Papeles el tiempo de los derechos

LA CERTIFICACIÓN EN EL NUEVO REGLAMENTO EUROPEO DE PROTECCIÓN DE DATOS Y ANTEPROYECTO DE LEY ORGÁNICA DE PROTECCIÓN DE DATOS

Jorge Viguri Cordero

Palabras clave: Certificación, estándares, RGPD, ALOPD.

Número: 11 Año: 2018

ISSN: 1989-8797

Comité Evaluador de los Working Papers “El Tiempo de los Derechos”

María José Añón (Universidad de Valencia)
María del Carmen Barranco (Universidad Carlos III)
María José Bernuz (Universidad de Zaragoza)
Manuel Calvo García (Universidad de Zaragoza)
Rafael de Asís (Universidad Carlos III)
Eusebio Fernández (Universidad Carlos III)
Andrés García Inda (Universidad de Zaragoza)
Cristina García Pascual (Universidad de Valencia)
Isabel Garrido (Universidad de Alcalá)
María José González Ordovás (Universidad de Zaragoza)
Jesús Ignacio Martínez García (Universidad of Cantabria)
Antonio E Pérez Luño (Universidad de Sevilla)
Miguel Revenga (Universidad de Cádiz)
Maria Eugenia Rodríguez Palop (Universidad Carlos III)
Eduardo Ruiz Vieytez (Universidad de Deusto)
Jaume Saura (Instituto de Derechos Humanos de Cataluña)

LA CERTIFICACIÓN EN EL NUEVO REGLAMENTO EUROPEO DE PROTECCIÓN DE DATOS Y ANTEPROYECTO DE LEY ORGÁNICA DE PROTECCIÓN DE DATOS.

Jorge Viguri Cordero

1. Introducción

El rápido desarrollo de las tecnologías en los últimos años a raíz de la globalización ha hecho posible que las organizaciones tengan amplias facultades para recopilar, procesar y compartir datos personales. Si bien es cierto que el auge de las nuevas tecnologías y servicios benefician tanto a las organizaciones, consumidores y usuarios como a la sociedad en su conjunto, no es menos cierto que el tratamiento de los datos personales son susceptibles de ser empleados para una multitud de fines (marketing, servicios personalizados, etc.), lo que evidencia los nuevos y mayores desafíos para la privacidad y protección de datos de los beneficiarios de los servicios. Estos retos inciden directamente en la falta de confianza generalizada de los usuarios[1], obstaculizando el desarrollo en el empleo de las citadas tecnologías.

Las cuestiones de privacidad y protección de datos se refieren a una amplia gama de aspectos de las operaciones técnicas, incluida la disponibilidad y la integridad de los servicios y datos, la confidencialidad, la certificación, la auditoría, etc. y su aplicación ha adquirido especial relevancia con el Reglamento General de Protección de Datos (RGPD), que no sólo contiene actualizaciones de los principios y disposiciones de la Directiva 95/46/CE de protección de datos (Directiva de protección de datos), sino que introduce sustanciales novedades en el tratamiento de los datos personales con objeto de responder a los desafíos que en la actualidad se presentan.

Una de esas novedades es la referencia explícita a la importancia de las iniciativas de los mecanismos de certificación, sellos y marcas en relación con la protección de datos, pues se enmarca la certificación como uno de los ejes vertebrales del sistema. Estos instrumentos fomentan la transparencia y el cumplimiento con el RGPD, pues permiten a las partes interesadas evaluar rápidamente el nivel de protección de los productos y sistemas respecto al citado Reglamento. Ahora bien, la experiencia nos

[1] Reding, V.,"The upcoming data protection reform for the European Union International Data Privacy Law", *International Data Privacy Law*, vol. 1, nº 1, 2011, pp. 3–5.

lleva a poner de manifiesto que éstos han tendido a focalizarse en garantizar una mayor eficiencia y eficacia de los procesos de tratamiento de datos en detrimento de su objeto principal, esto es, garantizar un nivel alto y por ende adecuado en la protección efectiva de los derechos humanos[2].

En este sentido, el RGPD[3] eleva las garantías de protección de datos mediante la inclusión de novedades sustanciales para hacer frente a estos problemas, enmarcándose como una de las piedras angulares para las operaciones de tratamiento de datos en el marco europeo de protección de datos.

El objeto de la presente comunicación se centra en el análisis del funcionamiento de los mecanismos de certificación en el nuevo RGPD y su coherencia con la nueva normativa española. A este respecto, se examinará el desarrollo legislativo de la certificación en la UE, el nuevo enfoque de la certificación a la luz del RGPD (tanto el concepto de la certificación como su naturaleza jurídica y su aproximación hacia un mecanismo voluntario a la par que necesario). Por otra parte, se llevará a cabo un estudio del alcance de la certificación en el RGPD y el Anteproyecto de Ley Orgánica de Protección de Datos (ALOPD) para finalizar con una serie de conclusiones al respecto.

2. Desarrollo legislativo de la certificación en la UE

En 1999, se inició del desarrollo de estándares técnicos aplicables al desarrollo de la normativa de protección de datos, cuando la Comisión Europea (CE), a través del CEN/ISSS[4], estableció la Iniciativa para la Normalización de la Privacidad en Europa (IPSE), tras el fracaso intento de apoyo por parte de la industria. La constitución de esta Iniciativa promovió el desarrollo de la normalización de la legislación europea de protección de datos constituyendo así, el primer hito hacia esa dirección[5].

Ahora bien, fue en este punto donde comenzó a explotarse la creación e implementación de los estándares en materia de certificación desde un enfoque puramente técnico. De hecho, en el ámbito de protección de datos, no fue hasta 2006

[2] De Hert, P., Papakonstantinou, V., "Three scenarios for international governance of data privacy: Towards an international data privacy organization, preferably a UN agency", *Journal of Law and Policy*, vol. 9, nº 2, 2013, p. 271-295.

[3] El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, OJ L 119, 4.5.2016, pp. 1–88

[4] En 1997, se creó el CEN/ISSS (Sistema de Normalización de la Sociedad de la Información) por el CEN (Comité Europeo de Normalización) como foco para sus actividades de las TIC (Tecnologías de la información y de la Comunicación). Más información http://ec.europa.eu/idabc/en/document/6990.html accedido el 9 de octubre de 2017.

[5] Dumortier, J., Goemans, C., "Online data privacy and standardization: towards a more effective protection?", en J. Dumortier e.a. (eds.), *A decade of research at the crossroads of law and ICT*, Larcier, Bruselas, nº 53, 2001, p. 69.

cuando la CE comenzó a apostar decididamente por los mecanismos de certificación[6] muy probablemente por el hecho de que la Directiva de protección de datos[7] no hacía referencia específica a los estándares técnicos, sino que se limitaba a establecer meras obligaciones a los responsables del tratamiento de datos[8]. A raíz de esa vertiente eminentemente técnica, fue la Directiva de procedimiento de información en materia de las normas y reglamentaciones técnicas[9] la que definió por primera vez este elemento en el apartado 6º del artículo 1 como *"una especificación técnica aprobada por un organismo reconocido de actividad normativa para aplicación repetida o continua, cuya observancia no es obligatoria (...)"*. Por ello, la incorporación de los estándares técnicos ha estado siempre más orientada hacia los criterios que prestan los servicios de la sociedad de la información en detrimento de su regulación legal en el ámbito de la protección de datos personales.

