El modelo europeo de protección de datos. Experiencias para la regulación chilena presente y futura

The european model of data protection. Experiences for present and future chilean regulation

Felio José Bauzá Martorell[*]
Universidad Islas Baleares
Islas Baleares, España

RESUMEN: Los países de Iberoamérica han emprendido en los últimos años un notable esfuerzo en materia de protección de datos, debatiéndose entre el modelo europeo, centrado en la privacidad, y el modelo americano, volcado en la seguridad. La aprobación y entrada en vigor del Reglamento Europeo de Protección de Datos y la tramitación por el Congreso Nacional de Chile de un proyecto de ley de protección de datos personales en la red constituye una magnífica ocasión para analizar la regulación de Iberoamérica, especialmente Chile, y compararla con el vigente modelo europeo.

ABSTRACT: The countries of Ibero-America have undertaken in recent years a significant effort in terms of data protection, discussing between the European model, focused on privacy, and the American one, focused on security. The approval and entered into force of the European Data Protection Regulation and the processing by the National Congress of Chile of a bill for the protection of personal data in the network is a great opportunity to analyze the regulation of Ibero-America, especially Chile, and compare it with the current European model.

PALABRAS CLAVE: protección de datos; privacidad; derecho fundamental; consentimiento; derecho al olvido.

KEYWORDS: data protection; privacy; fundamental right; consent; right to be forgotten.

INTRODUCCIÓN

La entrada en vigor del Reglamento Europeo de Protección de Datos y la tramitación por el Congreso Nacional de Chile de un proyecto de ley de protección de datos personales en la red –unido a la reforma constitucional que incluye la protección de datos entre los derechos fundamentales– constituye una ocasión magnífica para analizar el régimen jurídico de una materia tan sensible.

En Europa no constituye novedad la regulación de la privacidad, ya sea en sede internacional (Unión Europea, Consejo de Europa) o en un plano estrictamente estatal. La Carta de los Derechos Fundamentales de la Unión Europea (2000/C 364/01) reconoce expresamente en su art. 8 que toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan y obliga a que estos datos se traten de modo leal, para fines concretos y sobre la base del consentimiento de la persona

[*] Doctor en Derecho Pontificia Universidad de Comillas, Profesor Universidad Islas Baleares. Correo electrónico: fj.bauza@uib.es

Artículo recibido el 14 de septiembre de 2018 y aceptado para publicación el 8 de octubre de 2018

afectada, o en virtud de otro fundamento legítimo previsto por la ley, y reconoce que toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación y, por último, reserva el control de la privacidad a una autoridad independiente y autónoma.

Los Estados europeos se refieren directa o indirectamente a la protección de datos de carácter personal en sus Constituciones, como es el caso del art. 18.4 de la Carta española[1] y el art. 15 de la Italiana[2].

Las instituciones europeas, conscientes de que la protección de datos no conoce fronteras, vienen regulando esta materia –sin perjuicio de antecedentes remotos[3]– desde los años ochenta del pasado siglo. Así, resultó ciertamente pionero el Convenio 108 del Consejo de Europa de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, cuyo objeto consiste en garantizar, en el territorio de cada Parte, a cualquier persona física, sean cuales fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona.

Por su parte, el Parlamento y el Consejo de la Unión Europea aprobaron la Directiva 95/46/CE, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, calificada por la doctrina como la fuente clave de la normativa europea en el sector[4] y causa de la reforma de la legislación de protección de datos de los Estados miembros[5].

El derecho vigente en la materia es el Reglamento General de Protección de Datos (en adelante también RGPD), aprobado como Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que deroga la Directiva 95/46/CE[6]. A diferencia de la directiva, un reglamento comunitario goza de aplicabilidad directa en los Estados miembros, de manera que puede afirmarse sin riesgo a equivocarse que el RGPD diseña un modelo de protección de datos con clara intención de uniformidad.

La República de Chile está dando muestras de sensibilidad en esta materia por cuanto la Ley 21.096, de 5 de junio de 2018, reforma la Constitución Política agregando la protección de datos en el número 4º del artículo 19[7]. Esta reforma tiene especial

[1] *"La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos"*.

[2] *"Serán inviolables la libertad y el secreto de la correspondencia y de cualquier otra forma de comunicación. La limitación de los mismos solo podrá producirse por auto motivado de la autoridad judicial con las garantías establecidas por la ley"*.

[3] Véase FERNÁNDEZ CONTE y LEÓN BURGOS (2016).

[4] GARCÍA MEXÍA (2016) p. 24.

[5] España adaptó el régimen jurídico de la protección de datos hasta entonces previsto en la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de datos de carácter personal (LORTAD), a las previsiones de la Directiva comunitaria con la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de carácter personal (LOPD).

[6] Diario Oficial de la Unión Europea L119/1, de 4 de mayo de 2016.

[7] La Ley 21.096, de reforma constitucional, tiene su origen en una moción presentada por los Honorables senadores Sres. Felipe Harboe Bascuñán, Pedro Araya Guerrero y Ricardo Lagos Weber, y de los

importancia porque hasta la fecha la Carta no contemplaba la protección de datos y a partir de su entrada en vigor esta materia se convierte en un derecho constitucional, remitiéndose a una norma con rango de ley para determinar la forma y condiciones de su tratamiento y protección.

En todo caso y como miembro de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) desde 2010, a Chile le afectarían las Directrices de este Organismo sobre protección de la privacidad y flujos transfronterizos de datos personales de 1980, que constituyen principios de actuación en la materia[8].

En efecto, la República de Chile –a reservas de la aprobación del proyecto de ley de protección de datos de carácter personal que se encuentra en fase de tramitación en el Congreso Nacional[9]– regula esta materia en la Ley 19.628, de 18 de agosto de 1999, sobre Protección de la vida privada. Comparada con la normativa europea, esta Ley tiene una estructura muy elemental porque después de un Título Preliminar con disposiciones generales (art. 1), definiciones (art. 2) y un principio general de información a los titulares de datos (art. 3) contempla un Título I "De la utilización de datos personales" (arts. 4 a 11), II "De los derechos de los titulares de datos" (arts. 12 a 16), III "De la utilización de datos personales relativos a obligaciones de carácter económico, financiero, bancario o comercial" (arts. 17 a 19), IV "Del tratamiento de datos por los organismos públicos" (arts. 20 a 22) y V "De la responsabilidad por las infracciones a esta ley".

Esta legislación chilena fue pionera y como tal una de las primeras en América latina sobre protección de datos personales pero se aprobó con un contenido sensiblemente menor que el propio del proyecto[10] por lo que adolece desde un primer momento de una serie de insuficiencias, por ejemplo, ausencia de sanciones efectivas, falta de regulación del flujo transfronterizo de datos personales, autorización del uso de datos para marketing directo sin consentimiento del titular, ausencia de una autoridad administrativa de control, excepciones amplias al consentimiento para el tratamiento de datos[11].

---

exsenadores Sres. Hernán Larraín Fernández y Eugenio Tuma Zedán. Fue promulgada por el Presidente de la República el 5 de junio de 2018 y publicada el 16 de dicho mes.

[8] Las directrices de privacidad suponen la unanimidad internacional sobre las guías generales para la recogida y gestión de información personal. Los principios establecidos en las directrices de privacidad se caracterizan por su claridad y flexibilidad de aplicación, y por su formulación, que es lo suficientemente general para permitir su adaptación a los cambios tecnológicos. Los principios abarcan todos los medios del procesamiento informático de datos sobre individuos (desde computadoras locales a redes con complejas ramificaciones nacionales e internacionales), todos los tipos de procesamiento de datos personales (desde la administración de personal hasta la compilación de perfiles de consumidores) y todas las categorías de datos (desde datos de tráfico hasta datos de contenidos, desde el más trivial al más delicado). Los principios se pueden aplicar en los ámbitos nacional e internacional. A lo largo de los años se han utilizado en gran número de instrumentos de regulación nacional o de autorregulación y todavía se usan ampliamente en los sectores público y privado.

[9] Este proyecto recoge gran parte de las conclusiones y recomendaciones formuladas en agosto de 2016 por la Unidad de Evaluación de la Ley de la Cámara de los Diputados en su informe sobre la Ley Nº 19.628.

[10] VIOLLIER (2017) pp. 10-16 expone un cuadro comparativo entre la moción aprobada por el Senado y el proyecto finalmente aprobado por la Cámara de Diputados, con la intención de acotar el texto a los datos personales y remitir parte de su articulado a un proyecto de ley sobre libertades de opinión y de información.

[11] Véase JIJENA LEIVA (2001) pp. 22-24.

Algunas de las carencias denunciadas desde su publicación se fueron colmando con reformas puntuales a la Ley 19.628[12] pero se echa en falta en el derecho positivo chileno una reforma de carácter integral que adapte su régimen jurídico a la evolución social y económica del flujo de datos, con una amplia participación social, no solo del mundo empresarial sino que también de la doctrina y de la academia[13].

El proyecto de ley por el que se regula la protección de datos de carácter personal y se crea la Agencia de Protección de Datos Personales[14] supone un avance notable en la materia y se articula en torno al objetivo general de que el titular de los datos otorgue su consentimiento y mantenga bajo su control el uso de sus propios datos que efectúe cualquier persona. Su principal novedad consiste en la creación de una autoridad de control de carácter técnico y una institucionalidad pública que asuma los desafíos regulatorios y de fiscalización en materia de protección de las personas y tratamiento de los datos personales.

