Fecha de recepción: 19 de abril de 2013 / Fecha de aprobación: 26 de agosto de 2013

Revista de Derecho Comunicaciones y Nuevas Tecnologías

Malas leyes, peores reglamentos. Algunos apuntes críticos sobre el porvenir de la tutela de la persona frente al tratamiento de datos en el Perú

Leysser L. León

Universidad de los Andes
Facultad de Derecho
Revista de Derecho, Comunicaciones y Nuevas Tecnologías
No. 10, Julio - Diciembre de 2013. ISSN 1909-7786

Malas leyes, peores reglamentos. Algunos apuntes críticos sobre el porvenir de la tutela de la persona frente al tratamiento de datos en el Perú*

Leysser L. León**

Resumen

En este artículo, culminado en abril de 2013, el autor comenta críticamente algunas de las más controvertidas disposiciones contenidas en el recién promulgado Reglamento de la Ley peruana de Protección de Datos Personales. Se echa de menos, en especial, y atendiendo a la labor reglamentaria del Ministerio de Justicia reflejada en este dispositivo, una actitud consciente de los funcionarios acerca la importancia de la tutela de la autodeterminación informativa en los países que, como el Perú, siguen sin resolver graves males sociales, como la discriminación.

Abstract

In this article, finished in April 2013, the author comments critically some of the most controversial rules contained in the newly promulgated regulations for the Peruvian Data Protection Law. He regrets, especially, and in response to the drafting work of the Ministry of Justice reflected in those regulations, the absence of a conscious and official attention on the importance of the protection of informational self-determination in the countries where, like Peru, remain unsolved serious social issues, such as discrimination.

* Cómo citar este artículo: León, L. (Diciembre, 2013). Malas leyes, peores reglamentos. Algunos apuntes críticos sobre el porvenir de la tutela de la persona frente al tratamiento de datos en el Perú. *Revista de Derecho, Comunicaciones y Nuevas Tecnologías*, 10.

** Doctor en Derecho Privado por la Scuola Superiore Sant'Anna di Studi Universitari e di Perfezionamento di Pisa (Italia). Profesor de Derecho Civil y de Temas de la Sociedad de la Información en la Facultad de Derecho y Escuela de Posgrado de la Pontificia Universidad Católica del Perú. Profesor de Derecho Civil en las Facultades de Derecho de la Universidad de Piura-Sede Lima, de la Universidad del Pacífico y en la Academia de la Magistratura. Socio de la Asociación Italiana de Derecho Comparado. Miembro del Comité Científico Internacional de la Revista de Derecho Privado de la Universidad Los Andes de Colombia. Autor del volumen *El problema jurídico de la manipulación de información personal* (Palestra Ed., Lima, 2007) y de diversos ensayos en torno de la tutela jurídica y la autodeterminación informativa. lleon@pucp.edu.pe.

Palabras clave: datos personales, información personal, autodeterminación informativa, Ley Peruana de Protección de Datos Personales, Reglamento de la Ley Peruana de Protección de Datos Personales, flujo transfronterizo de datos personales, transferencia de datos personales, comparación jurídica crítica.

Keywords: personal data, personal information, informational self-determination, Peruvian Data Protection Law, Regulations of Peruvian Data Protection Law, cross border privacy rules, personal data transfers, critical legal comparison.

Sumario

I. PREMISA: LA REGLAMENTACIÓN DE LA LLAMADA "LEY (PERUANA) DE PROTECCIÓN DE DATOS PERSONALES" ANTE LA CRÍTICA

No pudieron los funcionarios del Ministerio de Justicia y Derechos Humanos del Perú, lamentablemente, corregir en la fase de reglamentación los graves errores de concepción[1] de nuestra mal llamada "Ley de Protección de Datos Personales" (LPDP). Ha quedado demostrado, así, que la mera acumulación de meses de trabajo (los transcurridos desde la promulgación de la LPDP, en junio de 2011), los encuentros académicos (aun cuando muy escasos), la divulgación de proyectos normativos y la generación de espacios para escuchar y atender la opinión de los involucrados no garantiza, en ninguna elaboración legislativa, un buen resultado final.

Múltiples, reiterados y, por ello, inexcusables, han sido los yerros públicamente cometidos por los encargados de la redacción de este Reglamento (Decreto Supremo N° 003-2013-JUS, del 21 de marzo de 2013). Tres de ellos representan, además, verdaderas extravagancias en el mundo de la tutela jurídica de la autodeterminación informativa:

i.) La injerencia, promovida y celebrada por las propias autoridades a las que se confió la tarea reglamentaria, de empresas nacionales y extranjeras en modo alguno interesadas (no de manera prioritaria, por lo menos) en la protección del derecho individual a decidir la revelación de datos personales y la finalidad para la cual los sujetos autorizan el tratamiento de la información que les concierne.

Es el eterno problema (rayando en una maldición para nuestro país) de los *lobbies* legislativos (en el Parlamento o en el Ejecutivo). Esta vez, sin embargo, no sólo intervinieron masivamente y ante los ojos de todos aquellos sujetos sobre los cuales recaerá la regulación (con sus obligaciones y mecanismos de sanción), sino también inusitados partícipes, tan interesados en lucrar con los servicios jurídicos conexos con esta área jurídica[2], novedosa en el Perú, cuanto perseverantes desconocedores de las bases jurídicas de la autodeterminación informativa.

ii.) El interés, enfatizado hasta el hartazgo, en la salvaguarda del desarrollo y de la "competencia económica" y la apriorística persecución de las alucinadas bondades de una "sociedad de la información", aunque el precio a pagar sea la atenuación de la tutela de la persona frente a la manipulación de sus datos[3].

1 Ver: LEÓN, Leysser, *"Manipulación de información personal y derechos fundamentales. Crítica del proyecto de «Ley de protección de datos personales»*", en "Actualidad Jurídica", Nº 210, Lima, 2011, p. 91 y s.

2 Ya más de diez años atrás, una nota periodística revelaba: "*Protección de datos: un negocio muy rentable*", en http://www.networkworld.es, edición del 1 de julio de 2002: "desde que las empresas se han empezado a preocupar por su adecuación a la LOPD y a ser conscientes de que muchas veces ellas solas no son capaces de hacerlo, por falta de personal técnico y jurídico cualificado, requieren de las prestaciones de compañías de seguridad y consultoría que se han apresurado a ofrecer este tipo de servicios". Tal es la situación en el Perú ahora, pero el interés suscitado por la normativa en el mercado profesional –del cual el autor de estos apuntes es activo partícipe desde hace casi una década– no debe hacer perder de vista que estamos ante una regulación que encuentra su razón de ser en la tutela de un aspecto de la personalidad.