[6] Comisión Europea, Comunicación de la Comisión al Consejo, Parlamento Europeo y Comité Económico y Social y el Comité de las Regiones, Una estrategia para una sociedad de la información segura - Diálogo, asociación y potenciación»", COM (2006) 251 final, Bruselas 31 de mayo, 2006 y Comisión Europea, 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. Bruselas, 2 de Mayo de 2007.

[7] Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, OJ L 281, 23.11.1995, pp. 31–50.

[8] A tal efecto, el Considerando 46 de la Directiva menciona la importancia de la adopción de medidas técnicas con objeto de garantizar la seguridad y de este modo, prevenir todo tratamiento no automatizado. Para ello, subraya que las citadas medidas deberán ser adecuadas teniendo en cuenta el estado de la técnica y el coste de su aplicación en relación con los riesgos que presente el tratamiento y con la naturaleza de los datos que deban protegerse. Del mismo modo, el art. 17 regula la seguridad del tratamiento al establecer en su apartado 1º lo siguiente*: "el responsable del tratamiento de aplicar las medidas técnicas y de organización adecuadas, para la protección de los datos personales contra la destrucción, accidental o ilícita, la perdida accidental y contra la alteración, la difusión o el acceso no autorizados, en particular cuando el tratamiento incluya la transmisión de datos dentro de una red, y contra cualquier otro tratamiento ilícito de datos personales. Dichas medidas deberán garantizar, habida cuenta de los conocimientos técnicos existentes y del coste de su aplicación, un nivel de seguridad apropiado en relación con los riesgos que presente el tratamiento y con la naturaleza de los datos que deban protegerse"*.

[9] Directiva (UE) 98/34/CE del Parlamento Europeo y del Consejo, por la que se establece un procedimiento de información en materia de las normas y reglamentaciones técnicas y de las reglas relativas a los servicios de la sociedad de la información, OJ L 204, 21 de julio de 1998, pp. 37–48, sustituida por la actual Directiva (UE) 2015/1535 del Parlamento Europeo y del Consejo, de 9 de septiembre de 2015, por la que se establece un procedimiento de información en materia de reglamentaciones técnicas y de reglas relativas a los servicios de la sociedad de la información, OJ L 241, 17 de septiembre 2015, pp. 1–15.

Sin embargo, el punto de inflexión en esta materia se produjo en 2010, cuando la CE encomendó un Estudio[10] en el que se avaluaron los desafíos causados por los desarrollos tecnológicos y que incidían directamente en cuestiones sobre privacidad. En el citado Estudio se arrojaron conclusiones relevantes en relación con la Directiva de protección de datos, pues ésta no exigía una aprobación formal de dichos códigos dentro de los sistemas jurídicos de los Estados miembros, lo que indirectamente implicaba divergencias considerables en cada uno de ellos [por ejemplo, en los Países Bajos, la "aprobación" de un código por la Autoridad de Protección de Datos (APD) no obligaba a los tribunales, mientras que en Irlanda, éstos podían integrarse formalmente en el régimen jurídico y convertirse en jurídicamente vinculantes][11]. Además, la CE comenzó a examinar los medios de fomentar aún más las iniciativas de autorregulación y a estudiar la viabilidad de establecer sistemas de certificación de la UE en el ámbito de la protección de datos[12].

Por otro lado, en el mismo año, el Parlamento Europeo (PE) solicitó a la CE que explorara los distintos medios a escala comunitaria y comprobara las posibilidades técnicas de garantizar la aplicación del proyecto del Sello Europeo de Privacidad, un mecanismo que certificaba el cumplimiento de la legislación de protección de datos de las páginas web[13]. Además, el Grupo de Trabajo del Artículo 29 también llevó a cabo una función de fomento de los mecanismos de certificación, sobre todo con objeto de otorgar una mayor ventaja competitiva[14].

Ahora bien, es el actual RGPD el que otorga verdadera naturaleza jurídica a la certificación, pues se articula como elemento clave y necesario para garantizar de forma efectiva la protección de los datos personales. En efecto, la certificación adquiere gran importancia ya no solo para garantizar el cumplimiento del RGPD en toda su extensión, sino para prevenir posibles violaciones en la privacidad de los sujetos.

No cabe duda que la política europea y las crecientes iniciativas legales en materia de privacidad y protección de datos se encaminan hacia el empleo de mecanismos de certificación ante la imposibilidad de que el ordenamiento jurídico puesta adaptarse

---

[10] Comisión Europea, *Estudio comparativo sobre diferentes enfoques de nuevos desafíos de privacidad*, en particular a la luz de los desarrollos tecnológicos, Informe Final, 20 de enero de 2010. http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf. Accedido el 13 de octubre de 2017.

[11] Comisión Europea, *Estudio comparativo sobre diferentes enfoques*..., *ob. cit*, p. 52.

[12] Comisión Europea, Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social y al Comité de las Regiones, *Un enfoque global de la protección de los datos personales en la Unión Europea,* COM(2010) 609 final, Bruselas, 4 de noviembre de 2010, p. 13.

[13] Parlamento Europeo, *Resolución sobre los efectos de la publicidad en el comportamiento de los consumidores* (2010/2052), 15 de diciembre de 2010. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2010-0484+0+DOC+XML+V0//ES. Accedido el 11 de octubre de 2017.

[14] Grupo de trabajo del artículo 29, *Opinión 3/2010 sobre el Principio de Responsabilidad*, WP 173, 13 de julio de 2010, p.17. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp173_en.pdf. Accedido el 8 de octubre de 2017.

eficazmente a una realidad dinámica y cambiante. No obstante, estos mecanismos operan actualmente en un ambiente de autorregulación y enfrentan problemas estructurales como falta de conocimiento del usuario, su potencial engañoso, la falta de supervisión reglamentaria y de armonización, el posible uso indebido de terceros así como el conflicto de intereses que pueden darse en la práctica[15].

Como veremos a continuación, pese a que en sentido estricto la certificación se encuadra como mecanismo voluntario, el RGPD prioriza en la adopción de medidas preventivas para evitar menoscabos en la privacidad de los sujetos, asegurando asimismo la seguridad y la portabilidad de los datos y evitar -o cuanto menos, reducir-, las sustanciales sanciones previstas.

3. La certificación en el nuevo RGPD

Los mecanismos de certificación en el ámbito de la protección de datos han adquirido especial popularidad en los últimos años[16] y no cabe duda que su éxito radica en el desarrollo tecnológico constante, pues requiere de continua y eficiente a esos cambios tecnológicos para garantizar el cumplimiento de la legislación de protección de datos desde un modo preventivo o proactivo[17].

---

[15] Rodrigues, R., Wright, D., Wadhwa, K., "Developing a privacy seal scheme (that works)", *International Data Privacy Law*, vol 3, nº 2, 2013, p.17.

[16] El mercado actual de mecanismos de certificación en materia de privacidad es heterogéneo pues se encuentran multitud de ellos operando a nivel comunitario. A modo de ejemplo, conviene destacar los principales sellos de certificación en materia de protección de datos en los últimos años: EuroPriSe (European privacy Seal), TRUSTe, TUV privacy seal, CNIL label o PrivacyMark System. La experiencia práctica de estos mecanismos ha evidenciado diversos problemas de enorme calado. Por un lado, la adhesión de una organización a un mecanismo de certificación no ha asegurado *per se* un alto nivel de protección. Por otro lado, a diferencia de otros ámbitos, los usuarios no suelen leer en detalle las políticas de privacidad que prevé el mecanismo de certificación, generando indiferencia en la práctica.