La coincidencia entre la entrada en vigor del RGPD, la reforma constitucional y la tramitación de una ley en materia de protección de datos en Chile, y la revisión en España de la Ley Orgánica de Protección de Datos[15] constituyen una ocasión para analizar el régimen jurídico comparado de esta institución[16] y aportar sugerencias sobre el régimen vigente de la regulación chilena sobre protección de datos, junto a las novedades que contiene el proyecto de ley en trámite.

A continuación, se analizan las características más sobresalientes del RGPD y de la reforma que se tramita en el Congreso Nacional de Chile.

I. NOTAS DEFINITORIAS DEL MODELO EUROPEO DE PROTECCIÓN DE DATOS

El RGPD construye un modelo europeo de protección de datos con características muy determinantes.

1. La consolidación de la protección de datos como derecho fundamental

[12] La Ley 19.812, publicada el 13 de junio de 2002, modificó la Ley 19.628 y el Código del Trabajo, a fin de que los datos personales de carácter económico, financiero, bancario y comercial dejaran de ser utilizados para discriminar a quienes postulan un puesto de trabajo; la Ley 20.463, publicada el 25 de octubre de 2010, prohíbe a los administradores de bases de datos personales de carácter financiero tratar datos relativos a deudas de personas físicas, cuando éstas se hubieran producido en el período en que la persona se encontraba sin empleo; la Ley 20.521, publicada el 23 de julio de 2011, prohíbe cualquier tipo de evaluación de riesgo comercial que no esté basa en información objetiva relacionada con la situación financiera de las personas; y la Ley 20.575, promulgada el 14 de febrero de 2012, consagra el principio de finalidad en la toma de datos personales.

[13] JIJENA LEIVA (2010) p. 415 critica que la Ley 19.628 naciera desde la óptica estrictamente empresarial, "con la asesoría directa de grupos, gremios y empresas interesadas en asegurar el negocio que constituye el procesamiento de datos personales".

[14] El proyecto tuvo su ingreso en la Cámara de Diputados en fecha 15 de marzo de 2017, y se encuentra pendiente de indicaciones en el primer trámite constitucional (Senado).

[15] Boletín Oficial de las Cortes Generales. Congreso de los Diputados. 24 de noviembre de 2017.

[16] Parte de la doctrina considera la Ley chilena 19.628 tributaria de la Ley española de 1992, cuando esta última fue derogada por la Ley Orgánica 15/1999, y a día de hoy existe una propuesta de Ley Orgánica de Protección de Datos de Carácter Personal en España. Véase VIOLLIER (2017) p. 8.

Las autoridades europeas vienen reconociendo la protección de datos como un derecho, y así el art. 8.1 de la Carta de los Derechos Fundamentales de la Unión Europea y el art. 16.1 del Tratado de Funcionamiento de la Unión Europea (TFUE) establecen que toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.

El ordenamiento interno de los Estados miembros se ha hecho eco de esta calificación y no en vano la Sentencia del Tribunal Constitucional español 94/1988 indicó que nos encontramos ante un derecho fundamental a la protección de datos en virtud del cual "se garantiza a la persona el control sobre sus datos, cualesquiera datos personales, y sobre su uso y destino, para evitar el tráfico ilícito de los mismos o lesivo para la dignidad y los derechos de los afectados; de esta forma, el derecho a la protección de datos se configura como una facultad del ciudadano para oponerse a que determinados datos personales sean usados para fines distintos a aquél que justificó su obtención"[17].

La estimación de derecho fundamental de la protección de datos viene expresa y directamente reconocida en el RGPD en el inicio de su Considerando (1)[18], al tiempo que este derecho se pone en relación al resto de derechos fundamentales de las personas[19].

El RGPD establece en su art. 1.2 que se protege los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales y consecuencia de ello es que se configura la protección de datos al más alto nivel, con categoría de derecho fundamental, con todo lo que ello implica de reconocimiento y resguardo.

Como he anticipado y en línea con el ordenamiento de otros Estados americanos[20], la reforma constitucional operada por la Ley 21.096 hace acopio de esta consideración y convierte a la protección de datos en un derecho constitucional, que debe entenderse como derecho fundamental[21]. En consecuencia, en este punto puede afirmarse una convergencia entre ambas regulaciones y una asimilación del régimen europeo por parte de la normativa chilena.

---

[17] SERRANO PÉREZ (2005) p 255.

[18] "La protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental".

[19] Conforme al Considerando (2), "Los principios y normas relativos a la protección de las personas físicas en lo que respecta al tratamiento de sus datos de carácter personal deben, cualquiera que sea su nacionalidad o residencia, respetar sus libertades y derechos fundamentales, en particular el derecho a la protección de los datos de carácter personal. El presente Reglamento pretende contribuir a la plena realización de un espacio de libertad, seguridad y justicia y de una unión económica, al progreso económico y social, al refuerzo y la convergencia de las economías dentro del mercado interior, así como al bienestar de las personas físicas".

[20] Otros ordenamientos, por ejemplo el mejicano, hacen acopio de la calificación de la protección de datos como un derecho fundamental. Véase GARCÍA GONZÁLEZ (2007).

[21] La Constitución chilena califica los derechos del art. 19 como constitucionales sin mencionar una categoría específica de derechos fundamentales y en la española de 1978 se distinguen diferentes categorías de derechos en función de su nivel de protección, por ejemplo, los derechos fundamentales y libertades públicas, los derechos constitucionales y los principios rectores de la política económica y social, pero una lectura al contenido de la Carta de Chile permite concluir que los derechos calificados como constitucionales son materialmente derechos fundamentales, todos ellos protegidos en la declaración Universal de Derechos Humanos.

2. Extensión del ámbito territorial de aplicación de las normas protectoras de la privacidad

El ámbito de aplicación territorial del Reglamento pone de relieve su vocación de eficacia más allá del territorio de sus Estados miembros. En efecto, el art. 3 RGPD incorpora al derecho positivo la doctrina expansiva del Tribunal de Justicia de la Unión Europea (TJUE) y en consecuencia se aplica al tratamiento de datos personales en el contexto de las actividades de un establecimiento del responsable o del encargado en la Unión, independientemente de que el tratamiento tenga lugar en la Unión o no[22].

Tanto en la Sentencia de 13 de mayo de 2014 (asunto *Google Spain*, C-131/12) como en la de 1 de octubre de 2015 (asunto *Weltimmo*, C-230/14), el TJUE adopta un criterio funcional y objetivo por encima de la vinculación territorial del domicilio social de la entidad que maneja datos personales:

> "De lo anterior se deriva, como señaló en esencia el Abogado General en los puntos 28 y 32 a 34 de sus conclusiones, una concepción flexible de la noción de establecimiento, que rechaza cualquier enfoque formalista según el cual una empresa estaría establecida únicamente en el lugar en que se encontrase registrada. Por lo tanto, para determinar si una sociedad, responsable de un tratamiento de datos, dispone de un establecimiento, en el sentido de la Directiva 95/46, en un Estado miembro distinto del Estado miembro o del tercer país en el que está registrada, procede interpretar tanto el grado de estabilidad de la instalación como la efectividad del desarrollo de las actividades en ese otro Estado miembro tomando en consideración la naturaleza específica de las actividades económicas y de las prestaciones de servicios en cuestión. Esto es válido concretamente para las empresas que se dedican a ofrecer servicios exclusivamente a través de Internet".

Por ello el RGPD se aplica en clave subjetiva y garantista al tratamiento de datos personales de interesados que residan en la Unión por parte de un responsable o encargado no establecido en la Unión, cuando las actividades de tratamiento estén relacionadas con la oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si a estos se les requiere su pago, o con el control de su comportamiento, en la medida en que este tenga lugar en la Unión.

El RGPD no es ajeno a las normas de Derecho internacional público de manera que igualmente se considera aplicable al tratamiento de datos personales por parte de un responsable que no esté establecido en la Unión sino en un lugar en que el Derecho de los Estados miembros resulte de aplicación (art. 3.3).

Esta vocación transfronteriza se halla presente en el proyecto de ley chileno, el que –consciente de la naturaleza global de las relaciones sociales y económicas– incorpora

[22] Véase RIPOL CARULLA (2016).

los principios rectores en materia de protección y tratamiento de los datos personales que han sido reconocidos en las directrices de la OCDE y en el derecho comparado: licitud del tratamiento, finalidad, proporcionalidad, calidad, seguridad, responsabilidad e información (art. 3).

De hecho, el proyecto de ley actualiza e incorpora nuevas definiciones legales, adaptándolas a las propias del derecho comparado, así como las recomendaciones técnicas de organismos internacionales y el estado actual del arte y de la técnica[23].

3. Régimen jurídico del consentimiento

La clave de bóveda de toda la arquitectura jurídica de la protección de datos consiste indudablemente en el consentimiento, que deviene fundamental para la transmisión de datos con la salvedad de que los mismos aparezcan en fuentes accesibles al público de acuerdo a nuestra normativa interna[24].