3 También a la Unión Europea se le reclama, por parte de las transnacionales, una atenuación de la normativa comunitaria sobre tutela de la autodeterminación informativa. Ver, sobre este punto, la nota "*Euro-*

¿"Competencia" frente a quién, por lo demás? ¿Frente a los países que tenían ya estas normativas? Los Estados Unidos de América no la tienen (y es muy probable que nunca la tengan), no obstante lo cual hemos firmado un *free trade agreement* (TLC) con ellos. ¿Y "competitividad" para qué? ¿Para que nos confíen, a precio más barato, las bases de datos (que nuestro legislador imitador llama, a la española, "bancos de datos") que en otros ordenamientos, con leyes mejor planteadas y más estrictas, sí se encuentran a seguro reparo? O ¿"competividad" para que en el Perú se pueda negociar libremente o con exigencias mínimas el intercambio retribuido de bases de datos personales?

Todo lo que debe entenderse sobre la competencia en este sector es –como bien se ha observado– que:

> si la competencia perfecta implica como condición necesaria una información puntual y completa entre todos los operadores (es decir, la ausencia de asimetrías informativas) es también cierto que el intercambio de dichas informaciones puede transformarse en un instrumento que facilita conductas colusivas"[4].

iii.) El silencio, consciente al parecer, frente al proceder de entidades estatales que afectan día tras día este aspecto del derecho general de la personalidad (RENIEC, SUNAT, Registro de Deudores Alimentarios, etc.).

En el marco normativo peruano, ahora completado con el Reglamento de la LPDP, el RENIEC seguirá percibiendo contraprestaciones por convenios de transferencia de nuestra información personal (la contenida en nuestros DNI) celebrados con los medios de comunicación (no siempre responsables en la utilización de los datos así obtenidos); la SUNAT persistirá en la exhibición de nuestra información (la contenida en el Registro Único de Contribuyentes) en su web institucional; y el Registro de Deudores Alimentarios mantendrá la práctica discriminatoria del etiquetamiento de sus inscritos, en la misma medida que su desinterés en actualizar o comprobar la verosimilitud de la información que acoge y que difunde universalmente permanece[5].

Es pasmosa, en esta línea de cuestionamiento, la relación de espacios excluidos, por voluntad legislativa, de la aplicación de la LPDP y su Reglamento. En nuestro país, contra la tendencia de los ordenamientos que cuentan con normas de tutela de la autodeterminación informativa, han sido consideradas "fuentes accesibles al público" (artículo 17 del Reglamento)[6], con len-

pean data protection laws to hit Indian software companies", en http://www.articles.economictimes.indiatimes.com, edición del 20 de marzo de 2013. Allí se describe cómo la expansión de los negocios de las firmas indias de software en el viejo continente resulta condicionada al aligeramiento de las cargas impuestas por las leyes europeasde protección frente a la manipulación de información personal.

4 TESAURO, Giuseppe, "Competizione economica: i vantaggi della protezione dei dati", en GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, Da costo a risorsa: *la tutela dei dati personali nelle attività produttive*, al cuidado de G. Rasi, Istituto Poligrafico e Zecca dello Stato, Roma, 2004, p. 213.

5 Ello porque nuestro muy peruano Registro de Deudores Alimentarios es de consulta libre, un *privacy common, un public good* sin restricciones. En cualquier lugar del mundo donde exista un terminal telemático se puede verificar, por lo tanto, que cierto ciudadano del Perú (fotografiado, por lo demás) tiene deudas alimentarias que honrar.

6 En esta norma del Reglamento peruano se copia, pero a la vez se amplía, el artículo 7 del Reglamento de la Ley española en materia,

guaje descuidado, "los medios de comunicación electrónica, óptica y de otra tecnología, siempre que el lugar en el que se encuentren los datos personales esté concebido para facilitar información al público y estén abiertos a la consulta general"; las "guías telefónicas, independientemente del soporte en el que estén a disposición y en los términos de su regulación específica"; "los diarios y revistas independientemente del soporte en el que estén a disposición y en los términos de su regulación específica"; los "medios de comunicación social"; las "listas de personas pertenecientes a grupos profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección postal, número telefónico, número de fax, dirección de correo electrónico y aquellos que establezcan su pertenencia al grupo"; si se trata de colegios profesionales, "podrán indicarse", además, "número de colegiatura, fecha de incorporación y situación gremial en relación al ejercicio profesional"; los "repertorios de jurisprudencia debidamente anonimizados"; los "Registros Públicos"; las "entidades de la administración pública", conforme a la Ley de Transparencia y de Acceso a la Información Pública; etc.

> La doctrina especializada se ha referido a estas fuentes de acceso libre como *privacy commons* o *public goods*, o sea, como bienes que pese a estar vinculados con la esfera personal de los individuos, se convierten, por obra del legislador, en bienes de todos. A la luz de semejantes deformaciones, no ha faltado quien especule o dictamine la "muerte" de la *privacy*[7].

Toda la labor reglamentaria nacional se ha caracterizado, además, por un censurable e indolentemente exhibido desconocimiento de los problemas locales y por la pervivencia de una, imperdonable a estas alturas, autolimitación formativa e informativa de sus actores: por un lado, el diálogo –cerrado y viciosamente facilitado por el idioma común– con la Agencia Española para la Protección de Datos y con expertos forjados en experiencias no del todo a la vanguardia en esta materia: Argentina, México y Colombia, país, este último, donde sólo en los próximos días entrará en vigor una normativa especial para el sector; y el apego, con cuestionables pinceladas de originalidad (que en ningún caso refuerzan la tutela objeto de la norma), al Reglamento español de Desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, aprobado por Real Decreto 1720/2007, del 21 de diciembre de 2007.

Como consecuencia de estos desaciertos y de muchos otros, creo que es poco probable que cobre arraigo en nuestra ciudadanía la gran importancia de este moderno, singular y trascendental aspecto de la personalidad jurídica. Paradójicamente, este panorama se vislumbra en

subtitulado "fuentes accesibles al público". La plantilla española, sin embargo, no hace referencia (como sí se hace en el artículo 17.1 de nuestro Reglamento) a medios "concebidos para facilitar información al público" o "abiertos a la consulta general" (esos que, como es bien sabido, abundan en páginas web de matriz peruana), ni a los "Registros Públicos", ni a las "guías telefónicas". En este último ámbito, donde el titular de los datos debería contar con una tutela jurídica reforzada más bien, lo que el legislador español señala es que tienen carácter de fuentes accesibles al público "las guías de servicios de comunicaciones electrónicas".

7 FROOMKIN, A. Michael, "*The Death of Privacy*?", en "Stanford Law Review", vol. 52, 2000, p. 1463 y s.

el Perú el mismo año en que se cumplen tres décadas del célebre fallo del Bundesverfassungsgericht sobre la Ley del Censo[8], aquel donde se estableció que:

Quien no pueda estimar con suficiente seguridad, qué informaciones sobre sí mismo son conocidas en determinadas esferas de su medio social, y quien no pueda de algún modo valorar el conocimiento previo que los posibles interlocutores tienen de uno mismo, puede verse restringido esencialmente en su libertad para planear o decidir con base en su propia autodeterminación. Un ordenamiento social y un orden legal en el que los ciudadanos no pudieran conocer quiénes, cuándo y en qué circunstancias saben qué sobre ellos, serían incompatibles con el derecho a la autodeterminación de la información[9].