Además, se han abordado otros problemas estructurales en la implementación de los sellos de privacidad, tales como la falta de disponibilidad y fácil acceso a la información, la dificultad para encontrar criterios o requisitos específicos para su adjudicación, la falta de respuesta a las solicitudes de información, la necesidad de confiar en información de ostras partes, las barreras del idioma o la no disponibilidad de ciertos esquemas de certificación. En este sentido, véase: Rodrigues, R., Barnard-Wills, D., Wright, D., de Hert, P., Papakonstantinou, V., *EU Privacy seals project, Inventory and Analysis of Privacy Certification Schemes: Final Report Study* Deliverable 1.4, Comisión Europea. Luxemburgo: Oficina de publicaciones de la Unión Europea, 2013, pp. 29-31. El documento se encuentra disponible en el siguiente enlace: http://www.vub.ac.be/LSTS/pub/Dehert/481.pdf. Accedido el 11 de octubre de 2017.

[17] La certificación al igual que la privacidad desde el diseño (Privacy by Design) o la privacidad por defecto (Privacy by Default) son ejemplos de medidas para garantizar el cumplimiento efectivo del RGPD desde un enfoque puramente proactivo. Por lo que respecta a estos dos últimos, vienen regulados en el artículo 25 del RGPD. Con arreglo a este artículo, se requiere que un responsable del tratamiento de datos aplique las medidas técnicas y organizativas adecuadas tanto en el momento de la determinación de los medios de tratamiento como en el momento del tratamiento, a fin de garantizar el cumplimiento de los

Con la obligatoria aplicación del nuevo RGPD el próximo 25 de mayo de 2018, la certificación en materia de protección de datos será una disciplina necesaria para reforzar los derechos de protección de datos de las personas, facilitar la libre circulación de datos personales en el mercado único digital y reducir la carga administrativa. De hecho, con objeto de aumentar la transparencia y el cumplimiento del RGPD, el Considerando 100[18] apuesta por el establecimiento de mecanismos de certificación y sellos y marcas de protección de datos que permitan a los interesados evaluar rápidamente el nivel de protección de datos de productos y servicios pertinentes.

Ahora bien, debemos esperar durante 2017 y 2018 para que, precisamente antes de la aplicación del RGPD, se proporcionen por parte de las autoridades de control y demás partes interesadas una importante actividad de mejora de los códigos de conducta y certificaciones actuales que supongan el verdadero *boom* necesario en la creación de nuevos mecanismos que permitan la consecución de los objetivos del RGPD.

3.1. El concepto de certificación. Una aproximación entre la certificación de normas de protección de datos vs. estándares técnicos.

Uno de los principales retos a los que se enfrenta la certificación es su enorme amplitud pues no se trata de un concepto jurídico en sentido estricto ni tampoco un concepto eminentemente técnico, pues resulta obvia su regulación en el nuevo RGPD.

Por todo ello, conviene analizar la naturaleza de estos mecanismos para poder entender mejor el potencial alcance que tendrán en un futuro.

La primera cuestión que conviene analizar es la definición de la norma susceptible de ser certificada. En este sentido, el Reglamento Europeo sobre la normalización europea[19] definió por primera vez norma desde el punto de visto de la certificación en el apartado 1º del artículo 2º como *"la especificación técnica adoptada por un organismo de normalización reconocido, de aplicación repetida o continua, cuya observancia no es obligatoria, y que reviste diversas formas: a) «norma internacional»: norma adoptada por un organismo internacional de normalización; b) «norma europea»:*

---

principios de protección de datos. Cualquier medida de privacidad mediante medidas de diseño puede incluir, por ejemplo, la certificación como técnica para garantizar el cumplimiento preventivo o proactivo del RGPD.

[18] El Considerando 100 RGPD estipula lo siguiente: *"A fin de aumentar la transparencia y el cumplimiento del presente Reglamento, debe fomentarse el establecimiento de mecanismos de certificación y sellos y marcas de protección de datos, que permitan a los interesados evaluar con mayor rapidez el nivel de protección de datos de los productos y servicios correspondientes"*

[19] Reglamento (UE) nº 1025/2012 del Parlamento Europeo y del Consejo de 25 de octubre de 2012 sobre la normalización europea, por el que se modifican las Directivas 89/686/CEE y 93/15/CEE del Consejo y las Directivas 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE y 2009/105/CE del Parlamento Europeo y del Consejo y por el que se deroga la Decisión 87/95/CEE del Consejo y la Decisión nº1673/2006/CE del Parlamento Europeo y del Consejo, DOUE núm. 316, de 14 de noviembre de 2012, pp. 12 a 33.

norma adoptada por una organización europea de normalización; c) «norma armonizada»: norma europea adoptada a raíz de una petición de la Comisión para la aplicación de la legislación de armonización de la Unión y d) «norma nacional»: norma adoptada por un organismo nacional de normalización".

Este concepto, al que el presente artículo denomina como estándar con objeto de diferenciarlo de una norma jurídica vinculante, ha sido posteriormente desarrollado en la reciente Directiva sobre ciberseguridad o NIS (Network Information Security)[20], lo que evidencia la *vis atractiva* de los estándares o normas técnicas en su vertiente técnica.

A mi juicio, hasta este punto resultaba más conveniente la denominación de estándares técnicos en lugar de normas técnicas, no ya porque gozaran de mayor *vis atractiva* al tratarse eminentemente de meras iniciativas de autorregulación sectoriales, sino también por su carácter potestativo y porque excedía de cualquier criterio estricto establecido en los textos legales. Ahora bien, junto con estos criterios, coexiste una nueva exigencia que más allá de la mera voluntariedad (recordemos que una vez la organización se someta a ellos, le resultarán vinculantes en toda su extensión)[21] y que a todas luces exceden del simple compromiso con la privacidad, pues se espera que los nuevos mecanismos contemplen una protección integral de varias dimensiones (jurídicas, técnicas, seguridad, sociales, etc.).

La certificación en materia de privacidad y protección de datos comenzaron a promoverse precisamente para dotar de una mayor transparencia al funcionamiento interno de una organización, pues muchas de ellas operaban con multitud de datos personales y los usuarios desconocían el uso que se hacía de los mismos. Es por ello por lo que se articulaba como un procedimiento para garantizar el cumplimiento de los requisitos específicos en materia de seguridad[22]. Con ello, el principal objetivo fue aumentar la confianza de los usuarios en el comercio electrónico[23], lo que evidenciaba la clara voluntariedad del sistema en su conjunto.

---

[20] Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo de 6 de julio de 2016 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión, OJ L 194, 19 de julio de 2016, p. 1–30.

[21] Viguri Cordero, J., "Los mecanismos de certificación (códigos de conducta, sellos y marcas)" en Rallo Lombarte, A., y García Mahamut, R. (eds.), *Hacia un nuevo derecho europeo de protección de datos*, Editorial Tirant lo Blanch. Valencia, 2015, p. 930.

[22] Por ejemplo, en materia de seguridad de la información, resultan aplicables dos estándares. Por un lado, la norma ISO/IEC 27001:2014 regula los requisitos de la tecnología de la información, las técnicas de seguridad y los Sistemas de Gestión de Seguridad de la Información (SGSI) y por otro lado, la norma ISO IEC 29100 que regula la tecnología de la información, técnicas de seguridad y el marco de privacidad.

[23] La Comisión Europea reconoció la necesidad de aumentar la confianza de los consumidores en las compras transfronterizas online mediante la adopción de medidas políticas apropiadas. Comisión Europea, Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social de las Regiones, *Agenda del consumidor europea - Impulsar la confianza y el crecimiento*, COM(2012) 225 final, Bruselas, 2 de mayo de 2012.
http://ec.europa.eu/consumers/eu_consumer_policy/our-strategy/documents/consumer_agenda_2012_en.pdf. Accedido el 11 de octubre de 2017.

