

DOCTRINA

Interés legítimo y tratamiento de datos personales: Antecedentes comparados y regulación en Chile

*Legitimate interest and personal data processing:
Comparative background and Chilean regulation*

Pablo Contreras Vásquez 

Universidad Autónoma, Chile

Pablo Trigo Kramcsák 

Abogado independiente, Chile

RESUMEN El texto examina el concepto de interés legítimo como fuente de licitud para el tratamiento de datos personales. Primero, se desarrolla el concepto de interés legítimo y su conexión con el principio de licitud del tratamiento de datos personales. Segundo, el texto examina las fuentes europeas y españolas del concepto de interés legítimo. Finalmente, se analiza el estatus del interés legítimo en la legislación chilena, tanto en la Ley 19.628, Sobre Protección de la Vida Privada, como en la legislación bancaria. El artículo concluye que el concepto de interés legítimo ha sido desarrollado en el derecho comparado y que, en el evento de reformar la Ley 19.628, deberían considerarse tales estándares en su recepción general en el derecho chileno.

PALABRAS CLAVE Interés legítimo, principio de licitud, datos personales.

ABSTRACT The article examines the concept of legitimate interest as a lawful basis for processing personal data. First, the concept of legitimate interest and its connection with the principle of lawfulness of processing personal data is developed. Second, the text examines the European and Spanish sources of the concept of legitimate interest. Finally, it analyzes the status of legitimate interest in Chilean legislation, both under Law 19.628, On the Protection of Privacy, and in banking legislation. The paper concludes that the concept of legitimate interest has been adequately developed in comparative law and that, in the event of amending Law 19.628, such standards should be considered in their general reception under Chilean law.

KEYWORDS Legitimate interest, lawfulness of processing, personal data.

Introducción

Quizás una de las cuestiones menos estudiadas en la literatura nacional de protección de datos personales es el denominado «interés legítimo». En efecto, no es posible encontrar referencias dogmáticas que sistematicen su concepto, analicen sus alcances o den cuenta de los debates en el derecho comparado, por nombrar algunas de las múltiples dimensiones a partir de las cuales se podría revisar esta fuente de legitimidad para el tratamiento de datos personales. Su ausencia en la Ley 19.628, Sobre Protección de la Vida Privada, podría explicar la falta de estudio sistemático. Sin embargo, la inclusión sectorial de este título para ciertas operaciones de tratamiento de datos en el ámbito bancario ya justificaría un repaso por algunos de sus aspectos fundamentales.

El principio de licitud constituye el pilar fundamental sobre el que descansa el derecho de protección de datos personales. En virtud de este principio, el tratamiento de cualquier información concerniente a una persona natural solo puede tener lugar si concurre previamente el consentimiento del titular u otra fuente habilitante prevista por la ley. Las fuentes o bases de legitimidad son aquellas hipótesis definidas legalmente y que, junto al consentimiento del titular, facultan el tratamiento de datos personales.

Tradicionalmente, el derecho de protección de datos personales ha reconocido al consentimiento del titular como fuente de licitud por antonomasia para el tratamiento de estos datos. Así, la aquiescencia del titular desempeñaría un rol predominante en la habilitación para el procesamiento de datos de carácter personal, al ser entendida como el mecanismo que garantizaría de mejor manera el debido ejercicio del derecho a la autodeterminación informativa. Distintos sistemas de protección de datos personales han asignado al consentimiento esta «función preferente» (Ferretti, 2014: 13), con el entronizado como la regla general de licitud, en el entendido de que permitiría a los individuos un efectivo control o dominio sobre su información personal y su potencial flujo.

El ordenamiento jurídico chileno reconoce dos fuentes de legitimidad para el tratamiento de datos personales: el consentimiento del titular del dato y la autorización legal (Alvarado, 2014: 206-8; Vial Claro, 2001: 27). En el primer caso, el titular accede a que sus datos sean tratados; en el segundo, el legislador ha determinado que los datos pueden ser tratados con independencia de la voluntad del titular. Estas bases de licitud están establecidas en la Ley Sobre Protección de la Vida Privada y son coherentes con el esquema constitucional actualmente en vigor. La reforma constitucional de 2018, a través de la Ley 21.096, estableció la autodeterminación informativa en la Constitución chilena. En efecto, actualmente, el artículo 19 numeral 4 dispone que la Constitución asegura a todas las personas «la protección de sus datos personales» y añade que «el tratamiento y protección de estos datos se efectuará en la forma y

condiciones que determine la ley». Mientras que el consentimiento del titular corresponde al ejercicio legítimo del derecho en cuestión —en este caso, autorizando el tratamiento—,¹ la Constitución remite a la ley para determinar las formas y condiciones para el tratamiento de datos personales.

El tratamiento de datos personales debe reconocer su fundamento en la protección y tutela de la autodeterminación informativa o, como también se le conoce, en el derecho fundamental a la protección de datos personales. A diferencia de lo que pudiere pensarse, el derecho de autodeterminación informativa no es un impedimento al tratamiento de datos personales, sino que, jurídicamente, da el sustento a dichos tratamientos (González Fuster y Gellert, 2012: 78). Este derecho supone el autocontrol y la autonomía de decisión del individuo, titular del derecho, respecto de su información personal e impone un mandato al legislador y a todos los órganos del Estado de protección de los datos personales. A pesar de que la autodeterminación informativa es reconocida en diversas legislaciones como un derecho fundamental, no reviste el carácter de un derecho absoluto, ya que debe ser considerado en relación a su función en la sociedad (González Fuster y Gellert, 2012: 77). De esta forma, el derecho a la protección de datos personales debe ser ponderado con otros intereses, derechos y valores reconocidos jurídicamente, así como también con los medios e instrumentos empleados (Kindt, 2013: 635). En la reserva de ley que fija la Constitución chilena, se autoriza la regulación y restricción del derecho y de la voluntad del titular y, a su vez, habilita al legislador para legitimar tratamientos que no requieren de la decisión autónoma del sujeto activo del derecho, de manera de poder conciliar el ejercicio del derecho con otros derechos fundamentales y bienes constitucionales, como pueden ser la libertad de expresión o el resguardo del orden público.

Esta clara preferencia por el consentimiento del titular ha ido cediendo terreno a nivel normativo. En este sentido, en los últimos años ha tenido lugar un amplio debate acerca del papel central del consentimiento como fuente de licitud para el tratamiento de datos, su alcance, efectividad y las condiciones necesarias para que los titulares de datos tomen decisiones informadas acerca del procesamiento de información personal por terceros (Kamara y De Hert, 2018: 1). A este respecto, se debe tener en especial presente la relación de manifiesto desequilibrio que por lo usual existe entre el titular de los datos y el responsable del tratamiento, lo que redundaría en detrimento del primero. Dada esta realidad, se ha enfatizado la necesidad de contar con regulaciones que contextualicen la privacidad y la protección de datos personales en los entornos actuales, procurando brindar una arquitectura o ecosistema normativo que permita la tutela de la autodeterminación informativa frente a las asimetrías

1. En gran parte de los países europeos continentales, el consentimiento ha formado parte de la doctrina constitucional a partir del desarrollo del derecho a la autodeterminación informativa (Ferretti, 2014: 13).

de poder entre titulares y responsables de tratamientos de datos (Hartzog, 2018: 93-196; Nissenbaum, 2010: 129-230; Solove, 2004: 94-123; 2013: 1.882-2.013).

No resulta aventurado asimilar este desbalance entre el responsable del tratamiento y el titular de los datos con el vínculo asimétrico que existe en los actos de consumo, entre consumidores y proveedores de bienes o servicios, que pone en entredicho la eficacia de autonomía de la voluntad del consumidor y el real valor de su libertad contractual. Incide en esta situación de desequilibrio el otorgamiento por parte de los titulares de datos de su consentimiento sin recibir antes información veraz, clara y oportuna sobre la finalidad y alcances del tratamiento, sirviéndose el responsable del tratamiento, al momento de recopilar dicha autorización, de políticas de privacidad que emplean un lenguaje complejo, tanto desde el punto de vista técnico como normativo, que no resulta inteligible al público general. En muchas ocasiones, las políticas de privacidad son vagas o confusas respecto de los usos futuros de los datos recopilados (Solove, 2013: 1.885).

Si bien en esta materia aún prima una concepción del consentimiento como una manifestación significativa de voluntad, emanada de un individuo plenamente consciente de la extensión y efectos de dicha autorización —rasgo reforzado con el reconocimiento de la dimensión granular del consentimiento—, lo cierto es que hoy se cuestiona si esta institución efectivamente asegura a los titulares de datos mayores grados de autonomía y control sobre su información personal.²

Así, se habla de una crisis de la suficiencia del consentimiento, que ha conllevado incluso su «desensibilización» (Schermer, Custers y Van der Hof, 2014: 178). Se han puesto demasiadas expectativas en los modelos normativos que descansan en una noción amplia de los alcances del consentimiento como fuente legitimadora del tratamiento de datos, esto es, de los enfoques de «autogestión de la privacidad» (Solove, 2013: 1.880). Más aún, se da la paradoja de que el consentimiento —al ser entendido como una salvaguarda en sí mismo— prevalecería incluso en escenarios en que la decisión del titular puede conllevar tratamientos en los que posiblemente habrá una ausencia de protección de sus datos (Balboni y otros, 2013: 246).

Es posible estimar que, a pesar de cumplir con todos los requisitos formales dispuestos por ley para su validez, el consentimiento se ha convertido en un acto irreflexivo y automático, especialmente en aquellos casos en que su otorgamiento opera como condición insoslayable para acceder a una determinada prestación, con especial énfasis en el mundo en línea, donde los titulares de datos, sin más, dan su autorización «todas las veces que se ven enfrentados a una solicitud de consentimiento» (Schermer,

2. Un consentimiento considerado válido desde un punto de vista técnico-legal, no está exento de ciertos problemas que pueden afectar su efectividad en orden a resguardar la autodeterminación informativa de los sujetos, tales como la sobrecarga de solicitudes de autorización («*consent fatigue*»), la sobrecarga de información sobre las condiciones del tratamiento y la ausencia de una elección significativa (Schermer, Custers y Van der Hof, 2014: 176).

Custers y Van der Hof, 2014: 171). Esta situación se explicaría por el hecho de que si el titular de datos no consiente en las condiciones impuestas por el proveedor de un determinado servicio, contenidas en un contrato de adhesión cuyas provisiones dan cuenta, muchas veces, de una autorización amplia para el tratamiento de información (recopilación de una gran cantidad de datos, para llevar a cabo diversas operaciones de tratamiento que satisfagan una multiplicidad de finalidades), el usuario-sujeto de datos se verá impedido en forma absoluta de disfrutar de dicha prestación.

De este modo, surge la necesidad de avanzar hacia un nuevo paradigma en materia de protección de datos personales, en el que la legitimidad del tratamiento radique, más bien, en garantizar niveles apropiados de protección,³ tratando al consentimiento como una entre varias alternativas equivalentes, en lugar de darle un estatus primario.⁴

En este orden de cosas, se sostiene que el consentimiento no constituye siempre la fuente habilitante más apropiada para legitimar ciertas operaciones de procesamiento de datos, tanto desde la perspectiva del titular de los mismos como del responsable del tratamiento, por lo que es necesario, en ciertos casos concretos, considerar otras fuentes de licitud como alternativas más apropiadas (Balboni y otros, 2013: 257). En este sentido, las nuevas tecnologías de análisis de *big data* y metadatos, que se alimentan de grandes conjuntos de datos obtenidos de diversas fuentes no relacionadas, han venido a dificultar la real posibilidad de obtener el consentimiento de los titulares de la información recopilada, por lo que se hace necesario justificar el tratamiento de datos bajo otras fuentes de licitud, como el interés legítimo, que ha llegado a ser considerado como el fundamento bajo el cual se llevarían a cabo la mayor parte de los procesamientos relacionados con transacciones comerciales (Ferretti, 2014: 14).

Es en medio de este escenario que aparece imperioso estudiar el interés legítimo como fuente de legitimidad para el tratamiento de datos personales. Este artículo busca llenar el vacío en la literatura local y anticipar ciertas inquietudes que pueden surgir a la hora de incluir el interés legítimo como parte de la reforma a la Ley de Protección de la Vida Privada. Si bien el interés legítimo es una de las materias que se está discutiendo actualmente en la reforma la Ley, no existen aportes doctrinarios que permitan dar contornos al concepto y a sus consecuencias normativas. El proyecto de ley, además, recién se encuentra en primer trámite constitucional y todavía no concluye su votación en particular, por lo que esta materia es una de las asignaturas pendientes por parte de los legisladores.⁵ Al existir diversas indicaciones legislati-

3. También se ha planteado la necesidad de repensar el consentimiento, por ejemplo, mediante el empleo de esquemas de *nudges* (Solove, 2013: 1.901).

4. Esto no obsta a considerar el consentimiento como una base de licitud preferente respecto de aquellos tratamientos de información que pueden tener un mayor impacto o generar mayores riesgos a los titulares de datos (Balboni y otros, 2013: 256).