II. LOS MALES DEL TRASPLANTE DE NORMAS EXTRANJERAS Y DE LA NO IDENTIFICACIÓN DE PROBLEMAS LOCALES

Comienza el Reglamento peruano repitiendo el error de señalar que con la LPDP se garantiza el "derecho fundamental a la protección de datos personales".

Esta expresión, pese a su amplia aceptación en el medio español[10] y europeo no está libre de generar equívocos. Los datos personales, considerados en sí mismos, no se "protegen" ni se "tutelan"; se "tutela" siempre a la persona. Con una dicción como la que se repite en la LPDP y en su Reglamento no habrán de faltar ciudadanos peruanos que interpreten la normativa íntegra como un reconocimiento legal de una titularidad ("propiedad") de la información personal[11] y que, guiados por dicha óptica, pretendan

8 65 BVerfGE, 1 (13 de diciembre de 1983), en SCHWABE, Jürgen (compilador), *Jurisprudencia del Tribunal Constitucional alemán*, trad. de M. Anzola Gil y E. Maus Ratz, Konrad-Adenauer-Stiftung, Berlín-México, 2009, p. 94 y s. Ver, sobre este importante precedente: SCHWARTZ, Paul M., "*The Computer in German and American Constitutional Law: Towards and American Right of Informational Self-Determination*", en "American Journal of Comparative Law", vol. 37, 1989, p. 675 y s., en especial, p. 687 y s.; y más recientemente: HORNUNG, Gerrit y Christoph SCHNABEL, "*Data Protection in Germany I: The Population Census Decision and the Right to Informational Self-Determination*", en "Computer Law & Security Report", vol. 25, Nº 1, 2009, p. 84 y s.

El diario español *"El País*", edición del 14 de abril de 1983, ahora disponible en http://www.elpais.com, cubrió así el acontecimiento: "Dos abogadas de Hamburgo y un estudiante de Derecho presentaron ante el Tribunal Constitucional de Karlsruhe la demanda de anticonstitucionalidad, por considerar que el intento de realizar el censo en la forma que quería el Gobierno supone un atentado contra el «libre desarrollo de la personalidad» y la libertad de expresión, «que incluye el derecho de negarse a declarar». [...]. El Gobierno asegura que no se podían cometer abusos, pero entre las preguntas que pedían los encargados de realizar el censo figuraban el número de teléfono, el nombre, la religión, base del sustento y un largo etcétera que inquietaba a muchos".

Los gestores de nuestra normativa de "protección de datos personales" deberían haberse preguntado (aunque, claro, eso habría significado desarrollar su capacidad de lectura e inculcarles hábitos de investigación que no poseen) si el Perú del siglo XXI es equiparable, en cuanto al desarrollo de la cultura constitucional y de los derechos fundamentales, a la Alemania de 1983.

9 SCHWABE, *op. cit.*, p. 96.

10 Ver, por ejemplo: PRIETO GUTIÉRREZ, Jesús María, "*Objeto y naturaleza del derecho fundamental a la protección de datos personales*", en "Boletín del Ministerio de Justicia", Año 58, Nº 1973, Madrid, 2004, p. 3119 y s.; y SERRANO PÉREZ, María Mercedes, "*El derecho fundamental a la protección de datos. Su contenido esencial*", en "Nuevas Políticas Públicas", Nº 1, 2005, p. 245 y s. Sí efectúa las precisiones terminológicas del caso, en cambio, LUCAS MURILLO DE LA CUEVA, Pablo, "*La construcción del derecho a la autodeterminación informativa y las garantías para su efectividad*" (2008), en http://www.fcje.org.es (web de la Fundación Coloquio Jurídico Europeo).

11 Tema fundamental, puntualmente ignorado por los artífices de la LPDP y de su Reglamento, sobre el cual existe bibliografía de obligatoria consulta por sobradas razones: LITMAN, Jessica, "*Information Privacy/Information Property*", en "Stanford Law Review", vol. 52, Nº 5, 2000, p. 1283 y s.; LEMLEY, Mark A., "*Private Property*", *ivi*, p. 1545 y s.; SCHWARTZ, Paul M., "*Property, Privacy and Personal Data*", en "Harvard Law Review", vol. 117, Nº 7, 2004, p. 2056 y s.

infructuosamente "reivindicar" algo de lo que consideren haber sido "despojados"[12], con el recurso apocalíptico de las nuevas tecnologías.

Lo que prosigue en nuestro Reglamento es un progresivo vaciado de contenido de términos básicos como "datos personales", "datos personales relacionados con la salud" y "datos sensibles"; operación de suyo censurable, si se toma en cuenta que todas estas nociones tenían ya un espacio natural en el glosario de la propia LPDP[13].

Esta "técnica de reglamentación" –considerémosla así– no merecería ser blanco de cuestionamiento si, por lo menos, sus autores se hubiesen ceñido a las directrices, buenas o malas que fueren de la LPDP. Pero no les bastó. Mientras en Italia, por ejemplo, son "datos personales" los que permiten identificar al individuo incluso de manera indirecta[14], nuestro Reglamento llama "datos personales" a la "información numérica, alfabética, gráfica, fotográfica, acústica, sobre hábitos personales o de cualquier otro tipo concerniente a las personas naturales que las identifica o las hace identificables a través de medios que puedan ser razonablemente utilizados". ¿Qué significará, por otro lado, la "utilización "razonable", cuya ambigüedad, ya presente en la LPDP (Art. 2.4), habría merecido precisiones imprescindibles en sede de reglamentación? Parece un dictado adecuado, más bien, a los intereses de quienes tratan datos personales, y no de los titulares de la autodeterminación informativa.

Luego se califica como datos personales "relacionados con la salud" a la "información concerniente a la salud pasada, presente o pronosticada, física o mental, de una persona, incluyendo el grado de discapacidad y su información genética". Nos preguntamos (y éste, por cierto, es el tipo de consultas que dirigen los "actores del mercado" y los "agentes de la competencia económica" a los docentes y abogados especializados en este campo): ¿qué sucede con los resultados del análisis de sangre al que debe someterse el solicitante de un préstamo bancario, conminado a facilitar una muestra de su plasma para efectos de que se fijen los términos y condiciones del seguro de desgravamen? ¿Esa "información", incluida la prueba de E.L.I.S.A., de la que puede llegar a depender la obtención del préstamo o la cuantificación exorbitante del seguro en mención, es "relativa a la salud"? La respuesta es afirmativa ¿no es verdad? Bueno, es probable que las aseguradoras y bancos no lo consideren así, porque la toma de la muestra no está ligada con un tratamiento sanitario. De todas formas, interrogado sobre la finalidad de su labor, el médico a cargo del análisis nos responde que los datos obtenidos se envían a la compañía de seguros y que ésta comunicará

12 No habiendo "propiedad", naturalmente, no puede haber "despojo". Pero con la información personal incorporada a una base de datos, se facilita, ante nuestros ojos, la "compra" y "venta" de estas singulares "mercancías". Con las leyes de protección de la persona frente a la manipulación de su información se persigue, justamente, regular esa mercantilización. Pero no se trata de la única ni de la principal finalidad, como equivocadamente cree el Director General de Protección de Datos Personales del Ministerio de Justicia. Ver: "*Entrevista*", en "*La Ley*", Año 6, Nº 61, febrero de 2013, p. 8.