Ahora bien, desde la entrada en vigor del RGPD, los mecanismos de certificación se articulan como instrumentos necesarios para promover la protección de privacidad desde su inicio, esto es, poniendo especial énfasis en la labor de prevención de las brechas de privacidad y protección de datos. En este sentido, ni la ausencia de regulación ni la regulación plena o reglamentaria es una opción viable para el futuro de la certificación de privacidad, sino que es necesario un enfoque corregulatorio para la viabilidad certificación de privacidad en Europa[24], tal y como así queda plasmado en el RGPD. De hecho, el Considerando 81 establece que la adhesión a un mecanismo de certificación aprobado simplemente puede servir de elemento para demostrar el cumplimiento de las obligaciones del presente Reglamento[25]. Por lo tanto, se deja en manos de la iniciativa privada el desarrollo y el alcance de la certificación, donde el RGPD se limita a establecer la posibilidad de demostrar el cumplimiento por medio de la certificación sin perjuicio de que puedan producirse violaciones aún siendo sometido a certificación.

En definitiva, convergen a mi juicio dos situaciones aparentemente contradictorias jurídicamente, por un lado, la necesidad en la promoción e implementación de mecanismos de certificación para garantizar el cumplimiento de sus disposiciones y por otro, la mera naturaleza potestativa o voluntaria de los mismos, que no certifica *per se* el cumplimiento de la legislación. Por esta razón, cabe poner de manifiesto que el término certificación goza de enorme amplitud en el RGPD y su naturaleza jurídica y su alcance variarán considerablemente en función del tipo de mecanismo de certificación.

3.2. La certificación: ¿Un mecanismo vinculante o potestativo?

En este punto, conviene destacar la necesidad en la implementación de la certificación puesto que aunque se traten de medidas voluntarias en sentido estricto, el mero avance tecnológico y sobre todo, el nuevo RGPD, las necesidades y exigencias del mercado hacen pertinente y *quasi* necesaria la aplicación de la certificación para la mayor parte de organizaciones que operan en el día a día con datos personales.

En definitiva, los mecanismos de certificación se han cristalizado como procedimientos *"semivinculantes"* por dos razones: en primer lugar, porque el alcance de la legislación puede variar en función del producto o sistema durante su progresivo desarrollo y en segundo lugar, para evitar o reducir el régimen sancionador que prevé el RGPD.

a) La certificación como método de cumplimiento efectivo del RGPD

[24] Rodrigues, R., Wright, D., Wadhwa, K., "Developing a privacy seal scheme...", *ob. cit.,* p.17.

[25] El Considerando 81 establece que *"(...). La adhesión del encargado a un código de conducta aprobado o a un mecanismo de certificación aprobado puede servir de elemento para demostrar el cumplimiento de las obligaciones por parte del responsable (...).*

No cabe duda que la regulación en el RGPD en materia de certificación es extensa pues supone una disciplina necesaria para asegurar el cumplimiento continuo de las disposiciones del RGPD ante los nuevos retos que evidencian los productos y sistemas en relación con la privacidad y la protección de los datos personales.

El Considerando 77 RGPD[26] prevé la posibilidad de implementar los códigos de conducta o certificaciones aprobados para articular los criterios necesarios en un momento determinado que requieran de medidas oportunas para garantizar el pleno cumplimiento del RGPD. Del mismo modo, el Considerando 166 RGPD[27] prevé expresamente la posibilidad de adoptarse actos delegados para determinar específicamente los criterios y requisitos que deben reunir los mecanismos de certificación, así como cualquier información necesaria para garantizar la adquisición de estos instrumentos.

Estaa previsiones son realmente significativas en aras de aumentar la publicidad de estos mecanismos de certificación, pues la experiencia ha puesto de manifiesto que en los últimos años las pequeñas y medianas empresas, por ejemplo, han sido reacias a adoptar en sus procedimientos internos tales certificaciones ya no solo por no calificarse como elementos vinculantes sino por sus elevados costes o por la falta de información generalizada de la que se dispone a día de hoy.

Además, el Considerando 168[28] articula también la posibilidad de adoptarse actos de ejecución sobre códigos de conducta o normas técnicas y mecanismos de certificación. De este modo, se faculta a la CE a adoptar tales actos con objeto de asegurar una mayor uniformidad de aplicación en todos los Estados miembros.

---

[26] Considerando 77 establece lo siguiente: *"se podrían proporcionar **directrices para la aplicación de medidas oportunas y para demostrar el cumplimiento por parte del responsable o del encargado del tratamiento,** especialmente con respecto a la identificación del riesgo relacionado con el tratamiento, a su evaluación en términos de origen, naturaleza, probabilidad y gravedad y a la identificación de buenas prácticas para mitigar el riesgo, que revistan, en particular, la **forma de códigos de conducta aprobados, certificaciones aprobadas".***

[27] Asimismo, el Considerando 166 establece que, *"(...) En particular, deben adoptarse **actos delegados en relación con los criterios y requisitos para los mecanismos de certificación, la información que debe presentarse mediante iconos normalizados y los procedimientos para proporcionar dichos iconos**. Reviste especial importancia que la Comisión lleve a cabo las consultas oportunas durante la fase preparatoria, en particular con expertos. Al preparar y redactar los actos delegados, la Comisión debe garantizar la transmisión simultánea, oportuna y apropiada de los documentos pertinentes al Parlamento Europeo y al Consejo".*

[28] Por otro lado, el Considerando 168 menciona por su parte que: *"El procedimiento de examen debe seguirse para la adopción de actos de ejecución sobre cláusulas contractuales tipo entre responsables y encargados del tratamiento y entre responsables del tratamiento; **códigos de conducta; normas técnicas y mecanismos de certificación**; el nivel adecuado de protección ofrecido por un tercer país, un territorio o un sector específico en ese tercer país, o una organización internacional (...)."*

b) Certificación y régimen sancionador en el RGPD.

El régimen sancionador implica un cambio trascendental respecto a lo establecido por la normativa actual de lo Estados miembros puesto que el RGPD dota a las sanciones de una finalidad puramente disuasoria tal y como así señala el Considerando 152 y el propio artículo 83 RGPD. A raíz de esto, las organizaciones deben no solo adoptar todas las medidas sean necesarias para garantizar el debido cumplimiento de la normativa de protección de datos sino que deben poder acreditarlo, ya que, de lo contrario, podrán hacer frente a importantes sanciones económicas.

Así, el propio RGPD recoge, que, las organizaciones se enfrentarán a multas cuantiosas que pueden ascender a la cifra mayor entre el 4% de su facturación anual o 20 millones de euros en caso de violaciones del Reglamento, lo que evidencia que en determinados casos, podrían, incluso, poner en riesgo la continuidad de las mismas. En este sentido, como se ha visto en el epígrafe anterior, pese a que las certificaciones son mecanismos de implementación meramente voluntarios, el estricto sistema de multas que prevé el RGPD hace inevitable su aplicación práctica, sobre todo en un novedoso marco jurídico que exige enormes esfuerzos a la mayor parte de las organizaciones por lo que respecta al cumplimiento exhaustivo de las disposiciones del citado RGPD.

