Revista catalana de dret públic #62

www.rcdp.cat

LA ADOPCIÓN DE INSTRUMENTOS DE CERTIFICACIÓN COMO GARANTÍA EFICIENTE EN LA PROTECCIÓN DE LOS DATOS PERSONALES

Jorge Agustín Viguri Cordero*

Resumen

El presente trabajo tiene por objeto el análisis de los mecanismos de certificación vigentes desde la efectiva aplicación del Reglamento General de Protección de Datos (RGPD). Como punto de partida, estos se abordan desde su enfoque eminentemente técnico y su aproximación al ámbito del derecho de protección de datos. Seguidamente, se examina la regulación de los mecanismos de certificación en el RGPD y las iniciativas que han sido impulsadas recientemente en España, Francia y el Reino Unido por sus respectivas agencias de protección de datos. A continuación, procedemos al estudio de los estándares internacionales ISO/IEC de la serie 27000, y, más concretamente, de las normas ISO/IEC 27001 (seguridad de la información) y 27701 (gestión de la información de privacidad) y sus correspondientes actualizaciones. Por último, se destacan aquellos beneficios más inmediatos de estas iniciativas y su margen de mejora en un futuro a corto plazo, una vez identificadas aquellas limitaciones más relevantes que afectan al efectivo cumplimiento del mencionado reglamento.

Palabras clave: RGPD; certificación; serie ISO/IEC 27000; protección de datos; seguridad de la información; datos personales.

THE USE OF CERTIFICATION MECHANISMS AS AN EFFICIENT GUARANTEE OF PERSONAL DATA PROTECTION

Abstract

The purpose of this paper is to analyse the certification mechanisms in force since the effective application of the General Data Protection Regulation (GDPR). As a starting point, we approach these mechanisms from their eminently technical focus and their approximation to the field of data protection law. Next, we examine the regulation of certification mechanisms in the GDPR and the initiatives that have recently been promoted in Spain, France and the United Kingdom by their respective data protection agencies. We then move on to the study of the ISO/IEC 27000 series of international standards, and more specifically ISO/IEC 27001 (information security) and 27701 (privacy information management) and their corresponding updates. Finally, the most immediate benefits of these initiatives and their scope for improvement in the short-term future are highlighted, once the most relevant limitations affecting effective compliance with the aforementioned regulation have been identified.

Key words: GDPR; certification; ISO/IEC 27000 series; data protection; information security; personal data.

* Jorge Agustín Viguri Cordero, investigador postdoctoral de derecho constitucional de la Universitat Jaume I. Facultad de Ciencias Jurídicas y Económicas, av. de Vicente Sos Baynat, s/n. 12071 Castelló de la Plana. jviguri@uji.es.

Artículo recibido el 18.11.2020. Evaluación ciega: 12.12.2020, 18.01.2021 y 01.02.2021. Fecha de aceptación de la versión final: 25.02.2021.

Citación recomendada: Viguri Cordero, Jorge Agustín. (2021). La adopción de instrumentos de certificación como garantía eficiente en la protección de los datos personales. *Revista Catalana de Dret Públic, 62*, 160-176. https://doi.org/10.2436/rcdp.i62.2021.3571.

Sumario

1 Introducción[1]

La efectiva aplicación del Reglamento general de protección de datos 2016/679 (RGPD) desde el 25 de mayo de 2018 y su ulterior adaptación por las legislaciones nacionales han supuesto que los ordenamientos jurídicos contemplen mecanismos de certificación, una serie de instrumentos que pretenden asistir activamente a las organizaciones en el cumplimiento de la normativa de protección de datos mediante la adopción de políticas, procedimientos y procesos adecuados y específicos en el seno de su funcionamiento ordinario y que ha llevado a que los modelos autorregulatorios de "buenas prácticas" en materia de tratamiento y protección de datos personales hayan cristalizado en un novedoso marco legal.

Precisamente, el RGPD apostó decididamente por la creación e implementación de estos mecanismos, de forma que tanto las autoridades supervisoras como los organismos de certificación acreditados nacionales pueden certificar a los responsables y encargados del tratamiento sobre el cumplimiento de la normativa de protección de datos, concediendo una "distinción" en forma de sello o marca de calidad fácilmente perceptible por las partes interesadas a un amplio elenco de productos, servicios y sistemas de tecnologías de la información (TI). Así lo recoge expresamente el RGPD en el apartado 1.º del artículo 24, al disponer lo siguiente: "[...] el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento [...]". De hecho, atribuye a la adhesión a un mecanismo de certificación en los términos del artículo 42 del RGPD una importancia clave, pues estos "podrán ser utilizados como elementos para demostrar el cumplimiento de las obligaciones por parte del responsable del tratamiento" (apartado 3.º).

Pero ¿qué es la certificación y cómo incide en el respeto de la legislación de protección de datos? Esta puede definirse como un proceso con una serie de constatados beneficios que no solo permiten demostrar el cumplimiento efectivo del nivel de seguridad apropiado, sino que también facultan a las organizaciones certificadas para proporcionar garantías suficientes en el cumplimiento de la normativa de protección de datos vigente. A su vez, facilitan la evaluación del riesgo de procesamiento y la evaluación de impacto de la protección de datos (EIPD), constituyen circunstancias de exoneración o atenuación de multas administrativas e, incluso, simplifican la portabilidad de los datos, gracias, en buena medida, al reconocimiento y validez general que reciben estos estándares por parte de un amplio conjunto de partes interesadas.

Ello no implica que cada responsable o encargado de tratamiento certificado cumpla fielmente con lo dispuesto en la legislación de protección de datos —en este caso, excedería del propio objeto de certificación—, sino que *respalda* la aplicación de ciertas certificaciones para proporcionar orientación sobre sus requisitos, *certifica* ante los reguladores que una organización cumple con sus criterios o requisitos y *garantiza* la supervisión por terceras partes —certificadoras, acreditadoras y autoridades de control. Este triple eje de vigilancia para los responsables y encargados del tratamiento de datos conecta directamente con la "función de aseguramiento", consistente en que las organizaciones certificadas pueden reducir o incluso evitar el severo régimen sancionador dispuesto en el RGPD y en las legislaciones nacionales. Por consiguiente, estos mecanismos se encuentran ligados al principio de responsabilidad proactiva del artículo 5.2 del RGPD (Rallo, 2019, p. 49; Bajo, 2019, p. 973; Gudín, 2018, p. 83) y deben encauzarse siguiendo los parámetros relativos a la seguridad de tratamiento del artículo 32 del RGPD, que dispone expresamente lo siguiente: "Teniendo en cuenta el estado de la técnica, los costes de aplicación, [...] el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo [...]".

Para tal fin, como examinó el estudio sobre la certificación presentado a la Comisión Europea en el año 2019, la certificación debería ser capaz de ofrecer más transparencia a los interesados, reducir la asimetría de la información que comúnmente desequilibra la relación con los responsables de los datos u ofrecer una ventaja competitiva en el mercado. Tan es así, que en el punto actual en el que nos encontramos, la certificación tiene por principal objetivo proporcionar una mayor seguridad a los responsables y encargados, pudiendo emplearse para demostrar el cumplimiento de la normativa de protección de datos. El procedimiento de certificación

1 El presente trabajo se ha elaborado en el marco de los proyectos de investigación RTI2018-095367-B-I00, del Ministerio de Ciencia e Innovación, y AICO/2019/205, de la Conselleria de Innovación, Universidades, Ciencia e Innovación Digital de la Generalitat Valenciana.

debe constituir una prueba útil para los responsables y encargados a la hora de verificar su cumplimiento, especialmente, en la fase inicial del vigente marco regulatorio, donde se enfrentan y adaptan a un nuevo panorama legal en el procesamiento de los datos (Comisión Europea, 2019, p. 16).