Hasta la aprobación del RGPD el derecho positivo en Europa –el propio de las instituciones europeas y el de los Estados miembros– vinculaba el consentimiento a una actitud pasiva del titular de los datos y tanto la Directiva de 1995 (art. 2.h) como la LOPD española (art. 3.h) identificaban el consentimiento del interesado como toda manifestación de voluntad, libre, específica e informada, mediante la que el interesado consentía el tratamiento de datos personales que le conciernan[25].

No obstante, el RGPD apuesta por una aceptación expresa y afirmativa del consentimiento y en su considerando (32) dispone que:

> "El consentimiento debe darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen, como una declaración por escrito, inclusive por medios electrónicos, o una declaración verbal. Esto podría incluir marcar una casilla de un sitio web en internet, escoger parámetros técnicos para la utilización de servicios de la sociedad de la información, o cualquier otra declaración o conducta que indique claramente en este contexto que el interesado acepta la propuesta de tratamiento de sus datos personales. Por tanto, el silencio, las casillas ya marcadas o la inacción no deben constituir consentimiento. El consentimiento debe darse para todas las actividades de tratamiento realizadas con el mismo o los mismos fines. Cuando el tratamiento tenga varios fines, debe darse el consentimiento para todos ellos. Si el consentimiento del interesado se ha de dar a raíz de una solicitud por

[23] Sobre la función uniformadora del Derecho por parte de organizaciones internacionales, véase GIMENO FELIÚ (2016).
[24] Parte de la doctrina chilena critica que la Ley 19.628 no defina con mayor precisión el concepto de fuente accesible al público, cuando constituye una excepción a la regla general del consentimiento expreso y como tal debe ser objeto de interpretación restrictiva. Véase ALVARADO (2014).
[25] Véase ADSUARA VARELA (2016).

> medios electrónicos, la solicitud ha de ser clara, concisa y no perturbar innecesariamente el uso del servicio para el que se presta".

El art. 4.11 RGPD define el consentimiento del interesado como toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen.

En Chile la Ley Nº. 19.628 exige ya en su art. 4 el consentimiento expreso y escrito del titular de los datos, salvo que el tratamiento venga autorizado por una ley o conste en bases de acceso público (art. 20). En este sentido el derecho vigente chileno resulta ejemplar y se debe reconocer que se adelantó a la regulación europea a la hora de exigir que el consentimiento fuera expreso[26]. El consentimiento se refuerza en el proyecto de ley como fuente de legitimidad del tratamiento de datos y se exige que el mismo deba ser libre, informado, inequívoco, otorgado en forma previa al tratamiento y específico en cuanto a su finalidad.

Particular atención presta el proyecto de ley a los datos sensibles y a los datos personales de menores. En el primer caso se eleva el estándar para el tratamiento de tales datos estableciendo que solo puede realizarse cuando el titular consienta libre e informadamente, en forma expresa, admitiendo únicamente las excepciones de que el titular haya hecho manifiestamente público el dato sensible o cuando exista una situación de emergencia médica o de salud. En el caso de menores, el tratamiento de datos de niños y niñas requiere el consentimiento previo, específico y expreso de quien tiene a su cargo el cuidado personal, mientras que respecto de los adolescentes se establece que sus datos sensibles solo pueden ser tratados con el consentimiento de quien tiene a su cargo el cuidado personal del menor.

4. Derecho al olvido

El derecho a la supresión de datos o al olvido aparece en el derecho europeo a raíz de la Sentencia del TJUE de 13 de mayo de 2014 (caso Mario Costeja y AEPD vs. Google, C-131/12) en el contexto de los motores de búsqueda de internet.

Para gran parte de la doctrina el derecho al olvido no es nuevo sino que supone una concreción de los derechos reconocidos de oposición y cancelación[27]. No obstante lo anterior y ante las muestras de preocupación por la supresión de datos en el entorno digital[28], el legislador comunitario contempló específicamente este derecho en su art. 17

[26] Que sea expreso no implica necesariamente que sea libre, informada e inequívoca. En estos puntos se encuentra la innovación del RGDP.
[27] PAZOS CASTRO (2015) p. 40.
[28] La Comunicación de la Comisión Europea al Parlamento Europeo, Consejo de la UE, Comité Económico y Social y Comité de las Regiones titulada *A comprehensive approach on personal data protection in the European Union*, COM (2010) 609 final, fechada en Bruselas el 4 de noviembre de 2010, ya manifestaba su preocupación por reforzar los derechos de acceso, rectificación, cancelación y oposición de los datos personales frente a los avances tecnológicos en el marco de la reforma de la normativa europea de protección de datos.

destacando antes su importancia en los Considerandos (6)[29] y (7)[30]. El RGPD reconoce el derecho del interesado a obtener sin dilación indebida del responsable del tratamiento de la supresión de los datos personales que le conciernan, quien estará obligado a suprimir con la mayor celeridad los datos personales si estos ya no son necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo, o el interesado retira el consentimiento en que se basa el tratamiento que se otorgó para un fin determinado[31] o se opone al tratamiento y no prevalezcan otros motivos legítimos para el tratamiento o se opone al tratamiento en relación a mercadotécnica directa[32], o los datos personales han sido tratados ilícitamente o deben suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento o se han obtenido en relación con la oferta de servicios de la sociedad de la información dirigidos a menores[33].

Curiosamente la regulación chilena no se aleja tanto de este modelo por cuanto la Ley Nº 19.628 se refiere al derecho convencional de cancelación en su art. 6 como una eliminación de los datos personales cuando su almacenamiento carezca de fundamento legal o hayan caducado. Otra cosa es que esta eliminación de datos pudiera desarrollarse y concretarse a quién corresponde la supresión o en qué supuestos se justifica su mantenimiento. El derecho al olvido en Chile ha sido objeto de preocupación y análisis, principalmente en el ámbito periodístico-digital[34].

En efecto, el RGPD atribuye al responsable del tratamiento, teniendo en cuenta la tecnología disponible y el coste de su aplicación, la adopción de medidas razonables, incluidas las técnicas, con miras a informar a los responsables que estén tratando los datos personales de la solicitud del interesado de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos.

El legislador europeo y de acuerdo con la casuística contempla excepciones a esta regla general en los siguientes casos: a) para ejercer el derecho a la libertad de expresión e información; b) para el cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento, o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al

[29] "La rápida evolución tecnológica y la globalización han planteado nuevos retos para la protección de los datos personales. La magnitud de la recogida y del intercambio de datos personales ha aumentado de manera significativa. La tecnología permite que tanto las empresas privadas como las autoridades públicas utilicen datos personales en una escala sin precedentes a la hora de realizar sus actividades. Las personas físicas difunden un volumen cada vez mayor de información personal a escala mundial. La tecnología ha transformado tanto la economía como la vida social, y ha de facilitar aún más la libre circulación de datos personales dentro de la Unión y la transferencia a terceros países y organizaciones internacionales, garantizando al mismo tiempo un elevado nivel de protección de los datos personales".

[30] "Estos avances requieren un marco más sólido y coherente para la protección de datos en la Unión Europea, respaldado por una ejecución estricta, dada la importancia de generar la confianza que permita a la economía digital desarrollarse en todo el mercado interior. Las personas físicas deben tener el control de sus propios datos personales. Hay que reforzar la seguridad jurídica y práctica para las personas físicas, los operadores económicos y las autoridades públicas".

[31] Artículos 6.1.a y 9.2.a RGPD.

[32] Artículo 21.1 y 2 RGPD.

[33] Artículo 8.1 RGPD.

[34] REUSSER MONSÁLVEZ (2018) p. 78.

responsable; c) por razones de interés público en el ámbito de la salud pública[35]; d) con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos[36], en la medida en que el derecho pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento; e) para la formulación, el ejercicio o la defensa de reclamaciones.

El proyecto de ley chileno en tramitación, consciente de la lesión que causa al honor y a la esfera privada de los individuos la publicación de sanciones administrativas o penales, refuerza el derecho al olvido, buscando un equilibrio entre el derecho a la información y la transparencia, con el derecho al honor y consiguiente restricción al acceso a datos desfavorables que no sean de interés público[37].

5. Derecho a la portabilidad

El RGPD acuña un nuevo derecho de los titulares de datos, autónomo e independiente de otros derechos, que consiste en la portabilidad de los datos a otros operadores y que no aparece expresamente recogido en Chile ni en la Ley 19.628, pero sí en el proyecto de ley, como también lo contempla el proyecto de ley orgánica española (art. 19).

