para la cual fueron recabados y respecto de la cual el interesado ha entregado su consentimiento ha acabado en caso de que el interesado lo solicite de manera expresa. Junto con la finalidad y voluntad, acaba el consentimiento.

En el caso del bloqueo, sin embargo, es distinto, pues los datos no se eliminan, sino que se siguen manteniendo en las bases de datos y, por tanto, se siguen "tratando", en los términos de la ley, siempre que hayan razones justificadas que hagan suponer que su supresión pueda perjudicar los intereses legítimos del interesado. En ese caso, este bloqueo también tiene un límite temporal, pues los datos se encontrarán bloqueados (sin ser borrados) solo durante el tiempo que dure ese eventual peligro para los intereses legítimos del interesado[31].

El Reglamento, entonces, opera sobre una base de regla general respecto a la solicitud de supresión de datos: todas las personas tienen derecho a pedir que se borren sus datos y las organizaciones, empresas o entidades procesadoras tienen la obligación de hacerlo, salvo en casos excepcionales, enumerados en el art. 17 del Reglamento. *Grosso modo*, se trata de datos personales que sean necesarios para ejercer el derecho a la libertad de expresión; datos cuya mantención responda a una obligación legal o, bien, a motivos de interés público (como salud pública, fines de investigación científica o histórica, etcétera).

Respecto al derecho al olvido cibernético, se exige a las entidades procesadoras adoptar medidas razonables (de carácter cibernético) para informar a otros sitios web que un interesado ha solicitado la supresión de sus datos personales.

[31] Valls (2016), p. 18.

Dentro de las excepciones legales mencionadas, en el derecho alemán, por ejemplo, existe la llamada "obligación de almacenamiento", que se aplica a diversos ámbitos y con diversos plazos dependiendo del caso. Un ejemplo es lo establecido en materia laboral, respecto de los documentos de los postulantes a un puesto de trabajo, los cuales se pueden mantener por un período de seis meses.

Otro ejemplo se encuentra en el ámbito tributario y de seguridad social alemana. De acuerdo con el art. 147 (1) números 2, 3 y 5 del Reglamento Tributario Alemán (Abgabeordnung/AO), se aplica un periodo de retención de a lo menos seis años a los documentos comerciales y de negocios tales como: facturas, notas de entrega, estimaciones de costos y recibos de hospitalidad y otros documentos relevantes para los impuestos, a partir del final del año calendario en que fueron creados.

En estos casos y en todos los otros que la ley lo requiera, de solicitarlo la persona, los datos no se podrán borrar, pues hay una exigencia legal que así lo impide, pero se deberán bloquear y el interesado deberá ser debidamente informado al respecto.

3. Problemas y desafíos del Reglamento

Tal como se explicó supra, el procesamiento de datos representa una serie de novedades e incertidumbres que, por cierto, requieren de tiempo para alcanzar "madurez" en su aplicación. Sin embargo, se puede adelantar una serie de dificultades que se presentan en la aplicación práctica del Reglamento y que implican muchas veces una dicotomía entre las pretensiones del legislador y la realidad.

a) El procesamiento de datos en países que carecen de resguardos y normativa y el problema de la territorialidad

Según el art. 2 del Reglamento, este no se aplica a datos de personas físicas que no se encuentren en la Unión Europea. Esto genera un problema evidente en materia de contratación internacional, en especial con Estados Unidos, donde la protección de datos es casi nula, y sin considerar el riesgo constante de los ciberataques tanto a escala europea como internacional[32], en el caso en que se produzca transmisión de datos o el uso de nubes para guardar datos[33]. Debido a la portabilidad y la capacidad de almacenamiento de los productos digitales de la época moderna, así como la rapidez en la obtención

[32] Al respecto véase, Valls (2015), p. 147 ss.

[33] Europol (2015), p. 8; Clough (2010), p. 150.

y distribución de datos a través de File-Sharing, Networking, Share-Hosting, Streaming-Hosting, etc.[34], constituye una de las mayores dificultades de la protección de datos, el poder controlar de manera efectiva la transmisión de datos de un controlador a otro, así como los delitos cibernéticos en general.