Y, aunque el conjunto de normas técnicas en el contexto de la protección de datos está evolucionando rápidamente, todavía existe una falta estructural de conocimiento en el mercado con respecto a la disponibilidad de estas normas técnicas relevantes. Ello viene motivado por la gran tipología de certificaciones existentes —incluso adscritas al ámbito de la privacidad y protección de datos. Así, el citado informe de la Comisión constata los efectos adversos que siguen produciéndose en este sentido, en esencia, la información que se puede obtener sobre estos mecanismos en sus respectivas páginas web resulta limitada, esta se encuentra dispersa o incluso se hace referencia al hecho de que cada esquema de certificación emplea terminología distinta (Comisión Europea, 2019, p. 33), por lo que se encuentra muy lejos de estar armonizada en el plano comunitario.

Para solventar estos efectos, emergen un conjunto de extensos estándares de referencia certificables por parte de organizaciones que operan con los datos de los ciudadanos de la UE.[2] Entre estos, la serie 27000 de la Organización Internacional de Normalización (ISO) / Comisión Electrotécnica Internacional (IEC) se encuentra conformada por destacados estándares relativos a la Seguridad de la Información en el ámbito internacional, los cuales proporcionan un excelente punto de partida en el cumplimiento de los requisitos técnicos y operativos necesarios para reducir el riesgo de vulneración de las disposiciones del RGPD (Chatzipoulidis et al., 2019, p. 17). Concretamente, la serie 27000:2019 sobre el Sistema de Gestión de la Seguridad de la Información (SGSI)[3] incorpora en su anexo D nuevas cláusulas de certificación que se aproximan al cumplimiento de la responsabilidad proactiva de las disposiciones del RGPD. Esta serie, objeto de estudio en el presente trabajo, ha supuesto un verdadero punto de inflexión en la certificación, integrando diversas cláusulas que hacen referencia a aquellos aspectos más esenciales previstos en el RGPD.

Pero lo que sin duda supone a nuestro juicio uno de los aspectos de mayor relevancia estriba en la incorporación de exigencias en materia de responsabilidad proactiva, seguridad de la información o —no menos notable— la concreción de las condiciones para efectuar las transferencias internacionales de datos en materia de certificación conforme a los artículos 42.1 y 46 del RGPD, cuestión sumamente relevante tras la Sentencia del Tribunal de Justicia de la Unión Europea (STJUE) *Data Protection Commissioner c. Facebook Ireland and Maximillian Schrems*, de 14 de julio de 2020,[4] que declaró la invalidez del conocido como "Escudo de Privacidad" o *Privacy Shield* entre Europa y Estados Unidos tras considerar que las garantías adecuadas, los derechos exigibles y las acciones legales efectivas en este país no gozaban de una protección equivalente a la garantizada dentro de la UE por el RGPD.[5] Se trata de un pronunciamiento con efectos trascendentales para la certificación, que debería —ahora sí— coronarse como un mecanismo pionero en la búsqueda de alternativas que garantice el intercambio de datos personales entre distintos Estados miembros y Estados Unidos, y que, de este modo, asegure en toda su extensión que el nivel de protección de las personas físicas previsto por el

2 Otros estándares adoptan criterios relacionados con la protección de la información y datos personales: UNE-EN e ISO/IEC 29100:2020 (ratificada). Tecnología de la información. Técnicas de seguridad. Marco de privacidad: UNE-EN e ISO 29134:2017 relativa a tecnología de la información. Técnicas de seguridad. Directrices para la evaluación del impacto de la privacidad y 29151:2017 sobre tecnología de la información. Técnicas de seguridad. Código de prácticas para la protección de la información de identificación personal; UNE-EN e ISO 9001:2015. Sistemas de gestión de la calidad. Requisitos, UNE-EN e ISO 22301:2015. Protección y seguridad de los ciudadanos. Sistema de gestión de la continuidad del negocio. Especificaciones. ISO/IEC 27017:2015. Tecnología de la información. Técnicas de seguridad. Código de prácticas para controles de seguridad de la información basado en ISO/IEC 27002 para servicios en la nube y UNE-EN e ISO/IEC 27018:2020 (ratificada). Tecnología de la información. Técnicas de seguridad. Código de práctica para la protección de identificación personal (PII) en nubes públicas que actúan como procesadores PII (ISO/IEC 27018:2019).

3 UNE-EN e ISO/IEC 27000:2019. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI). Visión de conjunto y vocabulario. En España, el Comité Técnico de Normalización 320 de UNE: Ciberseguridad y Protección de Datos Personales es el encargado de confeccionar y revisar las normas de la serie 27000

4 STJUE, *Data Protection Commissioner c. Facebook Ireland and Maximillian Schrems,* de 16 de julio de 2020. Asunto C-311/18 (ECLI:EU:C:2020:559).

5 Ello, tras determinarse que "la primacía de las exigencias relativas a la seguridad nacional, el interés público y el cumplimiento de la ley estadounidense" suponían una clara injerencia en los derechos fundamentales de las personas cuyos datos personales son transferidos a ese país (párrafo n.º 164 y sig.). Por analogía, véase igualmente STJUE, *Schrems*, de 6 de octubre de 2015. Asunto C-362/14, párrafo 86 (EU:C:2015:650).

RGPD no se vea menoscabado —y sin obviar fructíferas relaciones comerciales de la Unión Europea (UE) a nivel internacional— (considerando 101 y arts. 42.2 y 44 y sig. RGPD).

2 La certificación en materia de protección de datos

2.1 El concepto de los mecanismos de certificación en el RGPD y su experiencia en España, Francia y el Reino Unido

Los mecanismos de certificación de la privacidad y de protección de datos adquirieron notoria popularidad en la década pasada, en un mercado difuso y heterogéneo, donde una gran multitud de ellos operaba a nivel comunitario (Rodrigues, 2018, p. 149; Rodrigues et al., 2013, p. 30). Consecuentemente, la certificación no aseguraba *per se* un alto nivel de protección, un hecho agravado ante la generalizada indisponibilidad y trabas en el acceso a la información, la dificultad para encontrar sus criterios técnicos o las comunes barreras idiomáticas. Por si fuera poco, el ambiente de autorregulación interfería en la confianza de estos mecanismos, principalmente, ante la falta de supervisión reglamentaria y de armonización o el posible uso indebido por parte de terceros o su potencial engañoso (Rodrigues et al., 2013, p. 17).

Sin embargo, tras la aplicación del RGPD y ulterior desarrollo nacional, la certificación en este ámbito marcó un precedente en el impulso de una disciplina necesaria ya no únicamente para reforzar los derechos de protección de datos de las personas, sino también para facilitar la libre circulación de los datos personales en el conocido "mercado único digital"[6] y disminuir la ineficiencia vinculada a la gran carga administrativa. Es más, en aras de aumentar la transparencia y el cumplimiento del mencionado reglamento, el considerando 100 apostó por la creación de nuevas medidas de certificación que solventen los graves conflictos señalados con miras a facilitar a los interesados la evaluación del nivel de protección de datos de una o más operaciones de procesamiento y facultando a que el usuario "[...] de un modo sencillo, e incluso automático, conozca el nivel de protección de datos de los productos y servicios que considere utilizar" (Prego de Oliver, 2017, p. 66).

En el año 2019, el Comité Europeo de Protección de Datos (CEPD) concretó la asignación de tres componentes centrales para evaluar de una operación de procesamiento, englobando: los datos personales, los sistemas técnicos —infraestructura utilizada para procesar datos personales— y los procesos y procedimientos relacionados con las operaciones de procesamiento de datos (CEPD, 2019, p. 13). Por ende, aunque la certificación se encuadra *estricto sensu* como mecanismo fundamentalmente voluntario, este a su vez fomenta la adopción de medidas proactivas que eviten menoscabos en la protección efectiva de los datos personales, asegurando asimismo la seguridad y la portabilidad de los datos e impidiendo —o, cuanto menos, reduciendo— el régimen sancionador previsto en el presente reglamento. Precisamente, el artículo 83.2.*j* del RGPD dispone que la adhesión a mecanismos de certificación puede tenerse en cuenta para determinar la cuantía de la multa,[7] lo que evidencia la firme apuesta por implementar y certificar como medida proactiva de violaciones de datos personales. Dicha disposición no puede llevar a considerar que su obtención otorgue un salvoconducto automático hacia la exculpación en caso de infracción (López, 2017, p. 93).