13 Los artífices del Reglamento tropiezan aquí, inexcusablemente, con la misma piedra que ha causado tantos problemas de interpretación en el área de la contratación estatal, donde no son pocas las contradicciones entre la Ley y el Reglamento.

14 Codice in materia di protezione dei dati personali (Decreto Legislativo Nº 196, del 30 de junio de 2003): Art. 4.1.b).

sus conclusiones directamente al banco. ¿Bajo qué reglas y con cuáles compromisos se transferirá la información? ¿Circularán esos datos entre las demás compañías de seguros y bancos, en caso de no ser aprobado el préstamo o que el solicitante decline de celebrarlo? Lo desconocemos y lo seguiremos desconociendo, pese a la normativa especial aquí comentada. Hay, admitámoslo, un flujo de información sanitaria y sensible que tiene lugar al margen de la regla del consentimiento informado. Pero la visión de nuestro legislador ha sido tan corta (o ha sido recortada a propósito, por intervención de terceros) que esta temática, ligada con la vida del ciudadano común y corriente, no ha merecido su atención.

El remate de estos despropósitos es la definición de "dato sensible", que en la LPDP (Art. 2.1) aparecían caracterizados así:

> los datos biométricos que por sí mismos pueden identificar al titular; datos referidos al origen racial y étnico; ingresos económicos, opiniones o convicciones políticas, religiosas, filosóficas o morales; afiliación sindical; e información relacionada a la salud o a la vida sexual.

En el Reglamento (Art. 2.6), quebrantándose las jerarquías, se propone que los "datos sensibles" son aquellos referidos:

> a las características físicas, morales o emocionales, hechos o circunstancias de su vida afectiva o familiar, los hábitos personales que corresponden a las esfera más íntima, la información relativa a la salud física o mental u otras análogas que afecten su intimidad.

En esta definición, desastrosa, falta el objeto (la "persona natural"), pero eso no es lo más grave. Frente a nuestros ojos, se despoja de la condición de "dato sensible" a la información ideológica, religiosa y sobre sindicalización. El legislador peruano es tan "de avanzada" que rompe, sin miramientos, una regla respetada uniformemente por sus pares de América Latina[15]. En Chile (Ley 19.628, Art. 2.g) losa "datos sensibles" son los que se refieren:

> a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual.

En Argentina (Ley 25.326,Art. 2) son datos sensibles "los que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual"; en Uruguay (Ley Nº 18.331, Art. 4), son los que revelan "origen racial y étnico, preferencias políticas, convicciones religiosas o morales, afiliación sindical e informaciones referentes a la salud o a la vida sexual"; en México (Ley Federal, Art. 3.IV) son:

> los datos personales que afecten a la esfera más íntima de su titular, o cuya utilización inde-

15 Una visión global de la evolución de la tutela de la autodeterminación informativa en América Latina es ofrecida por TRONCOSO REIGADA, Antonio, "*El desarrollo de la protección de datos personales en Iberoamérica desde una perspectiva comparada y el reequilibrio de los modelos de protección de datos a nivel internacional*", en "Revista de la Red Académica Internacional de Protección de Datos Personales", Nº 1, 2012, p. 2 y s.

> bida pueda dar origen a discriminación o conlleve un riesgo grave para éste. En particular, se consideran sensibles aquellos que puedan revelar aspectos como origen racial o étnico, estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual.

Finalmente, en Colombia[16] (Ley 1581, Art. 5) se llama "datos sensibles", ejemplarmente, a los que:

> afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos.

En este punto nos hemos apartado incluso del modelo legal español (muy seguido, en cambio, en otros ámbitos de la normativa). En dicho ordenamiento, donde se habla de "datos especialmente protegidos" se llega incluso a prohibir (Ley Orgánica 15/1999, artículo 7.4) "los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico, o vida sexual"[17].

En este contexto, los trabajadores españoles que han migrado masivamente a Perú a causa de la crisis económica que atraviesa su país arribarán a un lugar de realidad inversa en cuanto a la tutela de la autodeterminación informativa: muy propicio para los empleadores, liberados de las pesadas "cargas" de la normativa ibérica y europea[18]. El alto precio a pagar por un puesto de trabajo en esta parte del mundo será el menoscabo de su status de ciudadanos del viejo continente o de la, en algún momento llamada, "Europa de los derechos"[19]. A lo mejor, a esta peculiar manifestación de la "competitividad"

16 Sobre la experiencia pre-regulatoria en el ordenamiento colombiano, ver: REMOLINA-ANGARITA, Nelson, "*¿Tiene Colombia un nivel adecuado de protección de datos personales a la luz del estándar europeo?*", en "International Law – Revista Colombiana de Derecho Internacional", vol. 16, 2010, p. 489 y s.

17 Esta importante temática fue materia de consulta ante la Agencia Española de Protección de Datos, la cual, en su Informe 0423/2009, publicada en http://www.agpd.es, confirmó que deben aplicarse a los "ficheros" que contengan datos "especialmente protegidos" sobre afiliación sindical, "el mismo nivel de seguridad que se prevea para los restantes datos de esta naturaleza".

En la propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (enero de 2012) se prescinde de una definición de "datos sensibles", pero, con evidente refuerzo de la tutela, se prohíbe "el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, la religión o las creencias, la afiliación sindical, así como el tratamiento de los datos genéticos o los datos relativos a la salud, la vida sexual, las condenas penales o medidas de seguridad afines".

18 Un panorama global sobre la tutela de la privacidad en las relaciones de trabajo es brindado por BERNABEI, Federico, *Nuove tecnologie e tutela della riservatezza nei rapporti di lavoro* (tesis), Libera Università Maria Ss. Assunta, Facoltà di Giurisprudenza, Año Académico 2009-2010. Disponible en: http://www.rivista.ssef.it. En la bibliografía especial sobre el tema siguen siendo ilustrativas las páginas de SIMITIS, Spiros, "*Reconsidering the Premises of Labour Law: Prolegomena to an EU Regulation of the Protection of Employees' Personal Data*", en "European Law Journal", vol. 5, 1999, p. 45 y s. En la bibliografía española: RODRÍGUEZ ESCANCIANO, Susana, "*Derecho a la protección de datos personales de los trabajadores como garantía de libertad sindical*" (2011), en http//www.ugt.es.

19 Ver: BIFULCO, Raffaele; CARTABIA, Marta; y Alfonso CELOTTO (al cuidado de), "*L'Europa dei diritti. Commento alla Carta dei Diritti Fondamentali dell'Unione Europea*", Il Mulino, Bologna, 2001, *passim*.

se referían, y lo siguen haciendo, los lobbistas entrometidos negativamente en la interpretación de la LPDP.