5. Para revisar el estado de tramitación de los proyectos refundidos, véase el proyecto de ley en Cámara de Diputados de Chile, disponible en <http://bit.ly/2R3ryUl>.

vas relativas al interés legítimo, parece prudente postergar su análisis sistemático en función del avance del proyecto de ley. Por ello, este artículo circunscribe su objeto al interés legítimo y el tratamiento de datos personales, en Chile y en el derecho comparado, con el fin de brindar mayores luces sobre este título habilitante para el tratamiento de datos personales.

El artículo se estructura de la siguiente forma. Primero, se desarrolla el concepto de interés legítimo y su conexión con el principio de licitud del tratamiento de datos personales. Segundo, el texto examina las fuentes europeas y españolas del concepto de interés legítimo. Finalmente, se analiza el estatus del interés legítimo en la legislación chilena, tanto en la Ley de Protección de la Vida Privada, como en la legislación bancaria. El artículo concluye que el concepto de interés legítimo ha sido adecuadamente desarrollado en el derecho comparado y que, en el evento de reformar la Ley, deberían considerarse tales estándares en su recepción general en el derecho chileno.

Interés legítimo

Concepto

El concepto de «interés legítimo» es difícil de conceptualizar, no solo por su alta indeterminación jurídica, sino porque, en la determinación de su sentido y alcance, han confluído diversas fuentes formales en el derecho comparado, desde decisiones judiciales hasta opiniones de grupos expertos. Un buen punto de partida supone desagregar sus componentes: el interés, que Ihering (1888: 328) identifica como utilidad, bien, valor y goce, más allá de un puro sentido económico o material; y el reconocimiento y tutela de este interés por parte del derecho. Este último rasgo lo distingue del interés simple, sin relevancia a nivel normativo.

En materia de protección de datos personales, el interés legítimo se ha configurado como una base jurídica que permite al responsable de una base de datos personales o a otro tercero el tratamiento de dicha información sin necesidad de recabar previamente el consentimiento del titular de la misma (Ferretti, 2014: 14). En este sentido, este interés vendría a atribuir y determinar una cierta calidad especial que un tercero, como sujeto interesado, tendría respecto de datos personales ajenos.

Es evidente que el interés legítimo constituye un concepto jurídico indeterminado (Guasch Portas y Soler Fuensanta, 2015: 438), que puede resultar vago y ambiguo (Ferretti, 2014: 23), considerando especialmente que su aplicación requiere ponderar las circunstancias concurrentes que rodean una operación de procesamiento de datos específica: la utilidad (beneficio material) que una o varias operaciones específicas de tratamiento de datos personales ajenos reporta al sujeto interesado, entendidas como herramientas idóneas (vínculo directo) para satisfacer una necesidad (interés) tutelado por el derecho, y el grado en que los derechos o la esfera jurídica del titular

de datos se ven negativamente afectados por dichos tratamientos (externalidad). La ponderación de estos elementos, en conjunto, permitiría determinar si el interesado se encuentra habilitado para ejecutar ciertas actividades de tratamiento sobre los datos personales de un tercero (licitud de la pretensión), sin concurrir el consentimiento de éste.

Respecto al interés tutelado, resulta menester la existencia de una necesidad legítima, esto es, reconocida por ordenamiento jurídico y compatible con los derechos de terceros —por ejemplo, la obtención de un provecho económico—, y susceptible de ser satisfecha mediante una o varias operaciones de procesamiento de datos. Así, estos actos de tratamiento específicos constituirían el medio apto para proveer un beneficio lícito al interesado, cuya obtención es consecuencia directa de dichos tratamientos.

En este sentido, corresponde establecer si la institución del interés legítimo para el tratamiento de datos personales, al identificarse con un beneficio o utilidad jurídicamente relevante, conlleva para el interesado un derecho subjetivo, a partir del cual surgen obligaciones correlativas para ciertos sujetos específicos, así como acciones procesales para amparar su ejercicio.

Pues bien, la existencia de un interés categorizado como legítimo da paso a una conducta activa —por ejemplo, ciertas operaciones de procesamiento de datos—, la que es permitida o autorizada por el marco normativo, siempre que no se afecte —de forma relevante— la esfera jurídica del titular de los datos. Si bien este «permiso» no reviste la calidad de un derecho subjetivo que suponga deberes correlativos o la posibilidad de establecer exigencias imperativas respecto de otros, sí reconoce la situación jurídica especial del interesado, de la cual puede obtener algún provecho o beneficio, habilitándolo a desplegar ciertas actividades particulares de procesamiento de datos personales bajo el amparo del derecho objetivo. Así, puede entenderse el interés legítimo como una situación jurídica activa en relación con la actuación de un tercero, que si bien no supone un derecho subjetivo, implica la facultad del interesado de exigir el respeto del ordenamiento jurídico (Tron, 2012: 252).

En definitiva, el interés legítimo del responsable de una base de datos o de un tercero pone a éstos en una posición jurídica subjetiva que los autoriza al tratamiento de los datos personales de otros, sin necesidad de que concurra la voluntad del titular de los datos u otra fuente de licitud. Con todo, cabe prevenir desde ya que el interés legítimo, en vista a un conjunto de complejidades que emanan precisamente de su carácter indeterminado, puede ser considerado como la base de licitud para el tratamiento de datos que exige los mayores niveles de rendición de cuentas, requiriendo una evaluación o balance de los riesgos y beneficios que conlleva su uso en diversos ámbitos.⁶

6. Centre for Information Policy Leadership, «Recommendations for implementing transparency, consent and legitimate interest under the GDPR», página 2, disponible en <http://bit.ly/2WCBCFZ>.

Interés legítimo: ¿Excepción al principio general de licitud o nueva base legitimadora?

En una primera fase, el interés legítimo fue entendido como una excepción a regla general habilitante para el tratamiento de datos personales, sin la autorización del titular. Luego, la evolución del derecho de protección de datos, especialmente en el ámbito europeo, ha implicado la expansión de las fuentes de licitud para su procesamiento más allá del binomio consentimiento-ley, sobre la base de la satisfacción de otros bienes jurídicos o derechos.

En este sentido, el Grupo de Trabajo del Artículo 29 (Article 29 Data Protection Working Party, WP29)⁷ sostuvo que el consentimiento sería uno de varios fundamentos jurídicos para tratar datos personales, en lugar del principal fundamento. Si bien tiene un papel importante, sostiene el WP29 que no excluye la posibilidad de que otros fundamentos jurídicos puedan ser más apropiados, ya sea desde el punto de vista del responsable del tratamiento o desde el punto de vista del titular de datos (Opinión 06/2014, página 16).

Así, actualmente se concibe el interés legítimo de terceros como una base habilitante para el tratamiento de datos bien definida y delimitada, cuyas hipótesis no permiten ya situarla en el campo de las meras excepciones al régimen general, constituyendo una fuente legitimadora independiente, con un estatuto diferenciado y con alcances diversos. Constituye una institución que no cumple el mero papel de sustituir al consentimiento del titular, por cuanto las consecuencias y alcance de las actividades de procesamiento que se sigan a propósito de esta fuente de licitud serán diferentes, incluso respecto del ejercicio de los derechos de acceso, rectificación, cancelación, oposición y portabilidad (ARCOP).

7. Órgano consultivo independiente, creado por la propia Directiva 95/46/CE, e integrado por las autoridades de protección de datos de todos los Estados miembros de la Unión Europea, el supervisor europeo de protección de datos y la Comisión Europea. Sus funciones incluían, entre otras, estudiar toda cuestión relativa a la aplicación de las disposiciones nacionales tomadas para la aplicación de la Directiva, con vistas a contribuir a su aplicación homogénea (artículo 30, apartado 1 de la Directiva 95/46/CE). Con la entrada en vigencia y aplicación del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, del 27 de abril de 2016, sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, el WP29 fue reemplazado por el Comité Europeo de Protección de Datos (European Data Protection Board, EDPB). El principal objetivo del EDPB, según establece el artículo 70 del referido Reglamento, es garantizar la aplicación coherente de las normas de protección de datos en la Unión Europea. El EDPB está compuesto por representantes de las autoridades de protección de datos de cada Estado miembro y por el supervisor europeo de protección de datos, pudiendo participar en sus reuniones la Comisión Europea, pero sin derecho a voto.

El interés legítimo en el derecho comparado

La institución del interés legítimo ha sido desarrollada principalmente por las distintas fuentes del derecho de la Unión Europea. En este contexto, resulta también destacable la forma en que España ha abordado el interés legítimo en su normativa interna, sea mediante la transposición del derecho de la Unión Europea o a través de regulación complementaria.⁸ A continuación, se examinan estas fuentes para contribuir en la delimitación del concepto.

La normativa de la Unión Europea⁹

La Directiva 95/46/CE

La Directiva 95/46/CE del Parlamento Europeo y del Consejo de la Unión Europea, 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, adoptada en 1995, regulaba el

8. A nivel regional, paulatinamente, diversas legislaciones han reconocido el interés legítimo como fuente habilitante para el tratamiento de datos personales. Así, Perú, dispone en el artículo 14 de su Ley 29.733 de Protección de Datos Personales, de julio de 2011, que no se requiere el consentimiento del titular de datos personales, para los efectos de su tratamiento, entre otros casos, «cuando el tratamiento de los datos personales sea necesario para salvaguardar intereses legítimos del titular de datos personales por parte del titular de datos personales o por el encargado de datos personales». (numeral 9). Brasil, por su parte, a través de su Ley General de Protección de Datos Personales, de agosto de 2018, establece entre las hipótesis que habilitan al tratamiento de datos personales el que éste sea necesario para atender a los intereses legítimos del controlador o de tercero, excepto en el caso de prevalecer derechos y libertades fundamentales del titular que exijan la protección de los datos personales (artículo 7, numeral 9). Finalmente, en Argentina, el Congreso Nacional está actualmente discutiendo un proyecto de ley que tiene por finalidad reemplazar su actual normativa sobre protección de datos, contenida principalmente en la Ley 25.326, sancionada en octubre de 2000. Entre otros aspectos, este proyecto contempla en su artículo 11, letra g) a los intereses legítimos perseguidos por el responsable del tratamiento o por un tercero como una nueva base de licitud para el tratamiento de datos personales, siempre que no prevalezcan los intereses o los derechos del titular de los datos, en particular cuando el titular sea un niño, niña o adolescente.

9. Se debe tener presente que la Carta de los Derechos Fundamentales de la Unión Europea, jurídicamente vinculante para los Estados miembros desde la entrada en vigor del Tratado de Lisboa, en 2009, vino a constitucionalizar, en su artículo 8, el derecho a la protección de datos personales, estableciendo que éstos deben ser tratados «sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley». Por otra parte, el Tratado de Funcionamiento de la Unión Europea dispone en su artículo 16 que «toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan». Agrega dicha norma que «el Parlamento Europeo y el Consejo establecerán, con arreglo al procedimiento legislativo ordinario, las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión, así como por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del derecho de la Unión, y sobre la libre circulación de estos datos».

procesamiento de datos personales dentro de la Unión Europea, fijando los objetivos en la materia, pero dejando a los Estados miembros escoger la forma y los medios a través de los cuales se alcanzarán dichos objetivos (obligación de transposición en el derecho interno).

Con miras a asegurar un nivel de protección adecuado entre los diversos Estados miembros, la Directiva establecía en su sección 2 (artículo 7) las condiciones generales de licitud en el tratamiento de los datos personales. Si bien la Directiva, como regla general, hacía descansar la legitimidad de este tratamiento en el consentimiento inequívoco del titular, contemplaba seis principios que contribuían a atenuar la exigibilidad de este consentimiento, como la ejecución de un contrato en el que el interesado sea parte; la aplicación de medidas precontractuales adoptadas a petición del interesado; el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento; la protección del interés vital del interesado; el cumplimiento de una misión de interés público o inherente al ejercicio del poder público; o la satisfacción del interés legítimo perseguido por el responsable del tratamiento o un tercero.

En el caso concreto del interés legítimo, disponía la Directiva, en su artículo 7, letra f), que

Los Estados miembros dispondrán que el tratamiento de datos personales sólo pueda efectuarse si: [...] f) es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección con arreglo al apartado 1 del artículo 1 de la presente Directiva.

A partir del tenor literal del citado artículo 7, letra f), se pueden identificar los tres elementos que configuran esta base de licitud: i) la existencia de un interés legítimo, del responsable del tratamiento o de un tercero; ii) la prueba de necesidad, esto es, el hecho de que el tratamiento resulta imprescindible para la satisfacción del referido interés, de modo que, si dicho objetivo se puede alcanzar de forma razonable de otra manera menos intrusiva, el interés legítimo no puede ser invocado; y iii) la prueba de balance o ponderación,¹⁰ dirigida a determinar, mediante un ejercicio de comparación, la prevalencia del interés legítimo del responsable del tratamiento o de un tercero, respecto de los intereses o derechos y libertades del titular de datos.¹¹

10. Este balance de los conflictos de intereses debe efectuarse teniendo especialmente presente lo dispuesto en el artículo 52 de la Carta de los Derechos Fundamentales de la Unión Europea, sobre el alcance y limitación de los derechos garantizados, en el que se entroniza el principio de proporcionalidad y el respeto del contenido esencial de los derechos.