Tras la efectiva aplicación del RGPD, los mecanismos de certificación se encuadran como uno de los instrumentos proactivos por excelencia para promover la protección de privacidad desde el inicio, esto es, poniendo especial énfasis en su labor de prevención de las brechas de protección de datos o *data breaches*. En efecto, ni la ausencia de regulación ni la regulación reglamentaria íntegra son opciones viables para el futuro de la certificación de privacidad y protección da datos, sino un enfoque eminentemente corregulatorio en el que, como plasma el considerando 81 del RGPD, la adhesión a un mecanismo de certificación aprobado "puede servir" de elemento para demostrar el cumplimiento de las obligaciones del presente reglamento.

En definitiva, el RGPD se limita a establecer la mera posibilidad de demostrar el cumplimiento por medio de la certificación, atribuyendo a la iniciativa privada el desarrollo y el alcance de la misma. Este diseña la certificación como un nuevo instrumento de "autorregulación supervisada" (Lachaud, 2018, p. 245), término

6 Sobre el Mercado único digital, véase la propuesta de Reglamento relativo a un mercado único de servicios digitales (Ley de servicios digitales), de 15 de diciembre de 2020. COM(2020) 825 final.

7 Las condiciones generales para la imposición de multas administrativas se prevén expresamente en el artículo 83 del RGPD, mientras que las sanciones se regulan en el artículo 84 del RGPD.

que goza de una enorme amplitud por cuanto exige promover e implementar mecanismos de certificación para garantizar el cumplimiento de sus disposiciones, aunque estos no certifican *per se* el cumplimiento exhaustivo de la legislación de protección de datos.

El apartado 1.º del artículo 42 del RGPD establece la función de promoción de los mecanismos de certificación por parte de los Estados miembros, las autoridades de control, el CEPD y la Comisión. Su aplicación debe llevarse 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 parece especificar implícitamente las cuatro vías sobre las cuales se asienta la futura viabilidad de la certificación, esto es: la labor de promoción, el fomento y continuo apoyo del régimen de certificación; la acreditación de los organismos de certificación, la certificación por las autoridades o agencias de protección de datos (APD), o la coexistencia de las tres anteriores (Fernández y Recio, 2016, p. 12; García, 2016, p. 12; Rodrigues et al., 2016, p. 8).

Además, el RGPD tipifica expresamente la naturaleza jurídica de la certificación, el *principio de voluntariedad y publicidad* vinculado a la transparencia del proceso (art. 42.3.º RGPD). Fruto de ello, continúa disponiendo que los mecanismos de certificación no limitan la responsabilidad del responsable o encargado del tratamiento (art. 42.4.º RGPD). Ahora bien, estos pueden acogerse a los mismos para 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 (art. 42.2.º RGPD). No obstante, en estos supuestos, deberá formalizarse el correspondiente contrato entre las partes o proceder a adoptar otros instrumentos jurídicamente vinculantes.

Ciertamente, este reglamento proporciona un mecanismo basado en la práctica de certificación de los últimos años, cuya actividad certificadora exige la plena participación de los organismos de certificación a través de una serie de requisitos:

a) La obligación de que estos instrumentos se expidan por organismos de certificación, por la autoridad de control competente[8] o por el CEPD,[9] y, en el supuesto de que los criterios requeridos en la certificación sean aprobados por este último, podrá dar lugar al llamado Sello Europeo de Protección de Datos de acuerdo con el artículo 43.5 del RGPD.

Dicha iniciativa tiene su precedente en el conocido Sello Europeo de la Privacidad (EuroPriSe), una propuesta de certificación de la UE fundada en el año 2007 para solventar los problemas que afectaban a los anteriores sellos de privacidad, concretamente, la generalizada desconfianza en este tipo de mecanismos. Este sentó las bases en la creación de una certificación del RGPD con validez general para el ámbito de aplicación del mismo. La versión v201701 vigente se encuentra operativa desde enero de 2017 e incorpora —con carácter general— las disposiciones legales del RGPD (EuroPriSe, 2017), lo que permite a las organizaciones certificadas demostrar la aplicación del marco legislativo europeo de protección de datos. Asimismo, proporciona una contundente respuesta a uno de los supuestos conflictivos más destacados que presentan determinados productos, servicios o sistemas TI, como es el caso de los drones, esto es: "[...] la necesidad de desarrollar un proceso de reconocimiento mutuo de las certificaciones y autorizaciones expedidas por los diferentes países dentro del entorno europeo, objetivos harto complicados debido tanto a la extensión de las áreas a las que afecta como a la necesidad de alcanzar soluciones globalmente aceptadas" (Pauner, 2016, p. 112).

Este sello posee un alcance territorial exclusivamente europeo —frente a la internacionalización de las normas ISO— e incluye criterios al RGPD a la par que referencias a los derechos de los usuarios y a la confianza de los productos, servicios o sistemas TI certificados. Una de las ventajas competitivas radica en el hecho de que su certificación permite a aquellas organizaciones que no pueden certificarse conforme a los estándares ISO/IEC demostrar el cumplimiento general del RGPD. Pese a todo, no conviene obviar dos inconvenientes de esta certificación: 1) solo tiene en cuenta el tratamiento de datos personales mediante nuevas tecnologías, y 2)

8 De conformidad con el artículo 58.3.º del RGPD, la autoridad de control posee, entre otras, la función de acreditar los organismos de certificación con arreglo al artículo 43, expedir certificaciones y aprobar criterios de certificación con arreglo al artículo 42.5.º.

9 Según establece el artículo 63 del RGPD con respecto al mecanismo de coherencia, se requiere la cooperación entre las autoridades de protección de datos entre sí y con la Comisión.

todavía no ha recibido el respaldo y aprobación de las distintas autoridades de control ni del CEPD conforme dispone el apartado 5.º del artículo 42 del RGPD.

Igualmente, vinculado a EuroPriSe, se han promovido otras iniciativas por parte de expertos en protección de datos, como el caso de *GDPRtEXT*. Este pretende certificar el cumplimiento de la normativa de protección de datos mediante un cuestionario basado en los requisitos del RGPD y EuroPriSe, transcribiendo estos criterios en un banco de preguntas que se emplean durante una auditoría y cuyas respuestas determinan el grado de cumplimiento de estas obligaciones legales (Pandit et al., 2018, p. 12).

b) Por su parte, el apartado 6.º del artículo 42 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, una disposición que permite al organismo de certificación decidir acerca del tratamiento que lleva a cabo una organización en el seno de su actividad. Todo ello, sin perjuicio de concretar el tiempo de expedición en los respectivos certificados y durante un período máximo de tres años renovables en las mismas condiciones conforme a lo dispuesto en el apartado 7.º.

El Grupo de trabajo del artículo 29 (GT 29) apuntó en el año 2018 que las normas de certificación debían incluir conocimientos especializados de protección de datos (GT 29, 2018, p. 12). Tal afirmación fue complementada ese mismo año por el CEPD, que recalcó que la certificación debía centrarse en demostrar el cumplimiento exhaustivo de sus disposiciones, incluyendo los siguientes tres componentes principales: los datos personales (alcance material del RGPD); los sistemas técnicos como la infraestructura, *hardware* y *software* o empleados que procesan datos personales, y los procesos y procedimientos relacionados con la operación de procesamiento (CEPD, 2018).

En este punto, conviene tener presente que el RGPD ha dotado de "relevancia legal a las conocidas certificaciones" (Hidalgo, 2016, p. 727). Los distintos modelos de certificación se encuentran regulados en el artículo 42 del RGPD y han sido diseñados como cláusula abierta, lo que implica no solo que los ordenamientos jurídicos nacionales tienen la facultad de desarrollar su extensión y su mayor o menor alcance, sino que las autoridades de supervisión están plenamente facultadas para emplear todo su conocimiento en este ámbito con objeto de evaluar los criterios de certificación en el ámbito de la protección de datos. Tanto es así que las APD europeas han ido implementando en los últimos años distintas iniciativas susceptibles de ser certificadas y que, en efecto, especifican aspectos técnicos y jurídicos relevantes que exceden de los previstos en sus ordenamientos jurídicos.