Y, de otro lado, es decepcionante comprobar que en un país desigual y asolado por los actos de discriminación en todos los niveles, el legislador peruano muestre haber perdido el rumbo, al olvidarse de ligar la naturaleza "sensible" de los datos personales con todo aquello que involucre un riesgo para la sociedad igualitaria. Esto ocurre precisamente cuando acabamos de ser parte, muy a pesar nuestro, de un absurdo proceso de revocación de autoridades municipales en la ciudad de Lima, donde la descalificación de los intervinientes *ad hominem*, por el solo hecho de tener una afiliación partidaria (impunemente divulgada en la Internet) estuvo a la orden del día.

III. LA INJERENCIA DE LOS DEFENSORES DE LA LIBRE CIRCULACIÓN DE LA INFORMACIÓN PERSONAL: ¿DURMIENDO CON EL ENEMIGO?

Vivimos también una época en la que se ha profundizado la brecha entre los países firmes en su decisión de tutelar la autodeterminación informativa y la nación caracterizada por promover, en sentido contrario, la libre circulación de la información personal[20].

Son constantes, en tal sentido, las noticias de impacto internacional que nos hacen saber, instantáneamente, gracias a la Internet, que, por ejemplo, Google Inc. está afrontando, en simultáneo, nada más y nada menos que seis procesos en distintos países de la Unión Europea (Reino Unido, Francia, Alemania, Italia, España y Holanda) por los cambios arbitrarios, no informados a los usuarios, y en abierta infracción de la legislación sobre autodeterminación informativa, de sus *privacy policies*[21].

En el año 2010, Google Inc., igualmente, recibió una carta de diez Agencias de "protección de datos" (Irlanda, Reino Unido, Italia, Alemania, Francia, Holanda, España, Nueva Zelanda, Israel y Canadá) en la que le expresaron preocupación porque "demasiado a menudo, el derecho a la privacidad de los ciudadanos se está olvidando en el despliegue de las nuevas aplicaciones tecnológicas"[22] (Google Buzz, en particular). La carta en mención imputa a la empresa destinataria un "decepcionante desprecio" por normas atinentes a derechos fundamentales,

20 Hay quien ha planteado esta oposición de enfoques en términos de "dignidad" (Europa) y "libertad" (USA): WHITMAN, James Q., "*The Two Western Cultures of Privacy: Dignity versus Liberty*", en "Yale Law Journal", vol. 113, Nº 6, p. 1151 y s., especiamente, p. 1189 y s. Esta posición ha sido contradicha por SCHWARTZ, Paul M., "*Regulating Governmental Data Mining in the United States and Germany: Constitutional Courts, the State and New Technology*", en "William and Mary Law Review", vol. 53, 2011, p. 381 y s.

Una destacable manifestación de este contrapunto internacional de culturas es abordado en el estudio de VANWANSSHNOVA, Matthew R., "*Data Protection Conflicts Between the United States and the European Union in the War of Terror: Lessons Learned from the Existing Sytem of Financial Information Exchange*", en "Case Western Reserve Journal of International Law", vol. 39, 2008, p. 827 y s. El autor efectúa un análisis de la decisión del Tribunal de Justicia de la Unión Europea que en mayo de 2006 declaró nulo un acuerdo entre la Unión Europea y los Estados Unidos de América en cuya virtud se transferían a este último país los registros de información personal de pasajeros de todas las aerolíneas.

21 Ver el artículo: "*Google facing regulatory action in six EU countries over privacy policy issues*", en http://www.out-law.com, publicada el 3 de abril de 2013.

22 Ver el artículo: "*Diez autoridades de protección de datos envían una carta de queja a Google*", en "El País", edición on-line del 20 de abril de 2010, http://www.elpais.com.

pese a tratarse de una empresa "líder del sector de Internet".

Y siempre Google Inc., en los últimos años, ha sido condenada en múltiples países de la Unión Europea y en América Latina por mantener información equivocada, desactualizada o, en cualquier modo, perjudicial para los titulares de los datos, en su servicio de búsquedas Google Search. En Francia, el resarcimiento ordenado judicialmente ha sido de 5,000€ (unos 16,000 nuevos soles)[23], mientras que en Argentina, ha alcanzado la importante cifra de 135,000USD más intereses[24]. En su país de origen, asimismo, Google Inc. ha sido condenada al pago de un resarcimiento de 7'000,000USD por la recolección de datos de redes inalámbricas mediante su publicitado Google Street View[25] (sí, ese mismo que muchos despreocupados vecinos de Lima miraban absortos por las calles de la ciudad, hace algunas semanas)[26].

Estamos, pues, ante una empresa con notorios antecedentes internacionales de aversión a la regulación en materia de autodeterminación informativa. ¿No eran tales antecedentes suficientemente reconocibles (basta efectuar una búsqueda en Internet) como para prestar atención a las actitudes de Google Inc. alrededor del mundo, y así dedicar un especial esfuerzo a prevenir su desenvolvimiento ilegal respecto de los titulares de datos personales peruanos[27]? ¿Dónde estaban en aquel momento las autoridades del sector? Muy probablemente, brindando audiencia y mostrando una bien intencionada, a la vez que inoportuna, apertura frente a las pretensiones de los regulados[28]. En Suiza, la activa y vigilante autoridad nacional en materia de tutela frente al tratamiento de información personal ha demandado a Google Inc. por los riesgos de la captación de rostros de personas y de placas de vehículos de ciudadanos helvéticos a través, precisamente, de Google Street View[29].

Esta sería la explicación (la única posible, a juicio de quien escribe) de preceptos normativos como aquel que establece que las disposiciones de la LPDP y el Reglamento son de aplicación al tratamiento de datos personales cuando (Art. 5.1) "sea efectuado en un establecimiento

23 Ver el artículo: "*Google pagará indemnización en Francia*", distribuido por la agencia de noticias Reuters, el 25 de septiembre de 2010, en http://www.lta.reuters.com.

24 Ver el artículo: "*Google y Yahoo deberán indemnizar a modelo argentina*", distribuido, el 16 de abril de 2013, por la agencia de noticias AFP, en http://www.clarin.com.

25 Ver el artículo: "*Google pagará por el barrido de datos de su servicio Street View*", en http://www.elpais.com, edición del 10 de marzo de 2013.

26 Ver el artículo: "*Street View: los vehículos de Google que recorren Perú*", publicado en http://www.terra.com, el 6 de diciembre de 2012.

27 De esto se advertía, tempranamente, en los artículos: "*Google preocupado por Ley peruana de protección de datos*", en http://www.elcomercio.pe, edición del 18 de mayo de 2011, y "*Critican proyecto de protección de datos personales*", en http://www.gestion.pe, edición del 30 de mayo de 2011.