11. Resulta particularmente problemática la subjetividad del responsable del tratamiento para deter-

Se entendía que el interés legítimo, por su naturaleza, brindaba a los Estados miembros de la Unión Europea un amplio margen para establecer los elementos que permitan determinar su existencia y alcances —al dictar la respectiva normativa de transposición—, lo que fue reconocido por la Comisión Europea en sus diversas evaluaciones sobre la implementación de la Directiva (Balboni y otros, 2013: 249).

A este respecto, resulta ilustradora la Opinión 06/2014, sobre el concepto de interés legítimo del responsable del tratamiento en virtud del artículo 7 de la Directiva 95/46/CE, adoptada por el WP29 en abril de 2014. Dicha Opinión, junto con sus dos anexos,¹² analiza y desarrolla los requisitos contenidos en el artículo 7, letra f) de la Directiva, con el objetivo de evitar interpretación o aplicaciones divergentes del mismo, que dan lugar a una falta de previsibilidad jurídica que redundaría en perjuicio de la posición de los titulares de datos y de la actividad de las empresas u otras organizaciones, estableciendo un enfoque más coherente y armonizado (Guasch Portas y Soler Fuensanta, 2015: 428).

En concreto, la Opinión 06/2014 da cuenta de un conjunto de etapas y criterios a seguir para evaluar o ponderar los intereses de las partes y determinar si prevalece o no «el interés o los derechos y libertades fundamentales del interesado que requieran protección». Para ello, es necesario llevar a cabo una prueba de balance o ponderación que permita establecer la posición prevalente y, en definitiva, si es posible invocar el interés legítimo.

Para el Grupo de Trabajo del Artículo 29, este juicio de ponderación de intereses contrapuestos estará sujeto a las circunstancias concurrentes de cada caso específico, con especial consideración de los siguientes elementos:

Evaluar el interés legítimo del responsable del tratamiento o del tercero, el que puede estar ligado al ejercicio de un derecho fundamental, un interés general u otros intereses cuya legitimidad es reconocida a nivel legal o social-cultural. Sostiene el WP29 que si bien el «interés» estaría estrechamente relacionado con el principio de finalidad, contenido en el artículo 6 letra b) de la Directiva, serían conceptos distintos. Así, en materia de protección de datos, la «finalidad» es la razón específica por la que se tratan los datos, esto es, el objetivo o la intención del tratamiento, mientras que el «interés» es un concepto más amplio, relativo al beneficio que el responsable de la base de datos o la sociedad pueden obtener a partir de su tratamiento.

minar, previo a la recopilación de los datos, la concurrencia de un interés legítimo habilitante. Dicho elemento, junto con la efectividad de la prueba de balance, solo podrían verificarse con certeza en caso de que la existencia del interés legítimo sea controvertida en sede judicial (Kamara y De Hert, 2018: 9).

12. La «Guía rápida sobre cómo realizar la prueba de balance del artículo 7 letra f)» y los «Ejemplos prácticos para ilustrar la aplicación de la prueba de balance del artículo 7 letra f)».

Por otra parte, este interés debe ser suficientemente concreto, real y actual.¹³ De esta manera, los intereses deben ser articulados con suficiente claridad, ya que si resultan demasiado vagos o especulativos no serán considerados.¹⁴ Respecto de la naturaleza del interés, se sostiene que puede variar, por lo que puede ser individual o general, sin encontrarse restringido únicamente a beneficios económicos o comerciales perseguidos por el responsable del tratamiento o un tercero (Opinión 06/2014, página 24). Con todo, el tratamiento de los datos debe conducir a la satisfacción de dicho interés, por lo que debe considerarse si no existe un método menos intrusivo para obtener el mismo resultado (Opinión 06/2014, página 40).

Respecto de la legitimidad de este interés, se señala que tiene que ser «aceptable» de acuerdo al ordenamiento jurídico, mencionándose, a título ejemplar y sin perjuicio si prevalece o no el interés del responsable del tratamiento, las siguientes actividades: el ejercicio del derecho a la libertad de expresión o información; el marketing directo; los mensajes no comerciales no solicitados, incluso para campañas políticas; el ejercicio de acciones judiciales, incluida el cobro de deudas a través de procedimientos extrajudiciales; la prevención de fraude, mal uso de servicios o lavado de dinero; la seguridad informática; el procesamiento de datos con fines históricos, científicos o estadísticos, o con fines de investigación, incluida la investigación de mercado (Opinión 06/2014, página 25).

En cuanto al interés legítimo de terceros, se trataría de un interés distinto y separado de aquel que puede radicar en el responsable del tratamiento.¹⁵ A este respecto, el WP29 menciona ejemplos que ilustran algunos contextos en que el interés legítimo de un tercero puede aplicarse, como la publicación de datos con fines de transparencia y rendición de cuentas, fines históricos o de investigación científica, y la satisfacción del interés público general —por ejemplo, combatir actividades ilegales como el lavado de dinero— (Opinión 06/2014, página 28).¹⁶

El impacto del tratamiento en los derechos o intereses del titular de los datos, prescindiendo especial atención a las respectivas evaluaciones de impacto que cubra cualquier posible consecuencia del tratamiento, la naturaleza de los datos personales en cuestión —especialmente si el tratamiento recae sobre datos sensibles—, la forma en

13. Solo los intereses que reúnan dichas cualidades, y que no sean meramente teóricos, podrán ser sometidos a una prueba de balance con los intereses del titular de datos.

14. Así, el interés legítimo tendría un carácter objetivo y no discrecional (Balboni y otros, 2013: 254).

15. El WP29 definió el concepto de «tercero» en su Opinión 01/2010, sobre los conceptos de «responsable» y «encargado» del tratamiento, adoptada en febrero de 2010. Se señala que tercero es cualquier actor que no tenga una legitimidad o autorización específica —que podría derivarse, por ejemplo, de su función como responsable o encargado del tratamiento, o como su empleado— en el procesamiento de datos personales.

16. Con todo, este interés no puede utilizarse para legitimar prácticas intrusivas que de otro modo no cumplirían con la prueba del artículo 8 numeral 2 de la Convención Europea de Derechos Humanos.

que éstos son tratados —por ejemplo, si los datos recabados serán cruzados con otra información, contenida en bases de datos diversas—, las expectativas razonables del titular de datos —por ejemplo, los grados de privacidad que el titular espera respecto de sus datos, lo que se puede deducir a partir de su conducta—, y el estatus del responsable del tratamiento y del titular de datos —con especial relevancia el hecho de que el titular de datos sea menor de edad o pertenezca a los segmentos más vulnerables de la sociedad—.¹⁷ Señala el WP29 que es importante tener en cuenta que, a diferencia del caso de los intereses del responsable del tratamiento, el adjetivo «legítimo» no es utilizado en el artículo 7 letra f) de la Directiva al referirse a los «intereses» del titular de datos, lo que implica un alcance más amplio para la protección de sus intereses y derechos (Opinión 06/2014, página 30).

Ponderación o balance provisional. Puede ser que, luego de la aplicación de las reglas anteriores, no sea posible determinar con claridad el interés predominante. En estos casos, para hacer prevalecer su interés, el responsable del tratamiento puede introducir medidas adicionales: por ejemplo, implementar mecanismos simples que permitan a cada titular de datos, individualmente y sin condiciones, oponerse al tratamiento (página 41).

Establecer garantías adicionales aplicadas por el responsable del tratamiento para evitar una afectación en los derechos de los titulares de datos, por ejemplo, limitando el volumen de datos recogidos, suprimir los datos después de su uso, y contemplando mecanismos de anonimización de datos (Opinión 06/2014, página 42).

En la Opinión 06/2014 se afirma que, al interpretar el alcance del interés legítimo debe adoptarse un enfoque equilibrado, que asegure niveles necesarios de flexibilidad al responsable del tratamiento en aquellas situaciones en que no exista un impacto indebido en los titulares de datos, entregando a éstos suficiente certeza jurídica y garantías en cuanto a que esta disposición abierta no será utilizada indebidamente (página 10).

Es importante destacar que el WP29 entiende que la naturaleza abierta del artículo 7 letra f) de la Directiva no implica que el interés legítimo deba entenderse como una fuente de legitimidad de carácter subsidiario y, por ende, menos restrictiva, destinada a llenar ciertos vacíos en caso de que no sea posible aplicar otra base habilitante para el tratamiento de datos personales. Sostiene este grupo que el referido artículo no debe ser tratado como un «último recurso» para situaciones raras o inesperadas, en las que se considera que no se aplican otros motivos para un procesamiento legítimo. Por consiguiente, no debe ser elegido automáticamente por los responsables del

17. Dependiendo de si el responsable del tratamiento es una organización individual o pequeña, una empresa multinacional o un organismo del sector público, y otras circunstancias que rodean la recopilación y procesamiento de los datos, su posición puede ser más o menos dominante con respecto al titular de la información personal.

tratamiento de datos, o extender excesivamente su uso, sobre la base de la percepción de que es menos restrictivo que las otras fuentes habilitantes (página 3).

Por otra parte, resulta relevante referirse al desarrollo jurisprudencial que ha tenido la regla del artículo 7 letra f) de la Directiva, a través de los fallos del Tribunal de Justicia de la Unión Europea. Si bien es posible encontrar fallos emblemáticos en materia de protección de datos, el Tribunal no tuvo muchas ocasiones para interpretar los fundamentos del artículo, y en las pocas ocasiones en que existió la oportunidad de hacerlo, no fue totalmente explotada (Kamara y De Hert, 2018: 21). Con todo, la jurisprudencia del tribunal da cuenta de ciertos criterios que sirven en la determinación del contenido y los alcances de la institución del interés legítimo, especialmente en lo relativo a la ponderación de derechos e intereses o prueba de balance.

A continuación, mencionaremos algunas de las sentencias más relevantes del Tribunal de Justicia respecto de las condiciones y alcances del interés legítimo:

El caso *Google Spain SL y Google Inc. con Agencia Española de Protección de Datos (AEPD) y Mario Costeja González* (C-131/12) tenía por objeto una petición de cuestión prejudicial planteada al Tribunal por la Audiencia Nacional española, en el marco de un litigio que versaba sobre una resolución de la AEPD que ordenaba a Google Inc. adoptar las medidas necesarias para retirar los datos personales del señor Mario Costeja de su índice e imposibilitara el acceso futuro a los mismos. Entre las cuestiones planteadas al Tribunal se incluía la posición jurídica, en base a la Directiva, de un proveedor de servicios de motor de búsqueda en internet.

La opinión del Abogado General del caso, Niilo Jääskinen, señalaba que parecía

obvio que la prestación de servicios de motor de búsqueda en internet persigue intereses legítimos [artículo 7 letra f) de la Directiva], concretamente: i) facilitar a los usuarios de internet el acceso a la información; ii) conseguir que la información cargada en internet se difunda de modo más efectivo, y iii) poner en marcha diversos servicios de la sociedad de la información proporcionados por el proveedor de servicios de motor de búsqueda en internet subsidiarios respecto al motor de búsqueda, como la provisión de publicidad mediante palabras clave. Estas tres finalidades están relacionadas con tres derechos fundamentales protegidos por la Carta, concretamente la libertad de información y la libertad de expresión (ambas recogidas en el artículo 11) y la libertad de empresa (artículo 16), respectivamente. Por consiguiente, un proveedor de servicios de motor de búsqueda en internet persigue intereses legítimos, en el sentido del artículo 7 letra f) de la Directiva, cuando trata datos disponibles en internet, incluidos datos personales.¹⁸

18. Conclusiones del abogado general Niilo Jääskinen, presentadas el 25 de junio de 2013, en Asunto C-131/12, párrafo 95.

Si bien la sentencia del Tribunal no confirmó explícitamente los argumentos del abogado general del caso, respecto del interés legítimo de los proveedores de servicios de motor de búsqueda en internet, estableció que la prueba de balance del interés legítimo dependía de las circunstancias individuales de cada caso concreto.

El caso *František Ryněš como Agencia checa de protección de datos de carácter personal* (C-212/13) tenía por objeto una petición de cuestión prejudicial planteada por la Corte Suprema Administrativa de República Checa, en el marco de un litigio entre el Ryněš y la Agencia checa de protección de datos. En concreto, se pedía al Tribunal dilucidar si el artículo 3, apartado 2 de la Directiva —sobre las actividades de tratamiento que quedan fuera del ámbito de aplicación de dicha norma— debía interpretarse en el sentido de que la utilización de un sistema de videovigilancia instalado por una persona física (Ryněš) en su vivienda familiar, con el fin de proteger los bienes, la salud y la vida de los propietarios de la vivienda y cuya vigilancia cubre asimismo el espacio público, constituía un tratamiento de datos efectuado en el ejercicio de actividades exclusivamente personales o domésticas.