En España, la Agencia Española de Protección de Datos (AEPD) fue una de las primeras APD en elaborar un marco de referencia para los delegados de protección de datos (DPD). Junto con la Entidad Nacional de Acreditación (ENAC), presentó el "Esquema de certificación de DPD" actualizado en diciembre de 2019 (AEPD, 2019). Este certifica a delegados mediante un examen en el que se evalúan los conocimientos y capacidades técnicas o profesionales (AEPD, 2019, p. 16) a través unos criterios de certificación elaborados por esta autoridad de control en colaboración con distintas partes interesadas. En esta misma línea, la Agencia Catalana de Protección de Datos (APDCAT) ha sido pionera en llevar a cabo un curso de certificación de los DPD para desempeñar sus funciones en el sector público catalán. Una iniciativa de certificación impulsada en coordinación con la Escuela de Administración Pública de Cataluña (EAPC) muy pertinente que ha puesto en valor la figura del DPD mediante una formación especializada y la concreción de unos requisitos que deben cumplir para la obtención de la correspondiente certificación específica.[10]

Por su parte, la Agencia de Protección de Datos de Francia (CNIL) también aprobó su primera certificación de habilidades del DPD conforme a su Ley de Protección de Datos, modificada por la Ley del 20 de junio de 2018, que otorgó a esta APD nuevas competencias en materia de certificación de personas. Consecuentemente, el 20 de septiembre de 2018 adoptó dos estándares para la certificación de DPD, un sistema de certificación de referencia que fija las condiciones de admisibilidad de las solicitudes, proporcionando un listado de diecisiete habilidades y conocimientos objeto de certificación.[11]

10 https://apdcat.gencat.cat/es/actualitat/noticies/noticia/LEscola-dAdministracio-Publica-i-lAutoritat-Catalana-de-Proteccio-de-Dades-presenten-el-primer-curs-de-certificacio-de-delegats-de-proteccio-de-dades-del-sector-public-catala.

11 Délibération n° 2018-318 du 20 septembre 2018 portant adoption des critères du référentiel de certification des compétences du

Se trata de un marco de acreditación que establece los criterios aplicables a las organizaciones que desean ser acreditadas por la CNIL para certificar las habilidades de los DPD.[12] Como destacó esta agencia, el funcionamiento de este sistema será objeto de reevaluación, a más tardar, en un plazo de dos años desde su entrada en vigor con el fin de adaptar y actualizar, si resulta necesario, los requisitos de las normas al esquema mencionado —aunque asegura que cualquier cambio en el sistema no afectará a las certificaciones o aprobaciones que ya se han emitido.[13]

Por lo que se refiere al Reino Unido, pese a que este país no cuenta todavía con un esquema de certificación del RGPD, el 28 de febrero de 2020 su APD, el Information Commissioner's Office (ICO), promovió una consulta pública para que las organizaciones presentaran sus propuestas para la futura la aprobación de los criterios del esquema de certificación.[14] Ahora bien, el alcance de sus esquemas de certificación está diseñado para abarcar, dentro de una operación específica de procesamiento de datos personales, un conjunto de operaciones evaluadas de acuerdo con los criterios previstos por el esquema de certificación y desarrollados por el organismo de certificación acreditado.

A diferencia de España o Francia, en el Reino Unido la certificación no puede emplearse para certificar a personas —como es el caso de los DPD—, sino únicamente a responsables y encargados de tratamiento de datos. Del mismo modo, conviene tener presente que, en septiembre de 2020, el ICO concluyó su Código de Prácticas, un documento que proporciona recomendaciones para aquellas organizaciones que recopilan datos personales de usuarios en el Reino Unido y que tiene previsto incorporar un esquema de certificación de adhesión a este código a finales de 2021.[15]

Dicho esto, y pese a las iniciativas anteriormente expuestas, lo cierto es que queda un largo camino para que la certificación sea una realidad plena. Todavía no se dispone de un esquema de certificación conjunto impulsado por las APD, respaldado por el CEPD y con validez general en todo el ámbito de aplicación del RGPD. Por lo tanto, estas autoridades deberán continuar cooperando y coordinándose entre sí para respaldar nuevos esquemas de certificación comunes y coherentes que definan aquellas especificaciones técnicas, criterios y requisitos de aquellos productos, servicios o sistemas TI susceptibles de certificación en el marco de la protección de datos (Rallo et al., 2015, p. 741; Rodrigues et al., 2016, p. 9).

2.2 Los organismos de certificación en el RGPD y su desarrollo en la norma ISO/IEC 17065:2012

A pesar de que los organismos de certificación se encuentran regulados en el artículo 43 del RGPD, estos no se encuentran conceptualizados como tales, sino que, en su defecto, contempla un exhaustivo catálogo de funciones y obligaciones en el marco del proceso de certificación. El apartado 1.º dispone que estos organismos tienen el deber de expedir y renovar las certificaciones una vez informada la autoridad de control, a fin de que esta que pueda retirar una certificación u ordenarle que no se emita si no se cumplen o si dejasen de cumplirse los requisitos para seguir manteniendo la certificación. Además, con objeto de asegurar su buen funcionamiento, los Estados deben garantizar que dichos organismos de certificación sean acreditados, bien por la autoridad de control, bien por el organismo nacional de acreditación, o por ambos. En el caso de los organismos nacionales de acreditación designados en el plano nacional, estos deben aplicar el Reglamento n.º 765/2008, por el que se establecen los requisitos de acreditación y vigilancia del mercado relativos a la comercialización de los productos (apartado 3.º).

Este precepto ha supuesto que cada Estado haya seguido un modelo distinto de control. Por ejemplo, en España el modelo de acreditación de las entidades de certificación del artículo 41.1 del RGPD ha sido concretado en el

délégué à la protection des données.

12 Délibération n° 2018-317 du 20 septembre 2018 portant adoption des critères du référentiel d'agrément d'organismes de certification pour la certification des compétences du délégué à la protection des données.

13 Desde el 4 de julio de 2019, Afnor Certification está acreditado por la CNIL para certificar este esquema durante un período de cinco años y asegura que el organismo aprobado cumple con las normas e instrucciones de esta APD.

14 https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/12/statement-on-ico-approved-certification-schemes.

15 https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/12/ico-publishes-new-data-sharing-code-of-practice.

artículo 39 de la LOPDGDD, y atribuye a la ENAC la función de acreditación.[16] Del mismo modo, el Servicio de Acreditación del Reino Unido o United Kingdom Accreditation Service (UKAS) es el organismo nacional de acreditación responsable de determinar la competencia técnica y la integridad de organizaciones que ofrecen servicios de certificación.[17] En cambio, en Francia la CNIL también ostenta el poder de acreditación de los organismos de certificación (Tambou, 2016, p. 44).

Seguidamente, una vez los organismos de certificación han sido acreditados, están facultados para desarrollar su plena actividad certificadora. Estos deben demostrar su independencia y pericia en relación con el objeto de la certificación, establecer procedimientos para la expedición, la revisión periódica y la retirada de certificaciones, sellos y marcas de protección de datos, así como disponer de procedimientos y estructuras eficientes y eficaces en el tratamiento de las reclamaciones relativas a infracciones de la certificación (art. 43.2.º RGPD). Las citadas actuaciones se encuentran plenamente sujetas a las instrucciones aprobadas por la autoridad de control, al margen de su responsabilidad durante el inicio —concesión— o finalización —retirada—, que, en todo caso, deberán ser motivadas (art. 43.5.º RGPD). Todo ello, dotando a las autoridades de control o los organismos nacionales competentes de poderes de revocación en los casos en los que el organismo de certificación no cumpla o deje de cumplir las condiciones de la acreditación (art. 43.7.º RGPD).

