
**RED ACADÉMICA INTERNACIONAL DE
PROTECCIÓN DE DATOS PERSONALES**

Revista Internacional de Protección de Datos Personales

RIPDP

PRESENTACIÓN

ANTONIO TRONCOSO REIGADA

Universidad de los Andes. Facultad de Derecho (Bogotá, Colombia)

No. 1 Julio - Diciembre de 2012. ISSN: 2322-9705

Es un motivo de alegría tener la oportunidad de presentar la *Revista Internacional de Protección de Datos Personales (RIPDP)*, una iniciativa de la Red Académica Internacional de Protección de Datos Personales. Esta Red es un proyecto auspiciado por la Comisión de Transparencia y Acceso a la Información del Estado de Nuevo León (México), que organizó un evento junto con la Universidad Autónoma de Nuevo León en octubre del 2010, marco institucional donde se constituyó esta Red. Por ello, es de justicia hacer un primer reconocimiento a sus Presidentes Honoríficos, Sergio Moncayo (CTAI) y Jesús Ancer Rodríguez (UNAM), quienes con su generosidad han permitido ponerla en funcionamiento. Como es sabido, son miembros fundadores: Oscar R. Puccinelli (Argentina), Nelson Remolina Angarita (Colombia), Alfredo Chirino Sánchez (Costa Rica), Antonio A. Martino (Italia), Ricardo Cantú Aguillén y Lina Ornelas Núñez (México), María de Lourdes Zamudio Salinas (Perú), Marcelo Bauzá Reilly (Uruguay) y Ana Brian Nougrères (Uruguay).

Es objetivo de la Red Académica Internacional de Protección de Datos Personales la difusión, colaboración, elaboración y mejora de normativas adecuadas y pertinentes de protección de datos personales a nivel internacional, promoviendo la celebración de eventos y publicaciones académicas de expertos y expertas de todo el mundo. Dentro de este marco se inscribe la iniciativa de poner en marcha la *Revista Académica Internacional de Protección de Datos*.

Quiero también reconocer el esfuerzo del Presidente Ejecutivo de la Red, Ricardo Cantú Aguillén y de su Secretario Académico, Nelson Remolina

Angarita, profesor de la Facultad de Derecho de la Universidad de los Andes (Bogotá, Colombia), para poner en marcha esta publicación que, estoy convencido, va a contribuir al fomento de la investigación académica sobre el derecho fundamental a la protección de datos personales y será un referente más en el estudio de este tema en el mundo. Las importantes y continuas novedades legislativas y jurisprudenciales sobre la protección de datos personales justifican la existencia de un medio académico que permita la difusión de trabajos científicos, esté abierto a todas las personas estudiosas y conocedoras de esta materia y sea un ámbito donde se puedan recoger las distintas perspectivas sobre protección de datos personales.

Aprovecho la oportunidad que me brinda la presentación de esta Revista, que sin duda se centrará en el análisis del ordenamiento jurídico de protección de datos personales, para resaltar la importancia de la autorregulación, algo a lo que también ha hecho una referencia extensa la propuesta de la Comisión Europea de Reglamento General de Protección de datos¹. Los regímenes normativos pueden resultar insuficientes cuando los datos personales se difunden por todo el mundo a través de las redes de TIC y en su tratamiento intervienen varias jurisdicciones, a menudo fuera de la Unión Europea. Así,

1 La Comisión Europea está impulsando la configuración de un nuevo marco jurídico europeo para la protección de los datos personales, a través de la aprobación el 25 de enero de 2012 de una Propuesta de Reglamento del Parlamento Europeo y del Consejo, relativo a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y a la libre circulación de estos datos —un Reglamento general de protección de datos—, que derogará la actual Directiva 95/46/CE - COM (2012) 10 final. Cfr. también la Comunicación de la Comisión “La protección de la privacidad en un mundo interconectado. Un Marco Europeo de Protección de Datos para el siglo XXI”, COM (2012) 9 final.