Si bien el Tribunal determinó que la instalación de cámaras de videovigilancia doméstica en el espacio público abarca un terreno no reservado a la esfera exclusivamente personal o doméstica, de manera tal que no cabía situarla dentro de las excepciones contempladas en el referido artículo 3, apartado 2 de la Directiva, sí reconoció que concurrían en este caso los intereses legítimos del señor Ryněš, como responsable del tratamiento, los que consistían concretamente en proteger los bienes, la salud y la vida de dicho responsable y los de su familia.

Para el caso *Patrick Breyer con República Federal de Alemania* (C-582/14), en proceso contencioso-administrativo, el señor Breyer había solicitado que se prohibiera a la República Federal de Alemania conservar o permitir que terceros conservasen, al final de las sesiones de consulta de los portales de internet de organismos federales alemanes, la dirección IP del sistema principal de acceso a estos sitios, en la medida en que dicha conservación no fuera necesaria para restablecer la disponibilidad del servicio de telecomunicación en caso de alguna falla.

El Tribunal Federal de Justicia de Alemania, al ser elevado el proceso en casación, planteó dos cuestiones prejudiciales al Tribunal: si una dirección IP dinámica registrada por un proveedor de servicios de medios en línea, con ocasión de la consulta por una persona de un sitio de internet, constituía respecto a dicho proveedor un dato personal; y si el artículo 7 letra f) de la Directiva debía interpretarse en el sentido que

se opondría a una normativa de un Estado miembro con arreglo a la cual un proveedor de servicios de medios en línea sólo puede recoger y utilizar datos personales de un usuario de esos servicios, sin el consentimiento de éste, cuando dicha recogida y utilización sean necesarias para posibilitar y facturar el uso concreto de dichos

servicios por ese usuario, sin que el objetivo de garantizar el funcionamiento general de esos mismos servicios pueda justificar la utilización de los datos tras una sesión de consulta de los servicios.

El Tribunal, junto con concluir que una dirección IP dinámica, mediante la cual un usuario accede a una página web, constituye un dato personal «cuando éste disponga de medios legales que le permitan identificar a la persona interesada gracias a la información adicional de que dispone el proveedor de acceso a internet de dicha persona», estableció que el derecho alemán aplicado al caso, en concreto el artículo 15 de la *Telemediengesetz* (Ley alemana relativa a ciertos servicios de comunicación e información electrónicos),¹⁹ tenía un alcance más restrictivo que el principio previsto en el artículo 7 letra f) de la Directiva. En este sentido, la referida regla debía interpretarse en el sentido de que el objetivo de garantizar el funcionamiento del servicio de telecomunicación podía ser considerado como un interés legítimo.

Reglamento General de Protección de Datos

El Reglamento 2016/679 del Parlamento Europeo y del Consejo de la Unión Europea, 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, aprobado en abril de 2016 y de cumplimiento obligatorio desde el 25 de mayo de 2018, vino a derogar la Directiva 95/46/CE, y se hizo aplicable de forma directa a todos los Estados miembros sin que fuera necesaria la dictación de legislación nacional de transposición.

El Reglamento contempla, en su artículo 6, las mismas fuentes de licitud para el tratamiento de datos personales que la Directiva 95/46/CE, sin establecer una jerarquía al momento de enunciarlas. Sin embargo, se ha incorporado un matiz relevante, al exigir que los tratamientos basados en el consentimiento del titular de datos se fundamenten en una manifestación de voluntad no solo inequívoca, sino que además libre, específica e informada (voluntad positiva), sujeta a una serie de nuevas condiciones, establecidas en el artículo 7 del Reglamento.

Esta nueva realidad ha hecho que el resto de las bases jurídicas de licitud para el tratamiento de datos cobren mayor protagonismo, especialmente el interés legítimo, que incluso podría ser visto como un resquicio (Kamara y De Hert, 2018: 4).

El interés legítimo se encuentra regulado, principalmente, en el apartado 1, letra f) del artículo 6 del Reglamento, con sus alcances precisados en los considerandos 47 a 49. Dicha regla habilita el tratamiento de datos personales, cuando exista un interés legítimo del responsable, o de un tercero, en términos similares al texto del artículo 7

19. Dispone el referido artículo 15 que «el prestador de servicios sólo podrá recoger y utilizar los datos personales de un usuario cuando sea necesario para posibilitar y facturar el uso de medios en línea (datos de uso)».

letra f) de la Directiva en cuanto a su configuración, anteponiendo siempre los derechos del titular de los datos. Señala dicha norma:

Artículo 6: Licitud del tratamiento

1) El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones: [...] f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero,²⁰ 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.

Según se desprende del texto, para determinar la procedencia del interés legítimo, al igual como disponía la Directiva, es necesario efectuar una ponderación, que dice relación con la determinación de su existencia, prueba de necesidad y prueba de balance, todo esto atendiendo a las circunstancias particulares de cada operación de tratamiento de datos respecto de la cual se pretenda invocar esta base de licitud. Ahora bien, a diferencia de la Directiva, la nueva regla contemplada en el Reglamento viene a establecer expresamente la posibilidad de tratar datos personales de niños sobre la base del interés legítimo, lo que requerirá prestar especial atención a sus intereses y derechos, al momento de efectuar la prueba de balance. Asimismo, establece que las autoridades no pueden invocar la existencia de un interés legítimo en las operaciones de tratamiento de datos personales que lleven a cabo en el ejercicio de sus funciones.²¹

En cuanto a la necesidad del tratamiento, debe estimarse que dicho requerimiento no implica que la actividad de procesamiento de datos deba revestir el carácter de «absolutamente esencial» para satisfacer un determinado interés, sino que ésta tiene que ser más que simplemente útil y más que una mera práctica habitual: debe consistir en una herramienta proporcional, dirigida de manera especial a alcanzar una finalidad específica. Por consiguiente, esta base de licitud no podría ser invocada si existe otra forma menos intrusiva para alcanzar la misma finalidad, o que implique el tratamiento de una menor cantidad de datos personales.²²

20. A su vez, el Reglamento contiene una definición de «tercero» en su artículo 4, numeral 10: «Persona física o jurídica, autoridad pública, servicio u organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable o del encargado».

21. Establece el Reglamento que «corresponde al legislador establecer por ley la base jurídica para el tratamiento de datos personales por parte de las autoridades públicas» (considerando 47). Debe tenerse presente que el artículo 7 letra f) de la Directiva 95/46/CE no hacía ninguna distinción respecto de la naturaleza privada o pública del responsable del tratamiento.

22. «Lawful basis for processing», Oficina del Comisionado de Información del Reino Unido, disponible en <http://bit.ly/2WDITLC>.

Por otra parte, el mismo Reglamento contempla, en su considerando 47 y a título ejemplar, situaciones en las que puede concurrir el interés legítimo del responsable del tratamiento:

Tal interés legítimo podría darse, por ejemplo, cuando existe una relación pertinente y apropiada entre el interesado y el responsable, como en situaciones en las que el interesado es cliente o está al servicio del responsable. En cualquier caso, la existencia de un interés legítimo requeriría una evaluación meticulosa, inclusive si un interesado puede prever de forma razonable, en el momento y en el contexto de la recogida de datos personales, que pueda producirse el tratamiento con tal fin. En particular, los intereses y los derechos fundamentales del interesado podrían prevalecer sobre los intereses del responsable del tratamiento cuando se proceda al tratamiento de los datos personales en circunstancias en las que el interesado no espere razonablemente que se realice un tratamiento ulterior. Dado que corresponde al legislador establecer por ley la base jurídica para el tratamiento de datos personales por parte de las autoridades públicas, esta base jurídica no debe aplicarse al tratamiento efectuado por las autoridades públicas en el ejercicio de sus funciones. El tratamiento de datos de carácter personal estrictamente necesario para la prevención del fraude constituye también un interés legítimo del responsable del tratamiento de que se trate. El tratamiento de datos personales con fines de mercadotecnia directa puede considerarse realizado por interés legítimo.²³

23. Respecto de la finalidad específica de la mercadotecnia directa, el Reglamento establece la posibilidad que implique la existencia de un interés legítimo del responsable, lo que puede no verificarse en todos los casos, por lo que sería necesario acudir a las legislaciones sectoriales o códigos de conductas internos de los Estados miembros para conocer sus alcances, esto es, en qué situaciones y bajo qué condiciones constituirá una base de licitud para el tratamiento de datos. En el caso de España, resulta esclarecedor el Informe Jurídico 195/2017 de la Agencia Española de Protección de Datos (AEPD), en el que se analizan, entre otras materias, la adecuada aplicación del considerando 47 del Reglamento. Este informe viene a dar aplicación práctica al considerando 47 recurriendo a su normativa doméstica, en concreto, la Ley 34/2002, de Servicios de la sociedad de la información y de comercio electrónico, que constituye una norma especial en relación con las comunicaciones que se lleven a cabo a través de medios electrónicos. El artículo 21 de la referida Ley prohíbe el envío de comunicaciones publicitarias o promocionales por correo electrónico u otro medio de comunicación electrónica equivalente que previamente no hubieran sido solicitadas o expresamente autorizadas por los destinatarios de las mismas, salvo que exista una relación contractual previa, siempre que el prestador hubiera obtenido de forma lícita los datos de contacto del destinatario y los empleara para el envío de comunicaciones comerciales referentes a productos o servicios de su propia empresa que sean similares a los que inicialmente fueron objeto de contratación con el cliente. Adicionalmente, la Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales, dispone en su artículo 23, numeral 4, que «quienes pretendan realizar comunicaciones de mercadotecnia directa, deberán previamente consultar los sistemas de exclusión publicitaria que pudieran afectar a su actuación, excluyendo del tratamiento los datos de los afectados que hubieran manifestado su oposición o negativa al mismo. A estos efectos, para considerar cumplida la obligación anterior será suficiente la consulta de los sistemas de exclusión incluidos en la relación publicada por la autoridad de control competente».

Asimismo, los considerandos 48 y 49 explican alcances adicionales del concepto de interés legítimo. Señala el considerando 48:

Los responsables que forman parte de un grupo empresarial o de entidades afiliadas a un organismo central pueden tener un interés legítimo en transmitir datos personales dentro del grupo empresarial para fines administrativos internos, incluido el tratamiento de datos personales de clientes o empleados. Los principios generales aplicables a la transmisión de datos personales, dentro de un grupo empresarial, a una empresa situada en un país tercero no se ven afectados.

El considerando 49, por su parte, indica que constituye un interés legítimo del responsable «el tratamiento de datos personales en la medida estrictamente necesaria y proporcionada para garantizar la seguridad de la red y de la información».

A partir de lo dispuesto tanto en el artículo 6, apartado 1, letra f) del Reglamento, como en los considerandos transcritos, se puede establecer que la evaluación para determinar la existencia de un interés legítimo que sirva de fuente de licitud para el tratamiento de datos personales constituye una «evaluación meticulosa» —especialmente respecto de la información personal de niños— que debe tener presente un nuevo factor no contemplado en la Directiva 95/46/CE: las expectativas razonables del titular de datos, basadas principalmente en su relación con el responsable del tratamiento.²⁴ Así, en aquellos casos en que el titular no espera razonablemente que se haga un tratamiento ulterior, podría entenderse que prevalece su interés.

En vista a lo anterior, la aplicación de este concepto conlleva a los responsables del tratamiento la necesidad de llevar a cabo una evaluación respecto de las perspectivas del titular de datos y su predictibilidad, la que deberá tener lugar al momento y en el contexto dentro del cual se verifica la recolección de sus datos, en vista a la consecución de finalidades concreta. Al sopesar esta expectativa razonable, cobrará especial relevancia la entrega al titular de los datos, por parte del responsable del tratamiento y de manera transparente, de información clara y oportuna acerca de las finalidades de la recopilación y tratamiento posterior de sus datos.

Por otro lado, en virtud a lo dispuesto en los artículos 13 y 14 del Reglamento, relativo a la obligación de información que recae sobre el responsable de la base de datos,²⁵ éste siempre deberá facilitar al titular de los mismos, cuando el procesamiento se base en el artículo 6, apartado 1, letra f), información sobre sus intereses legí-

24. Este criterio podría ser comparado con la doctrina de las expectativas razonables presente en otras áreas del derecho, como protección de los consumidores, derecho contractual y derecho de seguros (Kamara y De Hert, 2018: 16).

25. Los que emanan del principio de transparencia, contemplado en el artículo 5, apartado 1, letra a) del Reglamento.

timos o los de un tercero, que sirven como fundamento de dicho tratamiento.²⁶ Por consiguiente, el responsable debiese —más allá de solo indicar que el tratamiento de los datos se basa en el interés legítimo— estar siempre en condiciones de ilustrar sobre la existencia de un interés legítimo específico que lo habilite para operaciones concretas de tratamiento de datos personales.²⁷

Adicionalmente, a través de la aplicación del principio de responsabilidad, desarrollado en el artículo 24 del Reglamento, el responsable del tratamiento debe demostrar que el procesamiento de datos es conforme con el Reglamento, teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento. Asimismo, en virtud del deber de registro de las actividades de tratamiento, contemplado en el artículo 30, el responsable estaría sujeto a la obligación de documentar y demostrar la existencia de un interés legítimo que la habilite para el tratamiento de datos invocando el artículo 6, apartado 1, letra f).