Esta amplia facultad conferida a las autoridades de control o supervisión supone una novedad en la certificación que pretende reforzar el control en este tipo de iniciativas que han sido esencialmente autorreguladas. Se confiere al organismo de certificación funciones ordinarias para realizar el procedimiento de certificación y supervisar eficazmente la certificación emitida, con idependencia de la supervisión llevada a cabo por las autoridades de control.

Esta doble intervención —y, en concreto, la novedad de incluir a las autoridades de control— refleja el espíritu de elevar las garantías de la certificación en el ámbito de protección de datos. Sin embargo, esta extensión en el control de la certificación lleva a preguntarse cuál es el verdadero papel de las autoridades de control, puesto que nada se dispone sobre si estas son o no responsables en aquellos supuestos donde la certificación es inexacta, falsa u obsoleta —recordemos que estas están obligadas a revisar periódicamente los certificados emitidos— (art. 57.1.*o* RGPD). Este hecho podría acarrear cierto grado de reticencia y desconfianza entre las distintas APD (Kamara y De Hert, 2018, p. 20).

Es más, esta falta de tipicidad en el régimen de responsabilidad ha supuesto una de las principales barreras al reconocimiento transfronterizo de los mecanismos de certificación en este ámbito —ya no solo porque no esté expresamente regulado en el RGPD, sino por el amplio margen de maniobra del que disponen las autoridades de control para supervisar los mecanismos de certificación.

Con todo, este precepto no proporciona suficientes garantías en lo que afecta a la acreditación de criterios relativos a capacidad, integridad e independencia del organismo de certificación, aspectos sumamente relevantes que desarrolla —en toda su extensión— el estándar internacional ISO/IEC 17065:2012, por el que se regulan los requisitos de los organismos de certificación y que establece los "requisitos para la competencia, funcionamiento constante e imparcialidad de los organismos de certificación de productos, procesos y servicios" TI para la actividad de evaluación de la conformidad por parte de terceros. Dicho estándar pretende garantizar el cumplimiento de sus requisitos, la competencia e imparcialidad del proceso establecido en dicha conformidad, y, por ende, crear confianza en el cumplimiento de sus requisitos.[18]

16 El Gobierno designó a ENAC como único organismo nacional de acreditación independiente dotado de potestad pública para otorgar acreditaciones mediante la promulgación del 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. BOE, n.º 7, de 08/01/2011, pp. 1670-1673.

17 El UKAS es designado como el organismo nacional de acreditación por el Reglamento de Acreditación 3155/2009 y opera bajo un "Memorando de Entendimiento" con el Gobierno, a través de la Secretaría de Estado del Departamento de Negocios, Energía y Estrategia Industrial.

18 UNE-EN e ISO/IEC 17012:2012. Evaluación de la conformidad. Requisitos para el funcionamiento de diferentes tipos de organismos que realizan la inspección.

3 Las implicaciones de la norma ISO/IEC 27001 sobre seguridad de la información en el derecho a la protección de datos

3.1 La norma ISO/IEC 27001 y su conexión con el RGPD

La norma ISO/IEC 27001:2017[19] representa el marco internacional para la gestión de la seguridad de la información de las organizaciones e insta a la implementación de un modelo adecuado para establecer, implementar, operar, vigilar, revisar y administrar un SGSI. Constituye el precedente por antonomasia de certificación compatible con las exigencias del RGPD, pues insta a las organizaciones a la adopción de medidas organizativas y técnicas necesarias para asegurar un alto nivel de seguridad de la información conforme al artículo 32 del RGPD. Tanto es así que desarrolla controles y medidas de seguridad que pueden minimizar los riesgos jurídicos, técnicos o económicos sobre los que no se pronuncia de manera directa el mencionado reglamento.

El objetivo de esta norma se ha centrado en abordar los riesgos de seguridad de la información, posicionándose como una solución innovadora y de gran impacto global para combatir una gran tipología de riesgos y orientar a los operadores en sus actuaciones ordinarias. Es por ello por lo que se trata de un mecanismo relevante en el ámbito de la protección de datos que ofrece respuestas a la prevención de brechas en la privacidad y en la protección de los datos de los usuarios. Es más, esta norma ha venido complementándose con la ISO/IEC 27002:2017 sobre Seguridad de la Información,[20] la cual provee una serie de buenas prácticas para la gestión de la seguridad de la información a la par que aboga por preservar la confidencialidad, integridad y disponibilidad de la misma (Diamantopoulou et al., 2020, p. 645 y sig.). Sin embargo, ambas tienen objetivos distintos. Mientras que la norma ISO 27001 establece buenas prácticas para la gestión de la seguridad de la información, la gestión de riesgos y la adopción de medidas de seguridad para los SGSI, la ISO 27002 proporciona una lista de controles y buenas prácticas que pueden adoptarse como guías de referencia a la hora de implementar medidas tendentes a asegurar la seguridad de la información.

A diferencia del artículo 24 del RGPD, las mencionadas normas ISO desarrollan y especifican modelos de "buenas prácticas" en relación con la seguridad de la información, permitiendo a las organizaciones gestionar adecuadamente el procesamiento de los datos personales. Tales constatables beneficios se asemejan a una nueva variante de "moneda en la economía digital" en el intento por describirlos como herramientas sumamente valiosas para acometer los desafíos más esenciales que afectan a la aplicación del RGPD. Estos estándares se enmarcan —posiblemente— como la única solución viable para adaptarse a los continuos cambios de los productos y sistemas que procesan información personal relevante a los efectos del RGPD (Datoo, 2018, p. 17).

De tal forma, la norma ISO 27001 describe tres aspectos esenciales de la seguridad de la información: las personas, los procesos y la tecnología, un triple enfoque que concede a las organizaciones una función de protección de aquellas injerencias y amenazas comunes internas y externas y les brinda información relevante sobre la seguridad informática (Bilbao et al., 2011, p. 2 y sig.). Sin embargo, una de las cuestiones más destacables de esta norma estriba en su conversión como "referente global" tras su estrecha coherencia con los requisitos que prevé el artículo 42 del RGPD. De hecho, la certificadora canadiense Professional Evaluation and Certification Board (PECB) publicó un primer documento en el que relaciona los requisitos técnicos de la norma ISO/IEC 27001 –actualizado tras la publicación de la especificación de esta norma por el estándar ISO/IEC 27701 que abordaremos en el siguiente epígrafe– (PEBC, 2020, p. 10) con las cuestiones previstas en el RGPD, las cuales merecen concretarse en los siguientes tres puntos:

1. Por lo que se refiere a la responsabilidad proactiva en la protección de los datos y la evaluación de los riesgos asociados, el considerando 85 y el artículo 5.2 del RGPD instan a la realización de evaluaciones periódicas que identifiquen amenazas y vulnerabilidades específicas que pueden afectar

19 UNE-EN e ISO/IEC 27001:2017. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos.

20 UNE-EN e ISO/IEC 27002:2017. Tecnología de la información. Técnicas de seguridad. Código de prácticas para los controles de seguridad de la información. Para finales del año 2021 está prevista la publicación de una versión actualizada de esta norma, que está ya en un avanzado estado de revisión. El borrador puede consultarse en este enlace.

a los activos de información de las organizaciones, adoptando medidas eficaces para proteger esos datos.[21] Ello, tomando en consideración el "nivel de seguridad adecuado" (art. 32.2 RGPD) y la identificación inequívoca del responsable en toda la organización (art. 30 RGPD), aspectos que implementa directamente la norma ISO 27001 al prever que las organizaciones nombren a una persona que asuma la responsabilidad del SGSI (Lopes et al., 2019, p. 5).

2. Como ya hemos hecho referencia con anterioridad, el ámbito de aplicación de esta norma ISO resulta más concreto y determinado que el citado reglamento, puesto que especifica aquellas obligaciones que deben cumplir las organizaciones para garantizar la seguridad de la información (Irwin, 2018). En esta línea, la certificación de la norma ISO pretende promover la gestión eficaz de los riesgos de seguridad de la información de las organizaciones, adoptando las mejores prácticas internacionales en relación con procesos que incluyen una amplia tipología de información que excede de los datos personales a los efectos del citado reglamento. Su especial amplitud radica en la certificación no solo de personas, sino que se extiende a los procesos y la tecnología, lo que implica que las organizaciones pueden protegerse de los riesgos causados tanto por el funcionamiento de los productos, servicios o sistemas TI como por el personal que no está lo suficientemente formado o de aquellos procedimientos que resultan ineficaces.