Este derecho, cuyo espíritu se recoge en el Considerando (68)[38], hunde sus raíces en la legislación española, particularmente en el Real Decreto 2296/2004, de 10 de diciembre, por el que se aprueba el Reglamento sobre mercados de comunicaciones electrónicas,

[35] Artículo 9.2.h e i, y 3 RGPD.
[36] Artículo 89.1 RGPD.
[37] Sobre el debate entre el derecho a la información y la privacidad, véase ÁLVAREZ VALENZUELA (2016) p. 62.
[38] "Para reforzar aún más el control sobre sus propios datos, cuando el tratamiento de los datos personales se efectúe por medios automatizados, debe permitirse asimismo que los interesados que hubieran facilitado datos personales que les conciernan a un responsable del tratamiento los reciban en un formato estructurado, de uso común, de lectura mecánica e interoperable, y los transmitan a otro responsable del tratamiento. Debe alentarse a los responsables a crear formatos interoperables que permitan la portabilidad de datos. Dicho derecho debe aplicarse cuando el interesado haya facilitado los datos personales dando su consentimiento o cuando el tratamiento sea necesario para la ejecución de un contrato. No debe aplicarse cuando el tratamiento tiene una base jurídica distinta del consentimiento o el contrato. Por su propia naturaleza, dicho derecho no debe ejercerse en contra de responsables que traten datos personales en el ejercicio de sus funciones públicas. Por lo tanto, no debe aplicarse, cuando el tratamiento de los datos personales sea necesario para cumplir una obligación legal aplicable al responsable o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable. El derecho del interesado a transmitir o recibir datos personales que lo conciernan no debe obligar al responsable a adoptar o mantener sistemas de tratamiento que sean técnicamente compatibles. Cuando un conjunto de datos personales determinado concierna a más de un interesado, el derecho a recibir tales datos se debe entender sin menoscabo de los derechos y libertades de otros interesados de conformidad con el presente Reglamento. Por otra parte, ese derecho no debe menoscabar el derecho del interesado a obtener la supresión de los datos personales y las limitaciones de ese derecho recogidas en el presente Reglamento, y en particular no debe implicar la supresión de los datos personales concernientes al interesado que este haya facilitado para la ejecución de un contrato, en la medida y durante el tiempo en que los datos personales sean necesarios para la ejecución de dicho contrato. El interesado debe tener derecho a que los datos personales se transmitan directamente de un responsable del tratamiento a otro, cuando sea técnicamente posible".

acceso a las redes y numeración, mediante el que se facultaba a los abonados a conservar su número de teléfono al cambiar de operador telefónico[39].

En este sentido el art. 20 RGPD reconoce el derecho de los interesados a recibir los datos personales que les incumban, que hayan facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otros responsables del tratamiento sin que lo impida el responsable al que se les hubiera facilitado cuando el tratamiento esté basado en el consentimiento y el tratamiento se efectúe por medios automatizados.

Al ejercer su derecho a la portabilidad de los datos, al interesado se le reconoce el derecho a que los datos personales se transmitan directamente de responsable a responsable cuando sea técnicamente posible. Tal derecho no se aplicará al tratamiento que sea necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.

No puede infravalorarse este derecho a la portabilidad –que debe ceder ante el derecho al olvido– en un contexto de economía digital, de acelerado desarrollo tecnológico y de masificación en el uso de las tecnologías. La Ley 19.628 admite el tratamiento automatizado de datos (art. 5), así como el derecho del titular de datos a requerir información a los diferentes organismos públicos que almacenan el mismo dato a efectos de ejercer su derecho de acceso, rectificación y cancelación (art. 14). Pero la portabilidad –con sus consiguientes limitaciones a través del consentimiento expreso del titular– aporta indudables ventajas en un contexto caracterizado por el manejo de macro datos por organismos públicos y agentes privados[40].

6. Seguridad de los datos personales y autoridad de control

En una estrategia defensiva y anticipativa de la seguridad de los datos personales, el RGPD europeo gira esencialmente en torno a una aproximación basada en el riesgo[41]. Y este riesgo debe ser objeto de evaluación previa atendiendo a la naturaleza, el alcance, el contexto y los fines del tratamiento de datos. El RGPD obliga al encargado del tratamiento a ponderar el riesgo sobre la base de una evaluación objetiva mediante la cual se determine si las operaciones de tratamiento de datos suponen un riesgo o si el riesgo es alto[42].

El proyecto de ley chilena sobre protección de datos contempla una autoridad de control, denominada Agencia de Protección de Datos Personales, relacionada con el Presidente de la República a través del Ministerio de Hacienda, y afecta al Sistema de Alta Dirección Pública. A esta Agencia se le encomienda la función de velar y fiscalizar el cumplimiento del régimen jurídico en materia de protección de datos[43]. Comparado con el RGPD, se observa un déficit de las atribuciones a la Agencia chilena en ciernes, a

[39] Véase FERNÁNDEZ SAMANIEGO y FERNÁNDEZ LONGORIA (2016).
[40] Véase BAUZÁ MARTORELL (2017).
[41] MALDOFF (2016) p. 3.
[42] Véase RECIO GAYO (2016).
[43] De acuerdo con la Ley Nº 20.285, de Transparencia de la Función Pública y de Acceso a la Información de la Administración del Estado, estas funciones fiscalizadoras se atribuyen al Consejo Para La Transparencia, de manera que debería definirse con mayor precisión el modelo que se pretende.

la que se podría encomendar una función de seguridad que sí tiene la autoridad de control en los Estados europeos.

Es motivo de satisfacción la creación de una Autoridad de Control, a los efectos de velar por los derechos de los titulares de datos (ARCO) y cuyas resoluciones sean objeto de control jurisdiccional a través de la Corte de Apelación respectiva. No obstante, las autoridades de control en el RGPD llevan a cabo unas funciones más amplias, especialmente en materia de seguridad del tratamiento de datos, que les permiten desplegar un control preventivo al objeto de evitar una fisura en la seguridad en la recopilación, almacenamiento, tratamiento y cesión de datos.

A) SEGURIDAD DEL TRATAMIENTO

Con una finalidad netamente preventiva, el art. 32 del RGPD obliga al responsable y al encargado del tratamiento a aplicar medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que incluya: a) la *anonimización* y el cifrado de datos personales; b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento; c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico; d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

En la tarea de evaluación de la adecuación del nivel de seguridad el RGPD obliga a tener en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos. El Reglamento introduce el código de conducta, regulado en el art. 40 con el fin de contribuir a la correcta aplicación del RGPD, considerando las características específicas de los distintos sectores de tratamiento y las necesidades específicas de las microempresas y de pequeñas y medianas empresas. En este sentido, la adhesión a un código de conducta o a un mecanismo de certificación aprobado a tenor del artículo 42 podrá servir de elemento para demostrar el cumplimiento de los requisitos establecidos en materia de seguridad.

B) NOTIFICACIÓN DE UNA VIOLACIÓN DE LA SEGURIDAD DE LOS DATOS PERSONALES A LA AUTORIDAD DE CONTROL

El RGPD contempla la obligación que asiste al responsable del tratamiento, en caso de violación de la seguridad de los datos personales, de notificar a la autoridad de control competente sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y libertades de las personas físicas. El incumplimiento del plazo de notificación debe acompañarse de la indicación de los motivos de la dilación.

El art. 33 RGPD indica los requisitos de la notificación en los siguientes términos: a) describir la naturaleza de la violación de la seguridad de los datos personales, inclusive,

cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados; b) comunicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información; c) describir las posibles consecuencias de la violación de la seguridad de los datos personales; d) describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

C) COMUNICACIÓN DE UNA VIOLACIÓN DE LA SEGURIDAD DE LOS DATOS PERSONALES AL INTERESADO

No acaba aquí el protocolo en materia de seguridad porque –cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas– el responsable del tratamiento se encuentra obligado –al tenor del art. 34– a comunicar al interesado, en lenguaje claro y sencillo, sin dilación indebida, la naturaleza de la violación de la seguridad de los datos personales.

Esta comunicación deviene innecesaria si se cumple alguna de las siguientes condiciones: a) el responsable del tratamiento ha adoptado medidas de protección técnicas y organizativas apropiadas y ellas se han aplicado a los datos personales afectados por la violación de la seguridad de esos datos, en particular aquellas que hagan ininteligibles los mismos para cualquier persona que no esté autorizada a acceder a ellos, como el cifrado; b) el responsable del tratamiento ha tomado medidas ulteriores que garanticen que ya no exista la probabilidad de que se materialice el alto riesgo para los derechos y libertades del interesado; c) suponga un esfuerzo desproporcionado. En este caso, se optará en su lugar por una comunicación pública o una medida semejante por la que se informe de manera igualmente efectiva a los interesados.

D) EVALUACIÓN DE IMPACTO RELATIVA A LA PROTECCIÓN DE DATOS

Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento se encuentra obligado a realizar, conforme al art. 35 RGPD, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales, siendo así que una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares.

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

La evaluación de impacto relativa a la protección de los datos se requiere en particular en caso de: a) evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas

físicas o que les afecten significativamente de modo similar; b) tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9 apartado 1[44], o de los datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10[45]; c) observación sistemática a gran escala de una zona de acceso público.

Asimismo, la autoridad de control debe establecer y publicar una lista de los tipos de operaciones de tratamiento que requieran una evaluación de impacto relativa a la protección de datos, y comunicará esas listas al Comité Europeo de Protección de Datos pudiendo además establecer y publicar la lista de los tipos de tratamiento que no requieren evaluaciones de impacto relativas a la protección de datos.

Antes de adoptar las referidas listas, la autoridad de control competente aplicará el mecanismo de coherencia contemplado en el artículo 63 si esas listas incluyen actividades de tratamiento que guarden relación con la oferta de bienes o servicios a interesados o con la observación del comportamiento de estos en varios Estados miembros, o actividades de tratamiento que puedan afectar sustancialmente a la libre circulación de datos personales en la Unión.