Ahora, en caso de que se afecten los derechos o libertades del titular de datos, cabe preguntarse sobre la necesidad de acreditar la prevalencia del interés legítimo del responsable o de un tercero sobre los intereses o derechos y libertades fundamentales del titular de datos. Para resolver esto, debemos remitirnos a la norma que regula el derecho de oposición. Dispone el artículo 21, apartado 1 del Reglamento que cuando los datos personales sean objeto de un tratamiento basado en el interés legítimo, el titular tiene derecho a oponerse en cualquier momento al tratamiento, incluida la elaboración de perfiles, «por motivos relacionados con su situación particular». En este caso, el responsable del tratamiento deberá dejar de tratar estos datos, «salvo que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones».

Esto supone un cambio importante respecto de la regulación contemplada en la Directiva 95/46. La anterior norma europea reconocía en su artículo 14, letra a) el

26. Cabe señalar que, según dispone el considerando 60 del Reglamento, «los principios de tratamiento leal y transparente exigen que se informe al interesado de la existencia de la operación de tratamiento y sus fines. Los principios de tratamiento leal y transparente exigen que se informe al interesado de la existencia de la operación de tratamiento y sus fines. El responsable del tratamiento debe facilitar al interesado cuanta información complementaria sea necesaria para garantizar un tratamiento leal y transparente, habida cuenta de las circunstancias y del contexto específicos en que se traten los datos personales». Agrega el considerando 61 que «se debe facilitar a los interesados la información sobre el tratamiento de sus datos personales en el momento en que se obtengan de ellos o, si se obtienen de otra fuente, en un plazo razonable, dependiendo de las circunstancias del caso. Si los datos personales pueden ser comunicados legítimamente a otro destinatario, se debe informar al interesado en el momento en que se comunican al destinatario por primera vez».

27. Esto también supondría para el responsable del tratamiento la necesidad de acreditar que el tratamiento de datos en cuestión implica, como efecto directo, la satisfacción del interés legítimo invocado.

derecho de los titulares de datos a oponerse a aquellos tratamientos basados en un interés legítimo, en cualquier momento y por razones legítimas propias de su situación particular. No obstante, al señalar la referida disposición que la oposición debía ser «justificada», se entendía que ponía de cargo del titular de los datos la obligación de proporcionar justificación suficiente al ejercicio de este derecho. El artículo 21, apartado 1 vendría a alterar esta regla, ya que pone la carga probatoria en el lado del responsable del tratamiento, en cuanto a acreditar que su interés prevalece por sobre el interés del titular de los datos personales.²⁸

Cuando el tratamiento de datos personales tiene por objeto la mercadotecnia directa, la situación es distinta. El apartado 2 del referido artículo 21 establece en favor del titular un derecho absoluto a oponerse en todo momento al tratamiento de sus datos personales con dicha finalidad, incluida la elaboración de perfiles. De esta forma, la sola oposición del titular, y sin necesidad de que concurren otros requisitos, conlleva para el responsable la obligación de dejar de tratar dichos datos.

De igual manera, siempre que se verifique alguno de los supuestos del referido artículo 21, apartados 1 y 2, el titular tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan (artículo 17, apartado 1, letra c) y también derecho a obtener del responsable la limitación del tratamiento (artículo 18, apartado 1, letra d).²⁹

Respecto de la posibilidad de tratar bajo el fundamento del interés legítimo alguna de las categorías especiales de datos contempladas en el artículo 9 del Reglamento, esto es, aquéllos que

revelen el 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 la orientación sexual de una persona física

cabe señalar que el tratamiento de dichos datos está prohibido, salvo que se cumplan los requisitos especiales y específicos contemplados en el mismo artículo 9. Así,

28. A juicio del WP29, esta regla implica mejorar la obligación de rendición de cuentas (*accountability*) que recae sobre el responsable de la base de datos. Por lo demás, se estimaba que si el responsable del tratamiento no era capaz de demostrar al titular de los datos que, en un caso específico, prevalecía su interés, esto podía conllevar consecuencias más amplias en todas sus actividades de procesamiento de datos, en beneficio de todos los demás titulares de datos que puedan estar en una situación similar (Opinión 06/2014, página 52).

29. Respecto a otros derechos que asisten a los titulares de datos, cabe señalar que los tratamientos de información personales basados en el interés legítimo del responsable están excluidos del alcance de la portabilidad de datos (Ursic, 2018: 57).

el solo interés legítimo del responsable o de un tercero no constituyen fundamento jurídico suficiente para habilitar al tratamiento de estos datos especiales.³⁰

España

Ley Orgánica 15/1999

La Ley Orgánica 15/1999, del 13 de diciembre de 1999, de Protección de Datos de Carácter Personal, establecía en su artículo 6, apartado 1, que el tratamiento de datos personales requería el consentimiento inequívoco del afectado, salvo que la ley dispusiera otra cosa. No obstante lo anterior, el apartado 2 siguiente establecía que no era preciso dicho consentimiento cuando los datos se recojan para

el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado.³¹

En cuanto a la comunicación de datos personales objeto de tratamiento a un tercero, disponía el artículo 11, apartado 1, que ello solo era posible si el objetivo de dicha operación era «el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado». No obstante, el apartado 2 del referido artículo 11 establecía que dicho consentimiento no era preciso, entre otras causales, cuando se trataba de datos recogidos de fuentes accesibles al público (letra b).³²

30. Con todo, las fuentes de licitud contenidas en el artículo 6 y los requisitos especiales establecidos en el artículo 9 deben verificarse de manera conjunta. «When can we rely on legitimate interests?», Oficina del Comisionado de Información del Reino Unido, disponible en <http://bit.ly/2WDNp6N>.

31. Esto supondría una diferencia con la Directiva 95/46/CE, por cuanto mientras el artículo 7 de la Directiva sigue un sistema de lista de los principios que legitiman el tratamiento de datos, la normativa doméstica española articularía algunos de estos principios como excepción a la regla general del consentimiento del titular de datos (Rubí Navarrete, 2012: 14).

32. Con todo, respecto de los datos de carácter personal recogidos o elaborados por las Administraciones públicas para el desempeño de sus atribuciones, señalaba el artículo 21 de la Ley, en su apartado 3, que no obstante lo dispuesto en el artículo 11, apartado 2, letra b), éstos no podían ser comunicados a ficheros de titularidad privada sino con el consentimiento del interesado o cuando una ley prevea otra cosa.

Como puede apreciarse en el tenor literal de la normativa española, cualquier operación de tratamiento de datos personales —incluyendo su comunicación a terceros— sin que exista el consentimiento del titular e invocando la existencia de un interés legítimo exigía, además de la satisfacción del interés perseguido por el responsable del tratamiento o por el tercero al que se comuniquen los datos y el resguardo de los derechos y libertades fundamentales del titular, que dichos datos figuraran en fuentes accesibles al público.

Resulta importante precisar que la Ley, junto con definir en su artículo 3, letra j) las fuentes de acceso como «aquellos ficheros cuya consulta puede ser realizada, por cualquier persona, no impedida por una norma limitativa o sin más exigencia que, en su caso, el abono de una contraprestación», establecía un listado taxativo y cerrado de fuentes de acceso público sobre los cuales no se consideraba ninguna otra fuente. Éstas eran: el censo promocional; los repertorios telefónicos en los términos previstos por su normativa específica; las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo; y, finalmente, los diarios, boletines oficiales y los medios de comunicación.

Luego, el Reglamento de desarrollo de la Ley Orgánica de Protección de Datos, Real Decreto 1720/2007 del 21 de diciembre de 2007, vino a reproducir, en su artículo 10, las reglas de la Ley de Protección de Datos de Carácter Personal en lo que respecta a las bases de licitud para el tratamiento de datos. En este sentido, en su apartado 2, letra b) establecía, en términos similares al apartado 2 del artículo 6 de la Ley, que era posible el tratamiento o cesión de datos personales sin el consentimiento del titular cuando los datos en cuestión figuren en fuentes accesibles al público y el responsable del fichero o el tercero a quien se comuniquen tenga un interés legítimo para su tratamiento o conocimiento, sin que se vulneren los derechos y libertades fundamentales del titular de los datos.

Con todo, diversos autores entendieron que, a través de esta disposición, se había efectuado una transposición incorrecta de la Directiva 95/46/CE a las normas internas (Guasch Portas y Soler Fuensanta, 2015: 422). Dicha opinión se sustentaba en el hecho de que la Directiva, al regular el interés legítimo en su artículo 7, letra f), no exigía como requisito que los datos personales objeto de tratamiento se encontraran en fuentes accesibles al público.

Sobre esta base, la Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) y la Federación de Comercio Electrónico y Marketing Directo (FECEMED) interpusieron ante el Tribunal Supremo español recursos contenciosos administrativos contra la Administración General del Estado, solicitando declarar la nulidad de pleno derecho del referido Real Decreto y, subsidiariamente, declarar la nulidad, entre otras disposiciones, del artículo 10, apartado 2, letra b) del Real Decreto, por ser contrario al derecho comunitario europeo.

El Tribunal Supremo elevó una cuestión prejudicial al Tribunal de Justicia de la Unión Europea (caso *ASNEF y FECEMED con Administración del Estado*, asuntos acumulados C-468/10 y C-469/10) respecto de: la compatibilidad del derecho comunitario europeo con el hecho de que un Estado miembro aprueba o mantenga en vigor en sus disposiciones normativas nacionales obligaciones adicionales no contemplada en la Directiva 95/46/CE, que causen o supongan restricciones a la libre circulación de datos personales; y la compatibilidad del derecho comunitario con el hecho de que un Estado miembro establezca nuevas restricciones y requisitos adicionales a los supuestos que legitiman el tratamiento de datos personales establecidos en el artículo 7 de la Directiva 95/46/CE, o que el supuesto establecido en el artículo 7, letra f) de la Directiva no se configure como un principio para la legitimación del tratamiento de carácter autónomo, sino vinculado a la concurrencia de algún otro de los requisitos establecidos en el referido artículo 7.

La sentencia del Tribunal del 24 de noviembre de 2011, estableció que el artículo 7 de la Directiva 95/46/CE daba cuenta de una lista exhaustiva y taxativa de bases de licitud, de manera tal que los Estados miembros «no pueden ni añadir al artículo 7 de la Directiva 95/46 nuevos principios relativos a la legitimación de los tratamientos de datos personales ni imponer exigencias adicionales que vendrían a modificar el alcance de alguno de los seis principios establecidos en dicho artículo». Sobre esta base, el Tribunal concluyó que los Estados miembros no pueden introducir «principios relativos a la legitimación de los tratamientos de datos personales distintos a los enunciados en el artículo 7 de esa Directiva ni modificar, mediante exigencias adicionales, el alcance de los seis principios establecidos en dicho artículo 7». De tal manera, la Directiva 95/46 se oponía a toda normativa nacional que imponga exigencias adicionales que se sumen a los dos requisitos acumulativos mencionados en la letra f) de su artículo 7 (satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero y que no prevalezcan los derechos y libertades fundamentales del titular de datos).

Sobre si el artículo 7, letra f) de la Directiva 95/46/CE tenía efecto directo, el Tribunal señaló que dicha norma «es una disposición suficientemente precisa para poder ser invocada por un particular y aplicada por los órganos jurisdiccionales nacionales», de manera tal que «tiene efecto directo».³³

Con esta respuesta del Tribunal de Justicia de la Unión Europea, el Tribunal Supremo español dictó sentencia el 8 de febrero de 2012, en la que declaró la nulidad del artículo 10, apartado 2, letra b) del Real Decreto 1720/2007, por ser contrario a lo

33. Asimismo, respecto a la prueba de balance del interés legítimo, se dispuso que ésta dependía, en principio, de las circunstancias individuales de cada caso concreto, tomando en consideración los derechos contenidos en los artículos 7 (respeto de la vida privada y familiar) y 8 (protección de datos de carácter personal) de la Carta de los Derechos Fundamentales de la Unión Europea.

dispuesto en la Directiva 95/46/CE.³⁴ Esta anulación, junto con el efecto directo del artículo 7, letra f) de la Directiva, produjo un efecto de desplazamiento de las referencias a las fuentes accesibles al público en el tratamiento de datos personales basados en el interés legítimo. Si bien las fuentes accesibles al público siguieron existiendo como categoría jurídica, ya no pudieron ser consideradas *per se* como legitimadoras del tratamiento de datos. Con todo, respecto de aquellos datos que figuren en fuentes accesibles al público, podía entenderse que concurría un menor riesgo de lesión al titular, de manera tal que la ponderación podía inclinarse en favor del interés legítimo del interesado (Rubí Navarrete, 2012: 16).