Por lo que respecta a la certificación en el seno del régimen sancionador, el artículo 28 RGPD dispone por un lado en el apartado 5º, que la adhesión del encargado del tratamiento a un código de conducta podrá utilizarse como elemento para demostrar la existencia de las garantías suficientes en la aplicación de medidas técnicas y organizativas apropiadas conforme al RGPD. Por otro lado, el apartado 6º del citado artículo dispone que la relación contractual entre el responsable y el encargado del tratamiento podrá basarse en la certificación concedida[29].

Como consecuencia, la certificación adquiere en el RGPD una importancia transversal pues resulta de aplicación en cualquier tipo de acto jurídico y podrá gozar de presunción *iuris tantum* en el cumplimiento de las disposiciones del presente RGPD, lo que a asimismo, podrá disminuir o incluso evitar el rígido sistema punitivo. Así lo contempla el artículo 83 en el apartado j) al establecer explícitamente que las multas administrativas se impondrán, en función de las circunstancias de cada caso individual, y en todo caso, para determinar su cuantía se tendrá en cuenta la adhesión a códigos de

[29]El artículo 28 (Encargado del tratamiento) dipone en el apartado 5º lo siguiente: *"La adhesión del encargado del tratamiento a un código de conducta aprobado a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrá utilizarse como elemento para demostrar la existencia de las garantías suficientes a que se refieren los apartados 1 y 4 del presente artículo."* Asimismo, el apartado 6º establece que *"Sin perjuicio de que el responsable y el encargado del tratamiento celebren un contrato individual, el contrato u otro acto jurídico a que se refieren los apartados 3 y 4 del presente artículo podrá basarse, total o parcialmente, en las cláusulas contractuales tipo a que se refieren los apartados 7 y 8 del presente artículo, inclusive cuando formen parte de una certificación concedida al responsable o encargado de conformidad con los artículos 42 y 43."*

conducta en virtud del artículo 40 o a mecanismos de certificación aprobados con arreglo al artículo 42[30].

3.3. El alcance de la certificación en el RGPD y el ALOPD.

Por lo que respecta al RGPD, los mecanismos de certificación se encuentran regulados en el Capítulo IV denominado el responsable del tratamiento y encargado del tratamiento. En la Sección V, concretamente en el artículo 42, se regula la certificación en toda su extensión y en el artículo 43, el organismo de certificación.

En España, el ALOPD responde a la necesidad de elaborar una nueva LOPD para adaptar la legislación española al RGPD. Ahora bien, el nuevo texto contiene lagunas por lo que respecta a la certificación. Primero, con respecto a los esquemas de certificación, nada se regula acerca del periodo máximo de duración, el tipo de publicidad accesible, la revocación o la sujeción a futuros actos delegados o actos de ejecución de la Comisión y segundo, no aparece mencionada la figura de los organismos de certificación que si contempla el artículo 43 RGPD.

a) Los mecanismos de certificación

La doctrina ha interpretado las cuatro vías que el RGPD establece para implementar la certificación de protección de datos, esto es, la labor de fomento y apoyo del régimen de certificación, la acreditación de los organismos de certificación, la certificación por las APD o la coexistencia de las tres anteriores[31].

El artículo 42 RGPD establece en el apartado 1º esta función de promoción pues implica que los Estados miembros, las autoridades de control, el Comité y la CE deben promover la creación de estos mecanismos de certificación. Esta labor de promoción se debe llevar a cabo a la luz de las disposiciones del RGPD y para garantizar su implementación práctica, debe concretarse a la organización a la que va dirigida. En este sentido, el propio RGPD no atribuye mayor relevancia jurídica que la que pueda otorgarse en el futuro la Comisión mediante sus actos de ejecución[32].

El RGPD menciona la naturaleza jurídica de la certificación, esto es, el principio de voluntariedad y publicidad, vinculado con la transparencia de proceso, en el apartado 3º. Como consecuencia del mismo, el apartado 4º advierte que los mecanismos de

[30] El artículo 83 (Condiciones generales para la imposición de multas administrativas) dispone en el apartado 2º, letra j) lo siguiente: *Las multas administrativas se impondrán, en función de las circunstancias de cada caso individual, a título adicional o sustitutivo de las medidas contempladas en el artículo 58, apartado 2, letras a) a h) y j). Al decidir la imposición de una multa administrativa y su cuantía en cada caso individual se tendrá debidamente en cuenta: j) la adhesión a códigos de conducta en virtud del artículo 40 o a mecanismos de certificación aprobados con arreglo al artículo 42.*

[31] Rodrigues, R., Barnard-Willsa, D., De Hert, P., Papakonstantinou, V, "The future of privacy certification in Europe an exploration of options under article 42 of the GDPR", *International Review of Law, Computers & Technology*, vol. 30, nº 3, p.8, 2016.

[32] Rallo Lombarte, A., "Hacia un nuevo sistema europeo de protección de datos: las claves de la reforma", *Revista de Derecho Político*, núm. 85, septiembre-diciembre 2012, pp. 29-51.

certificación no limitan la responsabilidad del responsable o encargado del tratamiento. Ahora bien, éstos pueden acogerse a los mismos con objeto de demostrar la existencia de garantías adecuadas ofrecidas por los responsables o encargados no sujetos al presente RGPD en el marco de transferencias de datos personales a terceros países u organizaciones internacionales (apartado 2º). No obstante, en estos supuestos el RGPD establece la obligación de vinculación por medio contractual o mediante otros instrumentos jurídicamente vinculantes.

El mismo artículo 42 contiene una serie de formalidades básicas que deben reunir los mecanismos de certificación. Por un lado, la obligación de que estos instrumentos se expidan bien por organismos de certificación, bien por la autoridad de control competente[33] o por el Comité[34] (63), que en caso de los criterios requeridos en la certificación sean aprobados por éste último, podrá dar lugar al llamado Sello Europeo de Protección de Datos[35].

Dentro de estas formalidades, el apartado 6º dispone el compromiso de entregar toda la información y acceso a sus actividades de tratamiento que necesite para llevar a cabo el procedimiento de certificación. Se trata de una disposición que pretende elevar el estándar de protección de los mecanismos de certificación, pues permite disponer eficientemente de todos los datos e información relevantes para decidir acerca del tratamiento que lleva a cabo una organización en el seno de su actividad.

Respecto al tiempo de expedición, el apartado 7º establece un período máximo de tres años y que podrá ser renovada en las mismas condiciones, siempre que se sigan

[33] De conformidad con el artículo 58.3 RGPD, la autoridad de control posee las siguientes funciones: *"asesorar al responsable del tratamiento conforme al procedimiento de consulta previa contemplado en el artículo 36; emitir, por iniciativa propia o previa solicitud, dictámenes destinados al Parlamento nacional, al Gobierno del Estado miembro o, con arreglo al Derecho de los Estados miembros, a otras instituciones y organismos, así como al público, sobre cualquier asunto relacionado con la protección de los datos personales; autorizar el tratamiento a que se refiere el artículo 36, apartado 5, si el Derecho del Estado miembro requiere tal autorización previa; emitir un dictamen y aprobar proyectos de códigos de conducta de conformidad con lo dispuesto en el artículo 40, apartado 5; acreditar los organismos de certificación con arreglo al artículo 43; expedir certificaciones y aprobar criterios de certificación con arreglo al artículo 42, apartado 5; adoptar las cláusulas tipo de protección de datos contempladas en el artículo 28, apartado 8, y el artículo 46, apartado 2, letra d); autorizar las cláusulas contractuales indicadas en el artículo 46, apartado 3, letra a); autorizar los acuerdos administrativos contemplados en el artículo 46, apartado 3, letra b); aprobar normas corporativas vinculantes de conformidad con lo dispuesto en el artículo 47."*

[34] Según establece el artículo 63 RGPD con respecto al mecanismo de coherencia, es necesaria la cooperación entre Autoridades de Protección de Datos entre sí y con la Comisión.