3. Aunque el RGPD pretende demostrar mediante la certificación el cumplimiento de sus disposiciones, lo cierto es que la norma ISO lleva a cabo pruebas y auditorías periódicas que permiten reflejar, de forma actualizada, que su régimen de seguridad está funcionando de manera efectiva. Todo ello, mediante una evaluación independiente que determina si la organización en cuestión ha implementado aquellas medidas adecuadas para proteger los datos personales, un aspecto pertinente que pretende incrementar la escasa seguridad jurídica que han dispuesto comúnmente las iniciativas corregulatorias (ENISA, 2017, p. 10; Hildebrandt y Tielemans, 2013, p. 512; Kamara, 2017, p. 10).

Las medidas de seguridad de la ISO 27001 deben interpretarse en todo momento con los principios de integridad y disponibilidad que regula el artículo 5.1.*f* del RGPD. También debe aplicarse en sintonía con el concepto de "resiliencia", es decir, la capacidad de respuesta de la organización ante incidentes que puedan comprometer la seguridad de la información (Saiz, 2019, p. 389), y que, por consiguiente, requiera la adopción de todas aquellas medidas técnicas y organizativas adecuadas que reúnan un nivel de seguridad acorde al riesgo (art. 32 RGPD).

Cabe igualmente poner de manifiesto que la norma ISO 27001 se centra en reducir los riesgos para la seguridad de la información, constriñendo a las organizaciones a mantener la mejora continua del SGSI. Se trata de un procedimiento ineludible para garantizar el cumplimiento del RGPD, y que, como destacó la Asociación Internacional de Profesionales en Privacidad (IAPP, 2018), fomenta la concienciación del respeto de la protección de datos en el seno de las organizaciones, identificando —de concreto a genérico— aquellas medidas de seguridad más apropiadas. No menos relevante resulta la exigencia del establecimiento de una política de protección de datos a las organizaciones que pretenden certificarse, la cual debe detallar el procedimiento de tratamiento de datos con objeto de proporcionar orientación estratégica a la dirección y al personal de la organización y garantizar el cumplimiento del RGPD. Esta resulta aplicable a la totalidad tanto de los sujetos susceptibles de llevar a cabo directa o indirectamente un tratamiento de datos personales como de los procesos operativos disponibles a los efectos del mencionado reglamento.

Pese a todo, esta política no tiene entidad propia, puesto que pertenece —en sentido amplio— al ámbito de la seguridad de la información, un hecho que debería diferenciarse de una forma más precisa para proporcionar información sobre múltiples aspectos organizativos sobre protección de datos, tales como: la gestión de la recopilación del consentimiento, el cumplimiento de los derechos de los interesados, la transferencia de datos personales —incluso a terceros países—, la supervisión de las actividades de procesamiento de datos personales o la adaptación de los principios de protección de datos por diseño y por defecto con respecto a los sistemas y aplicaciones de la organización (Lambrinoudakis, 2018, p. 5).

21 La AEPD publicó la Guía práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD, en la que describe los procedimientos para proceder a la realización de un análisis de riesgos con objeto de establecer medidas de seguridad y control para garantizar los derechos y libertades de las personas.

Más allá de la perspectiva jurídica, el vínculo entre la norma ISO/IEC 27001 y el RGPD también ha sido examinado desde la perspectiva de la eficiencia. Así, a pesar de que ambas normas comparten el fiel compromiso de procesar y almacenar adecuadamente los datos confidenciales y sensibles, el proceso de certificación de esta norma permite a las organizaciones evitar la duplicidad de esfuerzos, costes y tiempo en el cumplimiento de las disposiciones del RGPD e incrementar la eficiencia comercial, y, en consecuencia, una mayor facilidad en el logro de sus objetivos (Middleton-Leal, 2018).

No cabe duda de que la certificación de la norma ISO/IEC 27001 puede aportar verdaderos beneficios en la gestión y funcionamiento interno de una organización, en efecto, tras ser diseñada como herramienta técnica que proporciona instrucciones claras sobre cómo proteger la información y reducir paralelamente las amenazas cibernéticas. Ahora bien, cabe resaltar que no contiene ninguna referencia expresa a los derechos de los interesados (capítulo 3 RGPD) y, con ello, toda una serie de cuestiones esenciales en la propia normativa de protección de datos quedan al margen de su ámbito de aplicación.[22]

Paralelamente, la naturaleza jurídica del RGPD supone, a grandes rasgos, una carencia de concreción técnica que, por el contrario, desarrollan en toda su extensión los estándares técnicos. La norma ISO/IEC 27001 ha suplido tales lagunas, proporcionando instrucciones en la implementación de acciones tendentes a minimizar los riesgos de seguridad que podrían conducir a incidentes de gran calado en el seno de una organización. Es más, como examinamos en el siguiente epígrafe, en el año 2019 fue publicada una extensión de esta norma, el estándar ISO/IEC 27701 para la gestión de la información de privacidad, la cual concreta una serie de requisitos y directrices mediante el establecimiento, implementación, mantenimiento y mejora continua de un sistema de gestión de información de privacidad. No se trata de un nuevo estándar, sino de una extensión de la ISO/IEC 27001 que especifica los aspectos sobre privacidad que deben adoptarse por parte de las organizaciones. De tal forma, estas deben disponer, con carácter previo, de la certificación de la mencionada norma para compatibilizar el cumplimiento de los criterios técnicos de seguridad de la información y de privacidad, integrando de este modo los requisitos previstos por el RGPD.

Por último, cabe destacar que la norma ISO 27001 contempla la incorporación de un/a director/a de Seguridad de la Información (u oficial de Seguridad),[23] profesional encargado/a de coordinar la totalidad de las actividades relacionadas con la gestión de la seguridad de la información en el seno de la organización certificada. Se trata de un precepto no vinculante —muy presumiblemente, por un aumento de costes que pudiera comprometer la viabilidad de algunas organizaciones, especialmente las de menor tamaño— y que se justifica en el propio espíritu de la norma, habida cuenta de que esta pretende adaptarse a la práctica totalidad de estas organizaciones.

El criterio de selección de esta figura debe centrarse no solo en las aptitudes y experiencia sobre TI, sino también en el conocimiento exhaustivo de los procesos de negocio (*business processes*) de la organización para desarrollar en el seno de la misma una cultura de seguridad basada en el riesgo. Ello, teniendo en cuenta que asume una serie de responsabilidades de distinta índole, tales como: la definición y supervisión del SGSI, la coordinación de todas las actividades relacionadas con el SGSI, la comunicación de información relacionada con el SGSI, el contacto con las autoridades y grupos de interés en el área del SGSI, la coordinación del proceso de gestión de riesgos, y la supervisión y coordinación del SGSI.

En este sentido, a diferencia de las funciones del DPD (art. 37 y sig. RGPD), el oficial de Seguridad a los efectos de certificación no tiene por qué conocer exhaustivamente la legislación de protección de datos, sino que se centra en la gestión de riesgos asociados con todos los procesos de negocio, administrando, entrenando y coordinando todos los aspectos de la seguridad de la información en las actividades de la organización. El DPD ostenta un papel intermedio e independiente entre los interesados, los responsables de datos y las autoridades de supervisión.

22 Véanse el consentimiento (art. 4.11.º RGPD), el derecho al olvido (art. 17 RGPD), la limitación de tratamiento (art. 18 RGPD), la rectificación o supresión de datos personales o la limitación del tratamiento (art. 19 RGPD), la portabilidad de datos (art. 20 RGPD), el derecho de oposición (art. 21 RGPD) o las transferencias internacionales (art. 44 y sig. RGPD).