Ley Orgánica 3/2018

Si bien las disposiciones del Reglamento son directamente aplicables en todos los Estados miembros de la Unión Europea, sin necesidad de normas internas de transposición, esto no excluye la posibilidad de intervención del derecho interno en las materias que abarca el Reglamento. A este respecto, el propio Reglamento, en su considerando 8, establece que «en los casos en que el presente Reglamento establece que sus normas sean especificadas o restringidas por el derecho de los Estados miembros, éstos, en la medida en que sea necesario por razones de coherencia y para que las disposiciones nacionales sean comprensibles para sus destinatarios, pueden incorporar a su derecho nacional elementos del presente Reglamento».

Así, en diciembre de 2018 entró en vigencia la Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales, la que deroga la Ley Orgánica 15/1999, adaptando la normativa española al Reglamento.³⁵

Respecto de la institución del interés legítimo, resulta relevante destacar que el título 4 de la Ley Orgánica 3/2018 establece una presunción, simplemente legal, de prevalencia del interés legítimo del responsable de bases de datos, respecto de las siguientes operaciones: el tratamiento de los datos de contacto y en su caso los relativos a la función o puesto desempeñado de las personas físicas que presten servicios en una persona jurídica; tratamiento de los datos relativos a los empresarios individuales y a los profesionales liberales; el tratamiento de datos personales relativos al

34. En la tramitación del contencioso administrativo se solicitó igualmente al Tribunal Supremo declarar la nulidad del artículo 6, apartado 2 de la Ley de Protección de Datos de Carácter Personal, por ser igualmente contraria a la Directiva (el artículo 10 apartado 2 letra b del Real Decreto 1720/2007 constituye casi una transposición del artículo 6, apartado 2, de la Ley), lo que fue rechazado por dicho tribunal, por carecer de atribuciones para anular normas de rango legal (Guasch Portas y Soler Fuentas, 2015: 424).

35. Entre otros aspectos relevantes, la Ley Orgánica 3/2018 contiene disposiciones específicas en materia de garantía de los derechos digitales (título 10), incluyendo, entre otros derechos, la neutralidad de internet, el acceso universal a internet, la seguridad digital y el testamento digital.

incumplimiento de obligaciones dinerarias, financieras o de crédito por sistemas comunes de información crediticia; y los tratamientos de datos que pudieran derivarse del desarrollo de cualquier operación de modificación estructural de sociedades o la aportación o transmisión de negocio o de rama de actividad empresarial.

En este sentido, el referido título 4 contempla una serie de requisitos que deben cumplir estas operaciones de tratamiento de datos para estar amparadas por esta presunción. Si bien el cumplimiento de dichos requisitos permite simplificar la verificación y ponderación del interés legítimo del responsable de la base de datos, se debe tener presente que esta presunción de licitud admite prueba en contrario, respecto de la falta de cumplimiento de cualquiera de los elementos establecidos en el artículo 6, apartado 1, letra f) del Reglamento. Por tanto, en la práctica, esta presunción implicaría alterar la carga probatoria respecto de la existencia o no del interés legítimo, que, según establece el Reglamento, recae sobre el responsable del tratamiento de datos.

El interés legítimo en Chile

Regulación general en la Ley de Protección de la Vida Privada

Tal como hemos afirmado, la actual Ley de Protección de la Vida Privada carece de una regla que habilite el tratamiento de datos personales en virtud de los intereses legítimos del responsable. Se debe tener presente que si bien originalmente el proyecto que culminaría en la Ley 19.628 estaba basado en normas sobre informática y protección de datos de países como Francia, Reino Unido y Noruega, durante la tramitación posterior fue cobrando relevancia la Ley Orgánica 5/1992 de Regulación del Tratamiento Automatizado de los Datos de carácter personal, adoptada por España en 1992 y que fuera expresamente derogada por la Ley Orgánica 15/1999, poco tiempo después de la entrada en vigencia de la norma chilena (Cerdea, 2012: 14). Pues bien, la Ley Orgánica 5/1992 restringía, en su artículo 6, las bases de licitud para el tratamiento de datos personales al consentimiento del titular y la habilitación legal.³⁶

Pese a ello, vale la pena revisar los escasos antecedentes de la historia de la Ley

36. La norma del consentimiento procedía de la primera propuesta de Directiva comunitaria de protección de datos, la que se seguía en gran medida en la ley alemana de 1990, basada a su vez en la sentencia del Tribunal Constitucional Federal alemán de 1983 (Herederer Higuera, 1998: 471), recaída en el recurso contra la Ley del Censo de Población de 1982, que recogía la expresión «derecho de autodeterminación informativa». Con todo, se exceptuaba el requerimiento del consentimiento del titular «cuando los datos de carácter personal se recojan de fuentes accesibles al público, cuando se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias, ni cuando se refieran a personas vinculadas por una relación comercial, una relación laboral, una relación administrativa o un contrato y sean necesarios para el mantenimiento de las relaciones o para el cumplimiento del contrato» (artículo 6, numeral 2).

19.628 referidos al interés legítimo, puesto que éstos evidencian que se trató de una fuente de legitimidad que estuvo en discusión hasta el último minuto.

La moción parlamentaria de 1993, que originó la Ley, carecía de toda referencia al interés legítimo.³⁷ Se trataba de un proyecto de ley que buscaba regular genéricamente la protección de la vida privada, pero que luego mutó a una ley de protección de datos personales (Anguita, 2007: 234-235). Si bien el proyecto tenía un título sobre protección de datos, en el primer trámite legislativo sólo se dio una discusión genérica referida a esta materia, puesto que se enmarcaba en un debate más amplio que alcanzaba diversas intromisiones al derecho a la vida privada.

Será en segundo trámite constitucional, en la Cámara de Diputados, que se adoptará un giro radical y el proyecto se acotará exclusivamente a la protección de datos personales (Anguita, 2007: 253). En la discusión en particular, se introdujeron al proyecto dos nuevos artículos, en los que se establecía una regla de finalidad del tratamiento de datos y se permitía, como excepción, un tratamiento diverso a la finalidad de su recolección cuando «provengan o se hayan recogido de fuentes accesibles al público o que a su respecto exista un interés legítimo y así se acredite».³⁸ Sin embargo, no hubo discusión de por qué incorporar tal excepción o cuál debería ser el contenido de la misma. En otros términos, se incluía el interés legítimo, pero no se daba cuenta o explicación respecto del concepto ni su alcance. Por lo tanto, sin mayor deliberación al respecto, la adición fue aprobada en particular tanto en la Comisión como en la Sala.³⁹

Es en el tercer trámite en que se discute sobre el alcance de la disposición referida al interés legítimo. En efecto, de acuerdo con el informe que consta en la historia de la ley, la Comisión

creyó pertinente limitar la utilización de los datos personales a los fines para los cuales hubieran sido recolectados, con la única excepción de que se trate de datos provenientes de fuentes accesibles al público. No encontró justificada la otra excepción que planteaba la norma, relativa a acreditar un interés legítimo, ya que constituye una exigencia de difícil determinación, que perfectamente puede ser satisfecha por alguno de los medios que contemplará el precepto: los fines de la recolección de los datos o el hecho de tratarse de una fuente accesible al público.⁴⁰

Para la Comisión, la ausencia de mayor precisión en el contenido y alcance del concepto de interés legítimo hacía razonable prescindir de este concepto. Es lamen-

37. Biblioteca del Congreso Nacional de Chile, «Historia de la Ley 19.628», pp. 3-10, disponible en <http://bit.ly/2WyRTvz>.

38. «Historia de la ley», p. 134.

39. «Historia de la ley», pp. 141 y 172.

40. «Historia de la ley», p. 218.

table que no haya existido al menos una referencia al derecho comparado en este punto. En efecto, el informe data de 1998 y ya estaba en vigor la Directiva 95/46/CE, tratada más arriba, por lo que era posible acceder a antecedentes sobre el interés legítimo a efectos de discutir su incorporación o exclusión.

En el tercer trámite, la Cámara de origen rechazó las enmiendas al proyecto y forzó la creación de una comisión mixta. Ahí se sellará la eliminación del interés legítimo en el proyecto de ley. La comisión mixta tomó como texto base la versión discutida en tercer trámite por el Senado (Anguita, 2007: 277), por lo que el proyecto ya tenía suprimido el interés legítimo como excepción al principio de finalidad. El informe de la comisión mixta reiteró la eliminación del interés legítimo y mantuvo solamente las fuentes accesibles al público como excepción a la regla general de que los datos personales sólo deben utilizarse para los fines para los cuales hubieran sido recolectados.⁴¹ La razón fue la misma: el interés legítimo «constituía una exigencia de difícil determinación».⁴² La comisión mixta aprobó de forma unánime la disposición y se consolidó el texto del actual artículo 9 de la Ley 19.628. Estos escasos antecedentes explican la omisión del interés legítimo en nuestra Ley de Protección de la Vida Privada.⁴³

Ley General de Bancos

Fuera del ámbito de la Ley de Protección de la Vida Privada, pero dentro del corpus normativo que regula las actividades de tratamiento de datos personales específicos, existe un reconocimiento de la institución del interés legítimo de un tercero como base habilitante para la comunicación de cierto tipo de información de carácter personal, de naturaleza bancaria.

41. «Historia de la ley», pp. 248-249.

42. «Historia de la ley», p. 249.

43. Por otra parte, a propósito del ejercicio por los titulares de datos del derecho a acceso, se planteó, siguiendo a la Ley Orgánica 5/1992 española, la posibilidad de establecer que el derecho a acceso sólo pudiera ser ejercido a intervalos no inferiores a doce meses, salvo que se acredite un interés legítimo al efecto, en cuyo caso podría ejercerse antes de que se cumpliera dicho plazo (Boletín 896-07, Primer Informe de Comisión de Constitución Legislación y Justicia de la Cámara de Diputados, recaído en el proyecto de ley sobre protección de la vida privada). Por otra parte, durante la tramitación de este proyecto se discutió sobre el interés legítimo a propósito del derecho a cancelación, contemplándose que no fuera posible su ejercicio cuando pudiese causar un perjuicio a intereses legítimos del afectado o de terceros (Boletín 896-07, Discusión en sala del Segundo Informe de Comisión de Constitución Legislación y Justicia de la Cámara de Diputados, recaído en el proyecto de ley sobre protección de la vida privada). Con todo, en ambos casos, el concepto de interés legítimo empleado debe ser diferenciado de aquel que constituye el objeto principal de este estudio, ya que no se trata de un «interés legítimo» como base jurídica habilitante para el tratamiento de datos personales, sino que se trató de técnicas jurídicas para acotar el derecho de acceso y el de cancelación.

Se debe tener presente que las disposiciones de la Ley de Protección de la Vida Privada —incluidas, desde luego, sus fuentes de licitud para el tratamiento— son aplicables, en términos generales, al procesamiento de toda clase de datos personales, esto es, cualquier información concerniente a personas naturales, identificadas o identificables. Quedan comprendidos aquí, por cierto, los datos personales de carácter patrimonial, económico, financiero, bancario o comercial, sean estos negativos —que dan cuenta de la existencia de alguna obligación o deuda (Jervis Ortiz, 2005: 125) y su eventual incumplimiento o cumplimiento incompleto— o positivos —relativos, en sentido amplio, a antecedentes que dan cuenta de la composición del patrimonio de una persona (Jijena, 2001: 84), como por ejemplo, sus bienes, depósitos, ahorros, ganancias, inversiones y demás acreencias que le pertenezcan.

Respecto del tratamiento de datos patrimoniales positivos, resultan plenamente aplicables las reglas generales contempladas en el título 1 de la Ley de Protección de la Vida Privada, de manera tal que su procesamiento podrá efectuarse cuando el titular de los mismos consienta expresamente en ello, exista una autorización legal o se extraigan de fuentes accesibles al público. En cuanto al procesamiento de datos patrimoniales negativos, si bien también son aplicables las normas contenidas en el referido título 1, la Ley dispone en su título 3 un conjunto de requisitos adicionales aplicables a ciertos actos específicos de tratamiento, esto es, su comunicación a terceros.

Según establece el artículo 17 de la Ley, el responsable del tratamiento sólo podrá comunicar a terceros información relativa a obligaciones de carácter económico, financiero, bancario o comercial siempre y cuando se verifique alguno de los siguientes casos calificados: que consten en letras de cambio y pagarés protestados; que consten en cheques protestados por falta de fondos, por haber sido girados contra cuenta corriente cerrada o por otra causa; y que digan relación con el incumplimiento de obligaciones derivadas de mutuos hipotecarios y de préstamos o créditos de bancos, sociedades financieras, administradoras de mutuos hipotecarios, cooperativas de ahorros y créditos, organismos públicos y empresas del Estado sometidas a la legislación común, y de sociedades administradoras de créditos otorgados para compras en casas comerciales. De igual manera, pueden comunicarse otras obligaciones de dinero que determine el presidente de la República mediante decreto supremo, las que deberán estar sustentadas en instrumentos de pago o de crédito válidamente emitidos, en los cuales conste el consentimiento expreso del deudor u obligado al pago y su fecha de vencimiento.⁴⁴ Fuera de esta categoría específica de datos, que

44. Con todo, dispone el artículo 17 de la Ley, en su inciso segundo, que «no podrá comunicarse la información relacionada con las deudas contraídas con empresas públicas o privadas que proporcionen servicios de electricidad, agua, teléfono y gas; tampoco podrán comunicarse las deudas contraídas con concesionarios de autopistas por el uso de su infraestructura».

puede ser denominada como «datos patrimoniales negativos comunicables» (Jervis Ortiz, 2005: 130), no será posible la comunicación de datos negativos a terceros.