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

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

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

E) CONSULTA PREVIA

Por último, en materia de seguridad el art. 36 contempla el procedimiento de consulta previa, que consiste en la obligación que asiste al responsable de consultar a la

[44] Origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientaciones sexuales de una persona física.

[45] Tratamiento de datos personales relativos a condenas e infracciones penales o medidas de seguridad conexas.

autoridad de control antes de proceder al tratamiento cuando una evaluación de impacto relativa a la protección de los datos muestre que el tratamiento entrañaría un alto riesgo si el responsable no toma medidas para para mitigarlo.

Cuando la Autoridad de Control considere que el tratamiento previsto podría infringir el RGPD, en particular cuando el responsable no haya identificado o mitigado suficientemente el riesgo, la autoridad de control deberá, en un plazo de ocho semanas desde la solicitud de la consulta, asesorar por escrito al responsable, y en su caso al encargado, y podrá utilizar cualquiera de sus poderes mencionados en el artículo 58. Dicho plazo podrá prorrogarse seis semanas, en función de la complejidad del tratamiento previsto. La autoridad de control informará al responsable y, en su caso, al encargado de tal prórroga en el plazo de un mes a partir de la recepción de la solicitud de consulta, indicando los motivos de la dilación. Estos plazos podrán suspenderse hasta que la autoridad de control haya obtenido la información solicitada a los fines de la consulta.

Cuando consulte a la autoridad de control, el responsable del tratamiento le facilitará la información siguiente: a) en su caso, las responsabilidades respectivas del responsable, los corresponsables y los encargados implicados en el tratamiento, en particular en caso de tratamiento dentro de un grupo empresarial; b) los fines y medios del tratamiento previsto; c) las medidas y garantías establecidas para proteger los derechos y libertades de los interesados de conformidad con el presente Reglamento; d) en su caso, los datos de contacto del delegado de protección de datos; e) la evaluación de impacto relativa a la protección de datos, y f) cualquier otra información que solicite la autoridad de control.

Como puede apreciarse, este procedimiento enfatiza el elemento nuclear del régimen de protección de datos, cual es la seguridad de los mismos, extremo que confiere un indudable carácter preventivo a fin de evitar las infracciones en materia de tratamiento y/o cesión de datos personales.

7. Principio de responsabilidad proactiva

En el contexto de anticipación del riesgo en materia de seguridad de los datos personales, el RGPD se muestra igualmente sensible a la responsabilidad de quien es el responsable del tratamiento de los datos[46]. No en vano el art. 24 RGPD considera que –teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento y los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas– el responsable del tratamiento debe aplicar medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el propio Reglamento. Dichas medidas deben ser objeto de revisión y actualización cuando sea necesario.

Cuando sean proporcionadas en relación con las actividades de tratamiento, entre las medidas mencionadas se incluirá la aplicación, por parte del responsable del tratamiento, de las oportunas políticas de protección de datos. La adhesión a códigos de

[46] AGUSTINA y BLUMENBERG (2015) p. 265.

conducta o a un mecanismo de certificación pueden ser utilizados como elementos para demostrar el cumplimiento de las obligaciones por parte del responsable del tratamiento.

Resulta obligado plantear este régimen de responsabilidad en la regulación chilena, por cuanto ni la Ley 19.628 ni el proyecto de ley contemplan otros actores que el titular de los datos personales y el responsable del registro o banco de datos, si bien olvidan la figura clave del encargado del tratamiento, que es quien –en la legislación comparada- efectúa personal y materialmente el tratamiento de datos.

En efecto, resulta cuestionable que el derecho chileno no cuente con un régimen de responsabilidad administrativa en el manejo de datos, debiendo por ejemplo comenzarse por identificar a la persona concreta que efectúa el tratamiento de datos por cuenta del responsable. En la legislación chilena se le ha otorgado a este agente la naturaleza de mandatario, aplicándosele las reglas del mandato contenidas en la legislación civil[47].

El proyecto de ley enfatiza el régimen de responsabilidades de los responsables de los datos en el sentido de obligarles a acreditar la licitud del tratamiento que realizan, deberes de información, deberes de reserva y confidencialidad, de información y transparencia. Sin embargo, se echa en falta la figura del encargado material del tratamiento, a quien deben hacerse extensivas todas las obligaciones y responsabilidades del responsable, cuando proceda.

La introducción de este principio es motivo de garantía del tratamiento de datos personales porque se puede apreciar que se ha pasado de un modelo basado en el cumplimiento concreto de la normativa a otro fundamentado en la responsabilidad activa de los responsables.

8. Protección de datos desde el diseño y por defecto

El RGPD en su art. 25 contempla una cuestión sumamente novedosa, cual es la protección de los datos desde su diseño y siempre por defecto (*privacy by default and privacy by design*). En este sentido y teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento se encuentra obligado a usar, en el momento de determinar los medios de tratamiento y en el del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización[48], concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos[49], e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados.

[47] LARA (2014) p. 33.

[48] La seudonimización se encuentra definida en el Art. 4.5) del Reglamento, como la información que, sin incluir los datos denominativos de un sujeto afectado –es decir aquéllos que lo pueden identificar de manera directa-, sí que potencialmente permiten, a través de la asociación con información adicional, determinar quién es el individuo que está detrás de los datos seudonimizados.

[49] El principio de minimización de datos (artículos 5 y 25 del RGPD) se refiere expresamente a la cantidad de datos recogidos, al perímetro del tratamiento, al período de tiempo de retención y al número de personas con acceso a los mismos.

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

Aun cuando el RGPD configura y desarrolla la protección de datos desde el diseño y por defecto como obligaciones, bien podrían considerarse como principios informadores del cumplimiento toda vez que afectan a la posición que debe adoptar el responsable del tratamiento en relación con las operaciones de su responsabilidad.

9. Registro de las actividades de tratamiento

Igualmente, el RGPD constituye una innovación en materia de registros, en la medida en que –no solo descansa la actividad registral en las autoridades de control– sino que obliga en su art. 30 a que cada responsable de tratamiento lleve un registro de las actividades de tratamiento efectuadas bajo su responsabilidad, con el siguiente contenido mínimo: a) el nombre y los datos de contacto del responsable y, en su caso, del corresponsable, del representante del responsable, y del delegado de protección de datos; b) los fines del tratamiento; c) una descripción de las categorías de interesados y de las categorías de datos personales; d) las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales; e) en su caso, las transferencias de datos personales a un tercer país o una organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49, apartado 1, párrafo segundo, la documentación de garantías adecuadas; f) cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos; g) cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad.

Cada encargado y, en su caso, el representante del encargado, se encuentra obligado a llevar un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de un responsable que contenga: a) el nombre y los datos de contacto del encargado o encargados y de cada responsable por cuenta del cual actúe el encargado, y, en su caso, del representante del responsable o del encargado, y del delegado de protección de datos; b) las categorías de tratamientos efectuados por cuenta de cada responsable; c) en su caso, las transferencias de datos personales a un tercer país u organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49, apartado 1, párrafo segundo, la documentación de garantías adecuadas; d) cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad.

Los registros deben constar por escrito, inclusive en formato electrónico. El responsable o el encargado del tratamiento y, en su caso, el representante del responsable o del encargado deben poner el registro a disposición de la autoridad de control que lo solicite.

La salvedad consiste en que estas obligaciones no se aplicarán a ninguna empresa ni organización que emplee a menos de 250 personas, a menos que el tratamiento que realice pueda entrañar un riesgo para los derechos y libertades de los interesados, no sea ocasional, o incluya categorías especiales de datos personales indicadas en el artículo 9.1, o datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10.

No puede pasar desapercibida esta novedad que sustituye la obligación de notificar los ficheros o tratamientos con datos personales a las autoridades de control por esta obligación de contenido práctico y con una clara intención de reducir cargas burocráticas.

10. Transferencia internacional de datos

El principio general de la transferencia internacional de datos previsto en el art. 44 RGPD consiste en que solo se realizarán transferencias de datos personales que sean objeto de tratamiento o vayan a serlo tras su transferencia a un tercer país u organización internacional si, a reserva de las demás disposiciones del Reglamento, el responsable y el encargado del tratamiento cumplen las condiciones establecidas en el mismo, incluidas las relativas a las transferencias ulteriores de datos personales desde el tercer país u organización internacional a otro tercer país u otra organización internacional, y siempre con el fin de asegurar que el nivel de protección de las personas físicas garantizado no se vea menoscabado.

Bajo esta premisa el Reglamento permite las transferencias basadas en una decisión de adecuación, en el sentido de que podrá realizarse una transferencia de datos personales a un tercer país u organización internacional cuando la Comisión –como se dirá más adelante– haya decidido que el tercer país, un territorio, o uno o varios sectores específicos de ese tercer país, o la organización internacional de que se trate garantizan un nivel de protección adecuado, sin que dicha transferencia requiera autorización específica alguna (art. 45).

Por último, el RGPD contempla que –a falta de la decisión de adecuación– el responsable o el encargado del tratamiento solo podrá transmitir datos personales a un tercer país u organización internacional si hubiera ofrecido garantías adecuadas y a condición de que los interesados que cuenten con derechos exigibles y acciones legales efectivas (art. 46).