la *Resolución de Estándares Internacionales sobre Protección de Datos Personales y Privacidad*, también conocida como Resolución de Madrid² ha resaltado el importante papel que la autorregulación puede jugar a estos efectos³. Igualmente, la Comisión Europea entiende que es necesaria la utilización de las propias tecnologías como aliadas para favorecer el respeto a este derecho, a través de la implantación de las llamadas tecnologías de protección de la privacidad –PET–⁴. Con estas iniciativas se trata de alcanzar sinergias con la industria para que esta proporcione equipos y software que permitan el cumplimiento de la legislación de protección de datos personales. Para la Comisión Europea, si bien “la responsabilidad jurídica del

cumplimiento de las normas de protección de datos personales recae en los responsables de su tratamiento, desde el punto de vista social y ético también recae en parte, por ejemplo, en quienes elaboran las especificaciones técnicas y quienes realmente desarrollan o ejecutan programas o sistemas operativos”.

Tanto la Comisión Europea como las autoridades de protección de datos están convencidas de que la mejora del nivel de cumplimiento del derecho fundamental a la protección de datos personales pasa por una labor de promoción que trate de poner este derecho fundamental en positivo. Así, frente a una cierta prevalencia de una imagen negativa de la protección de datos personales –con mensajes como el de que nadie cumple esta legislación–, es necesario lanzar una idea positiva de la protección de datos personales involucrando al propio sector, como por ejemplo, a través de la aprobación de Códigos de Conducta⁵ o el establecimiento de un modelo de certificación en privacidad para productos y servicios⁶. La defensa de la priva-

2 La Resolución de Estándares Internacionales fue aprobada en la Conferencia Internacional de Autoridades de Protección de Datos y Privacidad, celebrada en Madrid el 5 de noviembre del 2009.

3 Así, la propia Resolución de Madrid contiene un conjunto de medidas proactivas entre las que están “la adhesión a acuerdos de autorregulación cuya observancia resulte vinculante, que contengan elementos que permitan medir sus niveles de eficacia en cuanto al cumplimiento y grado de protección de los datos de carácter personal y establezcan medidas efectivas en caso de incumplimiento” (art. 22).

4 Las PET son “un sistema coherente de medidas de TIC que protege el derecho a la intimidad suprimiendo o reduciendo los datos personales o evitando el tratamiento innecesario o indeseado de datos personales, sin menoscabo de la funcionalidad del sistema de información”. La propia Directiva 2002/58/CE establece que “cuando proceda, se podrán adoptar medidas para garantizar que los equipos terminales estén fabricados de maneja compatible con el derecho de los usuarios de proteger y controlar el uso de sus datos personales” (art. 14.3). Cfr. *Comunicación de la Comisión al Parlamento Europeo y al Consejo sobre el fomento de la protección de datos mediante las tecnologías de protección del derecho a la intimidad (PET)*. Así, “gracias a dichas tecnologías, las infracciones de las normas de protección de datos y la vulneración de los derechos del ciudadano, además de estar prohibidas y sujetas a sanciones, resultarían más difíciles desde el punto de vista técnico”. Esta Comunicación de la Comisión es consecuencia del Primer informe sobre la aplicación de la Directiva sobre protección de datos y enlaza con la Comunicación de la Comisión *Una estrategia para una sociedad de la información segura* [COM (2006) 251 final, de 31 de mayo de 2006], donde se invitaba al sector privado a «estimular el despliegue de productos, procesos y servicios que favorezcan la seguridad a fin de evitar y combatir la sustracción de la identidad y otros ataques contra la privacidad». Con esta Comunicación, la Comisión trata de fomentar la utilización de las PET por parte de los responsables del tratamiento de datos y los consumidores.

5 Estos códigos tipo están previstos en la Directiva 95/46/CE (arts. 27-28), en la LOPD (art. 32) y han tenido un impulso en el RPDP (arts. 71-78), que ha previsto incluso garantías para su cumplimiento a través de órganos de supervisión independientes y de la imposición de sanciones.