28 Ver los artículos: "*Ministro de Justicia se reúne con representantes del empresariado por reglamento de Ley de Protección de Datos Personales*", en el website del Ministerio de Justicia y Derechos Humanos: http://www.minjus.gob.pe, 23 de mayo de 2012, y "*Ministro de Justicia debate sobre reglamento de Ley de Protección de Datos Personales*", en http://www.larepublica.pe, edición del 24 de mayo de 2012. En ambos documentos se destaca la presencia de representantes de Google Inc. en las reuniones convocadas. Se hizo de conocimiento público, asimismo, la participación de funcionarios de la Comisión Federal de Comercio de los USA y de la Oficina de Tecnología y Comercio Electrónico del Departamento de Comercio de los USA.

29 Ver el artículo: "*Suiza demanda a Google Street View*", en http://www.elpais.com, edición del 13 de noviembre de 2009.

ubicado en territorio peruano correspondiente al titular del banco de datos personales o de quien resulte responsable del tratamiento" de tal manera Google Inc., Yahoo y FaceBook quedan al margen de la regulación; o se eleva al rango de consentimiento "expreso" o "inequívoco" (Art. 12.3) la "manifestación consistente en «hacer clic», «cliquear» o «pinchar», «dar un toque», «*touch*» o «*pad*» u otros similares"; o la que reconoce (artículo 13) a la publicación de las "políticas de privacidad" (traducción literal de *privacy policies*) el carácter de modalidad de cumplimiento del "deber de información"; o la que reduce a la edad de catorce años –coincidentemente, la misma que Facebook ha decidido aplicar para las cuentas de su red social en España[30]– como requerida para consentir al tratamiento de datos personales (Art. 28), con la solitaria exigencia de que "la información proporcionada haya sido expresada en un lenguaje comprensible para ellos".

IV. SÍNTESIS SOBRE EL PROBLEMA DEL FLUJO TRANSFRONTERIZO DE DATOS PERSONALES

El flujo transfronterizo de datos es uno de los mayores riesgos que enfrentan los países donde la tutela de la autodeterminación informativa no está regulada[31]. Atendiendo a ésta, entre otras razones, se justificaba que el Perú adoptara una normativa especial en la materia.

Sólo que cuando se tomó la decisión política de promulgar la LPDP, el Perú ya había terminado de consolidarse como lugar de encuentro de las dos corrientes mundiales acerca de la información personal: la europea, de la autodeterminación informativa, y la estadounidense, de la libre circulación de la información.

En los meses previos a la publicación del Reglamento, fueron insistentes las consultas profesionales de empresas, buena parte de ellas subsidiarias o sucursales de entidades extranjeras, interesadas en decidir la localización geográfica de sus bases de datos (de sus "servidores"), por el temor a una regulación hostil para la transferencia de información personal en el Perú. Ecuador, Brasil y Estados Unidos eran algunos de los países que se mencionaban como idóneos para realizar estas transferencias, a pesar de que las disposiciones de la LPDP obligan a efectuarlas únicamente a países que tengan los mismos estándares de protección que el nuestro.

Se sabe también que en los años precedentes a la promulgación de nuestra LPDP múltiples empresas de *call-center* estaban interesadas en hallar una localización favorable (a sus propios intereses, naturalmente), libre de las burocráticas obligaciones que les imponen las leyes de

30 Ver el artículo: "*FaceBook eleva a 14 años la edad mínima para entrar en su red española*", en http://www.elmundo.es, edición del 18 de febrero de 2010. Nuestra norma proviene del artículo 13.1 del Reglamento de la Ley española: "podrá procederse al tratamiento de los datos de los mayores de catorce años con su consentimiento, salvo en aquellos casos en los que la Ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela. En el caso de menores de catorce años se requerirá el consentimiento de los padres o tutores".

31 Lo remarcaba SCHWARTZ, Paul M., "*European Data Protection Law and Restrictions on International Data Flows*", en "Iowa Law Review", vol. 80, 1995, p. 471 y s.

autodeterminación informativa en sus países de origen[32].

El marco legal peruano ha quedado perfilado como sigue:

a.) El flujo transfronterizo de datos personales está permitido si el titular de los datos ha brindado su consentimiento previo, informado, expreso e inequívoco para ello (LPDP, Art. 15.7). Pero obsérvese: no es que el consentimiento sea necesario de todas formas. Realmente, la circulación "consentida" es sólo una de las hipótesis en la que el flujo se considera arreglado a ley.

b.) En efecto, el flujo transfronterizo está permitido, sin consentimiento, por ejemplo, "cuando los datos personales sean necesarios para la ejecución de una relación contractual en la que el titular de los datos personales sea parte, incluyendo lo necesario para actividades como la autentificación del usuario, mejora y soporte del servicio, monitoreo de la calidad del servicio, soporte para el mantenimiento y facturación de la cuenta y aquellas actividades que el manejo de la relación contractual requiera" (LPDP, Art. 15.4). Estamos, qué duda cabe, ante una licencia clamorosa para la transferencia internacional de la información personal.

c.) Tampoco se necesita el consentimiento del titular para esta circulación fuera de nuestras fronteras "cuando el flujo transfronterizo de datos personales se realice para la protección, prevención, diagnóstico o tratamiento médico o quirúrgico de su titular; o cuando sea necesario para la realización de estudio epidemiológicos o análogos, en tanto se aplique procedimientos de disociación adecuados" (LPDP, Art. 15.6). Esta norma ha sido concebida, claramente, para la salvaguarda de una de las actividades más merecedoras de fiscalización en los países que cuentan con normativas de tutela frente a la manipulación de información personal (de datos sensibles, siendo precisos): los laboratorios multinacionales[33]. En la

32 Ver el artículo: "*Los datos personales de los españoles hacen las Américas*", en http://www.publico.es, edición del 11 de enero de 2007. Allí se informa que los datos de españoles, "cliente y en en ocasiones potenciales clientes de una compañía de telefonía [...] son transferidos a *call centers* de un «país que no proporciona un nivel de protección equivalente» al de las leyes de protección de datos europeas. Este traspaso de información sensible es hoy una práctica habitual y el principal receptor de datos es América Latina".

Los "principales destinos" de nuestro continente eran, en aquel entonces, Chile, Perú y Colombia. La LPDP y su Reglamento parecen haber sido concebidos para mantener (en lugar de erradicar) estas prácticas que han expuesto a otros países como "paraísos para el tráfico de datos". Si el Perú fuera comprendido entre éstos afrontaríamos la paradoja de ser un ordenamiento con una ley y un reglamento puramente decorativos que legitiman las prácticas abusivas en el sector. Sólo la empresa Jazztel, como se informa en http://www.samuelparra.com, el 15 de noviembre de 2011, transfirió, en el período 2009-2011, a 36 empresas distintas, ubicadas en Marruecos, Perú, Paraguay, Colombia, Chile y Guatemala, datos de ciudadanos europeos como nombre completo, dirección, teléfono e incluso datos bancarios. Para este proceso, que recibe el nombre de "deslocalización", Jazztel tuvo que solicitar al Director de la Agencia de Protección de Datos española la autorización respectiva, en 36 ocasiones diferentes(¡!).