[35] El Sello Europeo de Protección de Datos, del inglés European Privacy Seal (EuroPriSe) supone una de las iniciativas más destacables en materia de certificación más destacadas. Fue iniciado por la Unión Europea para solventar los problemas que se daban con los anteriores sellos de privacidad, esto es, la desconfianza en este tipo de mecanismos. Esta iniciativa se basa en la confidencialidad, calidad y seguridad en la gestión de los datos de carácter personal para lo que lleva a cabo un procedimiento de evaluación del producto o servicio por expertos legales y técnicos homologados que evalúan los criterios establecidos por la normativa europea de protección de datos. En última instancia, un organismo homologado independiente certifica su aprobación para la efectiva obtención del denominado EuroPriSe. De este modo, se garantiza que el producto o servicio cumple los criterios establecidos en un catálogo general fundamentado en las normativas europeas. Para mayor información acerca de esta iniciativa, véase https://www.european-privacy-seal.eu/EPS-en/Home. Accedido el 9 de octubre de 2017.

cumpliendo los requisitos pertinentes, que evidentemente podrán variar desde el momento en el que se otorgó en un principio la certificación. En este caso, establece el citado apartado que deberán de comunicarse aquellas circunstancias que requieran de modificación para adecuarse a las exigencias del RGPD.

Finalmente, el apartado 8º recoge el control efectivo de todos los mecanismos de certificación pues deberán guardarse en un registro a disposición pública por cualquier medio apropiado, esto es, tanto de forma física como telemática.

La certificación, tal como se establece en el RGPD, se encuentra en fase embrionaria y probablemente requerirá especificaciones adicionales, por ejemplo cuáles son los productos o sistemas susceptibles de certificación, así como los criterios y los requisitos[36].

La Agencia Española de Protección de Datos (AEPD) ha sido pionera en la elaboración de un marco de referencia para esta figura pues junto con la Entidad Nacional de Acreditación (ENAC), han presentado su Esquema de certificación de Delegados de Protección de Datos (DPD)[37] en virtud del artículo 36 ALOPD. Se trata un mecanismo de certificación del todo pertinente para que los DPDs puedan demostrar su reconocida competencia en la materia.

No cabe duda de que mediante su aplicación práctica, se aumentará la seguridad, fiabilidad y transparencia de esta nueva figura que prevé el RGPD en la sección 4 del Capítulo IV (Responsable del tratamiento y encargado del tratamiento) y que deberá ser incorporada por parte de los profesionales de la privacidad, empresas y entidades que traten con datos personales.

No obstante, conviene destacar la enorme labor que han venido realizando otras APDs a nivel europeo, pues ya han creado mecanismos de certificación en este contexto. A modo de ejemplo, a finales de agosto de 2015, la APD inglesa, denominada Information Commissioner's Officer (ICO), desarrolló su propio sello de protección de la privacidad, cuyo funcionamiento debía realizarse antes de la entrada en vigor del RGPD [38]. El mismo año, la APD francesa, conocida como la Comisión Nacional de

---

[36] Rodrigues, R., Barnard-Willsa, D., De Hert, P., Papakonstantinou, V, "The future of privacy certification in Europe...", *ob.cit*, p. 9.

[37] Las certificaciones serán otorgadas por entidades acreditadas por ENAC, siguiendo criterios de certificación elaborados por la AEPD en colaboración con los sectores afectados. La elaboración del Esquema ha contado con la participación de un Comité Técnico de Expertos, entre los que se encuentran representantes de sectores y asociaciones profesionales, empresariales, universidades y Administraciones Públicas.
http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2017/notas_prensa/news/2017_07_13-ides-idphp.php. Accedido el 11 de octubre de 2017. El Esquema de certificación de Delegados de Protección de Datos de la Agencia Española de Protección de Datos (Esquema AEPD-DPD). Redactado por la Unidad de Evaluación y Estudios Tecnológicos de la Agencia Española de Protección de Datos, 2 de octubre de 2017, Versión 1.1. El esquema puede encontrarse en el siguiente enlace: http://www.agpd.es/portalwebAGPD/temas/certificacion/common/pdf/ESQUEMA_AEPD_DPD.pdf Accedido el 11 de octubre de 2017.

[38] De hecho, el informe de 2014 que presentó los resultados anuales del ICO, que evaluaba el conocimiento de la Ley de Protección de Datos inglesa (Data Protection Act, DPA) y la Ley de Libertad

Informática y Libertades (CNIL), creó el llamado "Sello CNIL" que certifica el cumplimiento de la ley francesa de protección de datos («CNIL»)[39]. Por su parte, la APD italiana, el Garante per la Protezione dei Dati Personali puso de manifiesto a principios de 2017 su intención de proporcionar una importante actividad de mejora de los códigos de conducta y certificaciones para finales de 2017[40].

b) Los organismos de certificación

El Artículo 43 RGPD regula la figura de los organismo de certificación desde un enfoque meramente funcional. Es decir, no establece qué se entiende por organismo de certificación sino que se limita a establecer sus funciones y obligaciones en el proceso de certificación.

Para ello, dispone el citado artículo en su apartado 1º que estos organismos tienen el deber de expedir y renovar las certificaciones una vez informada la autoridad de control, a fin que ésta que pueda retirar una certificación u ordenarle que retire una certificación emitida u ordenarle que no se emita una certificación si no se cumplen o dejan de cumplirse los requisitos para la certificación.

Además, con el fin de asegurar su buen funcionamiento, los Estados miembros deben garantizar que dichos organismos de certificación sean acreditados o bien por la autoridad de control, esto es las APDs competentes[41], por el organismo nacional de acreditación designado en un estado miembro[42] o por ambos.

En España, la autoridad de control corresponde la Agencia Española de Protección de Datos (AEPD) a nivel estatal y a la Autoritat Catalana de Protecció de Dades (ACPD) y la Agencia Vasca de Protección de Datos (AVPD), a nivel autonómico y serán éstas las encargada de velar por el cumplimiento de la normativa sobre protección

---

de Información (Freedom of Information Act, FOIA) entre el público en general apuntó lo siguiente: *"Hay un amplio apoyo para la implementación de un nuevo sello de certificación que permita demostrar que un proveedor de servicios online ha sido acreditado en la protección de los derechos de la información, con cuatro de cada cinco encuestados (81%)".* Information Commissioner's Office (ICO), *Annual Track 2014. Individuals (Topline findings).* 20 de septiembre de 2014. https://ico.org.uk/media/about-the-ico/documents/1043485/annual-track-september-2014-individuals.pdf. Accedido el 12 de octubre de 2017.

[39] Commission Nationale de l'Informatique et des Liberte's (CNIL). *Labels CNIL*, 2015. http://www.cnil.fr/linstitution/labels-cnil/. Accedido el 12 de octubre de 2017.

[40] Garante per la Protezione dei Dati Personali, *Aclaraciones sobre GDPR*, 24 de enero de 2017. http://getsolution.it/garante-della-privacy-italiano-sul-gdpr/?lang=en. Accedido el 12 de octubre de 2017.

[41] En España, la AEPD, la ACPD y la AVPD son las autoridades estatales de control independiente encargada de velar por el cumplimiento de la normativa sobre protección de datos.