Una de las eventuales soluciones que se podría dar a esto es eliminar a escala mundial la territorialidad en materia de tratamiento de datos y delitos cibernéticos. De lo contrario, el nivel de entorpecimiento de las relaciones comerciales y de la persecución de la criminalidad será en el mediano y largo plazo insostenible, y quedarán dos opciones: o el Reglamento perderá total eficacia, pues los operadores comerciales simplemente tienen que contratar por razones de necesidad con operadores que se encuentran en India, Malasia, Brasil, Malawi, etc., donde no se aplica el Reglamento y no existe una legislación análoga o, bien, las relaciones comerciales se verán entorpecidas de manera definitiva. Es más probable que ocurra lo primero.

Por su parte, en materia de cibercrimen, una de las grandes dificultades que representan los delitos cibernéticos al momento de su detección y persecución es el problema de la territorialidad. El derecho penal es por excelencia un área de regulación local. Este paradigma de funcionamiento del derecho penal ha sido desafiado precisamente por los avances de la tecnología cibernética y, por tanto, por los modos de ejecución que revisten los delitos cibernéticos. Un ataque DDoS (ataque de denegación de servicio que impide a los usuarios de una red acceder a esta, y que puede bloquear servicios básicos como el tendido eléctrico o los semáforos de una ciudad, entre otras cosas) puede generar sus efectos en Chile, pero la generación de la saturación de la red puede provenir de Finlandia. La lógica indica que, en materia de delitos cibernéticos, la territorialidad como principio debería desaparecer y la cibercriminalidad deberían operar bajo el principio de jurisdicción universal como ocurre con crímenes de lesa humanidad, en el entendido de que ambos tiene como objeto de protección, bienes o intereses que son centrales para la conservación del Estado como organismo político y social[35].

b) La tautología de la supresión de datos

Tal como se viera con anterioridad, en materia de protección de datos, siempre "menos es más". Se deben tratar tan pocos datos como sea posible

[34] Sieber (2012), p. C 30.

[35] El principio de jurisdicción universal ha sido reconocido en el derecho interno por algunos ordenamientos tales como el español, que de hecho fue lo que llevó al juez Baltasar Garzón a perseguir en su minuto a Augusto Pinochet. Este es el principio rector del derecho penal internacional. Más sobre este principio en Ollé (2008), p. 95 ss.

y siempre que sea absolutamente necesario. Sin embargo, cuando existe un manejo de datos de gran cantidad la posibilidad de cometer errores del tipo tecnológico y humano incrementa. Un problema constante es lo que ocurre con la supresión o borrado de datos. Si el interesado ha solicitado de forma expresa que se borren sus datos, y no habiendo una causa legal para mantenerlos, estos –en un modelo ideal de aplicación del Reglamento– deberían borrarse de inmediato de toda base de datos posible que tenga la entidad procesadora. Sin embargo, es posible que ese mismo interesado, llegue de nuevo como contacto a manos de esa entidad, pues esta compró a otra entidad una determinada base de datos y el interesado se encontraba entre ellos. Debido a que la entidad –en un cumplimiento estricto de la ley– borró todo rastro de dicha persona, no tiene atisbo siquiera de que alguna vez haya pasado por sus registros ni tampoco –evidentemente– de que alguna vez haya solicitado borrar sus datos, pues claro, fueron borrados. Luego es probable que la entidad en el envío de información sobre, por ejemplo, nuevas ofertas, un saludo de Navidad, aniversario, etc., contacte otra vez a esta persona –que llegó, esta vez, a través de una base de datos comprada– y con eso infringe el Reglamento. Lo más probable es que esta persona denuncie ante la Agencia de Protección de Datos que corresponda a esta entidad por infracción del Reglamento, cuando en realidad la entidad está infringiendo el Reglamento, pues cumplió con el mismo. ¿Cómo podría, entonces, solucionarse un caso como este? Bloqueando a los contactos y estableciendo una suerte de "listas negras". De esta manera se garantiza que el interesado no será contactado de nuevo por esa entidad y si llega de nuevo a aparecer en la base de datos, producto de que se adquirió de un tercero procesador, donde figuraba esa persona, se le omitirá. El problema, sin embargo, es que no se está cumpliendo ni con la ley ni con la solicitud del interesado que quería: nunca más ser contactado por la entidad procesadora; y que se borraran los datos[36].