Adicionalmente, en virtud a lo dispuesto en el artículo 1 de la Ley 20.575, que Establece el Principio de Finalidad en el Tratamiento de Datos Personales, la comunicación de estos «datos patrimoniales negativos comunicables» sólo podrá ser dirigida al comercio establecido y a las entidades que participen de la evaluación del riesgo comercial, con la sola finalidad de evaluación de riesgo comercial y para proceso de crédito.

Pues bien, la Ley General de Bancos contemplaría una base de licitud distinta del consentimiento del titular de los datos o de la autorización legal —entendida en sentido estricto y no como reconducción—, para efectuar, respecto de cierta clase de datos patrimoniales, una determinada actividad de tratamiento (su comunicación a terceros). En concreto, la Ley, ya desde el año 1986, en su actual artículo 154, que regula el secreto y la reserva bancaria, dispone en su inciso primero que

las operaciones de depósitos y captaciones de cualquier naturaleza que reciban los bancos en virtud de la presente Ley estarán sujetas a secreto bancario y no podrán proporcionarse antecedentes relativos a dichas operaciones sino a su titular o a quien haya sido expresamente autorizado por él o a la persona que lo represente legalmente. El que infringiere la norma anterior será sancionado con la pena de reclusión menor en sus grados mínimo a medio.

A continuación, el inciso segundo de la citada norma agrega:

Las demás operaciones quedarán sujetas a reserva y los bancos en virtud de la presente Ley solamente podrán darlas a conocer a quien demuestre un interés legítimo y siempre que no sea previsible que el conocimiento de los antecedentes pueda ocasionar un daño patrimonial al cliente.

Del tenor literal del artículo 154, inciso segundo puede establecerse que respecto de operaciones amparadas por la reserva bancaria, esto es, distintas de los depósitos y captaciones recibidas por los bancos —sujetas al más estricto «secreto bancario»— y que, ciertamente, en vista a su amplitud, pueden tener aparejadas información de índole patrimonial concerniente a clientes personas naturales, se habilita a las entidades financieras a darlas a conocer o comunicarlas a terceros que «demuestren» un interés legítimo en ello, siempre y cuando no sea «previsible» que la comunicación de dichos antecedentes pueda ocasionar un «daño patrimonial» al cliente.

Concebida en estos términos, la referida regla importaría una verdadera excepción a las normas generales contempladas en la Ley de Protección de la Vida Privada respecto de los requisitos de licitud para el tratamiento de datos personales patrimoniales, cuyo alcance se extendería, en principio y al no hacer distinciones, tanto a

datos patrimoniales positivos como negativos. Con todo, la posibilidad de invocar⁴⁵ la existencia de un interés legítimo como base habilitante para ciertas operaciones de tratamiento de datos patrimoniales negativos, no obsta la necesidad dar estricto cumplimiento a los requisitos especiales aplicables a la comunicación de información sobre obligaciones de carácter económico, financiero, bancario o comercial, contempladas tanto en el título 3 de la Ley de Protección de la Vida Privada como en la Ley 20.575, atendida la especificidad y especialidad de dichas restricciones.

Para entender de mejor manera las implicancias de la institución del interés legítimo en la legislación bancaria, resulta de valor considerar la sentencia de la Corte Suprema a recurso de casación en el fondo, rol 8038-2011, del 25 de marzo de 2013, sobre juicio ordinario de nulidad de derecho público de la Resolución exenta 120/04, del 20 de diciembre de 2004, emitida por el Servicio de Impuestos Internos (SII). La sentencia objeto de casación, dictada por la Corte de Apelaciones de Santiago, había declarado la nulidad del referido acto administrativo, en el que se establecía que bancos e instituciones financieras debían informar al SII diversas operaciones que llevaran a cabo por encargo de terceros, que implicaran, fundamentalmente, la disposición de fondos en el exterior. La sentencia recurrida determinó que el SII habría excedido su competencia, vulnerando el secreto bancario establecido en la Ley General de Bancos.

La Corte Suprema, en la resolución del recurso de casación, y a propósito de la determinación de si el SII cumplía con los requisitos de autorización que permitían exceptuar la aplicación de la reserva bancaria, vino a fijar ciertos criterios en relación con los alcances del interés legítimo contenido en el inciso segundo del artículo 154 de la Ley General de Bancos, especialmente en cuanto a su existencia y la posibilidad de ocasionar un daño patrimonial al cliente del banco. Señaló la Corte, en el considerando 7 de la respectiva sentencia de reemplazo, que

es ineludible concluir que el Servicio de Impuestos Internos tiene un interés legítimo porque fluye directamente de sus facultades, y que dicho interés no es necesario acreditarlo cuando —como acontece en el caso *sub lite*— la información pretendida no está asociada a contribuyentes específicos. En esta última hipótesis resulta claro que el Servicio deba exponer circunstanciadamente las razones de su requerimiento.

Luego, en el considerando 11 de la sentencia se sostiene que la información requerida por el SII a través del acto administrativo impugnado

se halla sujeta a reserva bancaria en atención a su contenido, y que respecto de su conocimiento el órgano fiscalizador posee un legítimo interés, sin que pueda llegar a ocasionar daño patrimonial al titular de la información, todo lo cual conduce a reconocer la validez del referido acto administrativo.

45. Al amparo del artículo 154, inciso segundo, de la Ley General de Bancos.

A juicio de José Francisco García, la fundamentación de la Corte Suprema «fue exigua, en particular respecto del desarrollo del estándar de «interés legítimo», confirmando la tendencia en esta materia: la Corte Suprema no ha sido capaz de construir en su jurisprudencia uno que entregue claridad y certeza».⁴⁶

Teniendo presente este criterio de la Corte, resulta relevante analizar proyecto de ley que dio origen la Ley 21.130, que moderniza la legislación bancaria (Boletín 11.269-05), el que, entre otras disposiciones, buscaba modificar el artículo 154 de la Ley General de Bancos, precisando el objeto de secreto o reserva bancaria. El mensaje del proyecto, ingresado a la Cámara de Diputados en junio de 2017, tenía por objeto, entre otros aspectos, ratificar el interés legítimo para conocer información sujeta a reserva bancaria. Para ello, el proyecto original pretendía establecer en el texto de la Ley la presunción que los fiscales del Ministerio Público, el SII y la Unidad de Análisis Financiero tenían interés legítimo para conocer operaciones sujetas a reserva bancaria, y que no resultaba previsible el daño patrimonial al cliente titular de la información en cuestión.

Así, el título 2, numeral 4, letra d) del mensaje indicaba que,

con el objeto de situar el correcto alcance de la información sujeta a secreto y reserva bancaria, respectivamente, frente a las funciones fiscalizadoras del Servicio de Impuestos Internos, de control de la Unidad de Análisis Financiero y de dirigir las investigaciones de hechos constitutivos de delito por parte del Ministerio Público, se propone consagrar lo ya resuelto por la Corte Suprema sobre el interés legítimo que dichas instituciones tienen, en el ejercicio de sus atribuciones, para acceder a la información sujeta a reserva bancaria».

Agregaba el mensaje que «particularmente en el caso del Servicio de Impuestos Internos, el año 2013 el máximo tribunal de la República esclareció que dicho Servicio tiene un interés legítimo para conocer la información sujeta a reserva bancaria, interés que fluye directamente de sus atribuciones». Esta referencia debe entenderse hecha a la sentencia de reemplazo en la causa rol 8038-2011, del 25 de marzo de 2013.

No obstante lo anterior, el informe evacuado por la Corte Suprema durante la tramitación del referido proyecto de ley vino a refutar la interpretación plasmada por el presidente de la República en su mensaje. En el decimocuarto considerando de su informe, la Corte sostiene que,

respecto al basamento de esa aceptación del interés legítimo del Servicio de Impuestos Internos y de la Unidad de Análisis Financiero para conocer las operaciones amparadas por reserva, es importante aclarar lo verdaderamente expresado por esta Corte Suprema en la causa rol 8038-2011, pues no es exacto a aquello que parece

46. José Francisco García, «Corte Suprema, reserva bancaria e interés legítimo», Legal, *El Mercurio*, 19 de abril de 2013, disponible en <http://bit.ly/2WzhSTD>.

extraer de sus motivaciones el legislador del proyecto. [...] no es exacto desprender que en esta sentencia en autos rol 8038-2011 la Corte Suprema reconociera una presunción de interés legítimo del Servicio de Impuestos Internos para interferir en la reserva bancaria, puesto que, partiendo de la base que aquél debe probarse, señaló que en el caso *sub lite* dicha prueba no era indispensable en atención a que no se afectaba a contribuyentes determinados. De ahí que llegar a concluir que se reconoció una presunción general del interés legítimo del organismo en mención se aparta de la fundamentación de la sentencia que viene referida en el proyecto de ley que se revisa.

Agrega el decimoquinto considerando del referido informe:

A la luz de lo anterior y teniendo presente que las medidas invasivas de la privacidad de los ciudadanos requieren de una especial atención, parece cuestionable la iniciativa en cuanto presume el interés legítimo del Servicio de Impuestos Internos y de la Unidad de Análisis Financiero para interferir en la esfera de reserva, del mismo modo que lo hace en relación a no resultar previsible el daño patrimonial al cliente. Ambas circunstancias necesariamente debieran ser materia de prueba y de la resolución de la judicatura competente. De otra manera, se dejaría a la institucionalidad constituida por el Servicio de Impuestos Internos y la Unidad de Análisis Financiero en una situación de privilegio absoluto y, como contrapartida de ello, en una situación de indefensión al ciudadano.

Sobre la base de lo anteriormente expuesto, es posible establecer que la excepción al deber de reserva bancaria, contemplada en el inciso segundo del artículo 154 de la Ley General de Bancos, opera, simultáneamente, como una base jurídica de licitud para un tipo especial de tratamiento de datos —esto es, la comunicación de ciertos datos personales patrimoniales por parte del responsable de la respectiva base datos (el banco) a un tercero interesado—, sujeta a los siguientes supuestos:

- Los antecedentes o datos personales en cuestión deben estar relacionados con operaciones distintas de los depósitos y captaciones que los bancos reciban,⁴⁷ circunscribiéndose a aquella información que resulta inherente a estas operaciones bancarias.
- El tercero a quien se darán a conocer estos antecedentes debiese demostrar, previo a su comunicación, la existencia de un interés legítimo específico, esto es, que el hecho de conocer esta información permitirá satisfacer un interés de

47. El capítulo 2.1 de la Recopilación Actualizada de Normas de la Superintendencia de Bancos e Instituciones Financieras, señala en su numeral 1 que el concepto de captación «tiene en la legislación vigente una acepción amplia, de manera que cubre todas las operaciones, a la vista o a plazo, que involucran recibir dinero del público, sea como depósito, mutuo, participación, cesión o transferencia de efectos de comercio o en cualquiera otra forma».

relevancia jurídica, sea éste de carácter público o privado. En principio, puede entenderse que el beneficio que le reportará dicha comunicación no se restringe únicamente a una utilidad de tipo patrimonial.

- El banco responsable del tratamiento debe efectuar una evaluación respecto de la potencial afectación que pueda sufrir el cliente titular de datos, como consecuencia de la comunicación de sus antecedentes personales a terceros. Si bien dicha afectación se limita únicamente a daños de tipo patrimonial, y no moral, la posibilidad que como consecuencia de la comunicación pueda surgir este daño, por menor que sea, impediría darla a conocer, sin que fuese necesario recurrir a una ponderación o prueba de balance entre los derechos del titular de datos y el interesado.

Conclusiones

En nuestro país, el principio de licitud para el tratamiento de datos personales se estructura bajo un sistema binario de consentimiento o autorización legal, el que no está exento de problemas. En el derecho comparado, el sistema de títulos habilitantes para el tratamiento de datos personales es más complejo y ha integrado, a su vez, el interés legítimo del responsable como base legitimadora para el tratamiento de datos. El desarrollo de este concepto se ha dado, principalmente, a través de las interpretaciones del WP29, de Directiva 95/46/CE, de la jurisprudencia del Tribunal de Justicia de la Unión Europea y del Reglamento General de Protección de Datos. Este corpus es esencial para entender el alcance del interés legítimo. Adicionalmente, la experiencia española muestra la iteración dialógica entre la legislación nacional y la operación de los órganos de la Unión Europea, a efectos de aplicar el interés legítimo en un Estado nacional específico. Además, la legislación española ha sido particularmente influyente en nuestra propia regulación de datos personales, por lo que es citada constantemente como referente del derecho comparado.