[42] En España, de conformidad con el Reglamento (CE) 765/2008 del Parlamento Europeo y del Consejo (1) con arreglo a la norma EN ISO/IEC 17065/2012 y a los requisitos adicionales establecidos por la autoridad de control.

de datos. Por su parte, el organismo nacional de acreditación designado por medio del Real Decreto 1715/2010[43] corresponde a la ENAC.

Ahora bien, con carácter general, el ALOPD sufre un déficit de concreción del estatuto jurídico de algunas figuras que aparecen en él. Concretamente, y por lo que respecta a los mecanismos de certificación, resulta cuanto menos paradójico que el Capítulo IV que regula los códigos de conducta y la certificación del Titulo IV (responsable y encargado del tratamiento) no haga la más mínima alusión a la figura de los organismos de certificación que contempla el artículo 43 RGPD. Pese a que el artículo 40 del ALOPD regula los esquemas de certificación, simplemente articula la obviedad de que la función de acreditación de estos organismos de certificación será llevada a cabo por la ENAC, que comunicará a la AEPD y a las APD de las comunidades autónomas las concesiones, denegaciones o revocaciones de las acreditaciones. Ahora bien, nada se establece acerca del papel que juegan los certificadores en todo este proceso clave. En este sentido, debemos acudir al RGPD que en su apartado 2º[44], regula las condiciones que deben reunir los organismos de certificación así como la plena sujeción a las instrucciones aprobadas por la autoridad de control (apartado 3º).

En cuanto a régimen de responsabilidad, el apartado 5º establece que éstos serán responsables de la función ordinaria de certificación, esto es, tanto de la concesión como de la retirada que en todo caso, deberán ser motivadas. Todo ello sin perjuicio de que en el supuesto de que el organismo de certificación no cumpla o deje de cumplir las condiciones de la acreditación, la autoridad de control o el organismo nacional de acreditación competente pueda revocar la acreditación (apartado 7º). Por lo que respecta al tiempo de vigencia de la acreditación, el mismo apartado establece que se expedirá por un periodo máximo de 5 años y podrá ser renovada en las mismas condiciones.

---

[43] Real Decreto 1715/2010, de 17 de diciembre, por el que se designa a la Entidad Nacional de Acreditación (ENAC) como organismo nacional de acreditación de acuerdo con lo establecido en el Reglamento (CE) nº 765/2008 del Parlamento Europeo y el Consejo, de 9 de julio de 2008, por el que se establecen los requisitos de acreditación y vigilancia del mercado relativos a la comercialización de los productos y por el que se deroga el Reglamento (CEE) nº 339/93. «BOE» núm. 7, de 8 de enero de 2011, pp. 1670-1673.

[44] El apartado 2º del artículo 43 dispone que deben cumplir la siguientes condiciones: demostrar, a satisfacción de la autoridad de control competente, su **independencia y su pericia** en relación con el objeto de la certificación; respetar los criterios mencionados en el artículo 42, apartado 5, y aprobados por la autoridad de control que sea competente en virtud del artículo 55 o 56, o por el Comité de conformidad con el artículo 63; **establecer procedimientos para la expedición, la revisión periódica y la retirada** de certificaciones, sellos y marcas de protección de datos; dis**poner de procedimientos y estructuras para tratar las reclamaciones relativas a infracciones de la certificación** o a la manera en que la certificación haya sido o esté siendo aplicada por un responsable o encargado del tratamiento, y para hacer dichos procedimientos y estructuras transparentes para los interesados y el público, y demostrar, a satisfacción de la autoridad de control competente, que sus funciones y cometidos no dan lugar a conflicto de intereses.

Además, al igual que los organismos de certificación, la autoridad de control deberá hacer públicos los requisitos de acreditación y de certificación de una forma fácilmente accesible (entendemos como tal, su comprobación por algún medio telemático creado al efecto) y comunicar los requisitos y criterios al Comité que archivará en un registro todos los mecanismos de certificación y sellos de protección de datos y los pondrá a disposición pública por cualquier medio apropiado (apartado 6º).

Finalmente, el apartado 8º faculta a la CE para adoptar *actos delegados* (a fin de especificar las condiciones que deberán tenerse en cuenta para los mecanismos de certificación en materia de protección de datos) y de *ejecución* (que establezcan normas técnicas para los mecanismos de certificación). Esto responde directamente a la propia naturaleza de la certificación, pues son fácilmente actualizables y modificables con objeto de adaptarse a nuevos cambios o desarrollos.

4. Conclusiones

No cabe duda que el desarrollo incesante de las tecnologías ha puesto de manifiesto la vulnerabilidad de los productos o sistemas con respecto no solo a la seguridad, sino también en la protección de los datos personales. Todo ello está originando una generalizada falta de desconfianza de los usuarios con respecto a los productos o sistemas certificados.

Por fortuna, la aplicación del nuevo RGPD a partir del 25 de mayo de 2018 supondrá un avance en la protección efectiva del derecho de protección de datos. De hecho, el enfoque preventivo o proactivo constituye una de las piedras angulares del sistema y por ello, apuesta decididamente por la certificación, la privacidad desde el diseño (Privacy by Design) o la privacidad por defecto (Privacy by Default).

Por lo que respecta a los mecanismos de certificación, el RGPD eleva las garantías de protección de datos mediante la inclusión de novedades sustanciales para hacer frente a los problemas que se han venido dando en los últimos años. En este sentido, los mecanismos de certificación se enmarcan como iniciativas eficientes para demostrar el cumplimiento de la legislación.

Ahora bien, no debemos pasar por alto la naturaleza jurídica de los mismos pues estos instrumentos no dejan de ser iniciativas de autorregulación que el propio RGPD ha cristalizado como elementos corregulatorios por la vinculación que poseen las autoridades de supervisión. Por un lado, el artículo 43.5 establece la obligación que recae en los organismos de certificación de proporcionar a las autoridades de supervisión competentes las razones para conceder la certificación solicitada. Por otro lado, el artículo 58.2 otorga poderes amplios a tales autoridades pues tienen la facultad retirar una certificación directamente o por medio del organismo de certificación o obligar a éste a no emitir una certificación si los requisitos para la certificación no guardan relación con el RGPD o han dejado de cumplirse.

Cabe destacar asimismo, que la certificación no implica en ningún caso que cada controlador de datos o procesador certificado cumpla con lo dispuesto en el RGPD pues excedería del propio objeto de certificación. Es por ello por lo que el RGPD respalda el uso de códigos de conducta y certificaciones para proporcionar orientación sobre sus requisitos, señalar a los reguladores que una organización cumple con las disposiciones del mismo y ofrecer supervisión por parte de terceros como control adicional para los controladores y procesadores.

Otra de las particularidades de la importancia de la certificación, sino puede considerarse como la más relevante, está vinculada con el régimen sancionador. A pesar de la clara naturaleza voluntaria de la certificación, tal y como establece en el artículo 42.3 RGPD, las necesidades y exigencias del mercado requieren de la implementación de mecanismos de certificación. Las organizaciones deben acreditar la adopción de todas las medidas técnicas, organizativas a su alcance para garantizar el debido cumplimiento de la normativa de protección de datos (artículo 28.5 RGPD). Además, el artículo 83 j) dispone que para la determinación de la cuantía de la misma, se tendrá en cuenta la adhesión a códigos de conducta o a mecanismos de certificación.

En una comparativa entre el RGPD y la normativa española, es necesario destacar que tanto los mecanismos de certificación regulados (artículo 42 RGPD) y el organismo de certificación (artículo 43 RGPD) no guardan estrecha coherencia con el artículo 40 del ALOPD pues nada se regula acerca del periodo máximo de duración, el tipo de publicidad accesible, la revocación o la sujeción a futuros actos delegados o actos de ejecución de la Comisión y además, no se menciona la figura de los organismos de certificación que sí contempla REPD.