23 Se emplea comúnmente el término en inglés *Chief Information Security Officer* (CISO).

Sobre esta diferenciación, en septiembre de 2018, el Tribunal Administrativo Regional de Primera Instancia de Friuli Venezia Giulia (Italia)[24] dictaminó que la certificación como auditor/auditor principal de la norma ISO/IEC 27001 no podía equipararse a la figura de DPO, porque mientras que el auditor de las normas ISO 27001 dispone principalmente de habilidades técnicas, la labor del DPO radica en sus conocimientos legales. En consecuencia, el DPD no requiere de certificación, sino que sus conocimientos jurídicos pueden reflejarse de diferentes formas, por ejemplo, participando en seminarios o publicando artículos legales. Lo verdaderamente relevante es su ineludible independencia, cuestión que lo diferencia radicalmente del oficial de Seguridad y, como tal, "[...] no puede ocupar un cargo en la organización que le lleve a determinar los fines y medios del tratamiento de datos personales. Debido a la estructura organizativa específica de cada organización, esto deberá considerarse caso por caso" (GT 29, 2017, p. 18).

3.2 La norma ISO/IEC 27701:2019 sobre gestión de la información de privacidad

Finalmente, el novedoso estándar ISO/IEC 27701:2019 sobre gestión de la información de privacidad[25] constituye una extensión de las normas ISO/IEC 27001 y 27002, que integran la "seguridad de la información y la privacidad". Este estándar extiende sus requisitos hacia la protección de la privacidad de los individuos afectados por el procesamiento de sus datos personales. De tal manera, debe considerarse que la especial similitud de estas normas con los fines que persiguen los artículos 42 y 43 del RGPD supone la internacionalización de los principios de protección de datos del RGPD. Sin embargo, voces críticas afirman que el enfoque de ISO no es similar al que consagra el RGPD, instando a que las autoridades de supervisión colmen las brechas existentes entre los dos marcos y aclaren sus relaciones en un futuro a corto plazo (Lachaud, 2020, p. 4).

Por de pronto, el sistema de gestión de información personal previsto en la ISO/IEC 27701:2019 ha sido diseñado como una extensión y mejora del SGSI de la ISO/IEC 27001:2013, mediante la efectiva integración de un conjunto de requisitos y directrices adicionales de privacidad y protección de datos personales. Ambos sistemas deben certificarse conjuntamente, de forma que la organización certificable debe asegurarse previamente de que los datos personales administrados por la entidad cumplan con los requisitos de seguridad para, así, incorporar eficazmente otros aspectos adicionales contemplados en las subcláusulas 3.2 y 5.2.3 de la ISO/IEC 27701:2019.[26]

A diferencia de la seguridad de los datos del artículo 32 del RGPD, la dimensión integrada seguridad/privacidad de los estándares técnicos no exige el cumplimiento previo de los principios de integridad y confidencialidad (art. 5.1.*f* RGPD), sino que concreta la seguridad de la información con un distinto enfoque al previsto legalmente, previniendo y abordando la probabilidad y gravedad de los riesgos de los derechos y libertades de las personas físicas. Pero lo cierto es que este nuevo estándar fomenta un enfoque basado en el riesgo, previendo aquellas medidas de seguridad genéricas aplicables a los datos personales (art. 32.1 RGPD) y concretando aquellos requisitos de protección de datos de manera específica a su contexto, procesamiento y nivel de riesgo.

Igualmente, el estándar ISO/IEC 27701:2019 define sus propios criterios, que, con cierta asiduidad, difieren de sus homólogos en el RGPD, tales como la voluntariedad de los requisitos que deben reunir los encargados de tratamiento en el caso del estándar ISO —a diferencia del RGPD, cuyo artículo 28 tiene naturaleza vinculante. Todo ello motiva que estas normas técnicas no aseguren el pleno cumplimiento de las salvaguardas de protección de datos, sino una presunción e interés en el respeto de la legislación sumamente relevante y pertinente para aquellos productos, servicios o sistemas TI que requieren de continuas modificaciones. Por lo tanto, es común encontrar excepciones a la aplicación de controles de privacidad en casos tasados y concretos, tal y como recoge la norma ISO/IEC 27001 en la subcláusula 6.1.3.*b*, los cuales se justifican siempre y cuando

24 Sentenzia Tribunale Amministrativo Regionale per il Friuli Venezia Giulia, de 5 de septiembre de 2018. Publicada el 13 de septiembre de 2018. (N. 00287/2018 REG.PROV.COLL. N. 00135/2018 REG.RIC.).

25 ISO/IEC 27701:2019. Técnicas de seguridad. Extensión a ISO/IEC 27001 e ISO/IEC 27002 para la gestión de la información de privacidad. Requisitos y directrices.

26 Principalmente, estas subcláusulas prevén el conocido como Sistema de Gestión de Información Personal (PIMS), una extensión del SGSI anteriormente abordado que se centra en criterios relativos a la privacidad.

se encuentren reflejadas en la declaración de aplicabilidad de esta norma y bajo parámetros de necesidad y proporcionalidad.

4 Reflexiones finales y desafíos de futuro más inmediatos

Tras la aplicación del RGPD, los mecanismos de certificación se coronan como una de las herramientas proactivas esenciales para adaptarse a los continuos cambios que sufren los productos, servicios y sistemas TI y evitar así el incumplimiento de la legislación de protección de datos. De hecho, el carácter de cláusula abierta de la certificación en el RGPD ha propiciado que las APD hayan concretado su mayor o menor alcance en sus sistemas nacionales, tal y como han impulsado en España, Francia o el Reino Unido, entre otros.

De igual modo, el mercado de la certificación cuenta con múltiples iniciativas tanto a nivel europeo (EuroPriSe) como internacional (este es el caso de las normas ISO/IEC de la serie 27000), que han integrado las disposiciones del RGPD en sus criterios. Estos instrumentos constituyen un primer punto de partida para colmar las demandas actuales del mercado en el cumplimiento de requisitos técnicos y legales relacionados con la seguridad de la información. Sus correspondientes certificaciones suponen una adaptación dinámica y eficiente a los nuevos criterios vinculantes del RGPD con respecto a una amplia amalgama de productos, sistemas y servicios TI. Sin embargo, desde el punto de vista de la eficacia, la certificación de ambas normas no garantiza *per se* el efectivo cumplimiento del RGPD, sino una presunción relevante susceptible de comercialización por parte de distintas certificadoras.

Indudablemente, los dos estándares técnicos de referencia analizados perfeccionan este cometido, pese a que todavía se requiere un grado de mejora considerable en su intento de aproximación hacia un mayor nivel de coherencia con el citado reglamento. Por lo que se refiere al estándar 27001, aunque protege la información desde un enfoque centrado en la seguridad, no es menos cierto que carece de referencias expresas al núcleo duro del derecho a la protección de datos, como son los derechos de los interesados. Otro de los grandes problemas radica no solo en las (todavía) escasas organizaciones certificadas conforme a la norma ISO/IEC 27001, sino que, en aquellas que sí lo están, resulta frecuente que el alcance de la certificación se centre exclusivamente en una parte concreta de los procesos de la organización, aunque presumen de estar certificadas sin ningún tipo de distinción al respecto.

En cambio, aunque el estándar ISO/IEC 27701 integra directamente las disposiciones más destacadas del RGPD, su contenido y alcance difiere sustancialmente de este. La inclusión de criterios de seguridad y privacidad en el citado estándar implica que la protección de datos depende inexorablemente de la seguridad de la información, mientras que en el enfoque que se sigue en el RGPD la seguridad se circunscribe como un componente más de la protección de datos. Asimismo, otra de las diferencias más notables radica en el hecho de que la norma ISO promueve un enfoque basado en el riesgo con el fin de identificar y abordar los riesgos que afectan a la seguridad de la información aplicables a los datos personales, mientras que en el caso del RGPD este riesgo se contempla para identificar aquellos otros que afectan a los derechos y libertades de los interesados.

Referencias bibliográficas

Agencia Española de Protección de Datos. (2019). *Esquema de certificación de Delegados de Protección de Datos (Esquema AEPD-DPD)*. Versión 1.4.