6 Así, hay que señalar que la propia Comisión Europea ha incidido en la necesidad de “un sistema europeo de distintivos de protección de la intimidad, que incluiría asimismo un análisis de las repercusiones económicas y sociales. Gracias a dichos distintivos, los consumidores podrían reconocer fácilmente los productos que cumplen o favorecen el cumplimiento de las normas de protección de datos en el tratamiento de éstos, en concreto mediante la aplicación de PET apropiadas”. Cfr. también la *Comunicación de la Comisión al Parlamento Europeo y al Consejo sobre el fomento de la protección de datos mediante las tecnologías de protección del derecho a la intimidad (PET)* COM (2007) 228 final, de 2.5.2007, disponible en <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0228:FIN:ES:PDF>

La *Commission Nationale de l'Informatique et de Libertés* de Francia ha puesto en marcha una certificación en privacidad, algo

cidad se muestra, de esta manera, como una oportunidad de negocio y una ventaja competitiva para las empresas. Además, en relación con el funcionamiento de la economía, un sistema de certificación europeo en privacidad facilita los intercambios comerciales entre los distintos países, creando nuevas oportunidades de mercado. Obviamente, la generalización de un modelo de certificación obliga a resolver cuestiones como la configuración de la autoridad que valide las evaluaciones realizadas por los expertos o la acreditación de los expertos jurídicos y técnicos que realicen las evaluaciones —haciendo posible la obtención por su parte de un legítimo beneficio pero evitando su captura por parte de empresas—. Es razonable una cierta implicación de las autoridades de protección de datos dentro de un modelo de certificación —en la definición de reglas y procedimientos pertinentes y en la supervisión del funcionamiento del mismo—, siendo importante no confundir los reguladores con los regulados —la autoridad de control son las agencias de protección de datos; la autoridad de certificación y las empresas de auditoría son sectores regulados y sometidos a control—⁷.

que exigía su legislación. Hay que destacar el *Proyecto EuroPriSe*, que trataba de poner las bases para el establecimiento de un sello europeo de privacidad para productos y servicios de tecnologías de la información en los sectores público y privado, que fue financiado por la Comisión Europea a través del programa eTEN. El Supervisor Europeo de Protección de Datos destacó en su Informe anual de 2008 la importancia del proyecto *EuroPriSe*. Cfr. *Annual Report 2008*, del Supervisor Europeo de Protección de Datos, pág. 85 en http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Annualreport/2008/AR2008_EN.pdf Sobre *EuroPriSe*, cfr. más ampliamente *Privacy Law & Business*, Newsletter núm. 35, febrero, 2008, págs. 12-15. Cfr. también la información que obra en www.european-privacy-seal.eu/

7 La Comisión Europea insiste en que las autoridades de protección de datos deben formar parte de grupos que se encarguen de analizar la evolución de la tecnología, detectar los peligros que plantea en relación con los derechos fundamentales y la protección de datos personales y definir los requisitos técnicos para hacerles frente. Cfr.

La propuesta de Reglamento general de protección de datos que presenta la Comisión no solo ha avanzado en esta apuesta por la autorregulación, sino que ha convertido muchas de estas medidas en obligaciones del responsable del tratamiento. Así, señala claramente que la protección de datos personales debe ser tenida en cuenta en el diseño del sistema de información —la llamada “privacidad en el diseño”, *privacy by design*—, fijando para ello obligaciones para el responsable —tanto en el momento de la determinación de los medios de tratamiento, como en el tratamiento propiamente dicho— de implementar medidas y procedimientos técnicos y organizativos apropiados que garanticen la protección de los datos personales (art. 23). Además señala que la protección de datos debe ser una opción por defecto —la llamada “privacidad por defecto”—, que se materializa en la obligación del responsable del tratamiento de establecer mecanismos que permitan que, por configuración inicial, solo sean objeto de tratamiento los datos necesarios para cada fin específico, de manera que no se recojan ni se conserven datos más allá del mínimo necesario para los fines, tanto en lo que respecta a la cantidad de los datos como a la duración de su conservación, estableciéndose, asimismo, mecanismos que garanticen que, por defecto, los datos personales no sean accesibles a un número indeterminado