c) La responsabilidad del usuario y la responsabilidad del ente procesador

La base legal que otorga la licitud al tratamiento de datos atrás revisada (véase 2. f)) puede ser el contrato, la ley, el interés público, pero la más común es el consentimiento del interesado. Esto ha llevado, en la práctica, a que, en cada servicio público, oficina privada, servidor de Internet, etc., tengan a la mano

[36] Estas otras dificultades han sido tematizadas en la Evaluación sobre el Reglamento General de Protección de Datos, de la Conferencia Anual sobre Protección de Datos de 2019, Erfahrungsbericht der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zur Anwendung der DS-GVO (2020).

antes de realizar cualquier tipo de interacción, una forma de consentimiento –o, bien, un *banner* de *cookies* que operan como consentimiento, pese a que poca gente lee realmente los términos de uso de las páginas que usan *cookies*. La idea es que el tráfico en Internet se vea lo menos entorpecido posible. Sin embargo, en una decisión reciente, el Tribunal Europeo sostuvo que el consentimiento en el uso de *cookies* no bastaba como declaración de consentimiento del usuario, pues estas se utilizaban para recopilar información con fines publicitarios y con eso dependiendo de las páginas que el usuario visite, se pueden determinar sus gustos o tendencias[37]. El tribunal sostuvo que el derecho de la Unión está diseñado para proteger al usuario de cualquier intrusión en su privacidad, en particular contra el riesgo de que se incorporen a su equipo "identificadores ocultos" o instrumentos similares que lo puedan invadir en su privacidad. Deja claro, también, que el consentimiento debe darse para el caso concreto y que un consentimiento genérico no habilita para otros fines. Luego, debe haber una declaración activa por parte del usuario y no basta con el *cookie-banner* de la página. Curiosamente, la misma página del Tribunal Europeo cuenta para su navegación con un *cookie-banner* de las mismas características que ellos en su decisión judicial prohibieron[38].

El traslado de la responsabilidad al usuario en tanto deber de consentimiento informado es, por cierto, una vía inteligente para darle legitimación al tratamiento de datos. No obstante, es una medida muy poco realista. El usuario de Internet, por lo general, busca rapidez y no quiere usualmente leer contenido jurídico en las páginas sobre, por ejemplo, videojuegos.

Por otra parte, quien también se encuentra en una posición muy compleja es el llamado "delegado de protección de datos" , quien no solo tiene la responsabilidad de velar por el cumplimiento del Reglamento en una entidad determinada, sino, además, debe denunciar el no cumplimiento a la autoridad competente y, por último, tiene un deber de garante respecto de los posibles incumplimientos de la normativa. El problema que esto genera al interior de una empresa u organización, es lo que pasa generalmente con todas las medidas de Compliance: se generan problemas de control entre quienes controlan la empresa y quienes generan normas de control para quienes controlan a esa empresa.

[37] Véase un resumen de la decisión del tribunal en: https://curia.europa.eu/jcms/upload/docs/application/pdf/2019-10/cp190125de.pdf [fecha de consulta: 30 de abril de 2020].

[38] Véase la página oficial del tribunal: https://europa.eu/european-union/about-eu/institutions-bodies/court-justice_es [fecha de consulta: 30 de abril de 2020].

4. Consideraciones finales

El Reglamento que regula la autodeterminación informativa de los residentes europeos, es ciertamente un avance en términos de protección de la privacidad, en especial, en una época donde pareciera que los individuos están abriendo cada vez más espacios privados al escrutinio público: Instagram, Facebook, Snapchat, etc., son todas herramientas que al parecer no resguardan, sino que vulneran –aunque de manera consentida–, la privacidad.