Agencia Española de Protección de Datos. (2019). *Guía práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD*.

Agencia Europea de Seguridad de las Redes y de la Información. (2017). *Recommendations on European Data Protection Certification*.Versión 1.0.

Asociación Internacional de Profesionales en Privacidad. (1 de marzo de 2018). *2018 privacy tech vendor report*.

Bajo Albarracín, Juan Carlos. (2019). Consideraciones sobre el principio de responsabilidad proactiva y diligencia (*accountability*). Experiencias desde el *Compliance*. En José López Calvo (coord.), *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD*. Madrid: Wolters Kluwer.

Bilbao, Enrique, Bilbao, Alfonso, y Peciña, Koldo. (2011). *Physical and logical Security Risk Analysis model*. IEEE.

Chatzipoulidis, Aristeidis, Tsiakis, Theodosios, y Kargidis, Theodoros. (2019). A readiness assessment tool for GDPR compliance certification. *Computer Fraud & Security*, *8*.

Comisión Europea. (2019). *Data protection certification mechanisms. Study on Articles 42 and 43 of the Regulation (EU) 2016/679: final report*.

Comité Europeo de Protección de Datos. (2018). *Directrices 1/2018 sobre la certificación y la determinación de los criterios de certificación de conformidad con los artículos 42 y 43 del Reglamento 2016/679*.

Comité Europeo de Protección de Datos. (2019). *Directrices 1/2018 sobre la certificación y la determinación de los criterios de certificación de conformidad con los artículos 42 y 43 del Reglamento*. Versión 3.0.

Comité Técnico de Normalización 320. *Ciberseguridad y protección de datos personales*.

Datoo, Akber. (2018). Data in the post-GDPR world. *Computer Fraud & Security, 9*.

Diamantopoulou, Vasiliki, Tsohou, Aggeliki, y Karyda, Maria. (2020). From ISO/IEC27001:2013 and ISO/IEC27002:2013 to GDPR compliance controls. *Information and Computer Security*, *4*.

European Privacy Seal (EuroPriSe). (2017). *EuroPrise criteria for the certification of IT products and IT-based services* (v201701).

Fernández Sánchez, Carlos Manuel, y Recio Gayo, Miguel. (2016). Certificación en protección de datos personales. En José Luis Piñar Mañas (dir.), *Reglamento General de Protección de Datos.* Madrid: Editorial Reus.

García Bernadal, Francisco. (2019). La RGPD, certificación y SGSI. *Actualidad administrativa*, *1*.

Grupo de trabajo sobre protección de datos del artículo 29. (5 de abril de 2017). *Directrices sobre los delegados de protección de datos (DPD)* (16/ES WP 243 rev.01).

Grupo de trabajo sobre protección de datos del artículo 29. (6 de febrero de 2018). *Draft Guidelines on the accreditation of certification bodies under Regulation (EU) 2016/679* (18/EN WP261).

Gudín Rodríguez-Magariños, Faustino. (2018). Nuevo *Reglamento Europeo de Protección de Datos versus Big Data*. València: Tirant lo Blanch.

Hidalgo Cerezo, Alberto. (2016). Protección de datos de carácter personal relativos a la salud del paciente: fundamentos, protección a la intimidad y comentarios al nuevo Reglamento UE 2016/679. *Revista de Derecho UNED*, *18*.

Hildebrandt, Mireille, y Tielemans Laura. (2013). Data protection by design and technology neutral law. *Computer Law & Security Review*, *29* (5).

Irwin, Luke. (2018). *How ISO 27001 helps you achieve GDPR compliance*. IT Governance.

Kamara, Irene. (2017). Co-regulation in EU personal data protection: the case of technical standards and the privacy by design standardisation "mandate". *European Journal of Law and Technology*, *8* (1).

Kamara, Irene, y De Hert, Paul. (2018). Data Protection Certification in the EU: Possibilities, Actors and Building Blocks in a Reformed Landscape. En Rowena Rodrigues y Vagelis Papakonstantinou (eds.), *Privacy and Data Protection Seals. Information Technology and Law Series*. T.M.C. Asser Press.

Lachaud, Eric. (2018). The General Data Protection Regulation contributes to the rise of the certification as a regulatory instrument. *Computer Law & Security Review*, *34* (2).

Lachaud, Eric. (2020). *ISO/IEC 27701: Threats and Opportunities for GDPR Certification*.

Lambrinoudakis, Costas. (2018). The General Data Protection Regulation (GDPR) Era: Ten steps for compliance of data processors and data controllers. *International Conference on Trust and Privacy in Digital Business*. Springer International Publishing.

Lopes, Isabel María, Guarda, Teresa, y Oliveira, Pedro. (2019). *How ISO 27001 Can Help Achieve GDPR Compliance. 14th Iberian Conference on Information Systems and Technologies (CISTI)*. IEEE.

López Calvo, José. (2017). *Comentarios al Reglamento Europeo de Protección de Datos*. Sepín.

Middleton-Leal, Matt. (2018). *GDPR and ISO 27001 Mapping: Is ISO 27001 Enough for GDPR Compliance?* Netwrix.

Pandit, Harshvardhan, Fatema, Kaniz, O'Sullivan, Declan, y Lewis, David. (2018). GDPRtEXT - GDPR as a Linked Data Resource. En Gangemi Aldo, Anna Lisa Gentile, Andrea Giovanni Nuzzolese, Sebastian Rudolph, Maria Maleshkova, Heiko Paulheim, Jeff Z. Pan y Mehwish Alam (eds.), *The Semantic Web. ESWC 2018. Lecture Notes in Computer Science*. Springer.

Pauner Chulvi, Cristina. (2016). El uso emergente de drones civiles en España. Estatuto jurídico e impacto en el derecho a la protección de datos. *Revista de Derecho Político*, *95*.

Prego de Oliver Fernández, Juan Antonio. (2017). *La transparencia como elemento de apoyo al consentimiento en materia de protección de datos* (tesis doctoral, Universidad Carlos III de Madrid, Getafe).

Professional Evaluation and Certification Board. (2020). *The future of privacy with ISO/EC 27701*.

Rallo Lombarte, Artemi. (2019). El nuevo derecho de protección de datos. *Revista Española de Derecho Constitucional*, *116*.

Rallo Lombarte, Artemi, García Mahamut, Rosario, y Viguri Cordero, Jorge. (2015). Cooperación y coordinación entre Autoridades de Proteccion de Datos. En Artemi Rallo Lombarte y Rosario García Mahamut (eds.), *Hacia un nuevo derecho europeo de protección de datos*. València: Tirant lo Blanch.

Rodrigues, Rowena. (2018). Conclusion: What Next for Privacy Seals? En Rowena Rodrigues y Vagelis Papakonstantinou (eds.), *Privacy and Data Protection Seals. Information Technology and Law Series*. T.M.C. Asser Press.

Rodrigues, Rowena, Barnard-Wills, David, Wright, David, De Hert, Paul, y Papakonstantinou, Vagelis. (2013). *EU Privacy seals project: Inventory and analysis of privacy certification schemes. Final report study*. Oficina de Publicaciones de la Unión Europea.

Rodrigues, Rowena, Barnard-Wills, David, De Hert, Paul, y Papakonstantinou, Vagelis. (2016). The future of privacy certification in Europe: An exploration of options under article 42 of the GDPR. *International Review of Law, Computers & Technology*, *20* (3).

Rodrigues, Rowena, Wright, David, y Wadhwa, Kush. (2013). Developing a privacy seal scheme (that works). *International Data Privacy Law*, *3* (2).

Saiz Peña, Carlos Alberto. (2019). Seguridad de los datos, evaluación de impacto, códigos de conducta y certificación. En Artemi Rallo Lombarte (ed.), *Tratado de Protección de Datos. Actualizado con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales.* València: Tirant lo Blanch.

Tambou, Olivia. (2016). L'Introduction de la certification dans le règlement général de la protection des données personnelles: quelle valeur ajoutée? *Revue Lamy de Droit de l'Immatériel*.