Comunicación de la Comisión al Parlamento Europeo y al Consejo sobre el fomento de la protección de datos mediante las tecnologías de protección del derecho a la intimidad (PET), ya citada. Una de las cuestiones a resolver, también dentro del ámbito de la autorregulación, es la definición del parámetro utilizado para evaluar los productos por los expertos acreditados. Este parámetro para la evaluación debía ser hasta ahora, lógicamente, la Directiva 95/46/CE, pero esta ha sido transpuesta de manera diferente en los distintos países, persistiendo divergencias y faltas de armonización a nivel europeo.

de personas⁸. De esta forma, no recae sobre el usuario la selección inicial de las medidas de privacidad, sino que esta viene ya configurada por defecto⁹. La propuesta de Reglamento también defiende los Códigos de Conducta (art. 38), que están destinados a contribuir a la aplicación del Reglamento en sectores de tratamiento específicos y en los que deben implicarse tanto los Estados miembros como las autoridades de control y la propia Comisión¹⁰. Buena muestra de esta apuesta por la autorregulación es que los Códigos de Conducta pueden incluir otros procedimientos extrajudiciales y de resolución de conflictos, que permitan resolver las controversias entre los responsables y los interesados, pero todo ello debe ser sin perjuicio de los dere-

chos de los interesados y de su posibilidad de acudir a las autoridades de control. La propuesta de Reglamento también establece que la Comisión y los Estados miembros promoverán la creación de mecanismos de certificación y de sellos en materia de protección de datos que permitan a los interesados evaluar rápidamente el nivel de protección de datos que ofrecen los responsables y los encargados del tratamiento (art. 39). Estas medidas, junto con otras como la realización de informes de impacto en la protección de datos personales, la implementación de mecanismos de verificación y auditoría de carácter jurídico o la designación de un delegado de protección de datos, que dejan de ser iniciativas de autorregulación para convertirse en la propuesta de Reglamento en obligaciones del responsable, tratan de introducir la protección de datos dentro de la responsabilidad empresarial, convirtiendo a las empresas en un elemento estratégico del sistema de garantías del derecho a la protección de datos personales, que haga compatible el uso intensivo de las tecnologías y el tratamiento de datos personales necesarios para el funcionamiento global de la economía con el respeto a la privacidad de los usuarios y de los empleados.

8 La Resolución de Madrid de Estándares Internacionales de 2009, como hemos señalado antes, apostó también por medidas proactivas en defensa de la privacidad. Pero fue sobre todo la XXXII Conferencia Internacional de Autoridades de Protección de Datos, celebrada en Israel en el año 2010, la que adoptó una Resolución en la que se reconoce a la privacidad por diseño —y, dentro de ella, a la privacidad por defecto— como un elemento fundamental, instando a las Autoridades de Control a promover su implantación. Así, se materializa una preocupación porque el software se desarrolle desde el principio teniendo en cuenta las exigencias en materia de privacidad y las principales amenazas, y que la privacidad también sea un factor a tener en cuenta en el diseño de los servicios y procesos dentro de las empresas.

9 La privacidad por defecto en las redes sociales, en lo que respecta al nivel de acceso a la página personal, ha sido analizado por TRONCOSO REIGADA en *La protección de datos personales. En busca del equilibrio*, Tirant Lo Blanch, Valencia, 2010. Otro supuesto es el relativo a las *cookies*. En la actualidad, la configuración por defecto de tres de los cuatro navegadores más utilizados está predeterminada para aceptar todas las *cookies*, obligando al usuario a modificar la configuración inicial si desea bloquearlas. Recientemente *Google+* ha lanzado una nueva función para los usuarios de la red social, de forma que todos los que tengan una cuenta y utilicen el servicio de *Google Contact* para gestionar su libreta de direcciones puedan ver la información de sus contactos desde su perfil de la red social, integrándola dentro de la misma. No obstante, en este caso esta información solo puede ser vista de forma privada por el usuario y no será un dato al que tengan acceso sus contactos de *Google+*.

10 La regulación de estos Códigos de Conducta en la propuesta de Reglamento incluye referencias novedosas al tratamiento equitativo y transparente, a la información al público, a la protección de los niños y a los mecanismos de supervisión y garantía —que toma de nuestro RPDP—.

Antonio Troncoso Reigada

Presidente Emérito de la Red 2011-2015

Miembro Fundador