Junto con la regulación europea, no solo se creó un nuevo estatuto jurídico, sino que, al parecer, el "nuevo oro", los datos, son finalmente elevados a la categoría de "entes valiosos susceptibles de protección jurídica". Con esto se creó un nuevo bien jurídico y también un nuevo estatuto de intereses valiosos conocidos como datos. Estos no son personas, no son bienes, no son derechos, tienen un estatuto distinto de carácter cercano, pero no idéntico a los bienes en sentido patrimonial. Por datos se entiende en sentido semántico, la presentación o exposición de información que se encuentra en un estado perceptible, ya sea en el mundo real o irreal; mientras que, en un sentido sintáctico, se trata de la presentación o exposición de símbolos a través de códigos predeterminados. Cualquiera sea su definición, es indiscutible que son valiosos y que hay que protegerlos. La pregunta es si la regulación que hoy existe genera una protección suficiente. La regulación, si bien acabada, es una legislación que deberá ser sumamente dinámica en su actualización, pues

a) debe estar al tanto de los avances tecnológicos y estar al día respecto de ellos;
b) deberá ser definida en detalle por la regulación interna de los países miembros de la EU, labor ya cumplida, pero por sobre todo, requerirá de mucha interpretación jurisprudencial para llegar a ser una regulación precisa;
c) por último, la fiscalización por parte tanto de la Agencia de Protección de Datos en el ámbito europeo y nacional, como la labor de los responsables del tratamiento de datos, será clave y son estos organismos los que habrá que proteger y dotar de autonomía si lo que se busca es una aplicación eficiente de esta normativa.

Bibliografía

Bieber, Christoph (2012). "Datenschutz, Datenschutz als politisches Thema –von der Volkszählung zur Piratenpartei", in Jan-Hinrik Schmidt, Thilo Weichert (Hrsg.), *Datenschutz, Grundlagen, Entwicklungen und Kontroversen*, Bonn: Bundeszentrale für politische Bindung, pp. 34-44.

Clough, Jonathan (2010). *Principles of Cybercrime*, Cambridge: Cambridge University Press.

DKMS (deutsche Knochemmarkspnderdatei), www.dkms.de [fecha de consulta: marzo de 2020].

Erfahrungsbericht der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zur Anwendung der DS-GVO (2009). November. Disponible en www.datenschutz.rlp.de/fileadmin/lfdi/Dokumente/20191113_Erfahrungsbericht_DS-GVO.pdf [fecha de consulta: 30 de abril de 2020].

Europol (2015). "The Internet Organised Crime Threat Assessment" (OICTA). Disponible en www.europol.europa.eu [fecha de consulta: 30 de abril de 2020].

Franzius, Claudio (2015). "Das Recht auf informationelle Selbstbestimmung", in *Zeitschrift für das juristische Studium*, vol. 3. Gießen, pp. 259-270.

Hermstrüwer, Yoan (2016). *Informationelle Selbstgefährdung*, Tübingen, Mohr Siebeck.

Ollé Sesé, Manuel (2008). *Justicia Universal para Crímenes internacionales*, Las Rozas, Madrid: La Ley, .

Pieroth, Bodo; Bernhard Schlink, Thorsten Kingreen, Ralf Poscher (2016). *Staatsrecht, Grundrechte II*, 31. Aufl. Heidelberg: C.F. Müller.

Melnick, Edward L, Brian S. Everitt (eds.) (2008). *Encyclopedia of Quantitative Risk Analysis and Assessment*, West Sussex England: John Wiley & Sons Ltd., vol. I.

Nogueira, Humberto (2005). "Autodeterminación informativa y hábeas data en Chile e información comparativa", pp. 449-471. Disponible en www.juridicas.unam.mx [fecha de consulta: marzo de 2020].

Schlink, Bernhard (1986). "Das Recht der informationellen Selbstbestimmung", in *Der Staat*, vol. 25, N° 2, Berlin, pp. 233-250.

Sieber, Ulrich (2012). *Gutachten zum 69. Deutschen Juristentag. Strafen und Strafverfolgung im Internet*, München: Verlag C.H. Beck.

Valls Prieto, Javier (2015). "Fighting Cybercrime and protecting privacy", in María Manuela Cruz-Cunha, Irene Portela. *Handbook of Research on Digital Crime, Cyberspace Security, and Information Assurance*, Hershey, Pennsylvania: IGI Global, pp. 146-155.

Valls Prieto, Javier (2016). "Nuevas formas de combatir el crimen en internet y sus riesgos", en *Revista Electrónica de Ciencia Penal y Criminología*, n.° 18-22, pp. 1-36. Disponible en http://criminet.ugr.es/recpc/ [fecha de consulta: marzo de 2020].

WMDA (World Marrow Donor Association). Disponible en https://wmda.info/ [fecha de consulta: marzo de 2020].