Esta regulación que efectúa el RGPD es similar a la que contempla el proyecto de ley chileno, que adapta la regulación específica para la transferencia internacional de datos personales a los estándares y recomendaciones de la OCDE (Título V del proyecto, arts. 27 y ss). En este sentido hace descansar en la autoridad de control la determinación de qué países se consideran adecuados y cuáles no adecuados, permitiendo en el primer caso una amplia autonomía a los intervinientes para transferir datos, mientras que en el segundo solo se permite la transferencia en un conjunto de circunstancias que autorizan el envío de la información, bajo la responsabilidad legal de quien efectúa la transferencia de datos y con aviso previo a la autoridad de control.

11. Autoridades independientes de control

De forma muy exhaustiva el RGPD incide en el modelo europeo o continental de protección de datos (*data protection officer*) y prueba de ello es que fortalece su independencia.

El art. 51 el RGPD obliga a cada Estado miembro a establecer que sea responsabilidad de una o varias autoridades públicas independientes, supervisar la aplicación del Reglamento, con el fin de proteger los derechos y las libertades fundamentales de las personas físicas en lo que respecta al tratamiento y de facilitar la libre circulación de datos personales en la Unión. Todo ello en el marco de que cada autoridad de control debe contribuir a la aplicación coherente del Reglamento en toda la Unión, al tiempo que las autoridades de control deben cooperar entre sí y con la Comisión[50].

En lo que respecta a la independencia, el art. 52 obliga a que cada autoridad de control deba actuar con total independencia en el desempeño de sus funciones y en el ejercicio de sus poderes de conformidad con el Reglamento, y a que el miembro o los miembros de cada autoridad de control sean ajenos, en el desempeño de sus funciones y en el ejercicio de sus poderes de conformidad con el Reglamento, a toda influencia externa, ya sea directa o indirecta, sin que puedan solicitar ni admitir instrucción alguna.

Asimismo, el miembro o los miembros de cada autoridad de control deben abstenerse de cualquier acción que sea incompatible con sus funciones y no participarán, mientras dure su mandato, en ninguna actividad profesional que sea incompatible, remunerada o no.

A cada Estado miembro le corresponde garantizar que cada autoridad de control disponga en todo momento de los recursos humanos, técnicos y financieros, así como de los locales y las infraestructuras necesarios para el cumplimiento efectivo de sus funciones y el ejercicio de sus poderes, incluidos aquellos que haya de ejercer en el marco de la asistencia mutua, la cooperación y la participación en el Comité.

Cada Estado miembro debe garantizar que cada autoridad de control elija y disponga de su propio personal, que estará bajo la autoridad exclusiva del miembro o miembros de la autoridad de control interesada, y que cada autoridad de control esté sujeta a un control financiero que no afecte a su independencia y que disponga de un presupuesto anual, público e independiente, que podrá formar parte del presupuesto general del Estado o de otro ámbito nacional

Ante la laguna de la Ley Nº 19.628, el proyecto de ley contempla la creación de una autoridad de control, si bien con funciones de menor intensidad a las de los Estados europeos, en los que la autoridad de control interviene en funciones de seguridad de los datos.

[50] Conforme al art. 51.3 RDGP, "Cuando haya varias autoridades de control en un Estado miembro, este designará la autoridad de control que representará a dichas autoridades en el Comité, y establecerá el mecanismo que garantice el cumplimiento por las demás autoridades de las normas relativas al mecanismo de coherencia a que se refiere el artículo 63".

Un paso adelante en la regulación de la protección de datos que efectúa el proyecto de ley consiste en el diseño de un cuadro de infracciones administrativas (graduadas en leves, graves y gravísimas), y sus correspondientes sanciones, de acuerdo con un procedimiento administrativo del que es competente la Agencia Chilena de Protección de Datos, y cuyas resoluciones son –como he adelantado– susceptibles de revisión jurisdiccional.

12. Comité Europeo de Protección de Datos

Debe destacarse la creación en el RGPD del Comité Europeo de Protección de Datos, verdadero cimiento en el que se asienta el nuevo marco legal de la protección de datos de la Unión Europea y heredero de gran parte de las funciones que tenía atribuidas el grupo de Trabajo del Artículo 29 de la derogada Directiva 95/46/CE[51].

En este sentido en virtud del art. 68 se crea el Comité como organismo de la Unión, con personalidad jurídica propia, compuesto por el director de una autoridad de control de cada Estado miembro y por el Supervisor Europeo de Protección de Datos o sus representantes respectivos. La Comisión –órgano de gobierno de la Unión Europea– tiene derecho a participar en las actividades y reuniones del Comité, sin derecho a voto.

El Comité actúa con total independencia en el ejercicio de sus funciones –que el art. 70 enumera hasta un total de 27– y elaborará un informe anual en materia de protección de las personas físicas en lo que respecta al tratamiento en la Unión y, si procede, en terceros países y organizaciones internacionales, y el informe se hará público y transmitirá al Parlamento Europeo, al Consejo y a la Comisión.

Como he dicho en reiteradas ocasiones, si el flujo de datos no conoce fronteras, el régimen jurídico de la protección de los mismos debe tener una vocación transfronteriza, y de hecho el RGPD es una prueba de ella en el continente europeo. Por eso no debería descartarse que Chile, aprovechando los esfuerzos normativos que está llevando a cabo, promueva la creación de un organismo de ámbito iberoamericano, a quien corresponda la creación y diseño de estándares sobre la materia, al objeto de uniformizar el derecho estatal sobre la protección de datos, a imagen y semejanza del Comité Europeo.

II. CARACTERÍSTICAS ESENCIALES DE LA REFORMA CHILENA.

Sin perjuicio de la comparación de materias y sub materias específicas que se han expuesto en el epígrafe anterior, no puede dejar de señalarse que Chile afronta, con el proyecto de ley por el que se regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales, un nuevo escenario digital que demanda un nuevo régimen jurídico.

En efecto, en muy poco tiempo hemos asistido a una verdadera revolución que una sociedad globalizada y una economía abierta van imponiendo, por ejemplo, *big data*, internet de las cosas, robotización y *machine learning*, *cloud computing*, vehículos

[51] Véase CERVERA-NAVAS (2016).

autónomos, drones, impresiones 3D, *blockchain*, y que plantean al legislador retos jurídicos que no pueden dejar de atenderse[52].

La respuesta europea ante esta transformación digital se ha abordado desde una perspectiva regional, la Unión Europea, que obliga a los Estados miembros a adaptar sus legislaciones nacionales, sin perjuicio de la vocación transfronteriza a que he aludido. La República de Chile, en cambio, está reformando su legislación nacional, lo que afectará invariablemente a relaciones socio-económicas y transacciones en el interior de la nación, pero también transfronterizas, respecto de otros Estados con regulaciones dispares.

Por ello considero que debería aprovecharse el liderazgo chileno en la materia para plantear una regulación en el seno de una organización más amplia, como mínimo de ámbito regional, que contribuyera a la armonización de regímenes jurídicos, a imagen y semejanza de la actuación europea.

Con carácter general debe apreciarse el notable avance de la regulación chilena porque –de aprobarse el proyecto en el Congreso Nacional– la Ley Nº 19.628 pasa de 24 artículos a 60 y se conserva su estructura pues la reforma modifica preceptos existentes y agrega títulos y artículos *ex novo*.

Ya desde el frontispicio el proyecto de ley da una nueva redacción al objeto y ámbito de aplicación (art. 1), con un contenido más amplio y siempre en torno al respeto y protección de los derechos y libertades de los titulares de datos al tiempo que amplía considerablemente la relación de definiciones (art. 2): introduce conceptos que no aparecen en la Ley vigente como el proceso de anonimización o disociación, los derechos ARCO, el derecho a la portabilidad de datos personales, o el Registro Nacional de Cumplimiento y Sanciones, entre otros.

En materia de principios, como he avanzado, el art. 3 recoge los relativos a la licitud del tratamiento, finalidad, proporcionalidad, calidad, responsabilidad, seguridad e información.

El Título I, relativo en la Ley vigente a la utilización de datos personales, se sustituye por completo por una nueva regulación, que lleva por rúbrica "De los derechos del titular de datos personales", y en él se enumeran los derechos ARCO (arts. 5 a 8), a la portabilidad (art. 9), la forma y medios de ejercer los derechos (art. 10) y el procedimiento ante el responsable de datos (art. 12), que comprende el contenido mínimo de la solicitud y la obligación de responder expresamente en un plazo de diez días hábiles, de manera que –transcurrido este plazo sin haber resuelto– el titular puede dirigir directamente reclamación ante la Agencia de Protección de Datos Personales.