Pese a todo, la AEPD ha llevado a cabo un novedoso Esquema de certificación de Delegados de Protección de Datos (DPD), lo que se suma a los enormes esfuerzos de otras APDs a nivel europeo en la labor de creación y promoción mecanismos de certificación.

Sin embargo, cabe esperar al próximo 2018 para analizar los sucesivos mecanismos de certificación que proporcionen no sólo las APDs, sino también los organismos de normalización y en el que participen las demás partes interesadas para la mayor o menor consecución de los objetivos previstos en el RGPD.

5. Bibliografía

Commission Nationale de l'Informatique et des Liberte's (CNIL). "Labels CNIL.", 2015.. http://www.cnil.fr/linstitution/labels-cnil/. Accedido el 12 de octubre de 2017

Comisión Europea, Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social de las Regiones, Agenda del consumidor europea - Impulsar la confianza y el crecimiento, COM(2012) 225 final, Bruselas, 2 de mayo de 2012.
http://ec.europa.eu/consumers/eu_consumer_policy/our-strategy/documents/consumer_agenda_2012_en.pdf. Accedido el 11 de octubre de 2017.

Comisión Europea, Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social y al Comité de las Regiones, Un enfoque global de la protección de los datos personales en la Unión Europea, COM(2010) 609 final, Bruselas, 4 de noviembre de 2010, p. 13. http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_es.pdf. Accedido el 4 de octubre de 2010.

Comisión Europea, Estudio comparativo sobre diferentes enfoques de nuevos desafíos de privacidad, en particular a la luz de los desarrollos tecnológicos, Informe Final, 20 de enero de 2010.
http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf. Accedido el 13 de octubre de 2017.

Comisión Europea, Comunicación de la Comisión al Consejo, Parlamento Europeo y Comité Económico y Social y el Comité de las Regiones, Una estrategia para una sociedad de la información segura - Diálogo, asociación y potenciación, COM (2006) 251 final, Bruselas 31 de mayo, 2006. http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=LEGISSUM%3Al24153a. Accedido el 5 de octubre de 2017.

Comisión Europea, Comunicación de la Comisión al Parlamento Europeo y al Consejo, Fomento de la protección de datos mediante las tecnologías de protección del derecho a la intimidad (PET), COM (2007) 228 final. Bruselas, 2 de Mayo de 2007.
http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=LEGISSUM%3Al14555. Accedido el 5 de octubre de 2017.

De Hert, P., Papakonstantinou, V., "Three scenarios for international governance of data privacy: Towards an international data privacy organization, preferably a UN agency", *Journal of Law and Policy*, vol. 9, nº 2, p. 271-324, 2013.

Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo de 6 de julio de 2016 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión, OJ L 194, 19 de julio de 2016, p. 1–30.

Directiva (UE) 98/34/CE del Parlamento Europeo y del Consejo, por la que se establece un procedimiento de información en materia de las normas y reglamentaciones técnicas y de las reglas relativas a los servicios de la sociedad de la información, OJ L 204, 21 de julio de 1998, p. 37–48.

Directiva (UE) 2015/1535 del Parlamento Europeo y del Consejo, de 9 de septiembre de 2015, por la que se establece un procedimiento de información en materia de reglamentaciones técnicas y de reglas relativas a los servicios de la sociedad de la información, OJ L 241, 17 de septiembre 2015, p. 1–15.

Dumortier, J., Goemans, C., "Online data privacy and standardization: towards a more effective protection?", en J. Dumortier e.a. (eds.), *A decade of research at the crossroads of law and ICT*, Larcier, Bruselas, nº 53, p. 53-70, 2001.

Garante per la Protezione dei Dati Personali, Aclaraciones sobre GDPR, 24 de enero de 2017. http://getsolution.it/garante-della-privacy-italiano-sul-gdpr/?lang=en. Accedido el 12 de octubre de 2017.

Grupo de trabajo del artículo 29, Opinión 3/2010 sobre el Principio de Responsabilidad, WP 173, 13 de julio de 2010, p.17. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp173_en.pdf. Accedido el 8 de octubre de 2017 (Versión inglesa).

Information Commissioner's Office (ICO), Annual Track 2014. Individuals (Topline findings). 20 de septiembre de 2014. https://ico.org.uk/media/about-the-ico/documents/1043485/annual-track-september-2014-individuals.pdf. Accedido el 12 de octubre de 2017.

Parlamento Europeo, Resolución sobre los efectos de la publicidad en el comportamiento de los consumidores (2010/2052), 15 de diciembre de 2010. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2010-0484+0+DOC+XML+V0//ES. Accedido el 11 de octubre de 2017.

Real Decreto 1715/2010, de 17 de diciembre, por el que se designa a la Entidad Nacional de Acreditación (ENAC) como organismo nacional de acreditación de acuerdo

con lo establecido en el Reglamento (CE) nº 765/2008 del Parlamento Europeo y el Consejo, de 9 de julio de 2008, por el que se establecen los requisitos de acreditación y vigilancia del mercado relativos a la comercialización de los productos y por el que se deroga el Reglamento (CEE) nº 339/93. «BOE» núm. 7, de 8 de enero de 2011, páginas 1670 a 1673.

Reding, V.,"The upcoming data protection reform for the European Union International Data Privacy Law", *International Data Privacy Law*, vol. 1, nº 1, 2011, pp. 3–5

Reglamento (CE) 765/2008 del Parlamento Europeo y del Consejo (1) con arreglo a la norma EN ISO/IEC 17065/2012 y a los requisitos adicionales establecidos por la autoridad de control.

Reglamento (UE) nº 1025/2012 del Parlamento Europeo y del Consejo de 25 de octubre de 2012 sobre la normalización europea, por el que se modifican las Directivas 89/686/CEE y 93/15/CEE del Consejo y las Directivas 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE y 2009/105/CE del Parlamento Europeo y del Consejo y por el que se deroga la Decisión 87/95/CEE del Consejo y la Decisión nº1673/2006/CE del Parlamento Europeo y del Consejo, DOUE núm. 316, de 14 de noviembre de 2012, p. 12 a 33.

Rodrigues, R., Barnard-Willsa, D., De Hert, P., Papakonstantinou, V, "The future of privacy certification in Europe an exploration of options under article 42 of the GDPR", *International Review of Law, Computers & Technology*, vol. 30, nº 3, 2016, p. 248-270.

Rodrigues, R., Barnard-Wills, D., Wright, D., de Hert, P., Papakonstantinou, V., EU Privacy seals project, Inventory and Analysis of Privacy Certification Schemes: Final Report Study Deliverable 1.4, Comisión Europea. Luxemburgo: Oficina de publicaciones de la Unión Europea, 2013.

Rodrigues, R., Wright, D., Wadhwa, K., "Developing a privacy seal scheme (that works)", *International Data Privacy Law*, vol 3, nº 2, 2013, p.100-116.

Rallo Lombarte, A., "Hacia un nuevo sistema europeo de protección de datos: las claves de la reforma", *Revista de Derecho Político*, núm. 85, septiembre-diciembre 2012, pp. 14-56.

Viguri Cordero, J., "Los mecanismos de certificación (códigos de conducta, sellos y marcas)" en Rallo Lombarte, A., y García Mahamut, R. (eds.), *Hacia un nuevo derecho europeo de protección de datos*, Editorial Tirant lo Blanch. Valencia, 2015.