Ver también el artículo "Call Centers *peruanos, un negocio en crecimiento*", en http://www.esan.edu.pe, 16 de diciembre de 2010, donde, sin advertirse los peligros para la autodeterminación informativa, se saluda que el Perú atraiga "este tipo de intervsiones por la calidad y proactividad del trabajador peruano, por el costo competitivo de mano de obra, por la amabilidad en la atención con tono de voz neutro y sin acento, por la presencia de tecnología competitiva en el país, por los servicios inmobiliarios adecuados y por la estabilidad política que atraviesa el Perú".

33 Ver, sobre este "subsistema" propiamente dicho de la autodeterminación informativa: TAYLOR, Mark J., "*Health Research, Data Protection, and the Public Interest in Notification*", en "Medical Law Review", vol. 19, 2011, p. 267 y s.

normativa española, la excepción (Art. 34.d de la LO 15/1999) comprende únicamente la transferencia que "sea necesaria para la prevención o para el diagnóstico médico, la prestación de asistencia sanitaria o tratamiento médico o la gestión de servicios sanitarios".

d.) El flujo transfronterizo está permitido, incluso a países que no cuenten con niveles de protección adecuados, y sin responsabilidad para el transferente, si se hace en el marco de "tratados internacionales sobre la materia en los cuales la República del Perú sea parte" (LPDP, artículo 15.1), disposición que parafrasea defectuosamente el artículo 34.a de la LO 15/1999 de España: "cuando la transferencia internacional de datos de carácter personal resulte de la aplicación de tratados o convenios en los que sea parte España". La redacción de la norma y su referencia "a la materia" no permiten una interpretación certera de lo que se dispone, pero es previsible que se genere el entendimiento, por ejemplo, de que la transferencia de información a empresas domiciliadas en los Estados Unidos de América, en el marco de relaciones comerciales internacionales, promovidas por el TLC, sea considerada "inmune" a la regulación de nuestra LPDP.

Así, mientras que para recibir información personal de ciudadanos de la Unión Europea diversas empresas estadounidenses han tenido que esperar una decisión comunitaria que las reconoce como "puerto seguro" (*safe harbor*) para hacerse de los datos[34], en el Perú es la propia LPDP la que facilita, con su vaga referencia a los tratados de los que nuestro país forma parte, la transferencia hacia un territorio donde impera la regla de la "libre circulación de la información".

e.) La LPDP (Art. 15.8) dio carta libre a los reglamentadores para ampliar el elenco de las excepciones a la regla del "nivel de protección adecuado". Y la invitación no ha sido desatendida, pues el Reglamento incorpora a dicho régimen especial a "los datos personales que deriven de una relación científica o profesional del titular y sean necesarios para su desarrollo o cumplimiento". Aparecen nuevamente, pues, y sin el cuidado de mantener la obligación de "disociar" o "anonimizar" los datos, los intereses de laboratorios que escudándose en relaciones "científicas" transfieren a sus matrices en el extranjero bases con información sanitaria.

V. UN PANORAMA PREOCUPANTE

Cuánto quisiera, desde luego, que el cuadro trazado en estos acápites alcance, por lo menos, para suscitar un ánimo reflexivo en las autoridades y funcionarios que próximamente –no bajo este régimen, a lo mejor– tendrán bajo su responsabilidad la aplicación de nuestra normativa de tutela de la autodeterminación informativa. Cuesta creer que ante tantos aspectos funda-

34 Ver: EWING, Mike, "*The Perfect Storm: The Safe Harbor and the Directive on Data Protection*", en "Houston Journal of International Law", vol. 24, 2002, p. 315 y s.

mentales dejados de lado (con indicios de un olvido consciente y dirigido a la salvaguarda de intereses históricamente y abiertamente opuestos a los de los tutelados), la Autoridad Nacional de Protección de Datos Personales emita pronunciamientos candorosos como el difundido a través del portal del Ministerio de Justicia y Derechos Humanos, donde se autoelogia por "haber escuchado a todos los que tenían algo que decir" o por "haber construido un reglamento equilibrado, fruto de un proceso dialogante con quienes tienen algo serio que decir"[35]. Quienes conocen esta materia saben muy bien que en ninguna experiencia comparada, donde haya existido un convencimiento firme e informado en la autodeterminación informativa, se han efectuado concesiones como las brindadas (por mínimas que sean) con la LPDP y su Reglamento a los destinatarios de la regulación.

Pero faltan, y no puedo omitir anotarlo, ulteriores episodios negativos en esta historia: los primeros pronunciamientos de la Autoridad, desde ya condicionada por su visión de "diálogo" en un ámbito donde lo imperativo (puesto que se trata de un derecho fundamental, por más erradas que sean las referencias de la LPDP y el Reglamento a este punto[36]) debe primar; luego, arribarán los pleitos contencioso-administrativos de algún actor descontento con las multas, y por ese camino, estas normas especiales, urgidas de conocimientos técnicos, padecerán la interpretación (tal vez más alineada a la perspectiva constitucional) de la justicia ordinaria; los magistrados, acaso, echarán de menos un régimen especial de responsabilidad civil para la tutela de los perjudicados por las violaciones de la LPDP o su Reglamento[37]; y finalmente, no está descartado que el impredecible Tribunal Constitucional aborde de nuevo la temática, ni que en una eventual ponderación de derechos ante este fuero se termine sometiendo al parecer de sus miembros todo el sistema de protección individual frente a la manipulación de información personal. Porque en el Perú, muy

35 Ver la nota "*Protección de datos personales. Quién, qué y cómo de un reglamento*", del 6 de julio de 2012, en http://www.minjus.gob.pe.

36 La LPDP identifica su "objeto" (artículo 1) en la garantía del "derecho fundamental a la protección de los datos personales, previsto en el artículo 2 numeral 6 de la Constitución Política del Perú, a través de su adecuado tratamiento, en un marco de respeto de los demás derechos fundamentales que en ella se reconocen". La norma de la Carta Política a la que se hace referencia, sin embargo, no tiene ningún vínculo con la autodeterminación informativa. Es una disposición que hace referencia, en realidad, a un particular aspecto del derecho a la intimidad personal y familiar: "a que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar". Esto no es "autodeterminación informativa". Ver: LEÓN, Leysser, *El problema jurídico de la manipulación de información personal*, Palestra, Lima, 2007, p. 325 y s.

Como se aprende a partir de la célebre decisión del Bundesverfassungsgericht de 1983 (citada, retro, nota 8) la autodeterminación informativa está vinculada con la dignidad de la persona, que así se desenvuelve (con autodeterminación) como miembro de una sociedad libre. Su verdadero fundamento, por lo tanto, es el artículo 3 de nuestra Constitución: "la enumeración de los derechos establecidos en este capítulo no excluye los demás que la Constitución garantiza, ni otros de naturaleza análoga o que se fundan en la dignidad del hombre, o en los principios de soberanía del pueblo, del Estado democrático de derecho y de la forma republicana de gobierno".