El Título II de la Ley Nº 19.628, relativo a los derechos de los titulares de datos, se reemplaza por completo por una regulación relativa al tratamiento de los datos personales y de las categorías de datos personales, y comprende un primer párrafo relativo al consentimiento del titular, las obligaciones y deberes del responsable y el

[52] CERVERA-NAVAS (2018) p. 74.

tratamiento de datos en general. En el mismo se hace descansar el tratamiento de datos en el consentimiento de su titular (art. 12) pero contemplando una serie de excepciones cuando los datos se encuentren en fuentes accesibles al público, se refieran a obligaciones de carácter económico, financiero o bancario o el tratamiento es necesario para la ejecución o el cumplimiento de una obligación legal o de un contrato en que es parte el titular (art. 13). El proyecto de ley dedica especial atención a las obligaciones del responsable de datos (art. 14), regulando expresamente sus deberes de secreto (art. 14 bis), de información y transparencia (art. 14 ter), de adoptar medidas de seguridad (art. 14 quáter) y de reportar vulneraciones a las medidas de seguridad (art. 14 quinquies), así como la diferenciación de estándares de cumplimiento (art. 14 sexies), y concluye el párrafo con el régimen de cesión o transferencia de bases de datos personales (art. 15) y el tratamiento de datos por un tercero o mandatario (art. 15 bis). El párrafo segundo se dedica al tratamiento de los datos personales sensibles, con la regla general de que solo puede realizarse si su titular presta consentimiento libre e informado previo (art. 16), después se hace mención a los datos relativos a la salud (art. 16 bis), biométricos (art. 16 ter) y al perfil biológico humano (art. 16 quáter). El párrafo tercero se refiere al tratamiento de categorías de datos especiales: los relativos a niños, niñas y adolescentes (art. 16 quinquies), los datos personales con fines históricos, estadísticos, científicos y de estudios o investigaciones (art. 16 sexies), y datos de geolocalización (art. 16 septies).

El Título IV (arts. 20 y ss), concerniente al tratamiento de datos personales por los órganos públicos, también es objeto de reemplazo completo, arranca con la regla general de la licitud del tratamiento de datos que efectúan los organismos públicos (art. 20) y de los principios y normas aplicables (art. 21), que son los propios del art. 3, a los que se suman los principios de coordinación, eficiencia, transparencia y publicidad, y regla que conforme al art. 24 admite excepciones cuando: efectúen tratamiento de datos que se encuentran protegidos por normas de secreto o confidencialidad establecidas en sus respectivas leyes; realicen tratamiento de datos personales para la investigación, persecución, enjuiciamiento o sanción de infracciones penales, civiles y administrativas; efectúen operaciones de tratamiento de datos personales en actividades relacionadas con la seguridad de la nación, la defensa nacional o la mantención del orden público o la seguridad pública; se haya declarado estado de catástrofe o estado de emergencia, de conformidad a la ley y mientras permanezca vigente la respectiva declaración.

El art. 22 regula la cesión de datos entre organismo público y el 23 se refiere al ejercicio de los derechos del titular y reclamo de ilegalidad, el 25 regula específicamente los datos relativos a infracciones penales, civiles, administrativas y disciplinarias, y el art. 26 efectúa una remisión a un reglamento que enumere las condiciones para la cesión de datos entre organismos públicos.

El Título V, que en la Ley vigente atañe a la responsabilidad sancionadora, se sustituye por el régimen de la transferencia internacional de datos personales y en este sentido el proyecto de ley distingue las reglas aplicables a países con niveles de protección adecuados (art. 27) y no adecuados (art. 28), así como el régimen de exclusiones, comunicaciones y fiscalización (art. 29).

Los Títulos VI, VII y VIII son completamente nuevos. El primero se refiere a la Agencia de Protección de Datos Personales: el mandato de su creación y domicilio en la

ciudad de Santiago (art. 30), sus funciones y atribuciones (art. 31), la coordinación regulatoria con el Consejo para la Transparencia (art. 32), el régimen de su director o directora (art. 33), las incompatibilidades (art. 34), el personal (art. 35), y su patrimonio (art. 36).

El Título VII trata de las infracciones y sanciones, de los procedimientos y de las responsabilidades de los responsables de datos y en su párrafo primero comprende la tipificación de las infracciones leves, graves y gravísimas (art. 38) y las sanciones aparejadas (art. 39), las reglas para la determinación del monto de las cuantías (art. 40), las atenuantes de responsabilidad (art. 41), las sanciones accesorias (art. 42), el Registro Nacional de Cumplimiento y Sanciones, de acceso público y gratuito, y con una vigencia de sus anotaciones de cinco años (art. 43) y los plazos de prescripción (art. 44).

El párrafo segundo contempla los dos procedimientos administrativos: el de tutela de derechos (art. 46) y el de infracción de ley (art. 46), ambos formulados ante la Agencia de Protección de Datos Personales y cuya resolución será revisable en vía jurisdiccional ante la Corte de Apelaciones de Santiago o la del lugar donde se encuentre domiciliado el reclamante, a su elección (párrafo tercero, art. 47).

El párrafo cuarto se dedica a la responsabilidad de los órganos públicos, de la autoridad o jefe superior del órgano y de sus funcionarios, ya sea la responsabilidad administrativa de la autoridad o jefe superior del órgano público (art. 48), la propia del funcionario infractor (art. 49), así como específicamente los deberes de reserva y confidencialidad (art. 50). El párrafo quinto regula la responsabilidad civil del responsable de datos (art. 51) y el sexto incluye un régimen ciertamente novedoso que consiste en un modelo de prevención de infracciones pues los arts. 52 a 56 prevén que los responsables de datos, sean personas naturales o entidades o personas jurídicas, públicas o privadas, puedan adoptar modelos de prevención de infracciones con un contenido mínimo: (1) designación de un encargado de prevención o delegado de protección de datos personales, (2) definición de medios y facultades del encargado de prevención y (3) establecimiento de un programa de cumplimiento que a lo menos contemple i) la identificación del tipo de información que trata, el ámbito jurisdiccional en que opera, la categoría, clase o tipos de datos o bases de datos que administra, la caracterización de los titulares de datos y el o los lugares donde residen estos últimos, ii) la identificación de las actividades o procesos de la entidad, sean habituales o esporádicos, en cuyo contexto se genere o incremente el riesgo de comisión de las infracciones señaladas en el artículo 38, iii) el establecimiento de protocolos, reglas y procedimientos específicos que permitan a las personas que intervengan en las actividades o procesos indicados en la letra anterior, programar y ejecutar sus tareas o labores de una manera que prevenga la comisión de las referidas infracciones, iv) mecanismos de reporte hacia las autoridades para el caso de contravenir lo dispuesto en la presente ley, v) la existencia de sanciones administrativas internas, así como de procedimientos de denuncia o persecución de responsabilidades de las personas que incumplan el sistema de prevención de infracciones.

Este carácter preventivo de cualquier infracción en materia de protección de datos se refuerza con la supervisión y certificación del modelo por parte de la Agencia de Protección de datos Personales.

Por su parte, el Título VIII se refiere al tratamiento de datos personales por el Congreso Nacional, el Poder Judicial y organismos públicos dotados de autonomía constitucional, que parte –al igual que en el caso de los organismos públicos– de la regla general de la licitud del tratamiento de datos (art. 57) y del ejercicio de los derechos y reclamaciones (art. 58).

Por último y en relación a la coordinación entre la Agencia de Protección de Datos Personales y el Consejo para la Transparencia, este proyecto de ley reforma la Ley Nº 20.285, de Transparencia de la Función Pública y de Acceso a la Información de la Administración del Estado, en concreto da nueva redacción al art. 33.m para incluir, entre las funciones del Consejo, la de velar por la protección de los datos de carácter personal en los ámbitos de la transparencia de la función pública y el acceso a la información.

CONCLUSIONES

En materia de protección de datos existen dos concepciones ciertamente diferenciadas, cual es la europea– volcada en la privacidad– y la de Estados Unidos, que subordina la privacidad a la seguridad. Los países iberoamericanos han avanzado en los últimos años afrontando un proceso de aprobación de normas de protección de datos personales, más próximas al modelo europeo que al americano[53], y en consecuencia con una especial sensibilidad por la privacidad.

Sin embargo, como se observa, el modelo europeo ha evolucionado de manera significativa con la aprobación del RGPD, dejando un campo muy amplio a los países iberoamericanos para seguir desarrollando su legislación.

En el caso de Chile la Ley 19.628 permite recorrido para un desarrollo más amplio y garantista para el tratamiento de datos, de manera que puede adaptar instituciones y soluciones que ya el modelo europeo incorpora.

Otra cosa es que –dado el carácter transfronterizo de los datos en una economía cada vez más globalizada– entiendo que las iniciativas normativas en esta materia deberían tener una dimensión como mínimo regional, y para esto la Red Iberoamericana de Protección de Datos está llamada a ser el catalizador de este avance normativo.

El proyecto de ley de protección de datos de carácter personal que se encuentra en tramitación en el Congreso Nacional constituye una magnífica ocasión para revisar el modelo chileno sobre esta materia, a lo que se une la actualización de este régimen jurídico en España. En Chile existen instituciones académicas –Universidades (de Chile, Pontificia Universidad Católica de Valparaíso, Alberto Hurtado, Diego Portales, Mayor, Bernardo O'Higgins) y centros especializados (Centro de Estudios en Derecho Informático, Instituto Chileno de Derecho y Tecnología) con amplia experiencia en la investigación académica sobre protección de datos, cuyas aportaciones a la elaboración normativa pueden ser más que útiles.

[53] GREGORIO (2004) p. 385, TRONCOSO REIGADA (2012) p. 4.

De hecho, no son pocas las novedades que al día de hoy el proyecto de ley recoge, muchas de ellas en consonancia con el RGPD (v. gr., calificación de la protección de datos como derecho fundamental, creación de una autoridad de control, diseño de un régimen sancionador, portabilidad de datos, datos de menores, flujos transfronterizos de datos personales), si bien en algunos casos otras instituciones distan de hallar equiparación (v. gr., seguridad de los datos, encargado del tratamiento) y por ello deviene necesario una labor de reflexión y de análisis de la experiencia del derecho comparado, especialmente de los Estados europeos y su legislación adaptada al RGPD.