La revisión que hemos efectuado permite decantar ciertos componentes básicos del interés legítimo. En primer lugar, es un título habilitante que permite superar el esquema de consentimiento/autorización legal, pero que impone ciertas cargas en el responsable. El interés legítimo debe ser claro, determinado, específico y su satisfacción es consecuencia directa del tratamiento (en términos de necesidad). El responsable que esgrime un interés legítimo debe demostrar y establecer los supuestos a partir de los cuales surge o se funda. En definitiva, debe acreditar que es una conducta autorizada por el derecho. En este punto, debe destacarse que no basta con un mero o un simple interés. Más bien, debe tratarse de un interés propio, real, actual, específico, directo, o que reporta una utilidad real, aun cuando el beneficio no sea inmediato.

Al eximir del consentimiento del titular, se exige que se efectúe un examen de ponderación a efectos de velar por los derechos del sujeto de datos. Del tratamiento se pueden derivar externalidades negativas que infligen perjuicio al titular. En este caso, puede darse técnicamente una «afectación». ¿En qué consiste la afectación? Es un agravio a los derechos e intereses del titular de datos, que bien podría ser traducido como una privación, perturbación o amenaza a sus intereses o al legítimo ejercicio de sus derechos. El examen de ponderación deberá incorporar una evaluación del beneficio real y directo por parte del responsable y una comparación con los intereses o derechos del titular, en sentido amplio y que puede ser de distinta índole: intimidad, económico, comercial, profesional, bienestar psicosocial u otro. En materia de prueba, el responsable del tratamiento siempre tiene que, a lo menos, probar la existencia del interés legítimo. Si no se logra acreditar, entonces estaríamos ante un interés simple que no legitima el tratamiento de datos personales, con la consiguiente responsabilidad infraccional y civil que pudiere acarrear para quien trató ilegítimamente el dato.

Tras un examen de proporcionalidad —que considera tanto los intereses de los responsables del tratamiento como los derechos del titular de los datos—, esta hipótesis permitiría nuevos usos para los datos, los que resultarían esenciales en tiempos de *big data*, inteligencia artificial, aprendizaje automático y modelos de negocios innovadores basados en el procesamiento de información.

En nuestro país, la Ley de Protección de la Vida Privada no reconoce el interés legítimo como base habilitante para el tratamiento de datos personales, salvo en materia de legislación bancaria, respecto de operaciones de tratamiento acotadas. A partir de los alcances definidos en este artículo, es posible evaluar críticamente la labor legislativa que está estudiando la inclusión del interés legítimo como base de licitud de tratamiento de datos. El proyecto en tramitación pretende superar el esquema vigente de legitimación del tratamiento de datos, de carácter binario.⁴⁸ Su inclusión a nivel general requiere un examen crítico que dé cuenta de una aproximación integral en su regulación. Esto será objeto de futuras investigaciones, una vez que el proyecto haya avanzado y se hayan despejado algunas de las indicaciones legislativas que todavía están pendientes en primer trámite constitucional, lo que permitirá, al menos, tener una idea más clara de cómo podría recogerse el interés legítimo en el derecho nacional, con carácter general. Sin perjuicio de ello, algunas de las cuestiones se pueden proyectar, desde ya, como aspectos a considerar en la presente discusión legislativa.

Primero, será materia de discusión si el interés legítimo debiese explicitar taxativamente un catálogo de hipótesis que podrían ser subsumibles bajo tal concepto o si este listado debiese ser meramente ejemplificador, esto es, un catálogo abierto sus-

48. Para revisar el estado de tramitación de los proyectos refundidos, véase la página en el sitio web de la Cámara de Diputados, disponible en <http://bit.ly/2R3ryUl>.

ceptible de enfrentar nuevas realidades y de ser controlado por una autoridad garante del derecho a la protección de datos.

Segundo, se debería explicitar si el interés legítimo autoriza a tratar datos sensibles y si aquello no debiese tener impacto en los deberes del responsable del tratamiento.

Adicionalmente, debe abordarse la necesidad de restringir el tratamiento de datos personales, fundados en el interés legítimo, con finalidades distintas a las autorizadas originalmente por el titular, que hayan justificado su divulgación. Esta extensión del principio de finalidad debiese ser considerada a la hora de someter a límites al interés legítimo del responsable, teniendo especialmente presentes las expectativas razonables del titular de datos. En esta línea, es razonable fortalecer el principio de transparencia, el derecho de acceso, de oposición y de cancelación cuando el título habilitante del tratamiento sea el interés legítimo.

Las cuestiones de prueba serán las que gestionarán las asimetrías de poder entre titulares de datos y responsables del tratamiento. Por ello, en el evento de que se legitime el tratamiento por una fuente diversa al consentimiento o la autorización legal —como es en el caso del interés legítimo— se debe tener en cuenta un alivio probatorio para el titular y la carga de la prueba debiese recaer en el responsable.

Estas conclusiones permiten iniciar una nueva investigación en el evento que la reforma a la Ley de Protección de la Vida Privada avance en línea con el régimen europeo de protección de datos personales. Una incorporación parcial o sesgada del concepto de interés legítimo podría importar una merma significativa en la protección de los datos personales de un titular. Por ello, en el evento de un cambio legislativo, es conveniente considerar la experiencia comparada analizada en este artículo.

Reconocimientos

Este trabajo es parte de la investigación financiada por Fondecyt de Iniciación de la Comisión Nacional de Investigación Científica y Tecnológica, bajo el núm. 11180218, con el título: «El reconocimiento y protección de la autodeterminación informativa como marco teórico adecuado para la comprensión de los derechos de las personas en tanto límite al acceso a la información pública».


Referencias


- ALVARADO, Francisco (2014). «Las fuentes de acceso público a datos personales». *Revista Chilena de Derecho y Tecnología*, 3 (2): 205-226. DOI: [10.5354/0719-2584.2015.33276](https://doi.org/10.5354/0719-2584.2015.33276).
- ANGUITA, Pedro (2007). *La protección de datos personales y el derecho a la vida privada*. Santiago: Jurídica de Chile.

- BALBONI, Paolo, Daniel Cooper, Rosario Imperiali y Milda Macenaite (2013). «Legitimate interest of the data controller: New data protection paradigm: legitimacy grounded on appropriate protection». *International Data Privacy Law*, 3 (4): 244-261. DOI: [10.1093/idpl/ipt019](https://doi.org/10.1093/idpl/ipt019).
- BROWNSWORD, Roger (2009). «Consent in Data Protection Law: Privacy, fair processing and confidentiality». En Serge Gutwirth, Yves Poullet, Paul De Hert, Cécile de Terwangne y Sjaak Nouwt (editores), *Reinventing data protection?* (pp. 83-11). Dordrecht: Springer. DOI: [10.1007/978-1-4020-9498-9_4](https://doi.org/10.1007/978-1-4020-9498-9_4).
- CERDA, Alberto (2012). «Legislación sobre protección de las personas frente al tratamiento de datos personales». Material de estudio del Centro de Estudios en Derecho Informático, Facultad de Derecho, Universidad de Chile.
- FERRETTI, Federico (2014). «Data protection and the legitimate interest of data controllers: Much ado about nothing or the winter of rights?». *Common Law Market Review*, 51 (3): 843-868. Disponible en <http://bit.ly/2WIa1Dy>.
- GONZÁLEZ FUSTER, Gloria y Raphaël Gellert (2012). «The fundamental right of data protection in the European Union: In search of an uncharted right». *International Review of Law, Computers & Technology*, 26 (1): 73-82. DOI: [10.1080/13600869.2012.646798](https://doi.org/10.1080/13600869.2012.646798).
- GUASCH PORTAS, Vicente y José Ramón Soler Fuensanta (2015). «El interés legítimo en la protección de datos». *Revista de Derecho UNED*, 16: 417-438. DOI: [10.5944/rduned.16.2015.15245](https://doi.org/10.5944/rduned.16.2015.15245).
- HARTZOG, Woodrow (2018). *Privacy's blueprint: The battle to control the design of new technologies*. Cambridge: Harvard University Press.
- HEREDERO HIGUERAS, Manuel (1998). «La LORTAD y su futuro: La Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal». *Informática y Derecho*, 1998 (19-22): 463-498. Disponible en <http://bit.ly/2WA3Wcc>.
- IHERING, Rudolf von (1888). *L'esprit du droit romain dans les diverses phases de son développement*. Tomo 4. Trad. de Octave de Meulenaere. París: A. Marescq.
- JERVIS ORTIZ, Paula (2005). «Categorías de datos reconocidas en la Ley 19.628». *Revista Chilena de Derecho Informático*, 6: 111-144. DOI: [10.5354/0717-9162.2011.10727](https://doi.org/10.5354/0717-9162.2011.10727).
- JIJENA, Renato (2001). «La Ley 19.628 Sobre Protección de Datos de Carácter Personal. Una Visión General». En Jorge Wahl Silva (editor), *La Ley chilena de Protección de Datos Personales: Una visión crítica desde el punto de vista de los intereses protegidos*. Santiago: Ediciones Universidad de los Andes.
- KAMARA, Irene y Paul De Hert (2018). «Understanding the balancing act behind the legitimate interest of the controller ground: A pragmatic approach». *SRRN Electronic Journal*. DOI: [10.2139/ssrn.3228369](https://doi.org/10.2139/ssrn.3228369).
- KINDT, Els J. (2013). *Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis*. Amsterdam: Springer. DOI: [10.1007/978-94-007-7522-0](https://doi.org/10.1007/978-94-007-7522-0).

- NISSENBAUM, Helen (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford: Stanford University Press.
- RUBÍ NAVARRETE, Jesús (2012). «Tratamiento de datos personales. Satisfacción del interés legítimo. Ley de protección de datos. Sentencia Tribunal Supremo, de 8 de febrero de 2012. Sentencia TJUE, de 24 de noviembre». *Comunicaciones en Propiedad Industrial y Derecho de la Competencia*, 66: 7-19. Disponible en <http://bit.ly/2WDxxkI>.
- SCHERMER, Bart, Bart Custers y Simone van der Hof (2014). «The crisis of consent: How stronger legal protection may lead to weaker consent in data protection». *Ethics and Information Technology*, 16 (2): 171-182. DOI: [10.1007/s10676-014-9343-8](https://doi.org/10.1007/s10676-014-9343-8).
- SOLOVE, Daniel J. (2004). *The digital person: Technology and privacy in the Information Age*. Nueva York: New York University Press.
- . (2013). «PRIVACY SELF-MANAGEMENT AND THE CONSENT DILEMMA». *HARVARD LAW REVIEW*, 126: 1.880-1.903. Disponible en <http://bit.ly/2RhFBXt>.
- TRON, Jean Claude (2012). «¿Qué hay del interés legítimo? (Primera parte)». *Revista del Instituto de la Judicatura Federal*, 33: 247-267. Disponible en <http://bit.ly/2WFDME0>.
- URSIC, Helena (2018). «Unfolding the new-born right to data portability: Four gateways to data subject control». *SCRIPTed*, 15 (1): 42-69. DOI: [10.2966/scrip.150118.42](https://doi.org/10.2966/scrip.150118.42).
- VIAL CLARO, Felipe (2001). «La Ley 19.628 Sobre Protección de Datos de Carácter Personal: Una visión general». En Jorge Wahl Silva (editor), *Tratamiento de datos personales y protección de la vida privada: Estudios sobre la Ley 19.628 Sobre Protección de Datos de Carácter Personal*. Santiago: Ediciones Universidad de los Andes.

Sobre los autores

Pablo Contreras Vásquez es abogado. Doctor en Derecho por Northwestern University, Estados Unidos. Profesor de Derecho Constitucional y director del Centro de Regulación y Consumo de las Universidad Autónoma de Chile. Su correo electrónico es pablo.contreras@uautonoma.cl.  <http://orcid.org/0000-0002-1131-182X>.

Pablo Trigo Kramcsák es abogado. Licenciado en Derecho por la Pontificia Universidad Católica de Chile. Magister Legum (LL.M.) en Derecho Internacional por la Universidad de Heidelberg, Alemania y la Universidad de Chile. Analista senior de la Unidad de Normativa y Regulación del Consejo para la Transparencia. Su correo electrónico es pablo.trigo@alumni.uni-heidelberg.de.  <http://orcid.org/0000-0003-2385-4722>.

La *Revista de Chilena de Derecho y Tecnología* es una publicación académica semestral del Centro de Estudios en Derecho Informático de la Facultad de Derecho de la Universidad de Chile, que tiene por objeto difundir en la comunidad jurídica los elementos necesarios para analizar y comprender los alcances y efectos que el desarrollo tecnológico y cultural han producido en la sociedad, especialmente su impacto en la ciencia jurídica.

EDITOR GENERAL

Daniel Álvarez Valenzuela
(dalvarez@derecho.uchile.cl)

SITIO WEB

rchdt.uchile.cl

CORREO ELECTRÓNICO

rchdt@derecho.uchile.cl

LICENCIA DE ESTE ARTÍCULO

Creative Commons Atribución Compartir Igual 4.0 Internacional



La edición de textos, el diseño editorial
y la conversión a formatos electrónicos de este artículo
estuvieron a cargo de Tipografía
(www.tipografica.cl).