37 La LPDP contiene una sola, escueta e inútil, referencia a la responsabilidad civil. Es en el artículo 25, subtitulado "derecho a ser indemnizado", donde se establece: "el titular de los datos personales que sea afectado a consecuencia del incumplimiento de la presente Ley por el titular o por el encargado del banco de datos personales o por terceros, tiene derecho a obtener la indemnización correspondiente, conforme a ley". Se remite al Código Civil, por lo tanto. El problema es que nuestros magistrados no van a estar dispuestos a conceder resarcimientos a menos que verifique una "afectación" (daño emergente, lucro cesante, daños morales probados) al titular de los datos personales. En estos casos, por el contrario, estamos ante infracciones que por sí solas constituyen daños in re ipsa, o sea, daños que para ser resarcidos no requieren prueba concreta de los daños sufridos. El Reglamento, que no dispone absolutamente nada acerca de la tutela resarcitoria, ha sido una oportunidad perdida para el desarrollo, en función de la posición de la víctima, de la acción concedida por la LPDP.

a nuestro pesar, se ha olvidado que la autodeterminación informativa tenía que ser vista (y debe seguir siendo vista), en palabras de Stefano Rodotà, como un componente clave de la sociedad igualitaria, como un prerrequisito de inclusión social y como una herramienta imprescindible de defensa frente al establecimiento indeseado de una sociedad basada en el control y la supervisión, en la clasificación y en la selección social[38].

Bibliografía

Bernabei, Federico, *Nuove tecnologie e tutela della riservatezza nei rapporti di lavoro* (tesis), Libera Università Maria Ss. Assunta, Facoltà di Giurisprudenza, Año Académico 2009-2010. Disponible en: http://www.rivista.ssef.it.

Bifulco, Raffaele; Cartabia, Marta; y Alfonso Celotto (al cuidado de), "*L'Europa dei diritti. Commento alla Carta dei Diritti Fondamentali dell'Unione Europea*", Il Mulino, Bologna, 2001.

Ewing, Mike, "*The Perfect Storm: The Safe Harbor and the Directive on Data Protection*", en "Houston Journal of International Law", vol. 24, 2002, p. 315 y s.

Froomkin, A. Michael, "*The Death of Privacy?*", en "Stanford Law Review", vol. 52, 2000, p. 1463 y s.

Hornung, Gerrit y Christoph Schnabel, "*Data Protection in Germany I: The Population Census Decision and the Right to Informational Self-Determination*", en "Computer Law & Security Report", vol. 25, Nº 1, 2009, p. 84 y s.

Lemley, Mark A., "*Private Property*", en "Stanford Law Review", vol. 52, Nº 5, 2000, p. 1545 y s.

León, Leysser, *El problema jurídico de la manipulación de información personal*, Palestra, Lima, 2007.

León, Leysser, "*Manipulación de información personal y derechos fundamentales. Crítica del proyecto de «Ley de protección de datos personales»*", en "Actualidad Jurídica", Nº 210, Lima, 2011.

Litman, Jessica, "*Information Privacy/Information Property*", en "Stanford Law Review", vol. 52, Nº 5, 2000, p. 1283 y s.

Lucas Murillo de la Cueva, Pablo, "*La construcción del derecho a la autodeterminación informativa y las garantías para su efectividad*" (2008), en http://www.fcje.org.es (web de la Fundación Coloquio Jurídico Europeo).

Prieto Gutiérrez, Jesús María, "*Objeto y naturaleza del derecho fundamental a la protec-*

38 RODOTÀ, Stefano, "*Privacy, Freedom, Dignity*", discurso de clausura en la 26ª Conferencia sobre "Privacy and Personal Data Protection", Wroclaw, 16 de septiembre de 2004, en http://26konferencja.giodo.gov.pl. El ilustre autor italiano ejercía, en aquel entonces, la jefatura de la Autorità Garante per la Protezione dei Dati Personali.

ción de datos personales", en "Boletín del Ministerio de Justicia", Año 58, Nº 1973, Madrid, 2004, p. 3119 y s.

Remolina-Angarita, Nelson, "*¿Tiene Colombia un nivel adecuado de protección de datos personales a la luz del estándar europeo?*", en "International Law – Revista Colombiana de Derecho Internacional", vol. 16, 2010, p. 489 y s.

Rodotà, Stefano, "*Privacy, Freedom, Dignity*", discurso de clausura en la 26ª Conferencia sobre "Privacy and Personal Data Protection", Wroclaw, 16 de septiembre de 2004, en http://26konferencja.giodo.gov.pl.

Rodríguez Escanciano, Susana, "*Derecho a la protección de datos personales de los trabajadores como garantía de libertad sindical*" (2011), en http//www.ugt.es.

Schwabe, Jürgen (compilador), *Jurisprudencia del Tribunal Constitucional alemán*, trad. de M. Anzola Gil y E. Maus Ratz, Konrad-Adenauer-Stiftung, Berlín-México, 2009.

Schwartz, Paul M., "*The Computer in German and American Constitutional Law: Towards and American Right of Informational Self-Determination*", en "American Journal of Comparative Law", 1989, vol. 37, p. 675 y s.

Schwartz, Paul M., "*European Data Protection Law and Restrictions on International Data Flows*", en "Iowa Law Review", vol. 80, 1995, p. 471 y s.

Schwartz, Paul M., "*Property, Privacy and Personal Data*", en "Harvard Law Review", vol. 117, Nº 7, 2004, p. 2056 y s.

Schwartz, Paul M., "*Regulating Governmental Data Mining in the United States and Germany: Constitutional Courts, the State and New Technology*", en "William and Mary Law Review", vol. 53, 2011, p. 381 y s.

Serrano Pérez, María Mercedes, "*El derecho fundamental a la protección de datos. Su contenido esencial*", en "Nuevas Políticas Públicas", Nº 1, 2005, p. 245 y s.

Simitis, Spiros, "*Reconsidering the Premises of Labour Law: Prolegomena to an EU Regulation of the Protection of Employees' Personal Data*", en "European Law Journal", vol. 5, 1999, p. 45 y s.

Taylor, Mark J., "*Health Research, Data Protection, and the Public Interest in Notification*", en "Medical Law Review", vol. 19, 2011, p. 267 y s.

Tesauro, Giuseppe, "*Competizione economica: i vantaggi della protezione dei dati*", en GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Da costo a risorsa: la tutela dei dati personali nelle attività produttive*, al cuidado de G. Rasi, Istituto Poligrafico e Zecca dello Stato, Roma, 2004.

Troncoso Reigada, Antonio, "*El desarrollo de la protección de datos personales en Iberoamérica desde una perspectiva compara-*

da y el reequilibrio de los modelos de protección de datos a nivel internacional", en "Revista de la Red Académica Internacional de Protección de Datos Personales", Nº 1, 2012.

VANWANSSHNOVA, Matthew R., "*Data Protection Conflicts Between the United States and the European Union in the War of Terror: Lessons Learned from the Existing Sytem of Financial Information Exchange*", en "Case Western Reserve Journal of International Law", vol. 39, 2008, p. 827 y s.

WHITMAN, James Q., "*The Two Western Cultures of Privacy: Dignity versus Liberty*", en "Yale Law Journal", vol. 113, Nº 6, p. 1151 y s.