Solo desde la serenidad y la comprensión del universo de la protección de datos en su globalidad, puede llevarse a cabo una reforma integral del régimen chileno, más allá de meras reformas parciales. La entrada en vigor del RGPD, con una clara vocación transfronteriza y un marcado interés en la privacidad, constituye una ocasión de primer orden para abordar la regulación de esta materia, con un sentido regional Iberoamericano.

BIBLIOGRAFÍA CITADA

ADSUARA VARELA, Borja (2016): "El consentimiento", en PIÑAR MAÑAS, José Luis (Dir.), *Reglamento General de Protección de datos. Hacia un nuevo modelo europeo de privacidad* (Madrid, Editorial Reus), pp. 151-169.

ALVARADO, Francisco (2014): "Las fuentes de acceso público a datos personales", *Revista Chilena de Derecho y Tecnología*, nº 3, pp. 205-226.

ÁLVAREZ VALENZUELA, Daniel (2016): "Acceso a la información y protección de datos personales: ¿Puede el Consejo para la Transparencia ser la autoridad de control en materia de protección de datos?", *RDCN (Coquimbo)*, vol. 23, nº1, pp. 51-79. Disponible en: https://scielo.conicyt.cl/pdf/rducn/v23n1/art03.pdf, fecha de consulta: 8 de agosto de 2018.

AGUSTINA, José Ramón y BLUMENBERG, Axel Dirk (2015): "El Data Protection Officer en el marco de la responsabilidad penal de las personas jurídicas. Consideraciones a la luz del nuevo Reglamento Europeo de protección de datos", en RALLO LOMBARTE, Artemi y GARCÍA MAHAMUT, Rosario (Dirs), *Hacia un Nuevo Derecho Europeo de Protección de Datos* (Valencia, Tirant lo Blanch), pp. 247-274.

BAUZÁ MARTORELL, Felio José (2017): "Big data y open data en la Administración turística: acceso y reutilización de información", *Revista Vasca de Administración Pública*, núm. 108 (mayo-agosto), pp. 19-41. Disponible en: https://www.euskadi.net/r61s20001x/es/t59aWar/t59aMostrarFicheroServlet?t59aIdRevista=2&R01HNoPortal=true&t59aTipoEjemplar=R&t59aSeccion=38&t59aContenido=1&t59aCorrelativo=1&t59aVersion=1&t59aNumEjemplar=108, fecha de consulta: 20 de agosto de 2018.

CERVERA-NAVAS, Leonardo (2018): "El nuevo modelo europeo de protección de datos de carácter personal", en LÓPEZ CALVO, José (Coord.), *El nuevo marco*

regulatorio derivado del Reglamento Europeo de Protección de Datos (Madrid, Wolters Kluwer), pp. 71-78.

_____, (2016): "El Comité Europeo de Protección de Datos", en PIÑAR MAÑAS, José Luis (Dir.), *Reglamento General de Protección de datos. Hacia un nuevo modelo europeo de privacidad* (Madrid, Editorial Reus), pp. 527-538.

FERNÁNDEZ CONTE, Julen y LEÓN BURGOS, Diego (2016): "Antecedentes y proceso de reforma sobre protección de datos en la Unión Europea", en PIÑAR MAÑAS, José Luis (Dir.), *Reglamento General de Protección de datos. Hacia un nuevo modelo europeo de privacidad* (Madrid, Editorial Reus), pp. 35-50.

FERNÁNDEZ SAMANIEGO, Javier y FERNÁNDEZ LONGORIA, Paula (2016): "El derecho a la portabilidad de los datos", en PIÑAR MAÑAS, José Luis (Dir.), *Reglamento General de Protección de datos. Hacia un nuevo modelo europeo de privacidad* (Madrid, Editorial Reus), pp. 257-274.

GARCÍA GONZÁLEZ, Aristeo (2007): "La protección de datos personales: derecho fundamental del siglo XXI. Un estudio comparado", *Boletín mexicano de Derecho Comparado*, núm. 120, pp. 743-778. Disponible en: https://revistas.juridicas.unam.mx/index.php/derechocomparado/article/view/3933/4972, fecha de consulta: 5 de agosto de 2018.

GARCÍA MEXÍA, Pablo Luis (2016): "La singular naturaleza jurídica del Reglamento General de Protección de Datos de la UE. Sus efectos en el acervo nacional sobre protección de datos", en PIÑAR MAÑAS, José Luis (Dir.), *Reglamento General de Protección de datos. Hacia un nuevo modelo europeo de privacidad* (Madrid, Editorial Reus), pp. 23-34.

GIMENO FELIÚ, José María (2016): "Administración Pública y Derecho Administrativo en la Unión Europea. La consolidación de un modelo de uniformización jurídica", en BAÑO LEÓN, José María (Coord.), *Memorial para la reforma del Estado: Estudios en homenaje al Profesor Santiago Muñoz Machado. Vol. 1 (Tomo I)*, pp. 279-301.

GREGORIO, Carlos (2005): "Protección de Datos Personales. Europa vs. Estados Unidos, todo un dilema para América Latina", en CONCHA CANTÚ, Hugo *et al*. (Coords.), *Transparentar al Estado: la experiencia mexicana de acceso a la información* (1ª reimpresión de 1ª ed. 2004, México D.F., Universidad Nacional Autónoma de México), pp. 299-325. Disponible en: https://archivos.juridicas.unam.mx/www/bjv/libros/3/1407/12.pdf, fecha de consulta: 12 de agosto de 2018.

JIJENA LEIVA, Renato Javier (2001): "Sobre la no protección de la intimidad en Chile. Análisis de la Ley 19.628, de Agosto de 1999", *Revista Electrónica de Derecho Informático*, núm. 39, pp. 1-27.

_____, (2010): "Actualidad de la protección de datos personales en América latina. El caso de Chile", *Memoria del XIV Congreso Iberoamericano de Derecho e Informática* (Monterrey, UANL), pp. 401-419.

LARA, Juan Carlos *et al.* (2014): *La privacidad en el sistema legal chileno* (Policy Papers N° 8 ONG Derechos Digitales). Disponible en: https://www.derechosdigitales.org/wp-content/uploads/pp-08.pdf, fecha de consulta: 3 de julio de 2018.

LÓPEZ GARCÍA, Mabel (2014): "Derecho a la información y derecho al olvido en Internet", *La Ley Unión Europea*, núm. 17 de Julio 2014, pp. 41-50.

MALDOFF, Gabriel (2016): *The Risk-Based Approach in the GDRP: Interpretation and Implications* (White Paper). Disponible en: https://iapp.org/resources/article/the-risk-based-approach-in-the-gdpr-interpretation-and-implications/, fecha de consulta: 9 de agosto de 2018.

PAZOS CASTRO, Ricardo (2015): "El mal llamado derecho al olvido en la era de Internet", *Boletín del Ministerio de Justicia*, Año 69, núm. 2183 (noviembre), pp. 3-88. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=5342701, fecha de consulta: 16 de agosto de 2018.

RECIO GAYO, Miguel (2016): "Aproximación basada en el riesgo, evaluación de impacto relativa a la protección de datos personales y consulta previa a la autoridad de control", en PIÑAR MAÑAS, José Luis (Dir.), *Reglamento General de Protección de datos. Hacia un nuevo modelo europeo de privacidad* (Madrid, Editorial Reus), pp. 351-366.

REUSSER MONSÁLVEZ, Carlos (2018): *Derecho al olvido. La protección de datos personales como límite a las libertades informativas* (Santiago de Chile, Ediciones Der).

RIPOL CARULLA, Santiago (2016): "Aplicación territorial del Reglamento", en PIÑAR MAÑAS, José Luis (Dir.), *Reglamento General de Protección de datos. Hacia un nuevo modelo europeo de privacidad* (Madrid, Editorial Reus), pp. 77-95.

SERRANO PÉREZ, María Mercedes (2005): "El derecho fundamental a la Protección de Datos. Su contenido esencial", *Nuevas Políticas Públicas: Anuario multidisciplinar para la modernización de las Administraciones Públicas*, núm. 1, pp. 245-265. Disponible en: http://www.juntadeandalucia.es/institutodeadministracionpublica/anuario/articulos/descargas/01_NOT_01_serrano.pdf, fecha de consulta: 25 de julio de 2018.

TRONCOSO REIGADA, Antonio (2012): "El desarrollo de la protección de datos personales en Iberoamérica desde una perspectiva comparada y el reequilibrio en los modelos de protección de datos a nivel internacional", *Revista Internacional de Protección de Datos Personales*, núm. 1 (julio-diciembre), pp. 1-41. Disponible en: https://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/10_Antonio-troncoso_FINAL.pdf, fecha de consulta: 25 de julio de 2018.

VIOLLIER, Pablo (2017): *El Estado de la protección de datos personales en Chile* (Derechos Digitales América Latina). Disponible en: https://www.derechosdigitales.org/wp-content/uploads/PVB-datos-int.pdf, fecha: de consulta: 19 de julio de 2018.